

« *La sécurité informatique dans l'entreprise* »

**PROJET PROFESSIONNEL**

Kevin FREOA

Année universitaire 2002 - 2003

DESS Droit et Pratique du Commerce électronique

Université Paris V René Descartes

# **TABLES DES MATIERES**

1.	LA REGLEMENTATION RELATIVE A LA SECURITE INFORMATIQUE .....	11
1.1	<b>La réglementation française : la loi Godfrain</b> .....	11
1.1.1	<b>Les atteintes aux systèmes</b> .....	11
(a)	Accès et maintien frauduleux dans un STAD.....	11
(i)	Accès et maintien frauduleux dans un STAD <b>sans influence</b> .....	11
(ii)	Accès et maintien <b>avec influence</b> sur le système .....	15
(b)	Atteintes volontaires au <b>fonctionnement</b> d'un STAD.....	16
(i)	L'entrave au fonctionnement du système.....	16
(ii)	Le fait de fausser le fonctionnement du système.....	16
1.1.2	Les atteintes aux données.....	17
(a)	L'accès et le maintien frauduleux dans un STAD avec <b>influence sur les données</b> .....	17
(b)	Atteintes volontaires aux données contenues dans un STAD indépendamment de l'accès ou du maintien frauduleux.....	18
1.1.3	<b>Les modifications prévues par le projet de loi sur la confiance dans l'économie numérique</b> .....	21
(a)	Une nouvelle incrimination .....	21
(i)	<i>Le principe</i> .....	21
(ii)	<i>Les exceptions</i> .....	21
(iii)	<i>Le débat</i> .....	21
(iv)	<i>Le cas du "virus"</i> .....	22
(b)	L'aggravation des peines .....	22
(c)	L'introduction expresse de la terminologie informatique dans le Code de procédure pénale.....	23
1.2	<b>Les réglementations européenne et internationale</b> .....	24
1.2.1	<b>La Convention sur la cybercriminalité</b> .....	24
(a)	Présentation.....	24
(b)	Les grandes lignes de la convention .....	25
(i)	<i>Les infractions</i> .....	25
(ii)	<i>De nouvelles procédures</i> .....	26

(iii) <i>Les règles de la coopération internationale</i> -----	27
1.2.2 <b>Proposition de décision cadre de la Commission Européenne</b> .....	27
2.    LA PREVENTION JURIDIQUE .....	30
2.1 <b>Les techniques contractuelles de prévention</b> .....	30
2.1.1 <b>L'analyse des risques : étape nécessaire à la prévention contractuelle</b> .....	30
2.1.2 <b>Les techniques contractuelles</b> .....	31
(a)    Les clauses et les engagements spécifiques à la sécurité dans les contrats fournisseurs .....	31
(b)    Les contrats d'assurance .....	33
(i) <i>Le contrat "multirisque informatique"</i> -----	33
(ii) <i>Le contrat "extension aux risques informatiques" (ERI)</i> -----	38
(iii) <i>Le contrat "global informatique"</i> -----	40
2.2 <b>Les techniques préventives internes aux sociétés</b> .....	40
2.2.1 <b>La prévention des risques et la mise en place d'outils de surveillance des salariés</b> .....	40
(a)    La surveillance du salarié .....	41
(b)    L'utilisation d'un logiciel " <i>mail sweeper</i> " .....	41
2.2.2 <b>La mise en place de chartes informatiques</b> .....	42
(a)    Le contenu de la charte .....	42
(b)    La valeur juridique de la charte .....	45
CRIMINALITE INFORMATIQUE ET PROCEDURES CONTENTIEUSES .....	48
3.    LA MISE EN ŒUVRE PRATIQUE : CRIMINALITE INFORMATIQUE ET PROCEDURES CONTENTIEUSES .....	49
3.1 <b>Les organismes policiers spécialisés</b> .....	49
3.1.1 <b>La Brigade Centrale de Répression de la Criminalité Informatique ("BCRCI")</b> 49	
3.1.2 <b>Le rôle de l'Office Central de Lutte Contre la Criminalité liée aux Technologies de l'Information et de la Communication ("OCLCTIC")</b> .....	49

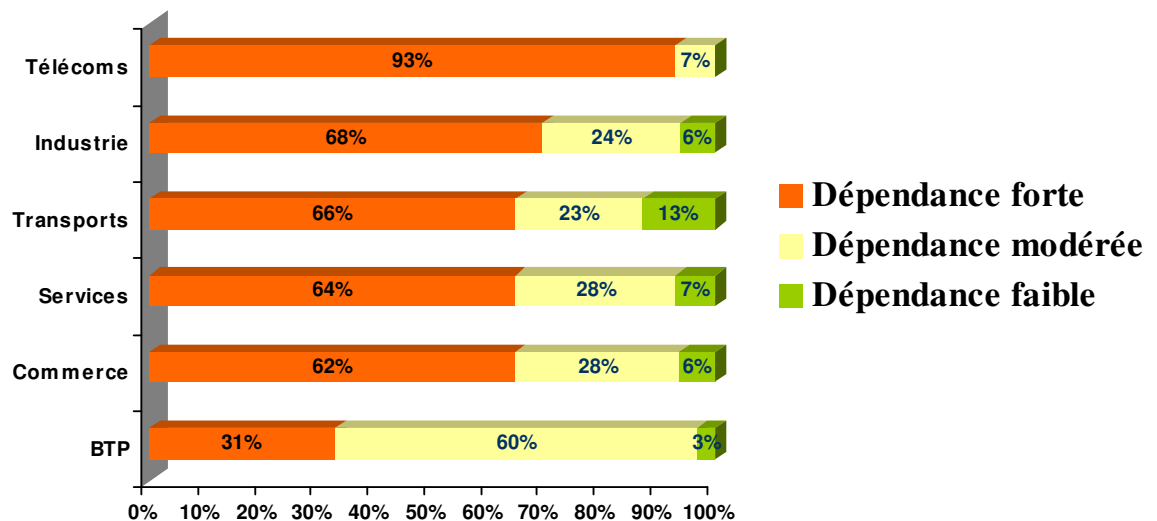
3.1.3	<b>Le Service d'Enquête sur les Fraudes aux Technologies de l'Information ("SEFTI")</b> .....	50
3.2	<b>Le recours à l'expertise</b> .....	52
3.2.1	<b>Le recours à l'expert "chargé d'obtenir une version claire des informations"</b> 53	
3.2.2	<b>Le concours des "moyens de l'Etat" à la mission de l'expert</b> .....	53
3.3	<b>Le renforcement des moyens d'investigation en matière informatique : le projet de loi sur la sécurité intérieure</b> .....	54
3.4	<b>L'appréhension internationale du traitement judiciaire des infractions informatiques</b> .....	54
3.4.1	<b>Les services compétents</b> .....	55
(a)	Interpol.....	55
	<b>Organisation</b> .....	55
	<b>Mission</b> .....	55
(b)	Europol .....	55
	<b>Mission</b> .....	55
3.4.2	<b>Les accords de Schengen</b> .....	56
(a)	Le système d'information SCHENGEN (SIS).....	56
(b)	La coopération policière dans l'espace SCHENGEN.....	56
	<b>Bibliographie</b> .....	59
	«Guide» de la sécurité informatique.....	60
(1)	Annuaire des organismes liés à la sécurité informatique.....	61
(2)	Les textes relatifs à la sécurité informatique.....	66

# INTRODUCTION

La sécurité informatique représente aujourd'hui une priorité stratégique et incontournable pour le développement des entreprises. Le titre III du projet de loi sur "la confiance dans l'économie numérique" dédié à l'aspect sécuritaire témoigne de l'enjeu de cette préoccupation et du besoin de renforcement et d'adaptation de la réglementation actuelle.

Selon le rapport "Etudes et statistiques sur la sinistralité informatique en France" de 2001 du CLUSIF ("**Club de la Sécurité des systèmes d'Information Français**"), l'impératif de sécurité est une préoccupation croissante des entreprises puisqu'en 2001, 62% des entreprises françaises (ce chiffre passe à 74% pour les entreprises de plus de 200 salariés) s'estimaient déjà très dépendantes de l'informatique, qui prend une place croissante dans la bonne marche de leurs activités.

L'analyse sectorielle de la dépendance des entreprises (de plus de 200 salariés) à l'informatique est la suivante :



(Source : "Études et statistiques sur la sinistralité informatique en France" de 2001, Clusif)

Cette dépendance démontre le sentiment de fragilité qui caractérise les entreprises victimes de piratage. Selon le CGSSI ("**Conseil en gestion de la sécurité des systèmes informatiques**"), **35%** d'entre elles reconnaissent avoir été attaquées au moins une fois au cours de l'année 2001. Toutefois, il est important de souligner le caractère relatif de ce chiffre dans la mesure où les entreprises n'aiment pas communiquer sur les attaques ou les défaillances de leurs systèmes d'information.

Les 5 pays les plus visés par des "attaques digitales" en 2002 :

<b>Pays</b>	<b>Nombre d'attaques</b>
<b>Etats-Unis</b>	26.792
<b>Brésil</b>	5.568
<b>Royaume-Uni</b>	4.950
<b>Allemagne</b>	4.621
<b>Italie</b>	2.652

(Source : mi2g.com, site sur le "*Risk management*"informatique).

En 2002, le CERT ("**Computer Emergency Response Team**") fait état d'une évolution critique : le nombre d'attaques constatées sur le territoire des Etats-Unis est passé de 52 658 à 82 094 entre 2001 et 2002 soit une augmentation de **55,9 %**.

En dépit de ce constat, la confiance des entreprises dans leur système d'information est en nette progression. Selon le CLUSIF, en 2001, **25%** d'entre elles s'estiment très bien protégées et **60%** relativement bien protégées.

La sensibilisation aux risques et la pratique des audits incitent néanmoins les entreprises à renforcer leurs dispositifs de protection informatique. Une enquête de l'AFAI ("**l'Association Française de l'Audit et du Conseil Informatiques**") révèle en France la présence d'un responsable de la sécurité et des systèmes informatiques dans **65%** des entreprises, tout secteur confondu. Allié aux dépenses de logiciels de protection et d'équipements physiques, l'enjeu de la sécurité constitue désormais un poste de dépense non négligeable et incontournable dans le budget des entreprises.

Pour faire face aux diverses formes d'intrusions informatiques (infection virale, prise des commandes à distance...) et aux atteintes à la sécurité d'un système informatique (aussi bien internes qu'externes), deux voies d'actions principales peuvent être envisagées :

- Recours à l'arsenal répressif prévu par la réglementation au niveau national et international
- Recours à des organismes et des procédures spécialisés
- Recours à des techniques préventives visant à limiter, prévenir et réduire les dommages pouvant résulter d'une attaque ou de l'atteinte à la sécurité d'un système :
  - D'une part, il y a des techniques contractuelles à l'égard des fournisseurs intervenant dans le cadre de la sécurité du système, et
  - D'autre part, il y a des techniques de prévention des risques internes aux entreprises.

## PARTIE 1 :

# LA REGLEMENTATION RELATIVE A LA SECURITE INFORMATIQUE

## **1. LA REGLEMENTATION RELATIVE A LA SECURITE INFORMATIQUE**

Dès 1988, la France s'est dotée d'un texte répressif, la loi Godfrain. Au niveau européen, l'influence provient essentiellement du Conseil de l'Europe avec la Convention sur la Cybercriminalité adoptée en 2001.

### **1.1 La réglementation française : la loi Godfrain**

La loi du 5 janvier 1988 qui traite "*des atteintes aux systèmes de traitement automatisé des données*" réprime pénalement de nombreux comportements. Ces infractions sont définies aux articles 323-1 à 323-7 du Code pénal. Ce dispositif sanctionne toutes les pénétrations non autorisées dans les Systèmes de Traitement Automatisé des Données (dits "**STAD**») ainsi que les atteintes portées au contenu (essentiellement les données d'un STAD) et crée une incrimination spécifique aux falsifications de documents informatiques.

Selon la doctrine, un STAD s'entend de tout ensemble composé d'une ou plusieurs unités de mémoire, de logiciel, d'organe d'entrée-sortie, et de liaison qui concourent à un résultat déterminé. La carte à puce est ainsi couverte par cette définition.

Les différentes infractions créées par la loi Godefrais sont constituées dès lors que l'élément matériel et l'élément intentionnel propres à chaque infraction sont réunis.

#### **1.1.1 Les atteintes aux systèmes**

##### **(a) Accès et maintien frauduleux dans un STAD**

La loi distingue selon que l'accès ou le maintien a entraîné ou non une altération sur le fonctionnement du système.

##### **(i) *Accès et maintien frauduleux dans un STAD sans influence***

L'accès est dit sans influence lorsqu'il ne provoque aucune altération sur le fonctionnement du système.

#### **Art 323-1, al. 1 du Code pénal :**

*"Le fait d'accéder ou de se maintenir, frauduleusement, dans **tout ou partie** d'un STAD est puni **d'un an d'emprisonnement et de 15.000 euros d'amende.**"*

### **Notions :**

- **L'accès**

Au regard de la jurisprudence, la notion d'accès dans un STAD peut être caractérisée soit par la pénétration dans un système, soit par une manipulation informatique ou autre manœuvre, par le biais d'une connexion ou d'appel d'un programme, opérée de manière frauduleuse, c'est à dire sans autorisation de l'entreprise.

### **Exemple :**

1. Le fait d'*usurper* le mot de passe et de se *connecter* dans un espace réservé d'un système ouvert au public, par exemple l'espace réservé d'un serveur web effectué sans droit d'accès correspondant. Une personne qui utiliserait un cracker de mots de passe en ligne afin de pénétrer sur l'interface d'administration d'un site web pourrait être incriminée sur ce fondement.

2. Le fait de "*sniffer*" grâce à un logiciel qui permet d'intercepter des fichiers sur un réseau ainsi que de récupérer les Ip et les mails.

- **Le maintien**

L'incrimination de maintien frauduleux vient compléter celle de l'accès frauduleux. Elle vise les situations où l'accès dans le STAD a été régulier, suivi d'un maintien qui ne l'est pas.

Lorsque l'accès a été régulier, le maintien devient irrégulier lorsque son auteur se trouve privé de toute habilitation à se maintenir dans le système. Le maintien frauduleux est caractérisé par diverses situations anormales telles que les connexions, les visualisations ou toute autre opération dirigée contre un système d'information.

Le fait d'accéder à un serveur web puis de manipuler des variables et de modifier des requêtes SQL afin d'avoir accès à des informations réservées peut être qualifié de *maintien frauduleux*.

### **Éléments constitutifs de l'infraction**

**L'élément matériel** : est constitué uniquement par l'accès ou le maintien en **tant que tel**, indépendamment du résultat, de sorte que même en l'absence de préjudice, l'auteur d'un tel accès ou maintien peut être condamné.

**L'élément moral** : le délinquant doit avoir eu conscience d'accéder ou de se maintenir anormalement i.e. sans droit dans le système.

L'accès et le maintien sont constitutifs d'une infraction lorsqu'ils ont été effectués **frauduleusement**. Le terme "frauduleux" suppose que l'intrusion et le maintien aient été volontaires et que leur auteur ait eu conscience de commettre une action illicite. Mais, il n'est **pas nécessaire pour autant que le délinquant ait eu l'intention de nuire**.

La jurisprudence, constante, considère que l'élément intentionnel du délit est caractérisé lorsque l'"accès [est] fait sans droit et en pleine connaissance de cause". Pour cela, "il suffit que le **"maître du système" ait manifesté l'intention d'en restreindre l'accès aux seules personnes autorisées**".

"L'absence de droit résulte de l'absence d'autorisation expresse du maître de système" (CA Toulouse, 3<sup>ème</sup> Chambre, 21 janvier 1999) étant observé que le caractère exprès de l'autorisation ne s'impose pas mais peut se présumer par un faisceau d'indices.

Le maître du système est la personne ou le service compétents pour autoriser l'accès.

A titre d'exemple, l'attribution nominative de codes d'accès à des personnes déterminées matérialise leur droit d'accès au système.

L'élément moral est souvent en pratique le plus difficile à démontrer.

L'incrimination visée par l'article 323-1 du Code pénal est très large et vise toutes les techniques d'accès frauduleux à un système et notamment l'utilisation d'un code d'accès exact par une personne non habilitée à accéder à un STAD.

Ainsi l'accès peut être réalisé via une connexion pirate tant physique que logique, via l'appel d'un programme sans habilitation ou via l'interrogation d'un fichier sans autorisation.

#### Jurisprudence :

- La Cour d'appel de Douai a considéré que le fait, pour une personne, d'être sans lien (client de la société) avec la société à laquelle le système d'informatique appartenait, suffisait à caractériser l'**accès** frauduleux, sans droit, ni titre (CA Douai, 4<sup>ème</sup> ch. 7 octobre 1992 : Gaz Pal. 1993 2 p. 326).

- Caractérise le délit de maintien frauduleux dans un STAD, le fait pour des employés, de prolonger abusivement leur **maintien** dans le système grâce à des systèmes d'inhibition et d'écrans noirs, durant des heures, voire des nuits entières, hors leur présence et à l'insu de leur entourage dans le seul but de multiplier le nombre de

points leur ouvrant droit à des cadeaux (CA de Paris, 9<sup>ème</sup> ch. A, 15 décembre 1999, Gaz. Pal. 21-23 janvier 2001 somm. P. 39).

Précisions : éléments indifférents

**(1) Absence de nécessité d'un préjudice**

L'accès ou le maintien frauduleux est sanctionné en lui-même, même en **l'absence de tout préjudice**. Ainsi, la captation d'informations ou l'utilisation du système ne sont pas requis dans la mesure où seul l'accès ou le maintien au système est incriminé par l'article 323-1 du Code pénal.

**(2) Absence de nécessité d'un dispositif de sécurité**

Il n'est pas nécessaire pour que l'infraction soit constituée, que l'accès au système soit limité par un dispositif physique ou logique de protection (exemple : *firewall*). Il n'est pas nécessaire de démontrer que le délinquant a "forcé" l'entrée du système. Il suffit que son exploitant ("le Maître du système") ait manifesté l'intention d'en restreindre l'accès aux seules personnes formellement autorisées.

Une affaire récente Kitetoo c/ Tati SA a permis de mettre deux règles en perspective. Dans cette affaire, le responsable du site Kitetoo (site journalistique spécialisé dans la sécurité informatique) était poursuivi par la société Tati pour avoir accédé de manière répétée aux bases de données personnelles du site tati.fr.

Tati a poursuivi cette personne pour accès frauduleux dans son STAD. Le prévenu invoquait l'absence de protection du site. Le TGI de Paris dans une décision en date du 13 février 2002 a donné gain de cause à Tati, estimant que l'existence de faille de sécurité ne constituait "*en aucun cas une excuse ou un prétexte pour le prévenu d'accéder de manière consciente et délibérée à des données dont la non protection pouvait être constitutive d'une infraction pénale.*"

Toutefois, bien que la loi Godfrain n'impose pas de protéger un système, son exploitant doit néanmoins prendre certaines précautions du fait d'autres réglementations, et notamment du fait de la loi "Informatique et libertés" du 6 janvier 1978.

En effet, l'article 226-17 du Code pénal réprime le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans **prendre toutes les précautions utiles pour préserver la sécurité de ces informations** et notamment d'empêcher qu'elles ne soient communiquées à des tiers non-autorisés.

Cependant dans son arrêt en date du 30 octobre 2002, la Cour d'Appel de Paris a réformé le jugement au motif que le fait d'accéder à des données nominatives stockées sur un site avec un simple navigateur, en présence de nombreuses failles de sécurité, n'était pas constitutif d'un accès et d'un maintien frauduleux dans un STAD.

La Cour a considéré qu'il ne pouvait être reproché à un internaute d'accéder ou de se maintenir dans les parties d'un site "*qui peuvent être atteintes par la simple utilisation d'un navigateur grand public*". La Cour ajoute que ces parties ne faisaient pas l'objet d'une protection de la part de l'exploitant du site ou de son prestataire de service et qu'elles devaient, à ce titre, être réputées non confidentielles, à défaut de toute mention contraire.

On peut donc considérer que la Jurisprudence crée une présomption simple, selon laquelle l'accès et le maintien dans un STAD (en l'espèce un site) non protégé permettant ainsi son accès par l'utilisation d'outil grand public (en l'espèce un navigateur) n'est pas répréhensible car non frauduleux au titre de l'infraction de l'article 323-1 du Code pénal.

### **(3) Indifférence du mode d'accès**

Ainsi dans un arrêt du 5 avril 1994, la Cour d'appel de Paris a considéré que "*l'accès frauduleux au sens de l'article 462-2 du Code pénal issu de la loi du 5 janvier 1988 et au sens de l'article 323-1 du Code pénal, vise tous les modes de pénétration irréguliers d'un système de traitement automatisé de données, que l'accédant travaille déjà sur la même machine mais à un autre système, qu'il procède à distance ou qu'il se branche sur une ligne de communication.*"

#### **(ii) Accès et maintien *avec influence* sur le système**

Il s'agit u maintien avec altération du fonctionnement du système.

**Art 323-1, al. 2 du Code pénal** prévoit que : "Lorsqu'il en est résulté [...] une altération du fonctionnement du système, la peine est de **deux ans d'emprisonnement et de 30.000 euros d'amende.**"

Dès lors que le maintien ou l'accès frauduleux entraîne une altération du système, la loi prévoit un doublement de la peine.

(b) Atteintes volontaires au fonctionnement d'un STAD

**Art 323-2 du Code pénal :**

"Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé des données est puni de **trois ans d'emprisonnement et de 45.000 euros d'amende.**"

(i) *L'entrave au fonctionnement du système*

Éléments constitutifs de l'infraction :

**Élément matériel** : Il suffit d'une influence négative sur le fonctionnement du système pour que l'acte d'entrave soit matérialisé. L'entrave vise à paralyser ou à retarder le fonctionnement du système. (Exemples : bombes logiques introduisant des instructions parasites, occupation de capacité de mémoire, mise en place de codification ou tout autre forme de barrage).

**Élément moral**: l'infraction est constituée pour autant que l'individu ait intentionnellement entravé le fonctionnement du système en ne respectant pas le droit d'autrui.

Jurisprudence :

L'envoi automatique de messages et l'utilisation de programmes simulant la connexion de multiple Minitel à un centre serveur, perturbant ainsi les performances du système et entraînant un ralentissement de la capacité des serveurs, a été considéré comme étant constitutif du délit d'entrave au fonctionnement d'un STAD (CA Poitiers, Ch. Acc., 20 janvier 1998 : Gaz Pal 2000 1 somm. P. 301)

(ii) *Le fait de fausser le fonctionnement du système*

Éléments constitutifs de l'infraction:

**Élément matériel** : c'est le fait de "fausser" le fonctionnement d'un STAD. Le but de cette altération est de **faire produire au système un effet différent de celui attendu.**

**Élément moral** : comme pour le délit d'entrave, l'intention doit être démontrée.

Jurisprudence :

Le fait d'avoir porté sur des fiches manuscrites de saisie informatique destinées à la constitution du fichier des produits d'une société, des mentions inexactes quant au code du taux de TVA applicable et d'avoir introduit ces données dans le système informatique de gestion de l'entreprise a été considéré comme constituant le délit d'altération volontaire des données du système (Cass. Crim., 5 janvier 1994 Gaz Pal. 1996 2 p. 419)

1.1.2 Les atteintes aux données

(a) L'accès et le maintien frauduleux dans un STAD avec **influence sur les données**

Il s'agit de l'autre infraction prévue par **l'article 323-1 al 2 du Code pénal** qui sanctionne, outre l'altération du fonctionnement du système, **la suppression ou la modification des données.**

L'accès et le maintien frauduleux avec influence font encourir des peines aggravées lorsqu'ils causent en outre un dommage (consistant en la modification ou la suppression), même involontaire aux données contenues dans le système.

La peine encourue est alors de **deux ans d'emprisonnement et de 30.000 euros d'amende.**

La **preuve** informatique de ces manœuvres est souvent difficile à rapporter en raison de la datation incertaine. Elle doit donc faire l'objet de précautions particulières liées à la matérialisation de l'élément probant : constat du dommage par un huissier ou par les services compétents de police ou de gendarmerie.

Jurisprudence :

Dans une affaire de fraude en matière de radiotéléphone, le délinquant reconnu coupable d'accès, de maintien et de modification des données dans le logiciel d'un radiotéléphone a été condamné à une peine de 18 mois d'emprisonnement avec sursis et une amende de 10.000 francs. Sur le plan des intérêts civils, il a été condamné solidairement avec les autres coupables à payer à France Télécom près de 2.000.000 de francs, (soit 304.878,05 euros), pour la réparation du préjudice matériel se traduisant par le montant des communications téléphoniques (T. corr Paris, 29<sup>ème</sup> ch. 2 avril 1992 ; Expertise septembre 1992 p 316).

- (b) Atteintes volontaires aux données contenues dans un STAD indépendamment de l'accès ou du maintien frauduleux

**Art 323-3 du Code pénal :**

"Le fait **d'introduire** frauduleusement des données dans un système de traitement automatisé ou de **supprimer** ou de **modifier** frauduleusement les données qu'il contient est puni **de trois ans d'emprisonnement et de 45.000 euros d'amende.**"

Éléments constitutifs de l'infraction :

**Élément matériel** : le texte permet de réprimer toute manipulation, suppression ou modification de données contenues dans un système, qu'elles qu'en soient les conséquences. Les pratiques incriminées correspondent à toute altération des données, fichiers, bases de données.

L'Internet accentue les difficultés. En effet, il est extrêmement difficile de connaître l'origine de l'accès.

**Élément moral** : le délit n'est constitué que si ces opérations sont faites avec une intention délictueuse et hors de l'usage autorisé. L'intention frauduleuse est constituée dès le moment où l'introduction des données s'effectue avec une volonté de modifier l'état du système et ce, quelles qu'en soient les conséquences sur le système.

Jurisprudence :

Le fait de modifier ou de supprimer intentionnellement des données contenues dans un STAD caractérise le délit, sans qu'il soit nécessaire que ces modifications émanent d'une personne n'ayant pas le droit d'accès ni que l'auteur soit animé de la volonté de nuire (Cass. Crim. 8 décembre 1999: Gaz Pal 27-28 octobre 2000 som p 45).

**Compléments sur la sanction :**

= Les peines complémentaires

En complément des peines principales évoquées, l'article 323-5 du Code pénal prévoit une série de peines complémentaires à l'encontre des **personnes physiques** coupables des délits prévus par la loi Godfrain.

Sept peines complémentaires sont encourues :

- **"L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26" ;**
- **"L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise" ;**
- **"La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution" ;**
- **"La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés";**
- **"L'exclusion, pour une durée de cinq ans au plus, des marchés publics"**
- **"L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés" ;**
- **"L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35".**

= La tentative

Pour tous ces délits, la tentative est punissable en application de l'article 323-7 du Code pénal qui prévoit que "la tentative est punie des mêmes peines."

Le fait que la tentative d'accès ou de maintien frauduleux soit sanctionnée au même titre que l'accès ou le maintien et ce quelle que soit la raison de l'échec, démontre le degré d'importance accordé par le législateur à toute atteinte aux STAD.

On peut distinguer **deux types de tentative** :

**La tentative achevée** : il s'agit de l'hypothèse où le résultat recherché par l'auteur de la tentative ne se produit pas, bien que tous les actes d'exécution aient été accomplis,

- soit en raison de l'étourderie, de la maladresse, de l'inaptitude, etc. de l'auteur (hypothèse de l'infraction manquée);

- soit en raison de l'impossibilité matérielle d'atteindre le résultat escompté, quelles qu'aient pu être par ailleurs la diligence et l'habileté de l'auteur (hypothèse de l'infraction impossible).

Dans les deux cas, la jurisprudence considère que la tentative est punissable.

**La tentative interrompue** : même si elle a fait l'objet d'un commencement mais a été interrompue, la tentative n'en reste pas moins punissable.

L'article 121-5 du Nouveau Code pénal pose en effet la règle selon laquelle la tentative interrompue est punissable si sont constatés :

- un commencement d'exécution, et
- l'absence de désistement volontaire.

= L'association de malfaiteurs

L'article 323-4 du Code Pénal réprime de façon particulière l'association de malfaiteurs organisée pour la préparation de l'une des infractions, punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

= La responsabilité pénale des personnes morales

La responsabilité pénale de la personne morale pour le compte de laquelle les infractions auront été commises peut être retenue (article 323-6 du Code pénal).

Elle encoure l'amende selon les modalités de l'article 131-38 ("*le taux maximum de l'amende est **égal au quintuple** de celui pour les personnes physiques*") et l'ensemble des peines complémentaires prévues à l'article 131-39 comprenant notamment la dissolution ou l'interdiction d'exercice de l'activité à l'occasion de laquelle l'infraction a été commise.

A cette occasion, il faut évoquer la délégation pénale, procédé par lequel un dirigeant transfère à l'un de ses salariés une partie de ses fonctions, ce transfert de pouvoir s'accompagnant d'un transfert de responsabilité pénale.

### 1.1.3 Les modifications prévues par le projet de loi sur la confiance dans l'économie numérique

Conscient de l'augmentation des atteintes aux STAD, le gouvernement Raffarin prévoit dans son projet de loi de renforcer l'arsenal répressif et d'augmenter les peines prévues par la législation actuelle.

#### (a) Une nouvelle incrimination

##### (i) *Le principe*

L'article 34 du projet de loi prévoit en effet d'insérer un article 323 3-1, al.1 au Code pénal qui serait rédigé comme suit : "**Le fait de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle même ou pour l'infraction la plus sévèrement réprimée.**"

##### (ii) *Les exceptions*

L'alinéa 2 du même article prévoit des exceptions lorsque de telles manœuvres sont justifiées par les besoins de la recherche scientifique et technique ou de la protection et de la sécurité des réseaux de communications électroniques et des systèmes d'information.

Ce nouvel article vise à sanctionner les personnes qui mettent à disposition les outils (notamment les virus informatiques ou les logiciels de prise de contrôle à distance) permettant de commettre les infractions qui sont d'ores et déjà réprimées pénalement.

##### (iii) *Le débat*

Cette nouvelle incrimination fait d'ores et déjà l'objet de critiques. Ainsi, les experts du CLUSIF mettent en avant les lacunes du texte. D'une part, ils critiquent l'**absence de la notion de "détention accidentelle"**. Ainsi, dans le cas d'un ordinateur contaminé par un virus, la victime se retrouve à détenir le programme de manière involontaire dans la mesure où ce type de nuisance se propage le plus souvent à l'insu des utilisateurs. Il en est de même pour les programmes de contrôle à distance, dont une partie est installée sur le poste de la victime. Les sociétés victimes d'hébergements clandestins malveillants pourraient donc être poursuivies sur le fondement des nouvelles incriminations.

Les activités de certains professionnels seraient ainsi mises en péril.

Néanmoins, comme nous l'avons vu précédemment, le comportement incriminé constituant une infraction pénale, le caractère intentionnel du comportement devra être rapporté.

D'autre part, certaines critiques concernent les exceptions prévues au second alinéa du texte. Sont exclues du champ d'application de la nouvelle incrimination la détention, l'offre, la cession et la mise à disposition lorsqu'elles sont justifiées par les besoins de la recherche scientifique et technique ou de la protection et de la sécurité des réseaux de communications électroniques et des systèmes d'information.

Cette exception est jugée **trop restrictive** par certains qui regrettent que les conseillers et les consultants ne puissent en bénéficier. Pour d'autres, au contraire, cette exception est **suffisamment large** puisqu'elle constitue une excuse pour les responsables de la malveillance virale qui n'auront qu'à revendiquer des recherches scientifiques pour échapper à la répression.

(iv) *Le cas du "virus"*

Enfin, des spécialistes déplorent le défaut de précision dans la description des programmes et outils incriminés. Le mot "**virus**" pourtant évoqué lors de l'élaboration du projet de loi ne figure pas expressément dans le texte.

(b) L'aggravation des peines

Le projet de loi prévoit d'augmenter les peines prévues par les articles 321-1 et suivant du Code pénal :

- Les peines de un an d'emprisonnement et de 15.000 euros d'amende se transforment en peine de **deux ans d'emprisonnement et 30.000 euros d'amende**.
- Les peines de deux ans d'emprisonnement et 30.000 euros d'amende se transforment en peine de **trois ans d'emprisonnement et 45.000 euros d'amende**.
- Les peines de trois ans d'emprisonnement et 45.000 euros d'amende se transforment en peine de **cinq ans d'emprisonnement et 75.000 euros d'amende**.

(c) L'introduction expresse de la terminologie informatique dans le Code de procédure pénale

Le projet de loi sur la confiance dans l'économie prévoit de compléter la terminologie du Code de procédure pénale en l'enrichissant des termes : "**données informatiques**"; "**documents informatiques**"; "**informations**" dans les articles afférents aux perquisitions et saisies.

A titre d'exemples,

L'article 30 de la LCEN prévoit de modifier l'article 94 du Code de procédure pénale et d'insérer désormais après les mots : «des objets» les mots : «ou des **données informatiques**».

*"Les perquisitions sont effectuées dans tous les lieux où peuvent se trouver des objets **ou des données informatiques** dont la découverte serait utile à la manifestation de la vérité."*

De même, la LEN prévoit de modifier l'article 97 du Code de procédure pénale en insérant deux nouveaux alinéas ainsi rédigés :

*«Il est procédé à la saisie des **données informatiques** nécessaires à la manifestation de la vérité en plaçant sous main de justice soit le support physique de ces données, soit une copie réalisée en présence des personnes qui assistent à la perquisition.*

*Si une copie est réalisée dans le cadre de cette procédure, il peut être procédé, sur ordre du juge d'instruction, à l'effacement définitif, sur le support physique qui n'a pas été placé sous main de justice, des **données informatiques** dont la détention ou l'usage est illégal ou dangereux pour la sécurité des personnes ou des biens».*

Ces insertions témoignent de la volonté d'adapter les textes existants à la réalité de la société de l'information.

## 1.2 **Les réglementations européenne et internationale**

### 1.2.1 **La Convention sur la cybercriminalité**

#### (a) Présentation

Outre la réglementation européenne du Parlement Européen (directives communautaires sur la protection des données personnelles, la signature électronique et la cryptologie), le texte majeur en matière de lutte contre les atteintes à la sécurité informatique est **la convention de Budapest sur la cybercriminalité du 23 novembre 2001** élaborée par le Conseil de l'Europe.

Cette convention a pour objet de lutter sur un plan international contre la criminalité informatique. Ce texte qui constitue une première au niveau mondial vise avant tout à garantir la sécurité des réseaux et de ses utilisateurs.

Les Etats signataires et adhérents à la Convention de Budapest

Les 44 pays membres du Conseil de l'Europe ont participé à l'élaboration de ce texte ainsi que le Canada, les Etats-Unis, le Japon (observateurs auprès de l'organisation) et l'Afrique du Sud qui ont pris une part très active dans le processus d'élaboration.

A ce jour, 33 Etats ont signé la Convention. Seuls deux d'entre eux ont aussi adhéré au texte en le ratifiant :

- **Les Etats signataires (par ordre chronologique des signatures)**

→ Etats membres du Conseil de l'Europe

Arménie, Albanie, Autriche, Belgique, Bulgarie, Chypre, Croatie, Estonie, Finlande, France, Allemagne, Grèce, Hongrie, Islande, Irlande, Italie, Luxembourg, Malte, Moldavie, Pays-Bas, Norvège, Pologne, Portugal, Roumanie, Slovaquie, Espagne, Suède, l'ex-République yougoslave de Macédoine, Ukraine.

→ Etats non-membres du Conseil de l'Europe

Canada, Japon, Afrique du Sud, Etats- Unis.

- **Les Etats ayant ratifié la Convention**

Albanie, Croatie.

(b) Les grandes lignes de la convention

La Convention détermine **trois principaux axes** de réglementation :

- l'harmonisation des législations nationales concernant la définition des crimes en matière de cybercriminalité,
- la détermination des moyens d'enquêtes et de poursuites pénales adaptés à la mondialisation des réseaux, et
- la mise en place d'un système rapide et efficace de coopération internationale.

(i) *Les infractions*

Les infractions retenues sont toutes soumises à deux conditions générales pour que la responsabilité pénale soit engagée :

→ **les comportements incriminés doivent toujours être commis de façon intentionnelle, et**

→ **les comportements incriminés doivent être commis "sans droit"**

Ces conditions devraient poser peu de difficultés de transposition en droit français puisqu'elles sont déjà prévues par la loi Godfrain.

Elles sont répertoriées selon **quatre grandes catégories** :

- les infractions portant atteinte à la confidentialité, l'intégrité et la disponibilité des données et des systèmes : accès illégal, interception illégale, abus de dispositifs
- les infractions informatiques : falsification et fraude informatiques
- les infractions se rapportant au contenu : actes de production, de diffusion, de possession de pornographie infantile. Le protocole additionnel à la Convention du 7 novembre 2002 portant sur l'incrimination des actes de nature raciste ou xénophobe commis à travers les réseaux informatiques a inclus une infraction contre la propagation d'idées racistes et la xénophobie à travers les réseaux

- les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes : la distribution à grande échelle de copies illégales d'œuvres protégées, etc.

(ii) *De nouvelles procédures*

La Convention prévoit la mise en place de procédures visant à faciliter la conduite des enquêtes dans le monde virtuel et consistant à favoriser une entraide judiciaire entre les pays adhérents à la Convention.

Sont ainsi prévues :

- la conservation des données stockées,
- la conservation et la divulgation rapide des données relatives au trafic,
- la perquisition des systèmes et la saisie de données informatiques,
- la collecte en temps réel des données relatives au trafic, et
- l'interception de données relatives au contenu.

Notamment, en vertu de cette convention,

- les autorités compétentes peuvent ordonner ou imposer la conservation des données informatiques lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification;
- la conservation des données informatiques ne pourra pas dépasser 90 jours;
- les autorités compétentes pourront ordonner à une personne la communication des données informatiques en sa possession ou sous son contrôle;
- les fournisseurs de services devront communiquer les données en leur possession ou sous leur contrôle relatives aux abonnés (identité, adresse postale, n° de téléphone, tout autre numéro d'accès, la facturation, le

paiement, l'endroit où se trouve les équipements de communication)

(iii) *Les règles de la coopération internationale*

A côté des formes traditionnelles de coopération pénale internationale prévues notamment par les conventions européennes d'extradition et d'entraide judiciaire en matière pénale, la nouvelle Convention exigera des formes d'entraide spécifiques à la lutte contre la cybercriminalité. Ainsi, les autorités judiciaires et les services de police d'un Etat peuvent agir pour le compte d'un autre pays dans la recherche de preuves électroniques, sans toutefois mener d'enquêtes ni de perquisitions transfrontalières.

Les informations obtenues devront être rapidement communiquées.

Ainsi, un réseau de contacts disponibles 24 heures sur 24 et sept jours sur sept est mis sur pied afin de prêter une assistance immédiate aux investigations en cours. Chaque pays devant mettre en place un tel contact.

### 1.2.2 **Proposition de décision cadre de la Commission Européenne**

Afin d'assurer la coopération judiciaire et policière des Etats membres de l'Union européenne pour lutter contre la cybercriminalité, la Commission européenne a également adopté le 23 avril 2002 une proposition de décision-cadre du Conseil relative "aux attaques visant les systèmes d'information". Les Ministres européens de la Justice et des Affaires intérieures, réunis en Conseil à Bruxelles, ont approuvé vendredi dernier (28 février) la proposition définissant une approche commune de lutte contre le cybercrime.

Cette proposition vise à rapprocher les règles et procédures pénales des Etats membres sur les infractions intervenant dans le domaine des systèmes d'information. La nouvelle réglementation doit être transposée avant le 31 décembre 2004 dans les Etats membres.

La proposition définit **différents types d'infractions** :

- l'accès illégal à un système d'information qui consiste dans l'accès intentionnel à un système d'information ("hacking") ;

- les perturbations graves de fonctionnement d'un système d'information ;
- la complicité et la tentative portant sur ces mêmes actes.

La nouvelle réglementation européenne prévoit que, en cas de "graves délits" que les pirates informatiques et les "contaminateurs" ("*virus spreaders*" ou diffuseur de virus) pourront être sanctionnés par une peine de une à cinq années de prison ferme.

- Le piratage informatique "par bande organisée" sera puni de deux à cinq ans de prison.
- En revanche, si le pirate agit de son propre chef, la peine sera alors comprise entre un et trois ans d'emprisonnement.

Les personnes morales peuvent voir leur responsabilité pénale engagée dans certaines conditions. Des peines mineures peuvent être prévues pour des atteintes mineures.

**La compétence des juridictions nationales** peut résulter :

- de la commission de l'infraction en tout ou partie sur le territoire national,
- lorsqu'elle est commise par un national et touche d'autres ressortissants de l'Etat, ou
- à l'initiative d'une personne morale ayant son siège dans l'Etat.

## PARTIE 2 :

# LA PREVENTION JURIDIQUE

## **2. LA PREVENTION JURIDIQUE**

Outre l'arsenal répressif mis à la disposition des victimes, les entreprises peuvent également avoir recours à des techniques préventives visant à prévenir, limiter et réduire les dommages résultant d'une atteinte à la sécurité informatique.

Les dommages matériels ou immatériels, directs ou indirects, pouvant résulter d'une atteinte à la sécurité d'un système informatique peuvent être considérables.

### **2.1 Les techniques contractuelles de prévention**

#### **2.1.1 L'analyse des risques : étape nécessaire à la prévention contractuelle**

Au terme d'un audit des risques, l'entreprise doit identifier sa propre vulnérabilité afin de :

- définir quelles sont **les actions à entreprendre** pour prévenir les sinistres informatiques, et
- **budgéter les dépenses** à investir dans la sécurité informatique.

Les **différents facteurs** de sécurité à prendre en compte peuvent se regrouper en **4 catégories** :

- **Ceux liés à l'organisation générale de l'entreprise** : sensibilisation de la direction aux risques informatiques, conditions d'exercice de responsabilités, structure sécurité et contrôles, prise en compte de la réglementation et des audits, environnement social et humain ;
- **Ceux liés à la sécurité physique** : environnement naturel (sol, sous-sol, climat) et artificiel (implantations industrielles voisines, pollution, bâtiments, sécurité incendies, dégâts des eaux, électrique, plans et procédures de sauvegarde, contrôle d'accès logique au système informatique, plan de secours, etc.) ;
- **Ceux liés à la sécurité des phases d'exploitation elles-mêmes** : analyse régulière des comptes rendus d'exploitation, de performances et des anomalies constatées, suivi de qualité, etc.
- **Ceux liés à la conservation du contenu** : analyse des solutions de back-up.

Il est important de souligner qu'un sinistre lié à la défaillance de la sécurité d'un système informatique peut ne pas être dû exclusivement à un criminel ou à un hacker. La responsabilité peut également incomber :

- au fournisseur de matériel ou logiciel "pare-feu" qui n'aurait pas fonctionné,
- au fournisseur d'accès au réseau de télécommunications qui aurait été négligent,
- au fabricant et/ou à l'installateur du réseau informatique de l'entreprise qui aurait mal défini l'architecture et les systèmes de protection,
- à un préposé de l'entreprise qui aurait commis un acte de malveillance ;
- au chef d'entreprise qui n'aurait pris aucune précaution en matière de sécurité et n'aurait pas protégé ses fichiers stratégiques,
- au fournisseur de logiciels de cryptologie qui n'aurait pas assuré la protection des clés.

En pratique, il est important de déterminer si l'entreprise sera indemnisée, par qui et à quelle hauteur. Pour répondre à cette attente concrète, les entreprises peuvent se couvrir par l'adoption de clauses contractuelles spécifiques dans leurs contrats avec leurs fournisseurs d'informatique et par la conclusion de différents contrats, notamment d'assurance.

## 2.1.2 Les techniques contractuelles

### (a) Les clauses et les engagements spécifiques à la sécurité dans les contrats fournisseurs

**1.** Dans le cadre des contrats conclus avec les fournisseurs d'informatique, il est important de s'assurer que le fournisseur prend l'engagement d'assurer au minimum la mise en place de **systèmes de protection (notamment firewall et anti-virus) conformes aux technologies disponibles sur le marché.**

Enfin, rappelons que pour être efficace, ces engagements devront être valables aussi bien lors de la première livraison du système que par la suite dans le cadre de la maintenance du système.

**2.** Il est important de prévoir à la charge du fournisseur une obligation contractuelle de **mise à jour régulière** du système informatique car en cas de défaillance du système de sécurité du fait de son caractère obsolète et si le client n'a pas prévu une telle obligation de mise à jour dans le contrat de fourniture, il ne pourra se retourner contre son fournisseur.

De plus, il est important de signer avec le fournisseur **un contrat de back-up**. Son objet est de prévoir les conditions dans lesquelles un fournisseur met à la disposition d'un client, qui se retrouve victime d'un incident l'empêchant de continuer à utiliser son système informatique, pour un temps déterminé, un matériel de substitution de configuration équivalente afin que celui-ci puisse continuer son activité et surtout les traitements et opérations essentiels à son activité et dont l'absence lui causerait un préjudice important.

Outre la mise à disposition d'une configuration équivalente, le contrat peut également prévoir la mise à disposition du client de locaux entièrement équipés et dédiés au Client (dits "salles de repli"), afin que celui-ci poursuive son activité pratiquement immédiatement après l'incident.

Exemples de clauses types relatives à la sécurité dans les contrats fournisseurs :

- *"Le Prestataire s'engage à livrer les antivirus [...], dans ses versions successives, pendant toute la durée du Contrat et ce afin d'assurer un niveau de sécurité maximum."*

- *"Le Prestataire s'engage à installer les firewalls de technologie Y, dans ses versions successives, au regard de l'évolution du système informatique du Client et de ses besoins en matière de sécurité pour toute la durée du Contrat et ce, afin d'assurer un niveau maximum de sécurité."*

- *"Le système mis en place par le Fournisseur devra présenter un niveau de sécurité au minimum conforme à l'état de l'art et de la technique."*

- *"Les logiciels, ainsi que toute nouvelle version de ceux-ci, devront avoir été vérifiés par le Fournisseur afin d'éviter toute contamination informatique du Client par un virus."*

- *"Le Fournisseur s'engage à prendre toutes les mesures nécessaires pour protéger la sécurité des fichiers, données, informations et éventuellement des logiciels du Client, à*

*s'assurer avant toute information ou prestation qu'une sauvegarde a été effectuée, et à garantir la confidentialité et la sécurité du système."*

(b) Les contrats d'assurance

Il est aujourd'hui indispensable pour une entreprise d'avoir une police d'assurance qui tienne compte du risque informatique. Les garanties proposées par les assureurs en matière informatique s'articulent autour de **trois types** de garanties :

- celles relatives au matériel et aux mesures indispensables à prendre pour la poursuite de l'exploitation d'une part, connue sous le nom de "**Tous risques informatiques**" ou "**multirisques informatiques**" ("TRI") ;
- celles relatives aux conséquences pour l'exploitant d'un système informatique de la fraude informatique d'autre part, connue sous le nom de "**Extension des risques informatiques**" ("ERI").
- **celles relatives à des garanties spécifiques contre le détournement ou encore une assurance concernant les échanges de données informatiques ("EDI") [Non traité dans les slides]**

Ces trois types de garantie peuvent se cumuler et être regroupés dans une police unique dite "**Globale Informatique**" ("GI").

A noter qu'il existe également des "garanties virus" en vogue en raison des dommages causés par certains virus très médiatiques.

(i) *Le contrat "multirisque informatique"*

Aussi appelés contrats "*tout risque informatique*", ces contrats couvrent essentiellement les dommages matériels directs susceptibles d'atteindre les biens de l'assuré, mais il peut également garantir les frais engendrés par la survenance du dommage et les pertes d'exploitation.

Cette garantie prend généralement en compte tous les dommages matériels subis par les biens assurés, sous réserve de l'application de quelques exclusions, ce qui se traduit particulièrement, dans la rédaction, par une formule type "tout sauf".

TABLEAU DES RISQUES GARANTIS PAR LE CONTRAT "MULTIRISQUE INFORMATIQUE"

	ELEMENTS COUVERTS	INDEMNISATION
<b>DOMMAGES MATERIELS DIRECTS</b>	<ul style="list-style-type: none"><li>• <u>Les biens garantis</u> Les biens matériels ou logiciels tels que répertoriés aux conditions particulières du contrat.</li><li>• <u>Dommmages garantis</u> Les dommages matériels garantis comprennent notamment la détérioration, la destruction ou le vol d'un bien assuré, y compris à la suite d'un acte de vandalisme."</li></ul>	<p>Elle est égale au montant des dommages aux biens garantis, dont la détermination varie selon la nature du bien endommagé et/ou de sa date de mise en service, diminué s'il y a lieu de la valeur du sauvetage, puis de la franchise.</p> <p>La valeur du sauvetage est la valeur des éléments encore utilisables après le sinistre.</p>

<p><b>FRAIS DE RECONSTITUTION DES MEDIAS (RINF)</b></p>	<ul style="list-style-type: none"><li>• <u>Définition</u></li></ul> <p>On entend, par médias, tous supports informatiques (carte, bande disque, cassette, etc) porteur d'informations directement utilisables sous cette forme par les biens assurés.</p> <ul style="list-style-type: none"><li>• <u>Objet de la garantie</u></li></ul> <p>La garantie consiste à prendre en charge la remboursement des frais réels que l'assuré doit exposer pour reconstituer les informations portées par les médias au moment du sinistre, lorsque ces informations ont été détruites ou ont disparu, à la suite d'un dommage garanti atteignant les matériels assurés, ainsi que, souvent, en cas de transport de ces médias.</p>	<p>L'indemnisation se fait sur la base du coût réel de la reconstitution des médias, dans l'état immédiatement antérieur au sinistre, sans pouvoir excéder le montant prévu pour cette garantie aux conditions particulières, sous déduction de la franchise.</p> <p>Il appartient à l'assuré de justifier de la reconstitution effective et de produire factures et mémoires s'y rapportant.</p> <p>L'indemnité est versée au plus tard dans un délai de un à deux ans à partir de la date du sinistre.</p>
---	---	--

<p><b>FRAIS SUPPLEMENTAIRES D'EXPLOITATION</b></p>	<p>• <u>Définition</u></p> <p>Il s'agit de la différence entre le coût total de traitement de l'information après un sinistre garanti et le coût total de traitement de l'information qui aurait normalement été supporté par l'assuré pour effectuer les mêmes tâches pendant la même période si aucun sinistre n'était survenu.</p> <p>Il s'agit de limiter les conséquences sur le traitement des informations, de l'interruption, totale ou partielle, du fonctionnement et de l'installation informatique.</p> <p>• <u>Objet de la garantie</u></p> <p>La garantie consiste dans le paiement à l'assuré des frais supplémentaires, qu'il doit réellement engager et ce d'un commun accord avec l'expert de l'assureur, pendant la période d'indemnisation pour pouvoir poursuivre son travail de traitement des informations dans des conditions, aussi proches que possibles du fonctionnement habituel, pour autant que ces frais résultent de dommages matériels garantis aux biens assurés.</p> <p>L'assureur ne délivrera sa garantie qu'après s'être informé sur la fiabilité du système informatique de l'assuré et sur l'existence d'un "plan de secours informatique".</p>	<p>L'indemnité est égale aux frais supplémentaires, réellement exposés par l'assuré d'un commun accord avec l'expert de l'assureur, sans pouvoir excéder le montant prévu pour cette garantie aux conditions particulières.</p> <p>L'assuré doit justifier de l'existence et du montant de frais supplémentaires, à l'aide de documents comptables, factures et tout autre moyen de preuve admissible.</p> <p>Il sera tenu compte des facteurs qui, indépendamment du sinistre, auraient eu une influence sur l'évolution de ce coût.</p> <p>La période d'indemnisation commence à la date de survenance du sinistre et prend fin le jour de la réparation ou du remplacement des biens informatiques assurés endommagés permettant à l'entreprise de retrouver les conditions normales de traitement des informations.</p>
--	--	---

<b>PERTES D'EXPLOITATION</b>	<ul style="list-style-type: none"><li>• <u>Définition</u> Les pertes d'exploitation sont essentiellement dues aux baisses du chiffre d'affaire. Un sinistre affectant partiellement ou totalement les biens assurés, est de nature à provoquer une baisse du chiffre d'affaires pendant une période plus ou moins prolongée. La garantie de l'assureur porte sur la "marge brute" de l'entreprise consécutive à un dommage direct subi par les biens garantis au contrat.</li><li>• <u>Objet de la garantie</u> La garantie de l'assureur consiste dans le paiement à l'assuré :<ul style="list-style-type: none"><li>- de la perte d'exploitation de la baisse du chiffre d'affaires, pendant la période d'indemnisation, et causé par l'interruption ou la réduction d'activité de l'entreprise.</li><li>- l'engagement, en accord avec l'assureur, de frais supplémentaires d'exploitation destinés à éviter ou à réduire la perte de marge brute due à la baisse du chiffre d'affaires, durant la période d'indemnisation.</li></ul></li></ul>	Le montant de l'indemnité due en cas de sinistre est constitué par : <ul style="list-style-type: none"><li>- la perte de marge brute obtenue par application du taux de marge brute à la différence constatée entre le chiffre d'affaires de la période d'indemnisation et le chiffre d'affaires de référence, celui des douze derniers mois qui précèdent le sinistre.</li><li>- les frais supplémentaires d'exploitation</li></ul>
------------------------------	--	--

<b>AUTRES FRAIS</b>	<ul style="list-style-type: none"><li>• <u>Objet de la garantie</u><ul style="list-style-type: none"><li>- honoraires d'expert</li><li>- intérêts bancaires</li></ul></li></ul>	
---------------------	---	--

(ii) *Le contrat "extension aux risques informatiques" (ERI)*

Ce contrat a pour objet la garantie des pertes de fonds et de biens consécutives à des fraudes, détournements, escroquerie, vol et actes de malveillance ou sabotage immatériel. Ce contrat peut également comporter des extensions de garantie aux pertes d'exploitation consécutives à une perte d'informations ou à l'utilisation non autorisée de ressources informatiques.

**(1) Garanties du contrat**

= Garanties de base

→ **Perte de fonds**

Il s'agit de fonds appartenant à l'assuré ou qui lui sont confiés. La garantie peut se situer soit au niveau des valeurs, dans les comptes financiers de la classe 5 du plan comptable général, soit dans les autres classes.

Classe 5 : 50 : valeurs mobilières de placement ; 51 : banques, établissements financiers et assimilés ; 53 : caisse ; 54 : régies d'avance et accréditifs ; 58 : virements internes ; 59 : provision pour dépréciation des valeurs mobilières de placement.

Ce sont, par exemple, des jeux d'écriture illicites ou des virements effectués au profit des clients.

Lorsqu'elles affectent les comptes d'autres classes, les fraudes concernent surtout les fausses factures impliquant les fournisseurs ou, en cas d'acte de malveillance, des passations d'écriture ayant pour effet d'entraîner la perte de créances sur des clients à l'insu de ceux-ci.

→ **Perte de biens**

Il s'agit de biens stockés ou en cours de fabrication, appartenant ou confiés à l'assuré.

Ce sera une sous-évaluation des biens de l'entreprise stockés ou en cours de fabrication (classe 3) avec récupération de la différence par l'auteur de l'infraction, en

cas de vol ou détournement ou une modification d'un programme de gestion de la composition des matières premières ayant pour effet d'endommager l'appareil de fabrication en cas de malveillance.

Ces pertes de fonds ou de biens sont garanties lorsqu'elles sont la conséquence d'un détournement, d'un abus de confiance, d'une fraude, d'une escroquerie, d'un vol tombant sous le coup des dispositions du Code pénal, quel que soit l'auteur de l'acte délictueux et qui apportent un profit financier à celui-ci sinon à d'autres personnes.

= Garanties facultatives

Ce sont :

- Les pertes d'exploitation résultant des pertes d'informations consécutives à une copie, à un vol ou à une altération du programme ou du fichier sur support informatique appartenant au système assuré.

Exemple : détournement d'un fichier "fournisseur" d'un distributeur permettant au bénéficiaire d'obtenir des conditions égales à celles du concurrent.

- L'utilisation non autorisée de ressources informatiques, c'est à dire le coût des heures de ressources informatiques perdues consécutif à toute utilisation, non autorisée par l'assuré, des ressources en matériel informatique au sein du système assuré.

Exemple : utilisation non autorisée d'un serveur de données entraînant une perte de revenus.

## **(2) Conditions de la garantie**

Avant de d'accorder toute garantie, l'assureur effectuera une analyse approfondie du risque. Au cours de cette analyse, il effectuera un contrôle général du système informatique, les sécurités logiques mises en place, les mesures de sécurité prévues au niveau de l'application.

La garantie ne pourra être mise en jeu que si l'assuré engage une action judiciaire (dépôt de plainte) même si les auteurs de l'infraction ne sont pas connus.

Le sinistre est imputé sur l'année d'assurance au cours de laquelle le fait générateur ou, en cas de sinistre continu, le premier fait générateur, est survenu.

S'agissant des risques spécifiquement informatiques, le fait générateur doit être interne au système informatique garanti, ce qui n'est pas sans poser de délicats problèmes de limites.

Ainsi sera pris en considération le fait pour une personne de violer le système d'identification et d'authentification et d'entrer sur écran des informations illicites, ou de modifier le contenu d'un état de sortie sur écran ou sur listing. Mais n'entrent pas dans la garantie les conséquences d'instructions données ou d'actions commises en amont du système informatique comme par exemple d'entrée sur écran d'informations illicites copiées sur un bordereau lui-même falsifié ou la copie d'éléments figurant sur un listing sorti du centre informatique.

(iii) *Le contrat "global informatique"*

Il comporte l'ensemble des garanties faisant l'objet des contrats examinés ci- dessus à savoir:

- les dommages matériels directs
- les dommages consécutifs à un dommage matériel direct
- les pertes d'exploitation après interruption du service
- les conséquences des fraudes, détournements, escroquerie, vols et actes de malveillance, et éventuellement des extensions comme les agios bancaires.

## **2.2 Les techniques préventives internes aux sociétés**

### **2.2.1 La prévention des risques et la mise en place d'outils de surveillance des salariés**

Il est important d'informer les salariés sur les risques d'atteinte à la sécurité informatique et il est obligatoire de les informer sur les outils de surveillance mis en place dans l'entreprise visant à assurer la sécurité du système informatique de l'entreprise.

(a) La surveillance du salarié

L'employeur a l'obligation d'informer au préalable et individuellement les salariés de tout dispositif de contrôle et de surveillance de leur activité sur le lieu de travail.

En effet, **l'article L. 121-8 du Code du Travail** dispose que : "*aucune information concernant personnellement un salarié ou un candidat à un emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ou du candidat à un emploi.*"

La licéité de la surveillance par la société de l'utilisation de la messagerie électronique de ses salariés est donc subordonnée à l'information préalable des salariés concernant le mode de surveillance en question.

Les salariés peuvent être informés par le biais d'une charte informatique, d'une mention spécifique dans leur contrat de travail ou d'un communiqué (art. L. 432-2-1 du Code du travail). **[Sous réserve que ces moyens n'ont pas tous la même force juridique et ne sont pas tous opposables aux salariés].**

Par ailleurs, la mise en place d'outils de surveillance suppose l'information et la consultation préalable du comité d'entreprise conformément à l'article L. 432-2-1 du Code du Travail : "*Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés.*"

Ainsi le Comité d'entreprise devra être informé et consulté lors de la mise en place d'un système de surveillance de l'activité des salariés, y incluant le contrôle de l'utilisation de la messagerie électronique de la société.

(b) L'utilisation d'un logiciel "mailsweeper"

Certaines entreprises utilisent un logiciel "mailsweeper", susceptible de scanner et de contrôler l'information transmise par leur système d'information. Ce logiciel a pour objectif d'identifier, de séparer et de bloquer des documents électroniques et e-mails, dans lesquels sont détectés des virus, des dysfonctionnements, du spamming ou tout langage ou code inapproprié. L'auteur du message ou celui qui l'a envoyé, recevra automatiquement un signal électronique l'informant que l'information a été bloquée. L'information bloquée peut être lue.

L'usage d'un tel système ne devrait pas être interdit en France. L'entreprise peut donc utiliser un tel système mais (i) en aucun cas elle ne pourra utiliser l'information bloquée

comme preuve d'une faute ou du non-respect d'une disposition légale ou réglementaire et (ii) seul l'administrateur réseau, qui a une obligation de secret en France, pourra éventuellement lire le contenu des enregistrements et des rapports sur les auteurs des informations bloquées ainsi que les avertissements reçus ou envoyés.

### 2.2.2 La mise en place de chartes informatiques

L'information des salariés en matière de sécurité informatique est de plus en plus souvent matérialisée par l'adoption d'une charte informatique intégrée au règlement intérieur visant à définir les droits et obligations des salariés quant à l'utilisation des outils informatiques de l'entreprise.

La mise en place d'un accès internet sur les postes personnels des salariés et l'augmentation des risques d'atteinte à la sécurité qui en découlent (notamment transmission de virus, téléchargement de logiciels contrefaisant) renforcent la nécessité de mettre en place une charte informatique.

#### (a) Le contenu de la charte

La charte informatique va définir les conditions d'accès et d'utilisation par les salariés des moyens informatiques de l'entreprise et notamment, les obligations en matière de sécurité, d'utilisation et de conservation des mots de passe, des limites d'utilisation de la messagerie électronique et d'Internet, d'établissement des moyens de prévenir l'apparition de virus.

De manière générale, le principe de proportionnalité des moyens utilisés au but recherché doit guider la rédaction de la charte.

Une première partie doit porter sur les enjeux essentiels pour la collectivité du personnel comme pour la pérennité de l'entreprise.

Ensuite, les clauses à prévoir :

- **Les aspects techniques** : du contrôle des envois, du respect des principes de sécurité, de la signalisation à la direction de tout incident, l'autorisation ou l'interdiction de connexion à Internet d'un poste déterminé, de l'utilisation de l'Intranet, enfin l'usage de la signature électronique et des mandats éventuels qui lui sont attachés.

*Le volume des envois, l'information immédiate de tout départ ou arrivée de collaborateur, avec interdiction d'accès dès le départ de l'entreprise, le respect impératif des principes de sécurité (codes*

*d'accès non divulgué, fermeture systématique du navigateur voire automatique en cas de départ du bureau) et la signalisation à la direction informatique de tout incident (virus, tentative d'intrusion), l'interdiction éventuelle de connexion à Internet à partir d'un poste ayant accès au réseau Intranet, de diffuser des messages à l'ensemble du personnel ou de faire des envois automatiques ; rappel, pour les firmes mondiales, des énormes différences de culture et la disparité dans la réglementation cryptologique, l'usage de la signature électronique et des mandats éventuels qui y sont attachés.*

- **La protection des données** : accès personnel, rappel de la Loi Informatique et Libertés, accès sécurisé, responsabilité du détenteur de fichiers nominatifs.

*Accès personnel avec son propre mot de passe qui ne doit pas être divulgué, limité aux seuls services nécessaires à sa propre activité professionnelle ; rappel de la loi Informatique et libertés sur la responsabilité du détenteur de fichiers nominatifs, avec les techniques adéquates pour en assurer le respect ; précautions nécessaires pour que l'accès à la boîte aux lettres soit sécurisé et protégé par la bonne gestion des mots de passe (confidentialité et renouvellement fréquent).*

- **L'utilisation à des fins personnelles** : conditions de diffusion des messages non professionnels, contrôle de l'utilisation d'Internet.

*La prohibition partielle de diffusion de messages à caractère non professionnel, quantification du caractère raisonnable de l'utilisation à des fins non professionnelles de l'Internet (contrôle en durée, en volume et toujours dans le cadre de la légalité et sans nuire à l'entreprise). Rappelons que l'interdiction totale et absolue d'utiliser sa messagerie professionnelle dans le cadre de sa vie privée est illicite et toute limitation doit être proportionnée au but recherché.*

- **Le rappel des interdictions** :

*Légales, des utilisations non autorisées (surf sur des sites internes ou externes sans rapport avec l'activité professionnelle précise du salarié, interdiction éventuelle de toute participation à des forums ou des*

*newsgroups ) ; rappel du retrait de la signature automatique en cas d'envoi de e-mails personnels.*

- **Les contrôles éventuels de l'employeur** : de l'activité interne comme externe du salarié et les moyens de contrôle

*Sur la nature tant interne (traces des transactions sur un ordinateur individuel, enregistrements) qu'externe (consultation des serveurs Internet externes à l'entreprise pour vérifier les informations déposées par le salarié sur les forums Internet externes) de l'activité du salarié, sur le contrôle volumétrique ou global des sites consultés, sur les moyens et dispositifs de contrôle utilisés.*

- **La responsabilité de l'employé** : peut être corrélativement engagée et justifier des sanctions disciplinaires ou un licenciement pour faute grave.

#### Exemples de Charte Technologique

<b>CHARTRE TECHNOLOGIQUE - PLAN ET DETAILS DES CLAUSES</b>	
<b>THEMES</b>	<b>CLAUSES</b>
<b>Introduction</b>	Contexte ; Enjeux ; Objectifs.
<b>Champ d'application</b>	Personnes concernées.
<b>Les outils de communication concernés (à l'exception des outils informatiques)</b>	Téléphone ; autocommutateurs téléphoniques ; télécopie, minitel, télex, visioconférence ; caméras de surveillance.
<b>Les réseaux informatiques</b>	Droit d'accès ; mot de passe ; modem ; utilisation d'Internet, messagerie ; droit d'auteur ; signature électronique ; fichier de journalisation.
<b>Les logiciels</b>	Installation ; téléchargement ; respect de la propriété intellectuelle ; anti-virus.
<b>L'utilisation des</b>	Règles générales ; disquettes et autres supports de données ; configuration du poste ; mobilité du matériel

<b>matériels informatiques</b>	informatique, responsabilité.
<b>La sécurité et la déontologie informatique</b>	Analyse et contrôle de l'utilisation des ressources ; respect de la confidentialité des informations ; protection des données personnelles ; protection des fichiers ; règles générales de sécurité ; respect de la personne.
<b>L'utilisation des outils informatiques par certaines catégories de salariés</b>	Institutions représentatives du personnel ; informaticiens et personnel du service informatique.
<b>Sanctions</b>	–
<b>Publicité, entrée en vigueur et modification de la charte</b>	Dépôt et date d'entrée en vigueur ; modifications.

(b) La valeur juridique de la charte

Pour être opposable aux salariés de l'entreprise, la Charte doit être adjointe au règlement intérieur dans la mesure où :

- d'une part, elle contient des règles générales et permanentes quant à l'utilisation du matériel professionnel, et
- d'autre part, elle relève de l'hygiène, de la sécurité et de la discipline (art. L. 122-34).

Elle est alors soumise à la procédure de l'article L. 122-36 qui impose le recueil de l'avis du Comité d'entreprise sur son contenu et de transmission du procès-verbal de la délibération du Comité d'entreprise à l'inspecteur du travail qui vérifiera la licéité du contenu de la charte.

Elle peut comporter des dispositions techniques (dimension maximum des mails, des pièces jointes, sécurisation des données) et de savoir-vivre (utilisation de l'en-tête, réponses rapides, formules diverses). Dans ce cas, une simple information du comité d'entreprise suffira.

Les chartes, hier répressives se feront plus consensuelles demain et offriront une alternative aux conventions collectives souvent vides de contenu car trop difficiles à négocier avec les partenaires sociaux.

Lorsqu'elles sont annexées au règlement intérieur, les chartes informatiques sont sanctionnées sur le plan disciplinaire. La faute grave peut justifier un licenciement tandis que la faute lourde permet en outre de rechercher la responsabilité civile du salarié pour le préjudice subi. La faute lourde est, en droit du travail français, limitée à **l'action dolosive, destinée à nuire** délibérément à l'entreprise.

Exemples de fautes :

→ **Absence de faute lourde**

Le fait de transférer moyennant rémunération un fichier-clients à un concurrent ne relève pas de la faute lourde mais de la seule faute grave puisque c'est par simple intérêt personnel que le salarié a agi. Tout comme fouiller le service comptabilité à la recherche de preuve. (Chambre sociale, 22 février 2000).

→ **Faute lourde**

De multiples courriers (postaux hier mais aussi mails aujourd'hui) adressés aux autorités administratives et financières ou à des tiers, et faisant état de la commission de graves délits pénaux de la part de la Direction générale "ne pouvaient que jeter le discrédit sur la société" et constituent une faute lourde (Cass. Soc., 30 mai 1995, n°2341), comme le seraient par analogie avec l'arrêt du 25 janvier 2000 des mails expédiés à des clients de l'entreprise et dénigrant des produits, ou l'ouverture délibérée de fichiers notoirement infectés.

L'arrêt du 28 juin 2000 a conclu à la faute lourde dans l'espèce suivante : deux salariés avaient de concert copié des images de la banque de données pour les remettre à l'entreprise concurrente, avec laquelle ils avaient signé un contrat ; puis ils avaient introduit un virus dans le logiciel de base et délibérément saturé les fichiers afin de rendre le système inutilisable. La Cour a constaté l'intention évidente de nuire, ce qui n'aurait pas été le cas s'ils s'étaient contentés de voler ou dupliquer les fichiers et a retenu la faute lourde.

Seule la faute lourde peut entraîner la recherche de la responsabilité civile du salarié, et donc le versement de dommages et intérêts : une clause de responsabilité contractuelle ou figurant dans le Règlement intérieur est inopérante.

## PARTIE 3 :

# CRIMINALITE INFORMATIQUE ET PROCEDURES CONTENTIEUSES

### **3. LA MISE EN ŒUVRE PRATIQUE : CRIMINALITE INFORMATIQUE ET PROCEDURES CONTENTIEUSES**

Après avoir étudié l'arsenal répressif mis à la disposition des victimes d'attaques informatiques, il convient d'en étudier la mise en œuvre et les organismes compétents en la matière.

Les comportements réprimés par la Loi Godfrain étant des infractions pénales, il convient d'exercer une action judiciaire pour les faire sanctionner.

Or, la poursuite des infractions que l'on vient d'étudier ne peut être efficace que si des outils adaptés sont mis à la disposition des magistrats et des policiers. Ainsi, l'augmentation de la criminalité informatique a nécessité la mise en place d'organismes et de procédures adaptées à ce nouveau type de criminalité. Désormais, dans le cadre des informations judiciaires et des enquêtes, le recours à des outils spécialisés est possible.

#### **3.1 Les organismes policiers spécialisés**

Du fait de la technicité des enquêtes en matière d'attaques informatiques, deux **services spécialisés** de la police judiciaire ont été créés à cet effet :

##### **3.1.1 La Brigade Centrale de Répression de la Criminalité Informatique ("BCRCI")**

La BCRCI est rattachée **au plan national** à la Direction Centrale de la Police Judiciaire. Cette entité est chargée spécifiquement :

- de mener des enquêtes ayant des aspects nationaux ou internationaux, et
- d'assister les Services Régionaux de Police Judiciaire et d'assurer l'interface avec les services internationaux (Interpol et Groupe de Travail Européen sur la Fraude Informatique).
- 

##### **3.1.2 Le rôle de l'Office Central de Lutte Contre la Criminalité liée aux Technologies de l'Information et de la Communication ("OCLCTIC")**

Cet office a été institué par le ministère de l'Intérieur (direction générale de la police nationale, direction centrale de la police judiciaire) par un décret du 15 mai 2000. (Décret du 15 mai 2000, n°2000-405, J.O. 16 mai 2000).

L'office a pour domaine de compétence les infractions spécifiques à la criminalité liée aux technologies de l'information et de la communication ainsi que les infractions dont la commission est facilitée ou liée à l'utilisation de ces technologies.

L'OCLCTIC accomplit plusieurs missions.

a) Les missions générales

- L'animation et la coordination, au niveau national, de la mise en œuvre opérationnelle de la lutte contre les criminels.

- L'assistance dans leurs missions des services de police et de gendarmerie nationales, ou tout autre service en cas d'infraction liée aux technologies de l'information et de la communication.

b) Les missions relatives à l'enquête

- Procéder, à la demande de l'autorité judiciaire, à tous les actes d'enquête et aux travaux techniques d'investigations en assistance aux services chargés d'enquêtes de police judiciaire sur les infractions dont la commission est facilitée par ou liée à l'utilisation des technologies de l'information et de la communication, sans préjudice de la compétence des autres offices centraux de police judiciaire.

- Intervenir avec l'accord de l'autorité judiciaire saisie, chaque fois que les circonstances l'exigent, pour s'informer sur place des faits relatifs aux investigations conduites.

- Au titre de ces compétences, l'OCLCTIC peut faire figure d'alternative ou de complément à l'expert.

### **3.1.3 Le Service d'Enquête sur les Fraudes aux Technologies de l'Information ("SEFTI")**

Créé en 1994 au sein de la sous direction des Affaires Economiques et Financières de la Direction de la police judiciaire parisienne, le SEFTI mène lui aussi ses enquêtes avec une compétence territoriale étendue à **la capitale et aux trois départements de la petite couronne**.

Il s'agit du plus important service de police français exclusivement chargé de lutter contre la criminalité informatique. Depuis janvier 2001, le SEFTI de la préfecture de police de Paris est une brigade appelée la "**BEFTI**".

## **MISSIONS**

Les missions du **SEFTI** et de la **BEFTI** sont les suivantes :

### a) Une mission d'investigation

La BEFTI a pour mission essentielle de lutter contre les atteintes aux systèmes de traitement automatisés d'informations, qu'il s'agisse des réseaux informatiques ou télématiques, ou des systèmes de télécommunications (GSM, autocommutateurs d'entreprise, etc).

Son domaine d'action ne se limite cependant pas aux intrusions dans les systèmes d'informations, mais vise également la lutte contre la contrefaçon sur supports numériques, la captation frauduleuse de médias télévisuels cryptés, ainsi que des incriminations traditionnelles utilisant les nouvelles technologies comme support de commission. Les incriminations concernées sont alors l'escroquerie (y compris, dans le milieu de la télématique), le détournement de fonds, l'abus de confiance, les atteinte aux biens (recel de vol), les atteintes à la personne (injures, diffamation) ou prévues par la loi du 29 juillet 1881 (Loi sur la liberté de la presse) perpétrées sur les réseaux.

Cette équipe de 22 fonctionnaires, traite en moyenne 500 plaintes par an. Avec des pics d'activité lorsqu'une nouvelle technologie apparaît, et son cortège de failles, comme les cartes télécoms ou de téléphone mobile par exemple.

### Nature des plaintes recensées à la BEFTI :

- 60% de ces plaintes émanent des entreprises.
- 1/3 concernent Internet, un autre tiers des intrusions,
- 22% concernent des escroqueries diverses, 9% la contrefaçon (pillage, copie illicite),
- 3% sont relatives aux attaques de PABX (*Private Automatic Branch Exchange*), et
- 1% concerne le non respect de la réglementation de la CNIL (Commission Nationale Informatique et Liberté).

Source : <http://www.symantec.fr/region/fr/resources/braquage.html>

La BEFTI apporte son concours aux enquêtes et aux instructions concernant des infractions commises au moyen d'outils informatiques. Lorsque la BEFTI est saisie d'une plainte, l'investigation se poursuit dans le cadre classique des poursuites policières : constatations (recherche des "empreintes" laissées par le pirate et des fichiers qui ont pu le piéger), auditions et perquisitions. Pour les cas les plus complexes, la BEFTI est assisté d'un expert judiciaire ou d'un ingénieur désigné par un magistrat.

b) Une mission de soutien technique

Le SEFTI assure également un soutien technique aux autres services de police.

c) Une mission pédagogique

Il remplit également une mission pédagogique en menant des actions d'information auprès d'organismes privés ou publics susceptibles d'être confrontés aux problèmes de fraudes informatiques.

### 3.2 Le recours à l'expertise

Outre la procédure classique d'expertise, la loi sur la sécurité quotidienne a créé une expertise spécifique aux technologies de l'information.

L'article 30 de la **loi du 15 novembre 2001 relative à la sécurité quotidienne** introduit un titre IV dans le premier livre du Code de procédure pénale. Ce titre comporte un Chapitre unique qui concerne "*la mise au clair de données chiffrées nécessaires à la manifestation de la vérité*". **Ce nouveau Chapitre est composé des articles 230-1 à 230-5 du Code de procédure pénale.**

Notons que **le projet de loi sur la confiance dans l'économie numérique** abroge ce dispositif en le reprenant à l'identique dans son article 27.

La loi semble donc renforcer les moyens d'investigation dans le domaine des technologies de l'information et de la communication en prévoyant **deux nouvelles mesures essentielles.**

### 3.2.1 Le recours à l'expert "chargé d'obtenir une version claire des informations"

Sans préjudice des dispositions traditionnelles relatives à l'expertise classique, la présente loi crée une **nouvelle forme de recours à l'expertise** propre au déchiffrement de certains documents.

Cette expertise est donc **spécifique** aux technologies de l'information.

L'article 230-1 alinéa 1<sup>er</sup> nouveau du Code de procédure pénale dispose :

*"[...] lorsqu'il apparaît que des données saisies ou obtenues au cours de l'enquête ou de l'instruction ont fait l'objet d'opérations de transformation empêchant d'accéder aux informations en clair qu'elles contiennent ou de les comprendre, le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut désigner toute personne physique ou morale qualifiée, en vue d'effectuer les **opérations techniques permettant d'obtenir la version en clair de ces informations ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement, si cela apparaît nécessaire**".*

### 3.2.2 Le concours des "moyens de l'Etat" à la mission de l'expert

L'article 230-1 aliéna 2 nouveau du Code de procédure pénale dispose :

*"Si la peine encourue est égale ou supérieure à deux ans d'emprisonnement et que les nécessités de l'enquête ou de l'instruction l'exigent, le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut prescrire le recours aux moyens de l'Etat soumis au secret de la défense nationale selon les formes prévues au présent chapitre."*

#### Les modalités du recours

L'article 230-2 poursuit en précisant que si l'autorité compétente décide d'avoir recours aux moyens de l'Etat, une réquisition écrite doit être adressée au service national de police judiciaire chargé de la lutte contre la criminalité liée aux technologies de l'information, avec le support physique contenant les données à mettre au clair ou une copie de celui-ci.

Le service de police auquel la réquisition a été adressée transmet cette dernière à un organisme technique soumis au secret de la défense nationale, et désigné par décret.

### **3.3 Le renforcement des moyens d'investigation en matière informatique : le projet de loi sur la sécurité intérieure**

Dans ses annexes, la loi d'orientation et de programmation pour la sécurité intérieure du 29 août 2002 prévoit l'élaboration d'un texte renforçant les prérogatives des officiers de police judiciaire, agissant dans le cadre d'une enquête liée à la criminalité informatique.

Le projet de loi sur la sécurité intérieure actuellement en discussion devant le Parlement comporte une **mesure nouvelle**.

Le texte permet aux officiers de police judiciaire, agissant dans le cadre d'une enquête judiciaire, sur autorisation d'un magistrat, d'accéder directement à des fichiers informatiques et de saisir à distance par voie télématique ou informatique, les renseignements qui paraissent nécessaires à la manifestation de la vérité.

Malgré l'ambiguïté de la formule, ce mode d'enquête à distance ne constitue pas une "télé-perquisition". En effet, les policiers pourront avoir un accès direct aux bases de données des opérateurs de télécommunications et des fournisseurs d'accès à Internet. En effet, la loi sur la sécurité quotidienne dans son **article 29** a inséré un article **L. 32-3-1, al. 2 au Code des Postes et Télécommunications**, qui oblige ces derniers à conserver les données de connexion de leurs clients pour une durée maximale d'un an.

Les annexes de la loi d'orientation et de programmation pour la sécurité intérieure ont néanmoins été édulcorées par rapport à leur première version. Les organismes ou personnes visés par la loi n'ont pas l'obligation de mettre en ligne les bases de données, ils sont simplement tenus de mettre les informations requises à la disposition des services de police dans les meilleurs délais.

### **3.4 L'appréhension internationale du traitement judiciaire des infractions informatiques**

Les infractions pouvant être commises simultanément dans plusieurs pays du fait des réseaux obligeant les investigations à se dérouler dans un contexte trans-frontière, l'informatique est susceptible de bouleverser les règles classiques de compétence.

Il faut, d'une part, présenter les services compétents en la matière et, d'autre part, fournir des éléments pour améliorer le traitement des procédures lorsque les enquêtes doivent se poursuivre à l'étranger.

### 3.4.1 Les services compétents

#### (a) Interpol

##### **Organisation**

Organisation Internationale de Police Criminelle (OIPC), Interpol vise à améliorer la coopération policière dans le monde grâce à des bureaux dans 178 pays membres. Ces bureaux sont des services de police permanents composés de policiers agissant dans le cadre de leur législation nationale. Ils constituent le relais national aux opérations de police sollicitées par les autres Etats membres.

L'antenne d'Interpol en France est rattachée à la direction centrale de la Police Judiciaire au sein de la sous Direction des ressources et liaison dans la Division des relations internationales.

##### **Mission**

Parmi ses attributions, Interpol a pour objet de faciliter la lutte contre la **criminalité informatique**.

L'organisation porte à la connaissance des services de police nationaux certains renseignements relatifs à des infractions, des délinquants et des victimes. Les infractions instruites par Interpol entrent directement en procédure.

#### (b) Europol

##### **Mission**

L'office européen de police (Europol) siégeant à La Haye, est un organe policier chargé du traitement des renseignements relatifs aux activités criminelles. Son objectif consiste à améliorer l'efficacité des services compétents des Etats membres et à intensifier leur coopération dans le cadre de la prévention et la lutte contre les formes graves de criminalité internationale organisée.

Le mandat d'Europol a été considérablement élargi. Aujourd'hui, Europol est compétent pour la lutte contre la **criminalité informatique** ou pour les formes de criminalité dont la commission est facilitée par Internet. Toutefois, les infractions doivent impliquer une structure ou une organisation criminelle et deux Etats membres ou plus, doivent être affectés.

Europol intervient en permettant l'échange d'informations et en fournissant des rapports, analyses, expertises et assistance technique aux enquêtes et aux opérations menées au sein de l'Union Européenne.

La liaison entre Europol et la France est assurée par l'unité nationale Europol, implantée au sein du ministère de l'Intérieur.

### 3.4.2 Les accords de Schengen

Certains articles de la **Convention des accords de Schengen** sont susceptibles d'avoir un lien avec une affaire de criminalité informatique.

#### (a) Le système d'information SCHENGEN (SIS)

Ce système permet l'échange d'informations entre les Etats signataires et la consultation automatisée des données sur les personnes et les objets signalés. Il participe, grâce à la mise place d'une coopération continue entre les Etats membres, à la préservation de l'ordre public.

Le SIRENE France est le point de contact national unique mis à la disposition des autres partenaires de l'espace Schengen pour assurer les échanges d'information et de documents avec les autres SIRENE. Il s'agit d'un service interministériel qui associe des policiers, des gendarmes et des magistrats.

#### (b) La coopération policière dans l'espace SCHENGEN

Outre l'échange d'informations, cette coopération suppose l'assistance mutuelle aux fins de la prévention et de la recherche de faits punissables et l'intensification de la coopération policière dans les régions frontalières.

Les principales dispositions traitant de cette entraide sont les suivantes :

- **Article 39-5 : Coopération judiciaire directe**

La Convention prévoit un modèle interministériel de convention de coopération transfrontalière policière et douanière qui fixe les règles de coopération directe entre les unités opérationnelles dans la zone frontalière et prévoit la création de centres de coopération policière et douanière.

Dans une même structure sont donc rassemblés les policiers, gendarmes et douaniers, mis à disposition de l'ensemble des services chargés de missions de police et de douane.

- **Article 40 : Le droit d'observation**

C'est la possibilité offerte à l'enquêteur de poursuivre une filature sur un Etat voisin.

- **Article 41 : Droit de poursuite**

Permet aux enquêteurs de poursuivre une personne prise en flagrant délit de participation ou de commission d'une infraction prévue par la convention, sans autorisation préalable au delà des frontières lorsque cette personne prend la fuite vers un état voisin.

- **Article 51 : Perquisitions et saisies**

La seule condition prévue, outre la compatibilité de la mesure avec la législation de l'Etat partie, est que l'infraction réponde quant à ses sanctions à certaines conditions précises prévues par la Convention.

## **BIBLIOGRAPHIE**

## BIBLIOGRAPHIE

### I) Ouvrages généraux :

- Droit pénal et procédure pénale, Jean Claude Soyer, LGDJ – Montchrestien, 16<sup>e</sup> édition (2002)

### II) Ouvrages spécialisés :

- Informatique, Télécoms, Internet, Alain Bensoussan, Editions Francis Lefebvre, édition 2002

- Lamy Droit de l'informatique et des réseaux, Michel Vivant et Christian Le Stanc, édition 2003

### III) Périodiques :

- Communication Commerce Electronique

- Expertises des systèmes d'information

- La Gazette du Palais, spécial technologies avancées

« GUIDE »

DE LA SECURITE INFORMATIQUE

**ANNUAIRE DES ORGANISMES LIES A LA SECURITE INFORMATIQUE**

**AFAI**

Association Française de l'Audit et du Conseil Informatiques

88, rue de Courcelles - 75008 Paris

Tél : 01.46.93.65.64

Site Internet : [www.afai.asso.fr/](http://www.afai.asso.fr/)

e-mail : [afai@afai.asso.fr](mailto:afai@afai.asso.fr)

**BCRCI**

Brigade Centrale de Répression de la Criminalité Informatique

101, rue des Trois Fontanot

92000 NANTERRE

Tél. : 01.40.97.87.72 et 01.40.97.83.12

Fax : 01.47.21.00.42

**BEFTI**

Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information

Commissaire Pascal Courtin

163, avenue d'Italie

75013 PARIS

Tél. : 01.40.79.67.50

Fax. : 01.40.79.77.21

Site Internet : [www.prefecture-police-paris.interieur.gouv.fr/carrieres/Metiers/cyberpolice.htm](http://www.prefecture-police-paris.interieur.gouv.fr/carrieres/Metiers/cyberpolice.htm)

**CEA**

Centre des Experts Agréés

37 rue de la Rochefoucauld

75009 Paris

Tél : 01.53.21.83.33

Fax : 01.53.21.83.30

Site Internet : [www.expert-cea.com/contact.asp](http://www.expert-cea.com/contact.asp)

e-mail : [cea@expert-cea.com](mailto:cea@expert-cea.com).

## **CERT**

Computer Emergency Response Team

CERT® Coordination Center  
Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213-3890  
U.S.A.  
Tél : +1 412-268-7090  
Fax : +1 412-268-6989  
Site Internet : [www.cert.org/](http://www.cert.org/)  
e-mail : [cert@cert.org](mailto:cert@cert.org)

## **CLUSIF**

Club de la sécurité des systèmes d'information français

30, rue Pierre Sépard  
75009 Paris  
Tél : 01.53.25.08.80  
Fax : 01 53 25 08 88  
Site Internet : [www.clusif.asso.fr/](http://www.clusif.asso.fr/)

## **CNIL**

La Commission Nationale de l'Informatique et des Libertés

21, rue Saint Guillaume  
75340 PARIS Cedex 07  
Tél. : 01.45.44.40.65  
Fax : 01.45.49.04.55  
Site Internet : [www.cnil.fr](http://www.cnil.fr)  
Minitel : 3515 CNIL

**Lien** vers le texte de la loi du 6 janvier 1978 : [www.cnil.fr/textes/index.htm](http://www.cnil.fr/textes/index.htm)

## **La Commission européenne - Représentations françaises**

### **Paris**

*Jean-Louis GIRAUDY*  
288, boulevard Saint-Germain  
F-75007 Paris  
Tél : (33-1) 40 63 38 00  
Fax : (33-1) 45 56 94 17/18/19

**Marseille**

Jacques HUCHET  
2, rue Henri-Barbusse (CMCI)  
F-13241 Marseille Cedex 01  
Tél : (33-4) 91 91 46 00  
Fax : (33-4) 91 90 98 07

**Conseil de l'Europe**

**Conseil de l'Europe**

67075 Strasbourg Cedex  
France  
Tél : +33 3 88 41 20 33  
Fax : +33 3 88 41 27 45  
Site Internet : [www.coe.int](http://www.coe.int)  
e-mail : [infopoint@coe.int](mailto:infopoint@coe.int)

**Lien** vers la Convention de Budapest sur la cybercriminalité :  
<http://conventions.coe.int/Treaty/FR/WhatYouWant.asp?NT=185>

**Bureau de Paris du Conseil de l'Europe**

55 av Kléber 75784 Paris Cedex 16  
Tél : 00 33 (0)1 44 05 33 60  
Fax : 00 33 (0)1 47 27 36 47  
e-mail : [documentation.paris@coe.int](mailto:documentation.paris@coe.int)

**EUROPOL**

Ministère de l'Intérieur  
Place Beauvau  
75008 Paris  
Tél : 01.47.07.60.60  
Site internet : [www.europol.net/](http://www.europol.net/)

**INTERPOL**

General Secretariat  
200, quai Charles de Gaulle  
69006 Lyon  
France  
Fax : (33) 4 72 44 71 63  
Site Internet : [www.interpol.int/](http://www.interpol.int/)  
e-mail : [cp@interpol.int](mailto:cp@interpol.int)

### **LEXSI**

Laboratoire d'Expertise en Sécurité Informatique

TOUR ORION

12-16 rue de Vincennes

93 100 MONTREUIL

Tél : 01.55.86.88.88

Fax : 01 55 86 88 89

Site Internet : [www.lexsi.com/](http://www.lexsi.com/)

### **MI2G**

Granville House

132-135 Sloane street

London

SW1X 9AX

United Kingdom

Tél (UK) : 07000 64 24 00

Fax (UK) : 07000 64 24 01

Tél (International) : +44 20 79 24 30 10

Fax (International) : +44 20 79 24 33 10

e-mail : [solutions@mi2g.com](mailto:solutions@mi2g.com)

Site Internet : [www.mi2g.com](http://www.mi2g.com)

### **OCDE**

Organisation de Développement et de Coopération Economiques

OCDE - Centre français

2, rue André Pascal

75775 Paris Cedex 16

France

Tél : +33 1.45. 24.82.00

Site Internet : [www.oecd.org/](http://www.oecd.org/)

e-mail : [news.contact@oecd.org](mailto:news.contact@oecd.org)

**Lien** vers les lignes directrices régissant la sécurité des systèmes et réseaux d'information : [www.oecd.org/FR/home/0,,FR-home-43-nodirectorate-no-no-no-13,00.html](http://www.oecd.org/FR/home/0,,FR-home-43-nodirectorate-no-no-no-13,00.html)

### **OCLCTIC**

Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication

101 rue des Trois Fontanot

92 000 Nanterre

Tel : 01.49.27.49.27

**SCSSI**

Le Service Central de la Sécurité des Systèmes d'Information

18, rue du Docteur Zamenhof

92131 Issy-Les-Moulineaux

Tél. : 01.41.46.37.20

Fax. : 01.41.46.37.01

Site Internet : [www.scssi.fr](http://www.scssi.fr)

## LES TEXTES RELATIFS A LA SECURITE INFORMATIQUE

### La loi Godfrain

Insérée dans le Code pénal aux articles 323-1 et suivants.

Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique.

Publication au Journal Officiel :

NOR : JUSX8700198L. 6 janvier 1988, p. 231

### La loi Informatique Fichier et libertés

Loi n° 78-17 du 6 janvier 1978 - Informatique Fichier et libertés.

Publication au journal Officiel :

7 janvier 1978, p.227

### Le projet de loi sur la confiance dans l'économie numérique (adopté le 15 janvier 2003 en Conseil des ministres)

Le texte est disponible sur le site Internet de l'assemblée nationale :

<http://www.senat.fr/>

**Lien direct :**

<http://www.senat.fr/leg/pjl02-195.html>

### La loi d'orientation et de programmation pour la sécurité intérieure

Loi n° 2002-1094 du 29 août 2002

Publication au Journal Officiel :

NOR : INTX020014L du 30 août 2002, p, 14398

### La Convention de Budapest sur la cybercriminalité du 23 novembre 2001

Le texte est disponible sur le site Internet du Conseil de l'Europe :

<http://www.coe.int>

**Lien direct :**

<http://conventions.coe.int/Treaty/FR/WhatYouWant.asp?NT=185>

### Les lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information du 25 juillet 2002

Le texte est disponible sur le site Internet de l'OCDE : <http://www.oecd.org>

**Lien direct :**

<http://www.oecd.org/FR/home/0,,FR-home-43-nodirectorate-no-no-no-13,00.html>

### La proposition de décision cadre de la Commission européenne relative "aux attaques visant les systèmes d'information" du 19 avril 2002

Le texte est disponible sur le site Internet de l'Union européenne :

<http://europa.eu.int>

**Lien direct :**

[http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=FR&numdoc=52002PC0173&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=FR&numdoc=52002PC0173&model=guichett)

**La Convention des accords de Schengen**

Le texte est disponible sur le site Internet de l'Union européenne :  
<http://europa.eu.int>