



U – PANTHÉON - SORBONNE – 1
UNIVERSITÉ PARIS 1

UFR 01 - Droit, Administration et Secteur Public

MASTER Droit de l'Internet Public - Administration - Entreprises
Année Universitaire 2006 – 2007

MEMOIRE

Présenté par Jean-François TYRODE
Session Septembre 2007

**« ÉLEMENTS DE PROCEDURE PENALE DANS LE CADRE DE
L'ATTEINTE AUX PERSONNES PAR LA CYBERCRIMINALITE EN
DROIT EUROPEEN »**

Président du Jury :

M. Le Professeur Georges Chatillon
Directeur du MASTER Droit de l'Internet Public - Administration - Entreprises

Membres du Jury :

Maître Pierre-Yves Margnoux
Avocat associé au Cabinet Derriennic & Associés

Table des matières

INTRODUCTION.....	3
PARTIE I : LES TECHNIQUES DE SECURISATION ET D'INVESTIGATION.....	3
CHAPITRE PREMIER : LES METHODES DE SECURISATION.....	3
Section première : la protection contre la captation d'informations personnelles confidentielles.....	3
Paragraphe premier : panorama des différentes attaques connues concernant l'atteinte aux personnes.....	3
Paragraphe deuxième : l'utilisation d'architectures techniques sécurisées contre les atteintes aux personnes.....	3
Paragraphe troisième : les moyens techniques de protection des données contre les atteintes aux personnes.....	3
Section deuxième : les obligations des FAI et hébergeurs et les techniques de protection juridiques.....	3
Paragraphe premier : les obligations imposées par la LCEN et les procédures de signalement.....	3
Paragraphe deuxième : la conservation des informations de connexion.....	3
Paragraphe troisième : l'indemnisation des prestataires techniques.....	3
CHAPITRE SECOND : LES METHODES D'INVESTIGATION.....	3
Section première : les services d'enquête judiciaire et les techniques d'investigation.....	3
Paragraphe premier : les services d'enquête judiciaire.....	3
Paragraphe deuxième : les techniques d'investigation.....	3
Paragraphe troisième : le matériel d'investigation, de prévention et d'aide à l'enquête.....	3
Section deuxième : parallèle entre l'investigation technique et la réglementation pénale.....	3
Paragraphe premier : la question de la preuve.....	3
Paragraphe deuxième : les précautions à prendre lors de la collecte des preuves dans une enquête préliminaire.....	3
<i>Sous paragraphe premier : la collecte des preuves lors d'un constat d'huissier, nos recommandations.....</i>	<i>3</i>
<i>Sous paragraphe deuxième : la collecte des preuves lors d'une perquisition, nos recommandations.....</i>	<i>3</i>
Paragraphe troisième : les difficultés d'établir la preuve lors de l'expertise judiciaire.....	3
PARTIE II : LES RELATIONS ENTRE LES INVESTIGATIONS TECHNIQUES ET LES ATTEINTES AUX PERSONNES.....	3
CHAPITRE PREMIER : CADRE LEGAL GENERAL DE L'ATTEINTE AUX PERSONNES.....	3
Section première : les atteintes à la vie privée par l'image.....	3
Paragraphe premier : les caractéristiques pénales de l'infraction.....	3
Paragraphe deuxième : les critères d'appréciation.....	3
Section deuxième : les atteintes par la diffamation et l'injure.....	3
Paragraphe premier : les caractéristiques pénales de l'infraction.....	3
Paragraphe deuxième : les critères d'appréciation.....	3
Section troisième : les atteintes par la provocation à la haine ou à la violence.....	3
Paragraphe premier : les caractéristiques pénales de l'infraction.....	3
Paragraphe deuxième : les critères d'appréciation.....	3
CHAPITRE SECOND : CAS DE L'ATTEINTE AUX MINEURS.....	3
Section première: les atteintes par un message à caractère pornographique, pédophile ou violent.....	3
Paragraphe premier : les caractéristiques pénales de l'infraction.....	3
Paragraphe deuxième : les critères d'appréciation.....	3
Section deuxième: les atteintes et agressions sexuelles sur les mineurs par Internet.....	3
Paragraphe premier : les caractéristiques pénales de l'infraction.....	3
Paragraphe deuxième : les critères d'appréciation.....	3
Section troisième: l'incitation des mineurs à la violence ou au suicide par Internet.....	3
Paragraphe premier : les caractéristiques pénales de l'infraction.....	3
Paragraphe deuxième : les critères d'appréciation.....	3
PARTIE III : LES INVESTIGATIONS INTERNATIONALES ET EUROPEENNES.....	3
CHAPITRE PREMIER : LES MOYENS MIS EN OEUVRE AU NIVEAU INTERNATIONAL POUR LUTTER CONTRE LA CRIMINALITE INFORMATIQUE.....	3
Section première: les institutions européennes.....	3
Paragraphe premier : l'organisation EUROPOL.....	3
Paragraphe deuxième : l'organisation EUROJUST.....	3
Paragraphe troisième : le système d'information SCHENGEN.....	3
Section deuxième: la convention sur la cybercriminalité du 23 novembre 2001.....	3

Paragraphe premier : les différentes catégories d'infraction.....	3
<i>Sous paragraphe premier : les infractions contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques.....</i>	3
<i>Sous paragraphe deuxième : les infractions et les falsifications informatiques.....</i>	3
<i>Sous paragraphe troisième : les infractions se rapportant au contenu.....</i>	3
Paragraphe deuxième : l'harmonisation relative aux procédures pénales et l'entraide judiciaire.....	3
CHAPITRE DEUXIEME : CAS DE CYBERCRIMINALITE ET TRAITEMENTS AU NIVEAU INTERNATIONAL.....	3
Section première: le cas des courriels non sollicités	3
Paragraphe premier : définition générale d'un courriel non sollicité.....	3
Paragraphe deuxième : les difficultés de la lutte contre l'envoi de courriels non sollicités.....	3
Section deuxième: le cas de la pédo-pornographie	3
Paragraphe premier : définition générale de la pédo-pornographie	3
Paragraphe deuxième : les difficultés de la lutte contre la pédo-pornographie.....	3
CONCLUSION	3
BIBLIOGRAPHIE.....	3
ANNEXES	3

Je tiens à exprimer mes remerciements à Monsieur le Professeur Georges Chatillon pour ses précieux conseils dans le cadre de la rédaction de ce mémoire.

INTRODUCTION

L'utilisation de systèmes et des réseaux informatiques est aujourd'hui un atout pour notre société. Cependant, elle tend à créer des menaces dans la mesure où une partie de plus en plus importante des transactions économiques et sociales sont effectuées à l'aide de l'outil informatique. Les réseaux facilitent en effet l'accès illicite à l'information et cette situation est exploitée par les cybercriminels, non seulement en Europe mais aussi à l'échelle de toute la planète.

C'est pourquoi, la sécurité des technologies de l'information, ainsi que la prévention de la cybercriminalité sont d'une grande importance pour notre société. La compréhension de la nature et de l'ampleur de la menace permet d'éduquer les utilisateurs finaux du réseau Internet, adopter des mesures techniques de protection contre la cybercriminalité, mais aussi permet d'élaborer un droit pénal efficace dans la lutte contre la délinquance informatique.

La délinquance informatique a pris un essor considérable avec l'augmentation du nombre d'utilisateurs reliés aux réseaux informatiques, et notamment depuis les années 90 avec le développement du web.

Internet a suscité au cours de ces années l'intérêt de regroupement d'individus organisés proposant des contenus illégaux, comme la pédo-pornographie ou bien l'incitation à la haine et à la violence.

Les nouvelles technologies, les ordinateurs et les réseaux sont aujourd'hui utilisés comme des outils, voire des armes, pour commettre des crimes.

La cybercriminalité se présente sous plusieurs formes :

- les infractions contre la confidentialité, l'intégrité, la disponibilité,
- les infractions informatiques traditionnelles telles que les fraudes à la carte bancaire ou la falsification de documents,
- les infractions se rapportant au contenu,
- les infractions constitutives d'une atteinte aux personnes et aux mineurs.

L'atteinte aux personnes par la cybercriminalité regroupe différentes sortes de cas de criminalité par l'usage de l'Internet, de l'attaque de sites de commerces en ligne avec vol de données personnelles des clients du site, jusqu'à la détention et la diffusion de contenus illicites, notamment dans le cadre de la pornographie infantine.

La captation de données personnelles, à l'aide, par exemple, des chevaux de Troie dissimulés dans d'autres programmes, représente aujourd'hui un phénomène de masse et un véritable danger pour l'internaute. Dans beaucoup de cas, ces chevaux de Troie sont distribués par des virus ou bien attachés à un mail en pièce jointe, et vont permettre d'enregistrer par

exemple les frappes de touche du clavier, dont le but de reconstituer le mot de passe d'un compte bancaire en ligne, pour l'envoyer ensuite à un tiers.

Face à ces nouvelles attaques, la protection peut être apportée par un système de prévention permettant une garantie en amont, mais aussi un système de répression générant cette fois-ci une garantie en aval.

En matière de système de prévention apportant une garantie en amont, les entreprises et les particuliers doivent suivre des règles de sécurité très strictes. Les entreprises doivent cloisonner leur système informatique afin d'éviter le vol de données personnelles. Les particuliers, quant à eux, doivent respecter les consignes de sécurité élémentaires en configurant de façon ad-hoc, à l'aide de logiciels de type anti-virus et pare-feux, leurs systèmes informatiques personnels.

Quant aux fournisseurs d'accès Internet (FAI) ou aux fournisseurs d'hébergement, ils doivent respecter le régime de responsabilité de la Loi pour la Confiance dans l'Economie Numérique du 21 juin 2004¹, et doivent, notamment depuis le décret du 24 mars 2006², conserver certaines données de connexion de leurs clients.

En matière de système de répression apportant une garantie en aval, différentes organisations sont présentes au sein de la Police, de la Gendarmerie Nationale et des autorités judiciaires.

Le développement de l'Internet contribue à faciliter les infractions portant atteinte à la personne, et la rapidité avec laquelle le réseau Internet s'est développé rend difficile le travail des officiers de police judiciaire et des experts judiciaires mandatés par les magistrats.

La Gendarmerie Nationale surveille Internet depuis la fin des années 90 et dispose, entre autres, de plus de 120 personnels « NTECH » spécifiquement formés aux techniques d'enquête propres aux infractions liées à cette criminalité. Le département IRGCN de Rosny-sous-Bois apporte un soutien technique aux différents services de recherche de la Gendarmerie.

Les juridictions peuvent par ailleurs faire appel à environ 300 experts judiciaires en informatique répartis sur toute la France, certains d'entre eux regroupés au sein de compagnies telles que la CNEJITA (Compagnie Nationale des Experts Judiciaires en Informatique et Techniques Avancées) ou bien de la CEESD (Compagnie Européenne des Experts Judiciaires en Techniques Avancées des Systèmes Digitaux).

Ces différentes organisations doivent respecter des techniques d'investigation éprouvées et exemptes de toute critique : à l'aide d'outils logiciels intégrés permettant d'accélérer les temps de traitements et de recherche, les investigateurs doivent respecter un certain nombre de règles très strictes, notamment afin de garantir la conservation de l'intégrité de la preuve numérique qui est exploitée.

¹ Loi n°2004-575 du 21 juin 2004

² J.O n° 73 du 26 mars 2006 page 4609

Par ailleurs, la qualité de la preuve numérique collectée au cours de l'investigation reste essentielle. Comment qualifier la force probante d'une preuve numérique extraite d'un système informatique ? Quelle est la nouvelle réglementation pénale en matière de consultation de sites à caractère pédo-pornographique ? Comment replacer la preuve collectée dans le contexte juridique pénal ? Quelles sont les recommandations à effectuer aux différents services de police et de gendarmerie dans le cadre d'une perquisition, dont la finalité est la saisie de matériel informatique ?

La notion d'atteinte aux personnes regroupe à la fois les atteintes à la vie privée, à l'honneur, à la dignité, mais aussi les atteintes aux mineurs.

Des opérations de police de grande ampleur sont régulièrement entreprises à l'encontre des personnes utilisant Internet pour échanger des images pornographiques mettant en scène des mineurs. La presse se fait également l'écho de cas d'atteintes sexuelles commises sur des mineurs contactés par leurs agresseurs sur le réseau.

La pédo-pornographie sur Internet inquiète à cause du relatif anonymat qui est ménagé sur le réseau, ainsi que la facilité avec laquelle les techniques numériques permettent la reproduction et la diffusion à vaste échelle de tous types de contenus (textes, images, vidéos...).

En France, le cadre juridique relatif à la pédo-pornographie sur Internet paraît relativement complet. D'autant plus que la récente loi du 5 mars 2007³ vient de modifier le Code pénal pour ajouter une nouvelle incrimination concernant la consultation de sites dont le contenu est à caractère pédo-pornographique.

L'ensemble de l'Europe met en œuvre une législation commune permettant de lutter contre la cybercriminalité, et en particulier contre la production, la diffusion et même la détention d'images pédo-pornographiques.

La cybercriminalité, qui est finalement le type de crime le plus « international », pose donc de nouveaux défis à la justice pénale qui se fonde historiquement sur le concept de contrôle territorial, ainsi qu'à la coopération internationale. A ce sujet, un traité international, la Convention sur la cybercriminalité de Conseil de l'Europe, a été signé en 2001 par 42 Etats, dont la France. Elle devrait aider les différents Etats signataires à relever ces défis.

Quelles sont les carences en matière pénale au niveau international ? Est-ce que ces éventuelles carences peuvent expliquer à elles seules l'accroissement et la diffusion de la pédo-pornographie sur Internet ?

³ LOI n° 2007-293 du 5 mars 2007 réformant la protection de l'enfance

<p style="text-align: center;"><u>PARTIE I : LES TECHNIQUES DE SECURISATION ET D'INVESTIGATION</u></p>

Internet a besoin d'être régulé suite au développement de nouvelles formes de criminalité portant atteinte à la personne.

Diverses techniques sont actuellement mises en place :

- des mesures de prévention constituant une protection en amont (Chapitre 1) : protection contre le vol d'informations personnelles confidentielles, obligations des fournisseurs Internet et fournisseurs d'hébergement ;
- des mesures de répression constituant une protection en aval (Chapitre 2) : techniques d'enquêtes judiciaires et d'investigation.

CHAPITRE PREMIER : LES METHODES DE SECURISATION

Section première : la protection contre la captation d'informations personnelles confidentielles

Avec l'expansion des nouvelles technologies, les infractions contre les équipements informatiques sont en hausse. Les entreprises et leurs clients sont la cible privilégiée des attaques informatiques. Les atteintes aux personnes constituent une part très importante des cas de cybercriminalité : ces attaques regroupent le vol de fichiers clients et de données personnelles, le vol de codes confidentiels des clients ou bien tout simplement la discréditation d'un dirigeant en phase de négociation d'un gros contrat.

Nous allons tout d'abord dresser un panorama des différentes attaques connues sur Internet, concernant spécifiquement l'atteinte aux personnes.

Puis nous tenterons d'expliquer les différentes parades permettant de lutter efficacement contre ces attaques, à la fois en terme d'architecture technique mais aussi à l'aide des outils juridiques.

Paragraphe premier : panorama des différentes attaques connues concernant l'atteinte aux personnes

Un panorama des actes de cybercriminalité en 2005 et 2006 qui est extrait du CLUSIF, résume les différentes méthodes de vols de données personnelles avec les risques d'usurpation d'état civil. Les informations obtenues frauduleusement peuvent être effectuées par les techniques d'intrusions sur les systèmes informatiques, les failles de sécurité des systèmes des entreprises ou des ordinateurs personnels des usagers, le vol d'équipement (portables), et même par les personnes elles-mêmes.

Nous allons détailler quelques unes des attaques les plus connues :

- Les chevaux de Troie avec comme exemple le « renifleur de clavier »⁴: le « renifleur de clavier » permettant en particulier de récupérer les mots de passe constitue une atteinte aux données personnelles par le vol d'identité des internautes. Le programme est installé sur l'ordinateur de l'utilisateur à son insu, et va enregistrer toutes les frappes au clavier. Il va collecter l'ensemble des informations saisies, les noms d'utilisateur et les mots de passe, puis va les envoyer au délinquant en vue d'une utilisation frauduleuse. Les organismes financiers victimes de ces attaques ont réagi

⁴ Appelé aussi « keylogger » en anglais

en mettant en œuvre le système de clavier virtuel pour la saisie du mot de passe d'accès au compte bancaire en ligne.

- La technique de « l'hameçonnage »⁵: permet d'obtenir de la part d'une personne des informations confidentielles. Le but est d'usurper l'identité d'une banque, de fournisseurs de services ou de sites marchands. La technique de « l'hameçonnage »⁶ se déroule en deux temps :
 - le délinquant va mettre en place un « site miroir » qui est la réplique exacte (ou extrêmement semblable) du site officiel, et plus particulièrement d'une page du site permettant d'accéder aux informations personnelles (nom d'utilisateur, mot de passe, numéro de compte bancaire, de carte bancaire, ...);
 - le délinquant va ensuite envoyer des e-mails en nombre important de façon à toucher le plus d'utilisateurs possibles. Dans cet e-mail, il demandera à l'utilisateur de se rendre sur le site afin d'y saisir un certain nombre d'informations, prétextant une mise à jour de son compte. Le lien HTML présent dans l'e-mail ne dirigera pas en fait l'utilisateur vers le site officiel mais vers le faux site du délinquant.

- La technique du « *pharming* » : cette technique d'attaque est une variante de la technique précédente. L'utilisateur reçoit un e-mail infecté par un virus qui, une fois installé à son insu, va modifier la résolution du cache DNS⁷ de l'utilisateur en modifiant artificiellement l'adresse IP associée à un site (site bancaire de l'utilisateur par exemple) par l'adresse IP du site frauduleux. L'insertion d'une adresse IP frauduleuse peut même être effectuée directement sur le serveur DNS du fournisseur Internet. Ainsi, lorsque la victime se connectera sur le site de sa banque, par exemple en insérant dans son navigateur la bonne adresse Internet, il sera en fait dirigé sur le site frauduleux, d'apparence identique au vrai site. Cette technique est très difficile à détecter par les utilisateurs car contrairement à la technique de « l'hameçonnage », l'adresse Internet affichée sur le navigateur de l'utilisateur est valide.

- Les recrutements de « mules » : il s'agit de recrutement de particuliers afin de récupérer en cash des fonds illégalement acquis par « hameçonnage » ou « renifleur de clavier ». Le délinquant va donc employer un internaute qui servira d'intermédiaire pour transférer des fonds en contrepartie d'une commission sur les fonds transférés. Cette technique d'attaque est effectuée en deux temps :
 - La première phase est la campagne de recrutement. Le délinquant envoie un mail en se faisant passer pour une société souhaitant développer son activité en France et proposant à l'internaute de travailler à son domicile quelques heures par semaines pour une rémunération intéressante
 - Si l'internaute « mord à l'hameçon », il entre alors dans une démarche d'embauche avec la signature d'un contrat de travail et l'envoi des ses coordonnées bancaires afin que les fonds puissent transiter par son compte

⁵ Connu aussi sous le terme de « phishing »

⁶ Le terme « phishing » est un mélange entre le phreaking, qui consiste à détourner les systèmes téléphoniques et le fishing désignant la pêche à la ligne.

⁷ DNS : Domain Name Resolution. Il s'agit d'un système permettant d'établir une correspondance entre une adresse IP et un nom de domaine Internet

-
- Le courriel non sollicité⁸, avec comme exemple les manipulations de cours de bourse⁹. Cette technique d'escroquerie financière repose sur le courriel non sollicité. Elle consiste pour le délinquant à investir en bourse, sur des titres de petites sociétés qu'il va acheter à bas prix. Puis le délinquant va envoyer des courriels contenant de fausses bonnes nouvelles concernant les sociétés en question. Une fois que les cours des actions ont grimpé suite à l'achat massif par les utilisateurs destinataires des courriels, le délinquant vend ses titres au plus haut et la victime se voit spoliée d'une partie de son investissement une fois que l'action a repris son cours normal.

Paragraphe deuxième : l'utilisation d'architectures techniques sécurisées contre les atteintes aux personnes

Comment se prémunir des attaques cybercriminelles ? Comment techniquement les entreprises doivent elles faire face aux menaces d'Internet afin de protéger leur clients ou leur salariés ? Comment l'utilisateur d'Internet peut il lutter pour écarter les tentatives de vols de ses données personnelles ?

La technique de protection d'un système informatique pourrait se résumer à organiser des périmètres de sécurité. La sécurité d'un système doit être pensée à plusieurs niveaux : l'entrée du réseau de l'entreprise, les serveurs de l'entreprise, et les ordinateurs des utilisateurs finaux.

Un des premiers éléments à mettre en place lors de la conception d'une architecture sécurisée d'une entreprise est d'installer des machines de « bastion ». Ces machines vont servir de rempart aux attaques venant d'Internet. Toutes les ressources sensibles (comme par exemple les bases de données hébergeant les coordonnées bancaires des clients d'un site de e-commerce) devront donc se situer derrière cette zone de « bastion » constituée du routeur d'accès au réseau et d'un pare-feu permettant de filtrer les flux Internet venant de l'extérieur.

Ce « bastion » appelée DMZ¹⁰ constituera en fait une zone jouant le rôle de tampon entre le réseau interne considéré comme de confiance et le réseau externe Internet, et contiendra tous les serveurs qui doivent être accessibles par l'Internet (serveur de mail, serveur Web, serveur FTP¹¹). Le pare-feu de la DMZ sera donc configuré pour autoriser uniquement les flux entrant vers la DMZ et interdire tout flux initié de l'Internet directement vers la zone interne à l'entreprise, et tout flux initié de la DMZ vers la zone interne à l'entreprise. Les flux initiés de la zone interne seront par contre autorisés vers Internet et vers la DMZ. La DMZ permet donc d'isoler les machines publiques (serveur de mail par exemple), des machines du réseau interne à l'entreprise.

Le second élément mis en place dans la DMZ est le serveur « proxy ». Le pare-feu joue le rôle de filtre au niveau du protocole TCP/IP, alors que le serveur « proxy » assure la protection du réseau au niveau applicatif. Cet élément va jouer le rôle de relais entre l'utilisateur de

⁸ Connu aussi sous le terme de « spam »

⁹ « Pump and Dump » en anglais

¹⁰ DMZ : DeMilitarized Zone (ou Zone Délimitarisée)

¹¹ File Transfer Protocol

l'entreprise et les serveurs sollicités. Lorsqu'un utilisateur de l'entreprise souhaite par exemple se connecter à Internet, il va tout d'abord se connecter au serveur « *proxy* » de l'entreprise. Le serveur « *proxy* » va ensuite relayer la requête vers l'extérieur pour assurer la connexion vers le serveur demandé. Il permet aussi de gérer l'authentification des utilisateurs internes qui souhaitent accéder à l'extérieur, ainsi que les fonctions de cache Web, mais aussi par son rôle de relais de filtrer les URL et de contrôler les requêtes sortantes suivant la politique de l'entreprise (accès à certains sites interdits notamment).

Enfin, le troisième élément que l'on trouvera dans la DMZ est le serveur « *reverse proxy* ». Il joue le rôle inverse du serveur « *proxy* » en établissant un relais entre l'utilisateur externe qui souhaite accéder à un serveur de l'entreprise qui ne se trouve pas alors directement exposé. Ce type d'élément est mis en place en général lorsque l'entreprise souhaite gérer un système d'authentification vers un des ses serveurs Web, vis-à-vis de l'Internet (exemple : un serveur de messagerie accessible par authentification de l'extérieur pour ses employés sera protégé par un serveur « *reverse proxy* »).

Le particulier devra quant à lui se prémunir des attaques extérieures en respectant les règles suivantes : installer sur son ordinateur personnel un « kit de sécurité » composé d'un anti-virus, d'un pare-feu et d'un détecteur de logiciels espions. Il devra aussi mettre à jour régulièrement son système d'exploitation.

Paragraphe troisième : les moyens techniques de protection des données contre les atteintes aux personnes

La protection des systèmes informatiques ne doit pas constituer le seul élément d'une politique de sécurité afin de lutter contre les attaques cybercriminelles. Il est impératif de protéger aussi l'information elle-même.

La sécurité de l'information repose sur 3 principes fondamentaux :

- la confidentialité des données : les informations ne seront accessibles que pour les personnes qui sont autorisées ;
- l'intégrité des données : les informations personnelles ne doivent pas être modifiées, lors d'un transfert par le réseau par exemple ;
- la disponibilité : le système doit répondre aux sollicitations des utilisateurs autorisés dans un délai imparti.

La confidentialité des données est assurée par une technique de chiffrement qui consiste à transformer une donnée initialement compréhensible par l'individu en une donnée incompréhensible. Cette technique utilise un algorithme dit à clé symétrique. Une clé qui va être distribuée aux deux acteurs de l'échange va permettre de chiffrer le message pour le premier acteur et de déchiffrer le message pour le second acteur. La contrainte de ce type de procédé est la distribution de la clé qui servira au chiffrement et déchiffrement pour chacun des acteurs concernés.

Pour cela, les techniques de chiffrement sont en général mixées avec les technologies à clés publiques utilisant des algorithmes asymétriques. La clé de chiffrement va être chiffrée avec la clé publique du destinataire du message chiffré, puis envoyée avec le message. Seul le destinataire du message qui possède sa clé privée pourra déchiffrer la clé de déchiffrement, et donc déchiffrer le message.

L'intégrité des informations consiste à vérifier que les données n'ont pas été modifiées de façon frauduleuse, à un moment donné. Le calcul d'intégrité est assuré par un algorithme dit de « *hashage* ». Cet algorithme va calculer une empreinte numérique de la donnée et cette empreinte aura une taille fixe. Toute modification ultérieure des données modifierait la valeur de cette empreinte. Ainsi, afin de vérifier si des données sont bien intègres dans le temps, il suffit alors de calculer régulièrement l'empreinte de la donnée et de la comparer avec l'empreinte qui aura été calculée initialement.

Enfin la disponibilité consiste à se prémunir contre les pannes, comme celle d'un disque dur par exemple. Les techniques utilisées dans les entreprises sont les techniques de type RAID¹². Cette technologie permet de répartir les données de l'entreprise sur plusieurs disques durs installés en « batterie » (d'un point de vue logique, le système d'exploitation ne voit qu'un seul disque dur), et d'apporter une tolérance aux pannes.

Section deuxième : les obligations des FAI et hébergeurs et les techniques de protection juridiques

Paragraphe premier : les obligations imposées par la LCEN et les procédures de signalement

Nous allons dans ce paragraphe rappeler le régime de responsabilité imposé par la LCEN (Loi pour la Confiance dans l'Economie Numérique) du 21 juin 2004¹³, auquel sont soumis les FAI¹⁴ et les hébergeurs de contenus.

Les FAI ne sont pas soumis à une obligation générale de surveillance des données qui circulent par leur infrastructure technique. De même les hébergeurs ne sont pas non plus soumis à une obligation générale de surveillance des données qu'ils stockent sur leurs serveurs.

En effet, la loi LCEN (Loi pour la Confiance dans l'Economie Numérique) du 21 juin 2004 dispose dans son article 6-I-7 : « *Les personnes mentionnées aux 1 et 2 ne sont pas soumises à une obligation générale de surveiller les informations qu'elles transmettent ou stockent, ni à une obligation générale de rechercher des faits ou des circonstances révélant des activités illicites* ».

Toutefois les FAI et hébergeurs sont tenus de signaler tout comportement illicite comme le précise la LCEN dans l'article 6-I-7 : « *Elles ont également l'obligation, d'une part, d'informer*

¹² RAID : Redundant Array of Inexpensive Disks

¹³ Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

¹⁴ Fournisseurs d'Accès Internet

promptement les autorités publiques compétentes de toutes activités illicites mentionnées à l'alinéa précédent qui leur seraient signalées et qu'exerceraient les destinataires de leurs services, et, d'autre part, de rendre public les moyens qu'elles consacrent à la lutte contre ces activités illicites ».

De plus, les fournisseurs d'accès et d'hébergement ont obligation de se soumettre aux décisions de justice destinées à faire cesser ou prévenir un dommage. C'est ainsi que la LCEN énonce dans son article 6-I-8 : « *L'autorité judiciaire peut prescrire en référé ou sur requête, aux fournisseurs d'hébergement ou, à défaut, aux fournisseurs d'accès, toutes mesures propres à prévenir un dommage ou à faire cesser un dommage occasionné par le contenu d'un service de communication au public en ligne* ». Ainsi, si une action à l'égard du fournisseur d'hébergement est impossible car le site illicite est hébergé dans un pays hors d'atteinte de la justice française, il sera demandé aux fournisseurs d'accès de prendre toutes mesure propre à faire cesser le dommage.

La responsabilité civile et pénale pour les personnes physiques ou morales prestataires d'hébergement n'est pas engagée « *si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible* » (article 6-I-3 de la LCEN).

De plus, cette connaissance est présumée si le fournisseur d'hébergement a reçu une information détaillée portant à sa connaissance le caractère illicite du site : date de notification, nom, prénoms, profession, domicile, nationalité, lieu de naissance du notifiant, la description du fait litigieux et les motifs pour lesquels le contenu doit être retiré.

Concernant la responsabilité civile et pénale du FAI, l'article 9 de la LCEN prévoit un nouvel article 32-3-3 dans le Code des Postes et des Communications Electroniques qui indique qu'il n'est pas en principe responsable du contenu sauf s'il est « *à l'origine de la transmission litigieuse* » ou s'il « *sélectionne ou modifie les contenus faisant l'objet de la transmission* ».

Les FAI et les hébergeurs sont ainsi soumis à des obligations mais avec un régime de responsabilité atténuée.

Cependant, pour les infractions les plus graves portant atteinte aux personnes telles que la pédo-pornographie ou bien l'incitation à la haine raciale et l'apologie de crimes, les FAI et hébergeurs doivent rester très vigilants et mettre en place des dispositifs de lutte contre ces infractions.

Les FAI et hébergeurs doivent mettre en place « *un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données* » contenues dans des sites présentant en particulier des images à caractère pornographique de mineurs, et ceci afin de concourir notamment à la lutte contre les infractions visées à l'article 227-23 du Code pénal.

Ils doivent également informer les autorités publiques compétentes de l'existence de ces sites et rendre publics les moyens qu'ils consacrent la lutte contre ces sites.

Si ces obligations n'étaient pas satisfaites, le FAI ou hébergeur serait puni de 1 an d'emprisonnement et 75 000 € d'amende.

Malgré ce régime de responsabilité atténuée imposé par la LCEN, comment les FAI doivent ils réguler le réseau Internet vis-à-vis des contenus attentatoires aux personnes ?

Cette régulation doit s'effectuer de leur propre initiative, dès lors qu'ils sont avertis de l'existence d'un site illicite. Pour cela, ils cesseront de fournir l'accès aux sites dont le caractère illicite leur est connu. Ils ont obligation de mettre en place des procédés de signalement et de rendre public tous les moyens consacrés à la lutte contre ces activités illicites.

La LCEN impose un dispositif « *facilement accessible et visible* ». Les dispositifs mis en place doivent donc être accessibles par tout internaute et doivent être simples d'utilisation, telle qu'une adresse Internet permettant l'ouverture d'un formulaire web de signalement.

Afin de lutter contre la pornographie enfantine, plusieurs fournisseurs d'accès se sont associés dès 1998 pour créer l'AFA¹⁵ (Association des Fournisseurs d'Accès). Une chartre permettant de lutter contre les contenus illicites sur Internet a été signée le 14 juin 2004 et l'adresse « www.pointdecontact.net » permet au public le signalement de tout contenu illicite au travers d'un formulaire. Si le site est hébergé en France, l'AFA avertira les autorités de police.

Par ailleurs, chaque fournisseur d'accès Internet propose une adresse email de signalement qui commence en général par « abuse ». Le FAI Free propose par exemple à l'internaute de renseigner et renvoyer un formulaire dès lors qu'un contenu illicite est présent sur Internet.

Dans le cas d'une tentative d'intrusion sur l'ordinateur personnel d'un utilisateur, il sera par contre nécessaire de récupérer l'adresse IP intrusive affichée par exemple par le pare-feu installé sur la machine, puis de consulter la base « Whois »¹⁶ (par exemple ripe.net) afin de connaître le propriétaire du groupe d'adresses IP correspondant, et enfin transmettre au fournisseur d'accès Internet ces informations, en indiquant faire l'objet d'une tentative d'intrusion à telle ou telle date.

¹⁵ <http://www.afa-france.com/>

¹⁶ Le site www.ripe.net contient par exemple l'accès à une base « Whois »

Paragraphe deuxième : la conservation des informations de connexion

Concernant la conservation des données des utilisateurs, les FAI, hébergeurs ainsi que les opérateurs de téléphonie fixes et mobiles, doivent respecter certaines obligations très strictes permettant l'identification des personnes.

Un premier décret d'application du 24 mars 2006¹⁷, pris en application de la loi du 23 janvier 2006¹⁸, détermine pour les opérateurs de communications électroniques les données à conserver pour les besoins des constatations pénales :

- les informations permettant d'identifier l'utilisateur (toutes les données fournies par exemple lors de l'abonnement) ;
- les données relatives aux équipements terminaux de communication utilisés (cela concernera surtout les opérateurs de téléphonie, dans les faits) ;
- les caractéristiques techniques (adresses IP) ainsi que la date, l'horaire et la durée de chaque communication ;
- les données relatives aux services complémentaires demandés ou utilisés, et leurs fournisseurs ;
- les données permettant d'identifier le ou les destinataires de la communication (mail, numéro de téléphone, etc.) ;
- s'y ajoutent, pour les activités de téléphonie, les données permettant d'identifier l'origine et la localisation de la communication.

Par ailleurs, la conservation de ces données est fixée pour une durée de 1 an à compter de l'enregistrement de la communication.

Dans la lignée du décret d'application du 24 mars 2006 et afin d'apporter des précisions complémentaires sur les données que doivent conserver FAI et hébergeurs, un projet de décret portant application à l'article 6 de la loi LCEN du 21 juin 2004 concernant principalement les logs de connexion Internet est en cours. Ce décret vient préciser en effet la nature des données à conserver par les FAI et hébergeurs, en vue de les délivrer si besoin à la police judiciaire sur simple demande.

La teneur des données devant être conservée selon la qualité du prestataire technique est la suivante :

¹⁷ J.O n° 73 du 26 mars 2006

¹⁸ Loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers

-
- les FAI devront par exemple se souvenir de l'identifiant de la connexion, l'identifiant attribué par le système d'information à l'abonné, les dates et heures de début et de fin de la connexion, les caractéristiques de la ligne de l'abonné ;

 - pour les hébergeurs (blog, hébergement de photos, hébergement de vidéo, de musique, etc.) ce devoir de mémoire annuel concernera l'identifiant de la connexion à l'origine de la communication, celui attribué par le système d'information au contenu et à la connexion, le type de protocole ou de réseau utilisé, la nature de l'opération, les dates et heures de l'opération et les pseudonymes utilisés.

La conservation de ces données devra s'effectuer dans des conditions garantissant la confidentialité et l'intégrité des données et permettre une extraction dans un bref délai pour répondre à une demande des autorités judiciaires.

L'association « IRIS »¹⁹ (Imaginons un Réseau Internet Solidaire), qui a pour but d'agir pour le développement de l'Internet, indique au sujet de ce projet de décret :

« Alors que ces données ne sont censées servir qu'à permettre l'identification de quiconque a contribué à la création du contenu d'un service, le projet de décret prévoit la conservation de données qui vont bien au-delà de cet objectif, par exemple le mot de passe fourni lors de la souscription d'un contrat d'abonnement ou lors de la création d'un compte auprès du prestataire Internet ».

Ce projet de décret nous semble effectivement inquiétant pour le respect des libertés individuelles comme le souligne Maître Gérard HAAS : *« En définitive, ce projet de décret constitue une véritable dissuasion au développement du numérique en France ».*

Cependant, ces informations sont, selon nous, essentielles dans le cadre d'une procédure pénale, dont le but est de rechercher toute preuve numérique concernant le contenu illicite d'un site Internet, ou bien la présence d'un mail diffamatoire encore présent sur le serveur d'un fournisseur de service de messagerie.

En effet, dans le cadre d'une telle procédure, l'expert en informatique mandaté par le Magistrat Instructeur, devra s'introduire, par tout moyen si la mission ordonnée par le juge le demande, sur le compte de messagerie distante du mis en cause afin d'y rechercher les preuves entrant dans le cadre du dossier. Or, sans la possibilité d'avoir recours au mot de passe de l'individu, ou bien aux informations associées (phrase clé permettant de se souvenir du mot de passe), il sera en général impossible pour l'expert d'accéder au compte du mis en cause, ce dernier prétendant la plupart du temps lors de l'interrogatoire « ne plus se souvenir de son mot de passe ».

¹⁹ <http://www.iris.sgdg.org/>

Paragraphe troisième : l'indemnisation des prestataires techniques

L'article R.213-1 du Code de procédure pénale prévoit un système d'indemnisation pour couvrir les frais de stockage des prestataires techniques. L'arrêté pris en application de l'article R.213-1²⁰ n'a été publié que le 22 août 2006 et contient une grille tarifaire correspondant à la fourniture de données des opérateurs de téléphonie fixe et mobile.

En 2004, le gouvernement a souhaité demander aux opérateurs téléphoniques de revoir à la baisse leurs tarifs lorsqu'ils doivent intervenir sur leurs lignes suite à une réquisition judiciaire ordonnée par un juge d'instruction.

Ces interventions peuvent aller de l'écoute téléphonique à l'identification d'un abonné à partir de son numéro de téléphone ou de son numéro de carte SIM, en passant par la fourniture de factures détaillées ou la localisation d'un individu grâce à son téléphone GSM.

L'enveloppe « téléphonie » des frais de justice représentait 70 millions d'euros en 2004 et 92 millions d'euros en 2005, contre 35 millions en 2002. Tous opérateurs confondus, la facture représentait 32% de l'augmentation des frais de justice en 2004. Il était en effet d'usage courant pour les opérateurs téléphoniques de pratiquer des tarifs « fantaisistes ». Une interception téléphonique correspondant à un appel coûtait à la justice entre 200 et 400 euros, alors que la surveillance d'un seul numéro pendant un mois pouvait aller jusqu'à 1500 euros. Concernant la localisation d'un individu, la facture pouvait atteindre 30 000 euros selon la durée de l'intervention.

En conclusion, les opérateurs téléphoniques avaient l'habitude de facturer à la carte.

L'arrêté du 22 août 2006 vient préciser, à l'aide de deux grilles tarifaires regroupant environ 40 prestations différentes, les tarifs à appliquer par les opérateurs de téléphonie suite à une demande d'information lors d'une réquisition judiciaire.

A titre d'exemple, l'identification d'un abonné à partir de son numéro d'appel ou de sa carte SIM est facturée par l'opérateur 6,50 euros. Le détail des trafics d'un abonné (avec date, heure et durée) sur une période de 1 mois est facturé 17,50 euros. Le détail géolocalisé des trafics d'un abonné sur une période de 1 mois accompagné de l'adresse du relais téléphonique est désormais facturé 35 euros.

Pourtant, l'arrêté, bien que très précis au sujet des demandes d'informations concernant des données issues de la téléphonie, l'est beaucoup moins au sujet des données issues de l'Internet. Quel est le tarif que doit appliquer un FAI suite à la demande d'identification d'un abonné Internet à partir d'une adresse IP ? L'arrêté du 22 août 2006 précise le point suivant : « *Pour les prestations ne figurant pas dans les tableaux annexés, le montant de remboursement prévu au I est déterminé sur devis* ».

²⁰ J.O n° 202 du 1 septembre 2006 page 13010

Quels sont alors les tarifs pratiqués par les FAI pour une demande d'information correspondant à une adresse IP ? Il semble que certains opérateurs tendent justement à tarifier les réquisitions judiciaires au prix fort.

Selon un article du site Zataz²¹: « *pour une simple identification d'adresse IP, une demande d'information liée à une Adresse Internet (IP) coûte, en France, 12 euros chez Club-Internet ; 17 euros chez Noos ; 20 euros chez Free ; 40 euros chez Wanadoo ; 55 euros chez Tiscali. Seul 9Telecom propose un forfait. D'abord 69 euros, puis 2 euros par I.P* ».

En outre, « *Chaque requête formulée auprès d'un fournisseur d'accès, interlocuteur incontournable de l'enquêteur, doit faire l'objet d'une autorisation cas par cas de la part d'un magistrat. Cette particularité est un frein certain à un type d'enquête dont la progression ne se conçoit que par voie de réquisition* », indique Eric Filiol et Philippe Richard²².

Ces tarifs aléatoires peuvent nous amener à poser la question des tarifs pratiqués dans une affaire de pédophilie qui fait intervenir plusieurs protagonistes et pour laquelle les forces de police auraient besoin d'identifier plusieurs centaines d'adresse IP.

²¹ www.zataz.com article du 2/01/06

²² E. Filiol et P.Richard sont les auteurs de l'ouvrage « Cybercriminalité - Enquête sur les mafias qui envahissent le Web » - Dunod – (p.167)

CHAPITRE SECOND : LES METHODES D'INVESTIGATION

Section première : les services d'enquête judiciaire et les techniques d'investigation

Paragraphe premier : les services d'enquête judiciaire

Les différents services d'enquête spécialisés sont décomposés de la façon suivante:

L'OCLCTIC (Office Centrale de Lutte contre la Cybercriminalité liée aux Technologies de l'Information et de la Communication). Cet organisme a été créé par le décret n°2000-405 du 15 mai 2000, et il s'agit d'un organisme interministériel créé au sein de la direction centrale de la police judiciaire et qui a pour mission principale de coordonner l'ensemble des actions de la police et de la gendarmerie en matière de lutte contre la cybercriminalité.

Cet organisme est dirigé par un commissaire divisionnaire, qui est assisté d'un adjoint, commissaire principal. L'office est composé de quatre groupes d'enquêtes, d'un groupe de soutien et d'une cellule de coordination. L'effectif est de quarante personnes affectées dans ces différentes entités, composé de 25 OPJ (Officiers de Police Judiciaire), soit des policiers et trois gendarmes.

Il intervient dans le cadre d'affaires concernant les atteintes aux systèmes automatisés de données, les fraudes aux télécommunications et les fraudes aux cartes de paiement et bancaires, et apporte son soutien technique aux enquêteurs responsables des perquisitions informatiques. Il est le correspondant des unités opérationnelles pour la mise au clair de fichiers cryptés comme le précise l'article 230-1 du Code de procédure pénale qui déclare : *« 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 ».*

Il est par ailleurs le point de contact en France pour la coopération policière internationale avec EUROPOL, INTERPOL et le G8, et, à ce titre, il gère les signalements effectués en ligne sur le site « www.internet-mineurs.gouv.fr » (site de protection des mineurs pour lutter contre la pédophilie dans le cadre notamment des hébergements de pages Internet à caractère illicite).

L'IRCGN (Institut de Recherche Criminelle de la Gendarmerie Nationale). Cet organisme dépend du Ministère de la Défense et dispose d'un département informatique (INL) qui a été créé en 1992, et dirigé par Eric Freyssinet, et dont la mission principale est de développer des

logiciels permettant de détecter automatiquement des images pédophiles connues, de rechercher et collecter des preuves numériques au cours d'expertises judiciaires afin de les rendre accessibles aux enquêteurs et aux magistrats. L'INL dispose d'environ 20 ingénieurs et techniciens spécialisés et est regroupée en 3 unités d'expertises :

- l'unité de traitement de l'information, où sont effectuées les analyses ou la réparation de tous types de supports informatiques (disques durs d'ordinateurs principalement). Une fois récupérées, exploitées et traitées, les données constituant des preuves numériques sont mises à disposition des magistrats ou des enquêteurs. La pédopornographie représente 60% à 80% des affaires de cette unité ;
- l'unité d'expertise électronique qui se charge de la récupération de données sur tout type d'objets électroniques : téléphones mobiles (téléphone GSM et sa mémoire, et cartes SIM), cartes bancaires, carte de décodage de télévision cryptée, agendas électroniques (assistants personnels de type PDA) ;
- l'unité d'expertise des réseaux informatiques et de télécommunication chargée de procéder à l'analyse des serveurs compromis et l'analyse poussée des traces Internet.

Le SJTRJD (Service Juridique et Technique de Recherche Judiciaire et de Documentation). Cet organisme dispose d'un département de lutte contre la cybercriminalité qui a été créé en 1998. Ce département est composé de 9 cybergendarmes qui ont pour mission de traquer les cybercriminels en assurant une surveillance continue de l'Internet en recherchant les infractions portant atteinte aux personnes et aux biens, et relative à la transmission de données à caractère illicite sur Internet : surveillance des sites, des forums de discussion, des « chats » et des réseaux d'échanges communautaires (« pair à pair »). Selon la complexité de l'affaire, ce département peut faire appel à l'IRGCN ou bien aux 120 enquêteurs spécialisés dénommés « N-TECH » (nouvelles technologies) affectés dans les unités de recherche. Les principales infractions traitées par ce service sont la diffusion sur l'Internet des recettes d'explosifs, le racolage, le trafic de stupéfiants et la pédocriminalité.

Le CNAIP (Centre National d'Images Péro-pornographiques). Cet organisme a été créé en 2003 au sein du STRJD et a la charge de collecter et de classer dans une base de données toutes les images (à ce jour plus de 470 000) et vidéos saisies au cours des enquêtes judiciaires, afin d'identifier les victimes de pornographie infantile. Afin d'accroître son efficacité en matière de lutte contre la pédo-pornographie, une division cybercriminalité a d'ailleurs été créée en 2005, composée du département de lutte contre la cybercriminalité existant et du Centre National d'Analyse d'Images Péro-pornographiques (CNAIP).

La BEFTI (Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information). Cette brigade a été créée en 1994 et dépend de la Direction de la PJ de la Préfecture de police de Paris. Sa mission, limitée à Paris et aux trois départements constituant la petite couronne, consiste à lutter contre les atteintes aux systèmes de traitement automatisés d'informations et la contrefaçon de logiciels ou de matériels, ainsi qu'à fournir une assistance technique aux autres services de police confrontés à la cybercriminalité.

La DGDDI (Direction Générale des Douanes et des Droits Indirects) et la DGCCRF (Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes). Ces deux directions ont mis en place une « cellule de recueil et d'analyse Internet » afin d'assurer une veille sur l'Internet, d'analyser les risques et rechercher les fraudes dans leurs domaines respectifs.

La DNRAPB (Division Nationale de Répression des Atteintes aux Personnes et aux Biens). Cet organisme prend en charge depuis 1997 le traitement des atteintes aux mineurs victimes et des infractions à la loi sur la presse liées au cyberspace.

Au niveau de la chaîne territoriale, les organismes sont les suivants :

Les BT (Brigades Territoriales) et BR (Brigades de Recherches). Les enquêteurs des brigades territoriales qui sont généralistes, bénéficient du concours des enquêteurs spécialisés (N-TECH) des unités de recherches (BR). Les N-TECH prennent en charge l'aspect technique des investigations judiciaires.

Les BDRIJ (Brigades Départementales de Renseignement et d'Investigations Judiciaires). Ces Brigades constituent le pôle criminalistique départemental de la Gendarmerie Nationale. Elles concentrent des effectifs de techniciens en criminalistique (techniciens en investigations criminelles et « N-TECH »).

Les juridictions peuvent par ailleurs faire appel à environ 300 experts judiciaires en informatique répartis sur toute la France, certains d'entre eux regroupés au sein de compagnies telles que la CNEJITA (Compagnie Nationale des Experts Judiciaires en Informatique et Techniques Avancées) ou bien de la CEESD (Compagnie Européenne des Experts Judiciaires en Techniques Avancées des Systèmes Digitaux).

Au niveau des Cours d'Appel, une liste d'experts judiciaires est constituée chaque année. Parmi eux, certains sont spécialisés en informatique et permettent de par leurs connaissances pointues de ce domaine, d'aider le Parquet ou les cabinets d'Instruction dans le cas d'affaires liées à la délinquance informatique.

Paragraphe deuxième : les techniques d'investigation

Quelque soit le type d'affaire, les investigations sur un support informatique répondent toujours à la même problématique : la preuve numérique à analyser (disque dur, clé USB, cartes mémoires par exemple) ne doit pas être modifiée pendant les opérations techniques.

L'enjeu est d'importance car les parties peuvent s'estimer avoir été lésées par la non conservation de l'intégrité de la preuve, ou bien le mis en cause pour lequel des photos illicites seraient retrouvées dans son ordinateur pourrait contester l'investigation technique si un seul bit de la preuve numérique a été modifiée.

La modification peut être involontaire : il suffit par exemple de démarrer un ordinateur dans l'environnement d'exploitation Windows, pour que de nombreux fichiers systèmes (date de dernière modification ou bien fichiers d'évènements) soient modifiés : il s'agit du « syndrome de la lecture destructive » dans le jargon informaticien.

Il convient donc, lors d'une investigation technique, dont le but est la recherche de preuves numériques à charge ou à décharge pour la personne mise en cause, de respecter une méthodologie d'analyse très rigoureuse, afin d'éviter toute contestation ultérieure.

Avant toute manipulation sur le support informatique (un disque dur par exemple), l'enquêteur doit procéder à un calcul d'empreinte numérique sur l'intégralité des données du support. Cette empreinte du support est calculée à l'aide d'un algorithme mathématique dit algorithme de « *hash* »²³. Toute modification de l'intégrité du support analysé entraînerait une modification de la valeur de cette empreinte.

Il faut s'interdire tout démarrage du support à analyser sur son système d'exploitation ou bien sur un autre système d'exploitation sans une protection en écriture du support informatique. Comme indiqué précédemment, cette négligence entraînerait des modifications non maîtrisables sur certains fichiers, en particulier sur les dates de modification, et serait dommageable si l'investigation technique doit reconstituer « l'emploi du temps informatique » du mis en cause.

Il est ensuite nécessaire dans un second temps d'effectuer une copie intégrale du support (appelée aussi copie « bit à bit ») en utilisant un dispositif de protection en écriture. Cette copie de tous les octets du disque dur permettra de récupérer les données présentes sur le support, mais aussi l'ensemble des données qui auraient été supprimés : en effet lorsque des données illicites sont effacées par le délinquant, les données ne sont pas supprimées physiquement mais c'est seulement le « lien » vers ces données qui est supprimé. Les données persistent donc dans la mémoire du support et il est donc alors possible de retrouver les fichiers effacés par une analyse des en-têtes des différents fichiers connus (fichiers document, fichiers image etc.).

Enfin, un calcul d'empreinte numérique sera effectué sur la copie réalisée, mais aussi à nouveau sur le support informatique une fois les manipulations terminées. La comparaison des 3 empreintes (empreinte initiale du support, empreinte de la copie du support, et empreinte finale du support) permettra alors de s'assurer des points suivants :

- les manipulations techniques, et entre autre la copie réalisée sur le support, n'ont pas modifié l'intégrité du support : la preuve numérique doit impérativement ne pas être altérée par les opérations d'investigation ;
- cette valeur d'empreinte, peut être vérifiée, lors d'une investigation ultérieure en cas de contre-expertise par exemple : cette analyse s'effectuera alors avec exactement les mêmes données que celle effectuée initialement ;
- la copie réalisée, et donc l'exploitation des données, prend bien en compte l'intégralité des octets du support ;

²³ Des exemples d'algorithmes de hash sont : SHA1 – Secure Hash Algorithm ou MD5 – Message Digest

Par ailleurs, l'enquêteur ne travaillera ensuite que sur la copie réalisée de manière à ne plus manipuler la preuve originale.

Les éléments à analyser au cours d'une investigation numérique seront différents en fonction de la nature du support à analyser et, bien entendu, de la nature de l'affaire.

Nous étudierons dans l'exposé ci-dessous le cas d'un disque dur d'ordinateur et d'un téléphone portable.

S'il s'agit d'un support informatique tel qu'un disque dur d'ordinateur, l'enquêteur pourra effectuer les analyses suivantes suivant la nature des preuves numériques qu'il doit rechercher :

- l'interprétation des traces de navigation Internet stockées sur le disque dur de l'ordinateur pour lesquelles il est possible de retrouver les différentes adresses de sites Internet et fichiers consultés par un utilisateur, ainsi que les dates associées à ces consultations. L'ensemble de ces éléments stocké dans le « cache Internet », a été téléchargé au moment de la consultation des sites Internet et sauvegardé sur le disque dur de l'utilisateur dans un répertoire spécifique du système. Cette méthode de sauvegarde dans un « cache » permet d'accélérer les temps de consultations, lors d'accès ultérieurs à ces mêmes sites ;
- l'interprétation des fichiers d'évènements de logiciels d'échange « pair à pair », pour lesquels il est possible de connaître les noms de fichiers téléchargés et les dates de téléchargement ;
- l'analyse des fichiers mails et des fichiers d'historique des conversations de messagerie instantanée ;
- la reconstruction du système de fichiers dans le cas de la recherche de preuves sur un support informatique qui a été formaté par le mis en cause ;
- la récupération des fichiers effacés par le mis en cause et la reconstruction des fichiers à l'aide de leur signature de début et de fin de fichiers, à partir de la zone de mémoire non allouée du support numérique analysé.

S'il s'agit d'un téléphone portable, l'analyse s'effectuera sur les trois types d'éléments suivants :

- La mémoire de la carte SIM ;
- La mémoire du téléphone portable ;
- Les fichiers mémorisés par l'opérateur téléphonique (numéros appelants et numéros appelés avec dates associées, et messagerie vocale).

L'exploitation de la carte SIM s'effectuera en utilisant un lecteur de carte à puce et un logiciel de lecture. Cette opération permettra entre autre de récupérer l'ensemble de l'annuaire téléphonique, mais aussi les « mini-messages » (SMS) encore présents et supprimés.

L'exploitation de la mémoire du téléphone s'effectuera en démarrant le téléphone sur une carte SIM de test et en utilisant un logiciel spécifique de lecture des informations du téléphone (« mini-messages », photos, vidéos).

L'exploitation des fichiers présents chez l'opérateur téléphonique s'effectuera à l'aide d'une requête au Service des Obligations Légales de l'opérateur en question, afin de pouvoir consulter à distance la messagerie vocale, et afin d'obtenir le listing des numéros appelants et appelés sur une période intéressant l'enquête.

Paragraphe troisième : le matériel d'investigation, de prévention et d'aide à l'enquête

Au cours de l'analyse d'un support informatique, les manipulations sur celui ci sont réalisées avec un risque important et non maîtrisé d'altération des données. Or il est impératif lors d'une enquête judiciaire, de préserver l'intégrité du support mis sous scellé, de façon à prouver que les investigations n'ont pas modifié, de façon accidentelle, les preuves recherchées sur le support et permettant d'éviter donc toute contestation ultérieure.

Il est alors impératif d'utiliser des boîtiers spécifiques appelés « bloqueurs en écriture », sur lesquels seront connectés le disque dur, la carte mémoire, la clé USB ou la carte SIM à analyser, ceci permettant de les verrouiller physiquement contre toute écriture ou effacement involontaire des données numériques.

D'une manière générale, le matériel d'investigation comprend une batterie de logiciels et de lecteurs en tout genre. Les logiciels les plus utilisés sont de véritables « couteaux-suisse » de l'investigation numérique : les logiciels « EnCase » ou « Forensic Toolkit » par exemple, permettent de réaliser une copie intégrale d'un support, mais aussi de réaliser une analyse poussée du support pour en extraire le moindre octet effacé et de reconstruire le fichier associé qui a été supprimé.

Plusieurs utilitaires permettent par ailleurs de « casser » les mots de passe de protection éventuellement positionnés sur certains fichiers dont on a souhaité rendre le contenu inaccessible.

Les enquêteurs de la Gendarmerie Nationale ont, en plus des outils précédents, recours à une série de logiciels d'investigations criminelles, conçus pour la plupart par le département Informatique et Electronique (INL) de l'IRCGN :

« MARINA » : Moyen Automatique de Recherche d'Images Non Autorisées. Ce logiciel créé en 2001 par le Capitaine Laurent Lesobre du département Informatique et Electronique, permet aux enquêteurs d'être assisté dans le cadre d'enquêtes à caractère pédophile, dans le but de matérialiser l'infraction pendant la garde à vue. Ce logiciel permet de rechercher et de

recupérer sur l'ordinateur du délinquant l'ensemble des images ou séquences vidéos à caractère pédophile qui s'y trouverait à l'aide d'une comparaison avec une base de connaissance renfermant plus de 600 000 signatures de fichiers récoltés au cours des différentes enquêtes.

« SIMANALYST » : ce logiciel créé en 1998 par le département ILN de l'IRCGN facilite la lecture du contenu d'une carte SIM de téléphone portable. L'enquêteur doit être en possession d'un lecteur de carte à puce permettant d'y insérer la carte SIM et du code PIN de la carte. Le logiciel après lecture de la carte, permet d'éditer un rapport indiquant les derniers numéros appelés, le répertoire téléphonique, les SMS présents et effacés et la dernière zone géographique où le téléphone était allumé.

« LogIRC » : ce logiciel permet de surveiller les groupes de discussion sur Internet.

« LogP2P » : ce logiciel permet de surveiller les réseaux d'échanges de fichiers « pair à pair ».

« ILOOK » : ce logiciel d'investigation et de recherche de fichiers effacés sur des supports informatiques n'est pas d'origine française, mais développé par le département du trésor américain (dont l'auteur est Elliot Spencer).

Concernant le cas particulier de recherches d'images illicites sur un disque dur, les analyses peuvent prendre plusieurs semaines et selon le Capitaine Duvinage, du département Informatique et Electronique (ILN) de l'IRCGN²⁴ : « *dans les affaires de pédopornographie, il n'est pas rare de trouver des disques durs contenant plus de 50 000 images, qui ne sont pas forcément toutes illégales. Une partie du tri se fait automatiquement mais il peut encore rester quelques 40 000 clichés à visualiser manuellement.* ». Il est en effet parfois très difficile d'effectuer la distinction entre un enfant mineur ou non sur une photo.

En outre, des moyens techniques importants ont été mis en place pour la recherche des délinquants du web liés à la pédo-pornographie, notamment afin d'automatiser les recherches et d'accélérer les temps d'analyse.

Le département de lutte contre la cybercriminalité du SJTRDJ, dont les enquêteurs ont le statut d'officier de police judiciaire, et qui est depuis 2004, un pôle de compétence en matière de pédocriminalité, a la possibilité par exemple de réquisitionner le fournisseur d'accès Internet afin d'obtenir les coordonnées de l'auteur du site illégal. Cette recherche de sites est effectuée notamment par l'utilisation de logiciels combinés à un glossaire constitué de mots-clés récoltés au fil des enquêtes, permettant de repérer facilement les sites illégaux. De plus, la boîte de signalement créée en 2002 « judiciaire@gendarmerie.defense.gouv.fr » permet à tout internaute de signaler les sites qui l'ont choqué.

Le CNAIP (Centre National d'Analyse d'Images Pédo-pornographique) effectue dans un premier temps les recherches d'images illicites sur un disque dur, avec une comparaison automatique à partir d'une base de signatures de fichiers connues à disposition des enquêteurs. La base de données, nommée CALIOPE, sans cesse réactualisée depuis 2003, est une base

²⁴ Gend'Info n°279 – La cybercriminalité, août – septembre 2005

centrale regroupant environ 480 000 photos de pornographie infantile recensées par les services de police et de gendarmerie, avec des informations sur les auteurs et les victimes. Le CNAIP collabore étroitement avec l'international au niveau des échanges de matières et de méthodes : si une photo a caractère pédo-pornographique impliquant un auteur étranger est identifiée, le dossier est transféré vers son pays d'origine.

Cependant, les logiciels d'aide à l'enquête spécifiquement développés pour ce type d'affaires ne sont pas toujours suffisants et la mémoire visuelle de l'enquêteur reste primordiale. Le recoupement des clichés, afin d'établir qu'ils ont été pris au même endroit et donc qu'il s'agit du même pédocriminel, nécessite par exemple une analyse détaillée de l'arrière plan des photos. Cette analyse n'est pas possible avec logiciels de reconnaissance automatique d'images.

Section deuxième : parallèle entre l'investigation technique et la réglementation pénale

Paragraphe premier : la question de la preuve

La preuve se définit comme l'établissement de la réalité d'un fait ou de l'existence d'un acte juridique. Lorsque les moyens sont préalablement déterminés et imposés par la loi, la preuve est dite légale ; dans le cas contraire, elle est dite libre.

La question est de savoir si les éléments de preuves retrouvés sur un disque dur d'ordinateur vont permettre d'emporter la conviction du juge.

En matière civile, la loi du 13 mars 2000²⁵ portant adaptation du droit de la preuve aux technologies de l'information est venue ajouter de nouvelles disposition dans le Code civil qui permettent de préciser la notion de preuve : « *La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission* ».

Autrement dit, toute preuve est admissible indépendamment de son support et le juge ne pourra donc pas rejeter par principe une photo, un email ou un document texte qui aurait été retrouvé dans un support informatique. Les preuves numériques sont donc admissibles, mais elles devront cependant posséder les critères propres à convaincre l'Instance de jugement.

D'autre part, l'article 1316-1 du Code Civil dispose que : « *l'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité* ».

La force probante de la preuve numérique pourra donc être variable : le fichier numérique retrouvé pourra constituer un commencement de preuve dans le cas où l'intégrité de ce fichier est

²⁵ Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information

contestable, ou bien aura une force probante indiscutable dans le cas où l'intégrité du fichier est prouvé, et son auteur est identifié de façon certaine (par exemple identification par sa signature en bas de page ou bien par son adresse IP).

Par exemple, dans une affaire de diffamation, une victime apporte comme preuve au juge l'enregistrement d'une page web sur laquelle se trouve des propos diffamatoires ou injurieux. Cette page pourra constituer un commencement de preuve mais n'aura pas une force probante indiscutable. En effet, il faudra, dans ce cas, tenir compte du fait que la page enregistrée sur le support électronique ou imprimée pourra avoir été préalablement modifiée avec un logiciel de retouche d'image. Son intégrité pourra alors être remise en cause.

Prenons un autre exemple. Dans la même affaire de diffamation, la victime apporte, cette fois ci, comme preuve un fichier mail reçu et diffamatoire, au format électronique. Afin d'apprécier la force probante de la preuve numérique, le plaideur devra apporter la preuve de la preuve, c'est-à-dire la preuve que l'élément de preuve apporté authentifie la personne dont il émane et son intégrité. Il devra donc organiser une sauvegarde du serveur de messagerie dont provient l'email ou bien du serveur où est hébergé le pare-feu qui a conservé le journal des événements. Dans ce cas, l'adresse IP retrouvée dans les fichiers d'évènements sauvegardés pourra authentifier de façon forte l'identité du diffamateur, puisque l'adresse IP représente un numéro identifiant de manière unique l'ordinateur d'un individu.

En matière pénale, tout mode de preuve est recevable car la preuve est libre, l'article 427 alinéa 1 du Code de procédure pénale déclare à ce titre : « *Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction* ». Le juge peut en outre s'appuyer sur les constatations des enquêteurs, sur les indices récoltés au cours de l'instruction, sur les témoignages et sur des éléments de preuves remises par la victime ou bien issus d'une conclusion d'expertise technique. Il est libre de se déterminer en fonction de l'élément de preuve qui lui semble le plus convaincant.

Selon l'article 427 alinéa 2 du Code de procédure pénale : « *le juge ne peut fonder sa décision que sur des preuves qui lui sont apportées au cours des débats et contradictoirement discutées devant lui* », le juge va donc s'appuyer sur un faisceau de preuves dont la décision sera favorable ou non à la victime : le juge n'est pas lié à la preuve mais prend une décision selon son intime conviction.

Cependant, même si le système de l'intime conviction du juge l'emporte en matière pénale, le juge pénal s'intéressera en tout premier lieu à la fiabilité de la force probante de la preuve, et s'appuiera sur l'avis de l'expert pour forger sa conviction, dont la validité des techniques probatoires doit être exempte de toute critique.

Il est donc indispensable afin d'apprécier la force probante de la preuve, et suivant le type d'affaire, de respecter la même logique de la force probante de la preuve numérique, telle que définie en droit civil.

En outre, lors d'une expertise judiciaire par exemple, l'importance de la conservation de l'intégrité d'une preuve numérique trouvée et de l'identité de la personne dont elle émane reste

selon nous primordial, et ces éléments devront ressortir clairement des conclusions de l'expertise, afin d'éclairer au mieux le juge.

Afin d'illustrer ce point, reprenons notre exemple précédent de mail diffamatoire. En règle général, le diffamateur prétendra ne pas être l'auteur du mail envoyé, en prétextant qu'une autre personne a envoyé ce mail à sa place, et ceci en falsifiant son identité. Le juge cherchera alors à connaître la véritable identité de l'émetteur du mail et à savoir si le mail n'a pas été falsifié.

Il conviendra alors :

- de comparer le mail présenté par la victime avec le mail encore présent dans son client de messagerie, et ceci afin d'écarter la thèse éventuelle de falsification. Cette manipulation permet d'attester ou non de l'intégrité du mail diffamatoire présenté par la victime ;
- de récupérer les fichiers d'évènements du serveur de messagerie pour en extraire l'adresse IP correspondant au mail recherché. Une analyse de l'en-tête Internet²⁶ du mail litigieux permettra d'effectuer une correspondance avec l'adresse IP et la date d'émission du mail retrouvées dans les fichiers d'évènements du serveur de messagerie. Cette analyse permettra donc d'identifier l'ordinateur émetteur du mail litigieux.

Paragraphe deuxième : les précautions à prendre lors de la collecte des preuves dans une enquête préliminaire

La preuve technique dans l'environnement numérique est essentielle car elle permet d'appuyer les aveux de l'auteur ou bien de disculper un individu qui serait accusé à tort.

Il est donc impératif de suivre au cours d'un constat d'huissier, d'une perquisition, ou bien d'une expertise judiciaire, une méthodologie précise et rigoureuse, de façon à obtenir la meilleure force probante de la preuve collectée.

²⁶ L'en-tête Internet d'un mail correspond à une partie du mail (le début du mail qui n'est pas visible lors de l'affichage du mail avec le client de messagerie), et qui contient l'ensemble des informations qui caractérisent le cheminement du mail à travers le réseau Internet, pour arriver à destination. Ces informations sont en général encapsulées suivant le protocole standard de transfert de courrier SMTP (Simple Mail Transfer Protocol). Ces informations permettent d'indiquer, le serveur SMTP d'où est parti le mail, l'adresse mail de l'expéditeur qui a envoyé le mail, les différents serveurs relais SMTP par où a transité le mail, et le serveur SMTP final où est arrivé le mail. D'une façon, générale, ces en-têtes apportent des informations sur le cheminement du mail, du point de départ jusqu'au point d'arrivée, avec les dates associées d'envoi et de réception.

Sous paragraphe premier : la collecte des preuves lors d'un constat d'huissier, nos recommandations

Le constat d'huissier est un document rédigé en vue de l'établissement de la réalité d'un fait matériel. Un constat d'huissier peut être réalisé dans le cadre d'une affaire pénale, afin de constater le fait à une date déterminée.

Prenons l'exemple d'une affaire dont le but est de constater à partir d'Internet et avec le concours d'un huissier, qu'un forum diffuse des propos diffamatoire envers un tiers. Le constat de l'huissier de justice a pour but d'apporter la preuve de cet acte, et doit être réalisé dans des conditions techniques propres à en garantir la fiabilité et le caractère probant.

Ainsi, avant un constat nécessitant une connexion à l'Internet, les opérations suivantes devront être effectuées par l'huissier :

- vérifier le paramétrage du navigateur Internet utilisé, afin de désactiver la connexion par serveur « proxy » le cas échéant²⁷ ;
- vider la mémoire cache locale de l'ordinateur utilisé pour la connexion Internet ;
- mentionner dans le procès verbal, l'adresse IP de l'ordinateur ayant servi aux opérations de constat afin de vérifier en cas de litige, grâce au journal de connexion du serveur litigieux interrogé, les pages réellement consultées pendant les opérations de constat.

A défaut, la connexion par le biais du serveur « proxy » rendra le constat d'huissier sans aucune force probante²⁸, puisque le serveur « proxy », par définition, pourra permettre l'accès à des pages Internet qui n'existent pas, ou qui n'existent plus sur le site cible à la date des constatations.

Ces précautions permettront d'être certain de l'origine des pages Internet consultées lors du constat et d'écartier toute possibilité que ces pages Internet aient été fournies par le serveur « proxy » et non par le site litigieux, objet du constat.

²⁷ Un serveur proxy est fourni par un FAI (Wanadoo ou Free), et possède en général une fonctionnalité de mémoire tampon qui permet d'accélérer les temps de consultations. Le serveur « proxy » garde en mémoire les pages Internet déjà consultées, qui seront directement fournies à l'internaute lors de consultations ultérieures des mêmes pages. Il faut pour cela que le serveur « proxy » soit configuré au niveau du navigateur de l'internaute.

²⁸ Voir CA Paris 17 novembre 2006 4^{ème} ch. Net Ultra / AOL France

Sous paragraphe deuxième : la collecte des preuves lors d'une perquisition, nos recommandations

Une perquisition dans l'environnement du numérique a pour but la saisie de matériel informatique, en vue d'une analyse technique ultérieure, de manière à collecter un certain nombre de preuves numériques en rapport avec l'affaire. Une perquisition peut par exemple être ordonnée par un Magistrat du Parquet, si un individu est soupçonné d'avoir diffusé par Internet des images pédo-pornographiques. L'ordinateur de l'individu soupçonné sera saisi à des fins d'analyse de son disque dur.

L'article 56 du Code de procédure pénal dispose en effet :

« Si la nature du crime est telle que la preuve en puisse être acquise par la saisie des papiers, documents, données informatiques ou autres objets en la possession des personnes qui paraissent avoir participé au crime ou détenir des pièces, informations ou objets relatifs aux faits incriminés, l'officier de police judiciaire se transporte sans désemparer au domicile de ces derniers pour y procéder à une perquisition dont il dresse procès-verbal ».

L'ensemble du matériel informatique saisi lors de la perquisition, et en rapport avec l'affaire, doit être placé sous scellé par l'officier de police judiciaire comme le précise l'article 56 alinéa 5 et 6 du Code de procédure pénale :

« 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, il peut être procédé, sur instruction du procureur de la République, 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 ».

Ainsi, une méthode rigoureuse permettant la collecte des preuves lors de la perquisition doit être suivie. Cette méthode conditionnera les résultats obtenus et les preuves numériques résultantes de l'expertise technique du matériel saisi.

Dans la suite de ce paragraphe, nous émettrons diverses recommandations, principalement à destination des officiers de police judiciaire, qui dans le cadre d'une perquisition auront à saisir du matériel informatique. Ces recommandations peuvent entrer par exemple dans le cadre une affaire de fixation et diffusion de contenu à caractère pédo-pornographique.

En début de perquisition et afin d'éviter la perte intentionnelle de données, les intéressés devront se voir interdire toute connexion aux ordinateurs objet de la saisie, l'envoi de mails ou l'utilisation de téléphones pour communiquer. Il est nécessaire de limiter les agissements des intéressés de manière à éviter qu'une tierce personne ne soit prévenue et n'efface par le réseau des preuves numériques intéressant l'enquête.

Une fiche de renseignement du matériel saisi devra être complétée par les officiers de police judiciaire, pendant le déroulement de la perquisition. Cette fiche doit mentionner le type d'ordinateur saisi, sa marque et son modèle. Par ailleurs, la date de début et de fin des opérations

de perquisition doit être renseignée car elle permettra lors de l'expertise de constater que l'ordinateur n'a pas été démarré après la saisie. Des photographies du matériel dans son environnement doivent accompagner la fiche de renseignement. Ces photos permettront à l'expert de comprendre le contexte de l'utilisation du matériel :

- l'ordinateur était-il connecté à un réseau ? Si tel est le cas, il existe peut-être un serveur caché non saisi, et qu'il convient de saisir rapidement ;
- le disque dur saisi seul était-il caché dans un tiroir ou dans un coffre fort ? Si tel est le cas, il contient peut-être des données chiffrées ou dissimulées. Ces informations collectées par les officiers de police judiciaires permettront à l'expert d'être vigilant sur la présence probable d'informations cachées.

Dans le cas d'une saisie de disques durs qui seront extraits de leurs unités centrales par les officiers de police judiciaire, des photos des unités centrales, avec la marque et le modèle, seront effectuées, ainsi que des photos des différents branchements. Ces photos permettront ensuite d'obtenir des renseignements techniques à partir du site Internet du constructeur. Le disque dur saisi qui a été extrait de l'unité centrale, et qui a été mis sous scellé, est-il le disque dur d'origine ? Si tel est le cas, la thèse de la personne soupçonnée qui prétend qu'elle a remplacé le disque dur d'origine par un disque dur d'occasion, et que les fichiers à caractère pédopornographique retrouvés sur son disque dur appartient au précédent utilisateur ne sera pas recevable.

Des photographies des branchements du matériel devront être prises, avant le démontage et la mise sous scellé. Ces photos permettront lors de l'expertise de savoir quels périphériques étaient utilisés avec l'ordinateur (disque USB externe, scanner, graveur de CD/DVD externe).

L'ensemble des sauvegardes (CDROM, disquettes, bandes de sauvegarde) devra être saisi dans leur totalité. La saisie de ces éléments permettra d'être certain de récupérer le maximum de données :

- l'intéressé supprime volontairement par exemple au dernier moment l'ensemble des photos pédopornographiques de son disque dur qui auraient pu l'incriminer. Ces fichiers, supprimés du disque dur, seront peut-être présents sur les supports de sauvegarde ;
- un CDROM contient peut-être des photos illicites alors qu'il est intitulé « Photos de vacances ».

L'ensemble des supports mémoires susceptibles de contenir de l'information numérique sera saisi. Si le disque dur saisi contient des données chiffrées, le mot de passe de déchiffrement peut se trouver sur un autre support, tel qu'une clé USB ou un organisateur personnel.

Les périphériques (imprimantes, scanners, graveurs externes, lecteurs externes, appareils photos) devront aussi être saisis :

-
- certaines imprimantes peuvent contenir de la mémoire (avec un disque dur intégré par exemple), dont l'utilité est de gérer la file d'attente des impressions. Il sera alors possible de retrouver des preuves numériques pendant l'analyse ;
 - le scanner pourra apporter des éléments d'identification sur les preuves papiers recueillies, si par exemple une rayure sur la vitre du scanner est présente et la même trace de rayure est aussi présente sur les impressions papiers ;
 - la saisie des lecteurs externes (par exemple un lecteur de cartes mémoires d'appareil photo) supposera la présence des cartes mémoires associées. Si les cartes mémoires associées ont été oubliées de la saisie, il conviendra de les rechercher dans des endroits où elles ont été cachées (tiroir ou coffre fort) ;
 - la saisie du graveur de CDROM externe pourra être intéressante si la personne soupçonnée prétend qu'il n'est pas à l'origine de la gravure du CDROM saisi contenant des photos illicites, car son graveur ne fonctionne pas. Une vérification de l'état de fonctionnement du graveur pourra alors être effectuée afin d'attester ou non la thèse de l'intéressé.

Les fiches descriptives contenant les comptes d'accès aux messageries distantes devront être recherchées et saisies. La connaissance des comptes d'accès permettra d'éviter la réquisition du fournisseur de messagerie dans le cas où l'analyse des mails sur une messagerie distante s'avère nécessaire.

Les factures d'achat du matériel devront être saisies. Ces éléments permettront d'attester que l'ordinateur était bien en possession de l'intéressé à partir de la date d'achat :

- l'intéressé ne peut pas prétendre ne pas avoir été en possession de son ordinateur à une date clé de l'affaire, postérieure à la date d'achat ;
- l'intéressé ne pourra pas prétendre avoir acheté son ordinateur d'occasion en indiquant que les photos pédo-pornographiques retrouvées sur son disque dur ne lui appartiennent pas.

Les documents suivants devront également être saisis :

- les documents comptables, car ils permettront de vérifier la liste des achats informatiques et de s'assurer que tout le matériel informatique a bien été saisi ;
- les manuels techniques, car ils permettront d'apporter certaines précisions techniques lors de l'expertise : le disque dur est-il bien le disque d'origine ?
- tout autre document spécifique au thème de l'informatique et pouvant intéresser l'affaire devra être saisi. Cette documentation permettra de connaître le niveau

technique de l'intéressé. S'intéresse t-il aux techniques de dissimulation d'informations ou aux techniques de piratage ?

Les logiciels disponibles sur le site de la saisie devront être saisis car ils permettront de savoir quels étaient les logiciels utilisés par l'intéressé. Utilise t-il des logiciels d'effacement sécurisé de disque dur permettant d'effacer toute trace de données, ou bien des logiciels de chiffrement de données ?

Les officiers de police judiciaire devront recueillir auprès de l'intéressé le maximum de données techniques et historiques sur le matériel, car l'ordinateur a une histoire, dans un contexte et sur une certaine durée. Le but est d'éclairer l'expert sur la vie de l'ordinateur qui évolue dans le temps avec des dates importantes, ce n'est pas un objet inerte. En effet, l'expert travaillera sur les saisies fournies par les officiers de police judiciaire mais ne se déplacera pas sur le site pour obtenir ces informations.

Ces informations, seront consignées dans une fiche d'enquête d'environnement, et devront être obtenues en employant les mêmes méthodes que pour un suspect, en impliquant les personnes présentes pour obtenir le maximum d'informations. Après la saisie, ces informations peuvent ne plus être les mêmes, les personnes ont « oubliée » ou bien ont adapté leur discours.

Nous préconisons donc les questions suivantes afin de reconstituer l'historique de l'ordinateur saisi lors d'une perquisition :

- A qui appartient l'ordinateur
- Quels sont les utilisateurs habituels ?
- L'ordinateur a-t-il prêté à quelqu'un ?
- Quelle est sa date d'achat ?
- Y a-t-il eu une panne ? Quelle est la date de la panne ?
- Quelle est la date de réparation ? Quelle est la date de maintenance ?
- Quelle est la date d'installation ou de réinstallation du système ?
- Quelle est la date de dernière utilisation ?

Si un expert judiciaire nommé doit réaliser ultérieurement une expertise technique sur le matériel saisi, les officiers de police judiciaire ne devront pas effectuer après la saisie, une quelconque recherche sur le matériel car les résultats d'expertise seraient alors faussés.

En outre les ordinateurs ne devront pas être démarrés après la perquisition et avant la mise sous scellé. Il y aurait en effet un risque d'effacement involontaire de fichiers et des modifications de l'environnement : les dates de certains fichiers seraient modifiées de façon non contrôlable alors même que l'utilisateur ne se sert pas du clavier. En effet, dans le cas de la reconstitution de « l'emploi du temps informatique » d'un internaute soupçonné de diffusion d'images à caractère pédo-pornographique, il n'y aurait alors plus de garantie sur le reste des fichiers, et ces manipulations mettraient le doute sur l'ensemble des données recueillies lors de l'expertise (exemple : fichiers systèmes permettant de déterminer la date de dernier démarrage et dernier arrêt de l'ordinateur).

Dans ce cas de figure, la Défense pourra alors argumenter que des éléments ont été modifiés sur les preuves collectés, l'intégrité de la preuve n'étant alors plus respectée, le risque sera d'affaiblir sérieusement l'expertise informatique qui suivra.

La saisie devra être finalisée par la constitution de scellés « fermés » : les données du matériel saisi ne devront pas être accessibles. Ainsi l'intégrité des preuves collectées lors de la perquisition sera garantie, et tout éventuel litige sur une modification des données après la saisie pourra être écartée.

La saisie devra ainsi se conclure par la fourniture au Magistrat mandant des éléments suivants :

- le matériel informatique saisi sous scellés fermés ;
- la fiche de renseignement de saisie ;
- la fiche d'enquête d'environnement sur le matériel.

Paragraphe troisième : les difficultés d'établir la preuve lors de l'expertise judiciaire

Lors de l'expertise, l'expert doit s'attacher, en particulier pour les affaires d'atteinte à la personne telles que la diffamation ou la pornographie infantile, à apprécier la fiabilité de la preuve récoltée au moment de l'analyse du support informatique, et ceci afin d'éclairer le juge qui doit forger son opinion par son intime conviction, la preuve au pénal étant libre.

Il s'agit par exemple de retrouver les traces d'une « activité informatique à caractère pédophile », par l'analyse des historiques de consultations Internet, ou bien les téléchargements « pair à pair ». Les octets des zones mémoires contenant les fichiers effacés doivent être analysés de façon à récupérer tout « morceau » de fichier ou de vidéo précédemment détruite.

Si le disque dur de l'ordinateur a été reformaté par l'intéressé, l'expertise doit reconstituer les anciens systèmes de fichiers de manière à récupérer les preuves avant formatage.

Un point de difficulté d'investigation rencontré fréquemment concerne les moyens mis en œuvre par le cybercriminel afin de crypter les données litigieuses ou bien d'en protéger leur accès.

La collecte des preuves numériques sur le système informatique qui est effectuée par l'expert mandaté par le juge, le placera alors à mi chemin entre le « hacker » et le « cracker » : le premier se borne à s'introduire dans un système informatique pour tester ses vulnérabilités, ou même seulement par plaisir. Il s'agit de l'intrusion. Le second, en plus de l'intrusion, va plus loin en commettant piratage et/ou destruction.

L'expert, ira en effet au-delà d'une seule intrusion, avec l'intention de prendre connaissance du contenu des fichiers de l'intéressé dans le système informatique, et d'extraire ceux d'entre eux pouvant constituer des preuves numériques permettant d'éclairer le juge.

Cependant, quelles sont les limites juridiques à ne pas dépasser dans le cadre de ces investigations ? L'expert est-il autorisé dans le cadre d'une enquête pénale, à procéder au décryptage de données numériques renfermant des preuves potentielles ?

L'article 158 du Code de procédure pénale précise : « *La mission des experts qui ne peut avoir pour objet que l'examen de questions d'ordre technique est précisée dans la décision qui ordonne l'expertise* », l'expert a tout pouvoir d'investigation technique, mais doit rester impérativement dans les limites du cadre de sa mission.

La loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne a inséré un article 230-1 dans le Code de procédure pénale qui répond à la question initiale qui était posée sur la licéité de décryptage de données au cours d'une enquête. Cet article prévoit en effet le recours à une personne qualifiée afin d'effectuer les opérations techniques permettant d'obtenir la version en clair des données retrouvées.

L'article 230-1 dispose : « *Sans préjudice des dispositions des articles 60, 77-1 et 156, 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* ».

<p style="text-align: center;"><u>PARTIE II : LES RELATIONS ENTRE LES INVESTIGATIONS TECHNIQUES ET LES ATTEINTES AUX PERSONNES</u></p>

L'essor d'Internet depuis les années 1995 a augmenté de façon significative les possibilités d'atteintes aux personnes.

L'attention des actes cybercriminels aujourd'hui se concentre principalement sur le racisme, les envois de courriels diffamatoires, l'incitation à la haine à partir des forums Internet, l'incitation à la violence, et la diffusion d'images pédo-pornographiques à partir des logiciels d'échanges.

Comment les atteintes à la vie privée, à l'honneur (diffamation et injure), et à la dignité (discrimination raciale) sont réprimées lorsqu'elles sont commises sur un réseau de communication électronique ? (Chapitre 1)

Quel est le cadre légal de l'atteinte aux mineurs dans le cas de la pédophilie ? (Chapitre 2)

Notre étude sera accompagnée d'exemples de jurisprudence et de cas d'expertises judiciaires permettant d'en définir les critères d'appréciation.

CHAPITRE PREMIER : CADRE LEGAL GENERAL DE L'ATTEINTE AUX PERSONNES

Section première : les atteintes à la vie privée par l'image

Paragraphe premier : les caractéristiques pénales de l'infraction

Dans le cas de la publication d'une photographie sans le consentement de l'intéressé, l'article 226-1 du Code pénal dispose que le fait de « *fixer, d'enregistrer ou de transmettre l'image* » d'une personne se trouvant dans un lieu privé, sans son consentement, constitue un délit.

La peine est de 45 000 euros d'amende et d'un an d'emprisonnement.

Les mêmes peines sont prononcées par l'article 226-2 du Code pénal pour « *le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes prévus par l'article 226-1* ».

Paragraphe deuxième : les critères d'appréciation

Récemment la Cour de Cassation, dans un arrêt du 22 mars 2005²⁹, a considéré que la personne qui diffuse sur un site Internet des photographies prises d'une autre personne dans son intimité et sans son consentement est passible de l'infraction prévue par l'article 226-1 du Code pénal.

Section deuxième : les atteintes par la diffamation et l'injure

Paragraphe premier : les caractéristiques pénales de l'infraction

L'infraction principale concernant la diffamation est définie et réprimée non par le Code pénal, mais par la loi du 29 juillet 1881 (« loi sur la liberté de la presse »).

La diffamation est définie à l'article 29 de la loi du 29 juillet 1881 : « *Toute allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel le fait est imputé est une diffamation. La publication directe ou par voie de reproduction de cette allégation ou de cette imputation est punissable, même si elle est faite sous forme dubitative ou si elle vise une personne ou un corps non expressément nommés, mais dont*

²⁹ CA Paris, 11^e ch., 22 mars 2005

l'identification est rendue possible par les termes des discours, cris, menaces, écrits ou imprimés, placards ou affiches incriminés ».

Rappelons par ailleurs que l'allégation se définit comme l'affirmation sur la foi d'autrui, sur la rumeur publique, ou reprise d'écrit ou de propos d'autrui.

Quant à l'injure, elle est également définie à l'article 29 de la loi du 29 juillet 1881 :
« Toute expression outrageante, termes de mépris ou invective qui ne renferme l'imputation d'aucun fait est une injure ».

Afin de caractériser un fait diffamatoire, ou injurieux, il conviendra d'analyser si le propos a fait l'objet ou non de publicité.

En effet prenons l'exemple d'un propos diffamatoire à caractère raciste ou discriminatoire. Si cette diffamation est reconnue comme étant publique, l'article 32 de la loi du 29 juillet 1881 s'appliquera pour l'application de la peine :

« La diffamation commise par les mêmes moyens envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non appartenance à une ethnie, une nation, une race ou une religion déterminée sera punie d'un an d'emprisonnement et de 45000 euros d'amende ou de l'une de ces deux peines seulement ».

Pour le même propos, mais cette fois-ci qualifié de propos injurieux, l'article 33 de la loi du 29 juillet 1881 s'appliquera pour la qualification de la peine :

« Sera punie de six mois d'emprisonnement et de 22500 euros d'amende l'injure commise, dans les conditions prévues à l'alinéa précédent, envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non appartenance à une ethnie, une nation, une race ou une religion déterminée ».

Si cette diffamation n'est pas reconnue comme étant publique, le propos diffamatoire sera alors réprimé par une contravention de diffamation non publique, c'est à dire une contravention de 4^{ième} classe suivant l'article R.624-3 du Code pénal:

« La diffamation non publique commise envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non appartenance, vraie ou supposée, à une ethnie, une nation, une race ou une religion déterminée est punie de l'amende prévue pour les contraventions de la 4e classe.

Est punie de la même peine la diffamation non publique commise envers une personne ou un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou de leur handicap ».

Pour le même propos à caractère raciste ou discriminatoire, mais cette fois ci qualifié de propos injurieux non publique, il s'agira alors d'une contravention de 4^{ième} classe suivant l'article R.624-4 du Code pénal :

« L'injure non publique commise envers une personne ou un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non appartenance, vraie ou supposée, à une ethnie, une nation, une race ou une religion déterminée est punie de l'amende prévue pour les contraventions de la 4e classe.

Est punie de la même peine l'injure non publique commise envers une personne ou un groupe de personnes à raison de leur sexe, de leur orientation sexuelle ou de leur handicap ».

Après avoir défini brièvement ces notions fondamentales, nous nous attacherons au cas de diffamation et injure sur le réseau Internet.

L'article 2 de la loi du 30 septembre 1986³⁰ (modifiée par la LCEN du 21 juin 2004) définit l'Internet comme un moyen de « *communication au public par voie électronique* ». Il dispose notamment :

« On entend par communication au public par voie électronique toute mise à disposition du public ou de catégories de public, par un procédé de communication électronique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère d'une correspondance privée ».

Ainsi toute mise à disposition du public par un site web, d'écrits, d'images ou de messages de toute nature qui n'ont pas le caractère de correspondance privée entrent dans le cadre de la diffamation, si les propos en question satisfont à la définition de l'article 29 de la loi du 29 juillet 1881.

Le cas particulier du courrier électronique peut entrer, ou non, dans cette interprétation et peut donc poser problème pour qualifier correctement l'infraction.

En effet, si le courrier incriminé est considéré par le juge comme étant de la correspondance privée, il n'entrera donc pas dans le cadre d'une diffamation publique : ce cas est celui par exemple d'un courrier diffamatoire envoyé par un individu à un petit groupe de personnes formant une communauté d'intérêt. L'infraction pourra être alors une diffamation non publique et sera réprimée comme contravention de diffamation non publique (art R.624-1 du Code pénal).

Dans le cas des forums sur Internet, le responsable du forum est libre de s'exprimer, mais sa liberté ne lui permet pas de tout dire et de tout écrire.

Il devra donc répondre devant la justice de ce qu'il publie et de ses propos si ceux ci constituent des infractions pénales ou s'ils causent un dommage à autrui. Il peut, également, être tenu pour responsable des commentaires échangés par des tiers sur son propre forum.

Dans le cadre des forums de discussion, il est nécessaire, là encore, de distinguer s'il s'agit de forums privés ou publics. En effet, cette distinction permettra, dans le cadre de propos diffamatoires, de savoir si l'on entre ou pas dans le cas de la loi du 29 juillet 1881 pour la qualification des faits.

Pour les forums publics, les propos éventuellement diffamatoires échangés, entreront dans le cadre de la qualification du fait de diffamation de la loi du 29 juillet 1881. Par contre, dans le

³⁰ Loi n°86-1067 du 30 septembre 1986 - Loi relative à la liberté de communication (Loi Léotard)

cas de forums privés, les propos échangés seront assimilés à de la correspondance privée, de la même façon que le courrier électronique à caractère privé.

Une décision de la Cour d'Appel de Paris du 5 juin 2003³¹ apporte notamment une définition de forum à caractère public dès lors que le filtrage du forum dépend de la seule déclaration des internautes : « *un message diffusé sur un forum de discussion a un caractère public dès lors que tout utilisateur du système de communication Internet est en mesure de se connecter librement sur ce forum, peu important l'utilisation requise d'un compte et d'un mot de passe en vue de participer au forum de discussion* ».

Paragraphe deuxième : les critères d'appréciation

L'infraction de diffamation est appréciée par la jurisprudence selon le critère qui est le suivant : il y a diffamation lorsque l'honneur d'une personne qui peut être identifiée, et qui est précisément nommée ou non, est atteinte publiquement d'une allégation de mauvaise foi.

Le Tribunal Correctionnel d'Arras a condamné récemment deux internautes à la suite de la diffusion sur un forum, de différents messages³².

A la suite des violences urbaines du mois de novembre 2005, des propos agressifs avaient été publiés sur un forum de discussion à la fois par l'auteur dudit forum mais également par divers commentateurs. Ces messages diffamaient, menaçaient de mort et outrageaient le maire de la commune d'Arras, un de ses adjoints, deux policiers et un juge d'instruction.

Dans une autre affaire autour du forum « monputeaux.com », un arrêt du 6 juin 2007 de la Cour d'Appel de Paris³³ a confirmé la décision de relaxe prononcée par le TGI de Paris le 17 mars 2006 à l'encontre du responsable de ce site. Le forum faisait référence à la conclusion par la municipalité d'un marché public pour un prix présenté comme anormalement élevé. Il se faisait l'écho du licenciement d'une employée qui avait dénoncé ce fait. Par ailleurs, il relatait les menaces proférées à l'encontre de ladite employée.

Le Tribunal avait estimé que les menaces n'étaient pas directement imputées à la commune de Puteaux et a écarté sur ce point le délit de diffamation. Il a considéré en revanche que les allégations relatives à la conclusion du marché constituaient un fait imputé à la personne publique portant atteinte à son honneur ou à sa réputation et qu'il s'agissait d'une diffamation au sens de l'article 29 de la loi du 29 juillet 1881.

Il a rejeté l'argument du responsable du forum selon lequel le site n'était pas public en raison du fait qu'il s'adressait à une communauté d'intérêt. En effet, il a retenu que le site concerné était accessible à tous les internautes et ne nécessitait pas d'identification préalable, contrairement à certains forums de discussion.

³¹ CA Paris, 1^{ère} ch., 5 juin 2003

³² Forum Droit sur l'Internet <http://www.foruminternet.org/actualites/lire.phtml?id=1009>

³³ CA Paris 11^e ch., A Arrêt du 06 juin 2007

http://www.legalis.net/jurisprudence-decision.php3?id_article=1936

Ensuite, le Tribunal a constaté que les éléments produits par le responsable du forum ne fournissaient pas la preuve des faits imputés à la commune de Puteaux de façon parfaite.

Enfin, les magistrats ont analysé l'intention de nuire de l'auteur, présumée en matière de diffamation. Pour renverser cette présomption, ils ont étudié les quatre conditions exigées par la jurisprudence, à savoir l'absence d'animosité, l'action dans un but d'information, la prudence dans l'expression des propos et l'obligation de vérifier l'information communiquée : les demandes de la commune de Puteaux seront donc rejetées par le TGI et la Cour d'Appel au motif que le responsable du forum faisait preuve de bonne foi.

Dans un autre exemple, un cas d'expertise judiciaire en correctionnel, une personne était poursuivie de chef de diffamation (articles 23, 29 alinéa1, 32 alinéa1, 42, 43 et 48 6° de la loi du 29 juillet 1881) pour avoir envoyé un mail à dix de ses amis, à propos d'une tierce personne concernant ses orientations sexuelles. Le mail litigieux avait été transféré par l'un des dix amis à la personne concernée par la diffamation.

L'expertise judiciaire informatique avait pour but d'identifier de façon certaine l'émetteur du mail litigieux reçu par la personne diffamée. En effet, le nom et prénom présents dans le champ « émetteur » du mail au format papier fourni au juge par la personne diffamée ne prouvaient rien.

Après s'être procuré le format électronique du mail, une analyse technique a été effectuée sur l'en-tête Internet de ce mail, les adresses IP des différentes machines par lesquelles le mail avait cheminé. Ensuite, une comparaison avec l'adresse IP du présumé diffamateur a pu démontrer de façon certaine que le mail avait bien été envoyé à partir de l'ordinateur du présumé diffamateur.

Lors de son procès, la défense a invoqué le caractère privé de l'échange de courrier qui avait été effectué à destination d'un groupe de personnes ayant des intérêts communs (il s'agissait d'un groupe de travail).

La diffamation a été qualifiée de non publique et l'intéressé a été condamné à une contravention de 4^{ème} classe (article R.624-3 du Code pénal).

Section troisième : les atteintes par la provocation à la haine ou à la violence

Paragraphe premier : les caractéristiques pénales de l'infraction

La loi sur la presse³⁴ réprime plusieurs formes de provocation, si celle-ci se manifeste par l'un des moyens énumérés par l'article 23 de la loi qui dispose :

« Seront punis comme complices d'une action qualifiée crime ou délit ceux qui, soit par des discours, cris ou menaces proférés dans des lieux ou réunions publics, soit par des écrits, imprimés, dessins, gravures, peintures, emblèmes, images ou tout autre support de l'écrit, de la parole ou de l'image vendus ou distribués, mis en vente ou exposés dans des lieux ou réunions publics, soit par des placards ou des affiches exposés au regard du public, soit par tout moyen de communication au public par voie électronique, auront directement provoqué l'auteur ou les auteurs à commettre ladite action, si la provocation a été suivie d'effet ».

C'est l'article 24 alinéa 8 de la loi sur la presse qui réprime la provocation publique (par l'un des moyen de l'article 23) et notamment ceux qui auront provoqué « à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou non-appartenance à une ethnie, nation, une race ou une religion déterminée ».

L'infraction de l'article 24 suppose une provocation publique et condamne à un an d'emprisonnement et 45 000 € d'amende. Si les mêmes faits ne sont pas publics, le Code pénal prévoit une contravention de 5^{ième} classe (article R.625-7 du Code pénal).

La loi du 13 juillet 1990³⁵ a complété la loi sur la presse en rajoutant notamment l'article 24bis qui prévoit de punir « ceux qui auront contesté, par un des moyens énoncés à l'article 23, l'existence d'un ou plusieurs crimes contre l'humanité », et donc notamment l'existence des camps d'extermination et des chambres à gaz où ont péri des millions de personnes.

Paragraphe deuxième : les critères d'appréciation

De nombreuses décisions ont sanctionnés les actes de provocation à la haine raciale à l'aide de l'outil Internet.

En 1999, une personne est condamnée selon les articles 23 et 24 de la loi de la presse, par le Tribunal de Grande Instance de Strasbourg³⁶

Pour avoir « par des messages écrits déposés sur des forums Internet publiquement et directement provoqué à la haine à l'égard des arabes à raison de leur appartenance à une race ».

³⁴ Loi du 29 juillet 1881

³⁵ Dite loi Gayssot - Loi no 90-615 du 13 juillet 1990 tendant à réprimer tout acte raciste, antisémite ou xénophobe

³⁶ TGI Strasbourg, 27 août 1999 <http://www.juriscom.net/jpt/visu.php?ID=296>

En 2000, l'ordonnance du juge Gomez³⁷ ordonne à Yahoo au sujet de la vente d'objets nazis :

« de prendre toutes les mesures de nature à dissuader et à rendre impossible toute consultation sur Yahoo.com du service de ventes aux enchères d'objets nazis et de tout autre site ou service qui constituent une apologie du nazisme ou une contestation des crimes nazis ».

Toujours en 2000, une personne lance des appels au meurtre vis à vis des membres de la communauté juive sur des forums de discussion, en utilisant des pseudonymes. L'auteur a été condamné par le TGI de Paris le 26 mars 2002³⁸ (article 29 du Code pénal) à dix-huit mois de prison avec sursis et trois ans de mise à l'épreuve pour provocation à la discrimination raciale et diffamation publique à l'égard de la communauté juive.

³⁷ TGI Paris, Ordonnance du 22 mai 2000 <http://www.juriscom.net/txt/jurisfr/cti/tgiparis20000522.htm>

³⁸ TGI Paris 17^e ch., 26 mars 2002, Monsieur R. T. c/ MRAP et Monsieur I. C.
<http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=320>

CHAPITRE SECOND : CAS DE L'ATTEINTE AUX MINEURS

Section première: les atteintes par un message à caractère pornographique, pédophile ou violent

Paragraphe premier : les caractéristiques pénales de l'infraction

L'infraction de détention et de diffusion d'un message pornographique, dont le contenu est une image représentant un mineur, est encadrée essentiellement par l'article 227-23, récemment modifié par la loi du 5 mars 2007³⁹.

L'article 227-24 du Code pénal incrimine quant à lui « *le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que ce soit et quel qu'en soit le support un message à caractère violent ou pornographique ou de nature à porter gravement atteinte à la dignité humaine, soit de faire commerce d'un tel message, est puni de trois ans d'emprisonnement et de 75000 euros d'amende lorsque ce message est susceptible d'être vu ou perçu par un mineur* ».

L'objet de cet article n'est pas en effet de sanctionner le commerce de l'immoralité mais la corruption qu'il peut générer sur les personnes mineures.

Ainsi, jusqu'au 5 mars 2007, l'infraction réprimée à l'article 227-23 ne pouvait être constituée qu'au vue des principaux alinéa suivants de l'article :

Alinéa 1 : « *Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75 000 Euros d'amende* ».

Il s'agit dans cet alinéa de la transmission de l'image par Internet au moyen par exemple de logiciels d'échange « pair à pair »⁴⁰, ou bien de leur enregistrement en vue de leur diffusion par ces mêmes logiciels d'échange.

Alinéa 2 : « *Le fait d'offrir, de rendre disponible ou de diffuser une telle image ou représentation, par quelque moyen que ce soit, de l'importer ou de l'exporter, de la faire importer ou de la faire exporter, est puni des mêmes peines* ».

Il s'agit dans cet alinéa de la diffusion de l'image au moyen par exemple d'un support informatique de type CDROM.

Alinéa 5 : « *Le fait de détenir une telle image ou représentation est puni de deux ans d'emprisonnement et 30000 euros d'amende* ».

³⁹ Loi n° 2007-297 du 5 mars 2007 réformant la protection de l'enfance

⁴⁰ Appelé aussi « peer to peer » en anglais

Il s'agit dans cet alinéa de la simple détention de l'image, par l'enregistrement volontaire de l'image par l'utilisateur (provenant d'Internet par exemple), dans un des répertoires de son disque dur, en vue de sa conservation.

En effet, la première condamnation pour détention en France d'images pornographiques de mineurs achetées sur Internet a été prononcée par le Tribunal Correctionnel du Mans, le 16 février 1998⁴¹. L'intéressé avait sciemment constitué un stock de fichiers d'images de nature pornographique et pédophile téléchargées à partir d'Internet, et donc obtenues « *à l'aide du délit d'enregistrement, de transmission et de diffusion, par quelque moyen que ce soit, de l'image d'un mineur présentant un caractère pornographique* ». L'intéressé avait en effet utilisé un ordinateur de son secrétariat connecté à Internet et avait commis l'imprudence de régler ses achats avec sa carte bancaire. Il a été condamné sur le fondement des articles 227-23 et 227-24 du Code pénal.

Prenons maintenant le cas d'un individu qui consulte des sites Internet contenant des images pornographiques représentant des mineurs, sans pour autant enregistrer volontairement dans un répertoire spécifique de son disque dur ces différentes images.

Lors d'une consultation de sites Internet, les fichiers constituant le site sont en général téléchargés et sauvegardés de façon transparente, dans un répertoire système du disque dur appelé répertoire temporaire du cache Internet. Les éventuelles « vignettes » représentant des images contenues dans des pages visualisées du site, seront donc par le même mécanisme, téléchargées dans ce répertoire de cache. Ce mécanisme, souvent méconnu des internautes, permet d'accélérer les temps de traitement lors des accès ultérieurs au même site Internet.

Il est donc intéressant de se demander si la présence d'images pédo-pornographiques dans le répertoire temporaire du cache Internet, suite à la consultation de sites illicites par un individu, constitue une infraction suivant l'article 227-23 du Code pénal. Est-ce que finalement le fait de consulter un site Internet contenant des images pédo-pornographiques est réprimé par cet article 227-23 ?

Avant la récente modification par la loi du 5 mars 2007⁴², la consultation de sites illicites n'était pas prise en compte par l'article 227-23. La modification apportée par cette loi a permis la modification de l'alinéa 5 de l'article 227-23 qui dispose dorénavant : « *le fait de consulter habituellement un service de communication au public en ligne mettant à disposition une telle image ou représentation ou de détenir une telle image ou représentation par quelque moyen que ce soit est puni de deux ans d'emprisonnement et 30000 euros d'amende* ».

Nous allons analyser par un cas de jurisprudence pourquoi l'ajout de cette incrimination par la nouvelle loi était indispensable.

En octobre 2003, un individu s'était connecté, au moyen d'un ordinateur mis à la disposition du public par une commune, à des sites pédophiles pour regarder des images de mineurs à caractère pornographique. A la suite de ces connexions, il a été trouvé trace des sites consultés dans la mémoire temporaire de l'appareil (répertoire du cache Internet). L'individu est

⁴¹ Legalis.net - Tribunal de grande instance du Mans Jugement correctionnel du 16 février 1998

⁴² Loi n° 2007-297 du 5 mars 2007 réformant la protection de l'enfance

alors poursuivi sur le fondement de l'article 227-23 du Code pénal pour détention d'images de mineurs à caractère pornographique.

L'arrêt du 1er avril 2004 de la Cour d'Appel de Lyon⁴³, confirmé par l'arrêt de la Cour de Cassation du 5 janvier 2005⁴⁴, prononce la relaxe de l'intéressé. au motif « *que la détention d'images de mineurs présentant un caractère pornographique n'était pas caractérisée par la simple consultation de sites pédophiles à l'aide d'un ordinateur, la mise en mémoire temporaire des images consultées étant automatique et qu'en définitive le prévenu n'avait fait que laisser une trace de son passage sur les sites pornographiques consultés à l'aide d'un ordinateur ne lui appartenant pas* » et que la loi ne vise pas « *la simple consultation de sites pornographiques mettant en scène des mineurs* ».

Ce cas de jurisprudence semblait donc bien confirmer que la consultation de sites pédo-pornographiques n'apparaissait pas comme un délit. D'après les dispositions de l'article 227-23 du Code pénal à l'époque, les photos exclusivement retrouvées dans le cache Internet ne pouvaient donc pas constituer un délit puisqu'elles ne faisaient pas l'objet d'une intention de les enregistrer, ni de les détenir, de la part de l'internaute, lequel n'était même pas sensé connaître l'existence de cet enregistrement effectué hors de son consentement.

En conclusion, cet arrêt permettait, certes, de protéger la personne qui s'était connectée par accident sur un site à connotation pédophile, mais également certains pédophiles, « visiteurs » d'habitude de sites illicites, qui auraient ou pas eu connaissance de cette décision jurisprudentielle.

C'est pourquoi, l'élargissement de l'incrimination prévue à l'article 227-23 alinéa 5 du Code pénal tendant à sanctionner « *le fait de consulter habituellement un service de communication au public en ligne mettant à disposition une telle image* » a pour but de répondre à la réalité des pratiques des pédophiles et de l'utilisation habituelle qu'ils font des moyens de communication en ligne : ils consultent mais ne détiennent pas forcément les images ou représentations litigieuses.

Cette nouvelle incrimination permet désormais de poursuivre une personne qui consulte un site à caractère pédo-pornographique sans pour autant avoir effectué une impression ou un enregistrement de ces images sur un support, contournant ainsi l'arrêt de la chambre criminelle de la Cour de cassation de 2005 énoncé précédemment, édictant que les traces de la consultation de sites à caractère pédo-pornographique dans la mémoire temporaire d'un ordinateur ne suffisent pas à caractériser l'infraction de détention prévue à l'article 227-23 du Code pénal.

Cette nouvelle infraction vient donc s'ajouter à celle de la détention simple d'une image illicite qui était déjà définie à l'alinéa 5 et qui est punie des mêmes peines, soit 2 ans d'emprisonnement et 300 000 € d'amende.

⁴³ CA Lyon 4ème ch Arrêt du 01 avril 2004 Ministère public / Jean Luc B., http://www.legalis.net/jurisprudence-decision.php3?id_article=1446

⁴⁴ Cass, Ch Crim., 5 janvier 2005, Ministère public / Jean Luc B., http://www.legalis.net/jurisprudence-decision.php3?id_article=1447

Cet amendement a fait l'objet d'une modification lors de sa discussion en première lecture en séance publique devant l'Assemblée nationale. En effet, il a été proposé de préciser que la consultation d'images pédo-pornographique ne peut être incriminée que si elle est habituelle, ceci afin d'exclure de l'incrimination pénale la consultation unique et accidentelle de tels sites. Une question a été posée lors des débats mettant en avant la difficulté tenant à la détermination du critère « d'habitude ». En effet, force est de constater que lorsqu'un internaute se rend dans un cybercafé ou un espace public numérique, il sera difficile de déterminer qu'il a consulté de façon habituelle des sites à caractère pédo-pornographique. Rappelons que selon la définition donnée en droit pénal, il y a habitude dès la commission du second acte délictueux⁴⁵.

Paragraphe deuxième : les critères d'appréciation

La nouvelle incrimination rajoutée à l'alinéa 5 de l'article 227-23 du Code pénal ne permettra cependant pas de simplifier la constatation de l'infraction, une saisie du matériel informatique utilisé étant toujours nécessaire. Par exemple, l'identité des internautes s'étant connectés à des sites à caractère pédo-pornographique, recueillie via la collecte des adresses IP récupérées dans les traces des sites litigieux, ne suffira pas, selon à nous, à caractériser les faits. Cette collecte devra être complétée par plusieurs vérifications nécessaires, qui seront effectuées impérativement sur le matériel de l'internaute.

Ainsi, l'ordinateur d'un individu soupçonné de s'être rendu coupable de tels actes, devra être analysé afin de vérifier plusieurs points sensibles :

- le caractère « habituel » de la consultation devra être démontré. La définition juridique de la notion d'habitude, c'est à dire le côté récurrent ou multi-répétitif de faits homologues est important. Cependant, nous pensons que la périodicité l'est également, si on veut aboutir à une véritable appréciation juridique de tels faits. Il sera donc nécessaire d'établir une analyse entre le nombre d'images retrouvées dans le cache de consultation Internet, les dates de dernier accès de ces images, et la fréquence de consultation des sites à connotation pédo-pornographique, de façon à montrer que l'intéressé s'est connecté plusieurs fois à des périodes différentes sur ce type de sites. Nous pensons ainsi qu'il est important d'aller au-delà de la définition de la notion d' « habitude » afin de caractériser les faits ;
- le caractère volontaire de la consultation de l'intéressé devra être démontré. En effet, certaines pages Internet ou virus reçus par mail peuvent contenir du code malveillant et se connecter à l'insu de l'intéressé sur des sites pédo-pornographiques, alimentant alors le cache Internet. Par exemple, un site licite de pornographie adulte pourra rediriger automatiquement l'internaute, contre sa volonté, sur des sites à caractère pédophile. Il faudra exclure les images retrouvées suite à ce type de consultation involontaire ;

⁴⁵ Cf définition de l'infraction d'habitude – Droit Pénal Général – J.LARGUIER – p.70

- l'identité certaine de l'auteur des consultations devra être démontrée. Une analyse technique devra démontrer que l'ordinateur de l'intéressé n'a pas été l'objet d'un piratage, ou bien que son adresse IP n'a pas été usurpée. Par ailleurs, les consultations dans des cybercafés amèneront des difficultés supplémentaires pour connaître l'identité des auteurs ;
- le nombre d'images retrouvées (pouvant atteindre plusieurs centaines, voire plusieurs milliers), ce qui éclairera le juge sur le profil psychologique de l'intéressé.

Par ailleurs, un autre point difficile à apprécier est celui dont dispose l'alinéa 6 de l'article 227-23 du Code pénal : « *Les dispositions du présent article sont également applicables aux images pornographiques d'une personne dont l'aspect physique est celui d'un mineur, sauf s'il est établi que cette personne était âgée de dix-huit ans au jour de la fixation ou de l'enregistrement de son image* ».

En effet, en pratique, il est difficile d'apprécier le caractère pédo-pornographique des images. De nombreuses images en circulation sur le réseau sont de nature ambiguë. Elles présentent par exemple des protagonistes majeurs de scènes pornographiques comme étant des mineurs. Elles représentent aussi des personnes mineures dans des scènes aux limites de la pornographie. Le juge est donc soumis, dans ces cas de figure, à des difficultés d'appréciation des preuves retrouvées. Cependant, dans de nombreuses affaires, la minorité des personnes ne peut être remise en cause.

Quand à l'article 227-24 du Code pénal, ces dispositions sont mises en œuvre si le contenu du message litigieux peut être vu par des mineurs.

Par exemple, une personne avait envoyé les 5, 6 et 11 avril 2001 plusieurs messages électroniques destinés, selon lui, à un correspondant autre que celui qui les avait effectivement reçus. Ce dernier, constatant que les deux premiers courriers étaient accompagnés de photographies présentant un caractère morbide ou sexuel, et que le troisième fournissait l'adresse d'un site sur lequel pouvaient être consultées des photographies morbides, porta plainte auprès des services de gendarmerie.

Des poursuites furent exercées contre l'auteur des messages sur le fondement de l'article 227-24 du Code pénal. Il fut condamné par le Tribunal Correctionnel pour l'envoi du 3^{ème} message contenant l'adresse du site qui contenait des images à caractère violent.

Le Ministère Public requit la confirmation de ce jugement, estimant que la communication du lien par lequel est possible l'accès à un site comportant des messages violents ou pornographiques « *participe de leur diffusion en permettant la circulation des photographies litigieuses* ». Autrement dit, la diffusion était punissable à cause du lien Internet qui constituait une clé d'exploitation.

La Cour d'Appel reconnaît par contre que l'élément moral de l'infraction n'existe pas car l'intéressé n'avait pas eu l'intention de réaliser les éléments du délit dont il avait à répondre : « *Le courrier électronique est assimilable à une correspondance privée. Il est protégé par un mot de passe personnel et confidentiel qui est composé par l'utilisateur au moment de sa connexion à*

internet ou à sa boîte aux lettres électronique. Son titulaire est le seul à y avoir accès et il est responsable de son utilisation. Ce n'est que par sa volonté ou sa négligence qu'un mineur peut la consulter ».

La Cour de Cassation confirme la décision de la Cour d'Appel : *« dès lors que l'envoi à un tiers majeur d'un message ne contenant que l'adresse d'un site et le lien permettant d'y accéder ne suffit pas à caractériser le délit prévu par l'article 227-24 du Code pénal ».*

Dans une autre affaire récente du 2 juillet 2007 où il est question d'univers virtuel, deux associations familiales portent plainte contre la société américaine Linden Research, éditeur de Second Life, univers virtuel en ligne sur Internet.

Les associations ont saisi le juge des référés du TGI de Paris, afin d'interdire l'accès des mineurs à Second Life, en mettant en cause l'accès possible par des mineurs à des messages à caractère violent ou pornographique. Elles critiquent essentiellement le fait que *« les avatars représentant des enfants peuvent se faire greffer un sexe masculin ou féminin et avoir des relations sexuelles virtuelles avec des prostituées »*⁴⁶.

Le juge des référés a considéré que les associations n'apportaient pas la preuve *« de la réalisation effective d'un trouble grave à caractère manifestement illicite ou d'un risque de dommage imminent pouvant affecter les mineurs, de nature à justifier la prise de mesures immédiates ».*

Section deuxième: les atteintes et agressions sexuelles sur les mineurs par Internet

Paragraphe premier : les caractéristiques pénales de l'infraction

Le viol est réprimé par vingt ans de réclusion criminelle lorsqu'il résulte de l'utilisation du réseau Internet comme le dispose l'alinéa 8 de l'article 222-24 du Code pénal :

« Lorsque la victime a été mise en contact avec l'auteur des faits grâce à l'utilisation, pour la diffusion de messages à destination d'un public non déterminé, d'un réseau de télécommunications ».

La loi du 5 mars 2007⁴⁷ a notamment rajouté un article 227-22-1 dans le Code pénal lorsque le réseau Internet sert à mettre en relation des adultes avec des mineurs, permettant aux premiers d'émettre des propositions de nature sexuelle à destination des seconds :

« Le fait pour un majeur de faire des propositions sexuelles à un mineur de quinze ans ou à une personne se présentant comme telle en utilisant un moyen de communication électronique est puni de deux ans d'emprisonnement et de 30 000 Euros d'amende.

Ces peines sont portées à cinq ans d'emprisonnement et 75 000 Euros d'amende lorsque les propositions ont été suivies d'une rencontre ».

⁴⁶ Nouvel Observateur, Second Life demeurera ouvert aux mineurs, 2 juillet 2007

⁴⁷ Loi n° 2007-297 du 5 mars 2007 réformant la protection de l'enfance

Paragraphe deuxième : les critères d'appréciation

En général, le Code pénal n'incrimine pas les incitations à commettre des viols ou agressions sexuelles qui ne seraient pas suivies d'effet⁴⁸.

Cependant, en octobre 2006, un homme a été condamné à trois ans de prison dont deux avec sursis par le Tribunal de Grande Instance de Saint-Quentin⁴⁹ pour avoir posté sur un forum de discussion un message « *incitant au crime de viol, en réunion, à l'encontre de madame X, alors que cette provocation n'a pas été suivie d'effet* ».

Le prévenu s'était fait passer pour la victime et avait envoyé un message où celle-ci prétendait rechercher un groupe de cinq hommes en précisant « *que cela se passerait chez moi et j'aimerais beaucoup que ça ressemble à un cambriolage qui tourne au viol* ». Ce message comportait également un accès à une photographie de la victime. Cette dernière qui a porté plainte avec constitution de partie civile avait été alertée par le SRPJ (Service Régional de Police Judiciaire) d'Amiens qui opère une surveillance d'Internet, et plus particulièrement de certains groupes de discussion.

L'infraction était notamment réprimée par l'article 222-24 du Code pénal, et nous remarquons que la condamnation a été effective alors que la provocation n'a pas été suivie d'effet.

Section troisième: l'incitation des mineurs à la violence ou au suicide par Internet

Paragraphe premier : les caractéristiques pénales de l'infraction

La provocation au suicide est réprimée par l'article 223-13 du Code pénal qui dispose : « *Le fait de provoquer au suicide d'autrui est puni de trois ans d'emprisonnement et de 45000 euros d'amende lorsque la provocation a été suivie du suicide ou d'une tentative de suicide.*

Les peines sont portées à cinq ans d'emprisonnement et à 75000 euros d'amende lorsque la victime de l'infraction définie à l'alinéa précédent est un mineur de quinze ans ».

⁴⁸ Forum des droits de l'Internet - Recommandation – Les enfants du Net II – Pédopornographie et pédophilie sur l'Internet – janvier 2005 - p.16

⁴⁹ TGI St Quentin, 17 octobre 2006, Ministère public, Chantal X... , Aline Y... / Stéphane H., http://www.legalis.net/jurisprudence-imprimer.php?id_article=1795

Paragraphe deuxième : les critères d'appréciation

L'Internet peut inciter au suicide, c'est le cas notamment des blogs et de la récente affaire des tentatives de suicide à Ajaccio en mai 2007 des deux adolescentes. Dès le début de l'enquête, les blogs des adolescentes sont pointés du doigt concernant leur tentative de suicide. Les enquêteurs avaient d'ailleurs entrevu à partir de l'analyse de leurs blogs un malaise existentiel, mais rien qui n'expliquait le suicide.

Ce n'est pas le cas d'autres exemples de blogs qui donnaient des conseils d'aide au suicide, ou de personnes qui ont orchestré en ligne leur propre mort.

Ces drames relancent la surveillance des plateformes de contenus, telle que « Skyblog », premier hébergeur de blogs en France où la direction a dû mettre en place une équipe pour surveiller en continu plus de 130 millions d'articles et de commentaires

Benoît Desavoye⁵⁰ indique d'ailleurs à ce sujet : « *Comme c'est virtuel, les personnes ne se rendent sans doute pas compte que ce qu'elles écrivent ou lisent dans le cyberspace est vécu par des personnes bien réelles* ».

⁵⁰ Benoît Desavoye est l'auteur de l'ouvrage « Les Blogs », Ed M2 Eds, mars 2005

<p style="text-align: center;"><u>PARTIE III : LES INVESTIGATIONS INTERNATIONALES ET EUROPEENNES</u></p>

L'évolution des technologies de l'information a des conséquences évidentes sur la criminalité organisée « traditionnelle ». Si l'utilisation de systèmes et de réseaux informatiques représente un progrès certain pour la société, elle n'en accroît pas moins sa vulnérabilité puisque l'essentiel des transactions économiques et sociales se fait dorénavant par ce biais. Les groupes terroristes, les réseaux de pornographie ou de pédophilie, les commerces illicites, les trafics d'êtres humains et les délinquants informatiques exploitent cette vulnérabilité et voient leurs activités facilitées et développées par l'expansion de ces nouveaux modes de communication.

La cybercriminalité représente donc une menace nouvelle sans frontière à laquelle tous les pays sont confrontés, obligeant les gouvernements à adapter leurs mesures de lutte.

Pour faire face à ces menaces, des moyens de droit pénal ont été mis en place au niveau du Conseil de l'Europe: un traité international, la Convention sur la cybercriminalité, a été signée le 23 novembre 2001 par 42 Etats, dont les Etats-Unis, le Japon, l'Afrique, le Canada, et la France. Cette convention est entrée en vigueur en France avec l'adoption du décret du 23 mai 2006⁵¹ (Chapitre 1).

En dépit des moyens juridiques mis en place au niveau européen, le caractère international et anonyme du réseau Internet rend difficile l'application de ces lois (Chapitre 2).

⁵¹ Décret n° 2006-580 du 23 mai 2006 portant publication de la Convention sur la cybercriminalité

<p style="text-align: center;">CHAPITRE PREMIER : LES MOYENS MIS EN OEUVRE AU NIVEAU INTERNATIONAL POUR LUTTER CONTRE LA CRIMINALITE INFORMATIQUE</p>
--

Section première: les institutions européennes

Paragraphe premier : l'organisation EUROPOL

EUROPOL, est l'office européen de police créé en 1992. Il s'agit de l'organe en charge de la facilitation des opérations de lutte contre la criminalité au sein de l'Union Européenne.

La Convention portant création de l'office européen de police a été signée et ratifiée par tous les Etats membres de l'Union Européenne et EUROPOL exerce l'ensemble de ses missions depuis le 1er juillet 1999.

Chaque Etat de l'Union Européenne désigne une unité spéciale de police nationale chargée des relations avec EUROPOL et délègue des officiers de liaison qui participent aux travaux d'échange d'information et d'analyse.

EUROPOL, dont le siège est situé à La Haye (Pays-Bas), est composé de 590 personnes dont 90 officiers de liaison.

Les Etats membres de l'Union Européenne ont créé EUROPOL pour accroître la sécurité au sein de l'espace européen. Il facilite l'échange de renseignements entre polices nationales en matière de stupéfiants, de terrorisme, de criminalité internationale et de pédophilie. Il coordonne et centralise des enquêtes à l'encontre d'organisations criminelles de dimension européenne, voire internationale. Il apporte notamment son expertise technique à ces différentes opérations menées au sein de l'Union européenne, sous le contrôle et la responsabilité juridique des Etats membres concernés. Il souhaite plus généralement améliorer l'efficacité des services compétents des Etats membres et intensifier leur coopération dans le cadre de la prévention de la lutte contre les formes graves de criminalité internationale organisée.

EUROPOL a participé notamment à une affaire qui a permis l'interpellation, le 14 juin 2005, de près de 30 personnes dans le cadre d'une vaste opération, lancée en août 2004 à travers 13 pays européens, contre la pornographie infantile sur Internet.

Paragraphe deuxième : l'organisation EUROJUST

Institué en 2002, EUROJUST est l'unité de coopération judiciaire européenne. Il s'agit d'un nouvel organe de l'Union Européenne chargé d'améliorer l'efficacité des autorités judiciaires des États membres dans leur lutte contre les formes graves de criminalité organisée transfrontalière.

EUROJUST stimule et améliore la coordination des enquêtes et des poursuites et il soutient également les États membres pour renforcer l'efficacité de leurs enquêtes et de leurs poursuites.

EUROJUST joue un rôle unique en tant que nouvel organe permanent dans le domaine judiciaire européen. Il a pour mission de promouvoir le développement de la coopération au niveau européen dans les affaires pénales. EUROJUST est dès lors un interlocuteur privilégié pour les institutions européennes telles que le Parlement, le Conseil et la Commission.

Cette organisation apporte son concours dans les enquêtes relatives aux affaires de criminalité organisée, en partie sur la base de l'analyse effectuée par EUROPOL.

Le collège d'EUROJUST se compose de 27 membres nationaux, un membre étant nommé par chacun des États membres de l'Union Européenne. Les membres nationaux sont des juges ou des procureurs expérimentés de haut niveau et certains d'entre eux bénéficient de l'aide d'adjoints et d'assistants.

Paragraphe troisième : le système d'information SCHENGEN

La convention de Schengen, qui a été signée le 14 juin 1985, prévoit la suppression des contrôles d'identité aux frontières entre les pays signataires. Le territoire sans frontières ainsi créé est communément appelé espace Schengen.

Le Système d'Information Schengen est une base de données commune permettant aux autorités de chaque État membre de disposer, grâce à une procédure d'interrogation automatisée, de signalements sur des personnes ou des objets. Plus de dix millions d'individus y sont répertoriés. Il est opérationnel depuis le 26 mars 1995, date de la mise en vigueur de la convention d'application Schengen. Ce système d'information est susceptible d'être employé au profit de la répression de la diffusion et du recel d'images pédopornographiques entre États signataires.

Section deuxième: la convention sur la cybercriminalité du 23 novembre 2001

Le réseau Internet ne permet plus de respecter les prérogatives territoriales des Etats. En outre, l'application de la loi pénale et de la procédure pénale se pose en de nouveaux termes dès lors qu'est concerné l'emploi des nouvelles technologies.

Pour faire face à ces nouveaux enjeux, le comité des ministres du Conseil de l'Europe, le 8 novembre 2001 a adopté une Convention sur la cybercriminalité, ouverte à la signature des Etats membres à Budapest le 23 novembre 2001 à l'occasion de la Conférence internationale sur la cybercriminalité, et entrée en vigueur avec l'adoption du décret du 23 mai 2006⁵².

Paragraphe premier : les différentes catégories d'infraction

Sous paragraphe premier : les infractions contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques

L'article 2 de la Convention porte sur « l'accès illégal » et vise l'infraction consistant à créer une menace ou attenter à la sécurité (confidentialité, intégrité, disponibilité) d'un système ou des données informatiques. Le piratage ou l'intrusion illicite dans un système informatique est donc couvert par cet article. L'article 3 vise l'interception illégale, c'est-à-dire la protection du droit au respect des données transmises. L'article 4 porte sur l'atteinte à l'intégrité des données, c'est-à-dire la protection des données et des programmes informatiques, à l'encontre des dommages occasionnés délibérément. L'article 5 est relatif aux atteintes à l'intégrité des systèmes et vise à pénaliser l'entrave intentionnelle à l'usage légitime des systèmes informatiques. L'article 6, relatif aux dispositifs illégaux, a pour but de prohiber la fabrication, la possession et la diffusion de programmes informatiques - tels que les virus, les vers, les chevaux de Troie ou autres dispositifs - permettant de commettre des infractions pénales, ainsi que le trafic des mots de passe ou des codes d'accès.

Sous paragraphe deuxième : les infractions et les falsifications informatiques

L'article 7 de la Convention vise à combler les lacunes du droit pénal se rapportant à la falsification classique qui requiert la lisibilité visuelle des déclarations contenues dans un document et ne s'appliquent pas aux données enregistrées sur support électronique. L'article 8 vise, quant à lui, les nombreuses fraudes informatiques comme par exemple l'escroquerie à la carte bancaire.

Sous paragraphe troisième : les infractions se rapportant au contenu

L'article 9 porte sur les infractions se rapportant à la pornographie infantile. Il s'agit de renforcer les mesures de protection des enfants, notamment en ce qui concerne l'exploitation sexuelle, en opérant une modernisation du droit pénal, de manière à restreindre plus efficacement

⁵² Décret n° 2006-580 du 23 mai 2006 portant publication de la Convention sur la cybercriminalité

l'usage des systèmes informatiques dans le cadre de la commission d'infractions sexuelles à l'encontre des enfants.

Cet article 9 réprime les faits suivants :

- le fait de produire de la pornographie infantine en vue de la diffuser par le biais des moyens informatiques ;
- d'offrir de la pornographie infantine par le biais d'un moyen informatique ;
- le fait de diffuser ou de transmettre de la pornographie infantine par le biais d'un système informatique ;
- le fait de se procurer ou de procurer à autrui de la pornographie infantine par le biais d'un système informatique ;
- ainsi que la possession de pornographie infantine dans un système informatique ou un moyen de stockage de données informatiques.

L'aspect « matériel » de l'infraction est également prévu par cet article qui est ainsi rédigé :

« Aux fins du paragraphe 1 ci-dessus, la pornographie infantine comprend toute matière pornographique représentant de manière visuelle :

- a- un mineur se livrant à un comportement sexuellement explicite ;*
- b- une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite ;*
- c- des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite ».*

Paragraphe deuxième : l'harmonisation relative aux procédures pénales et l'entraide judiciaire

Les différentes incriminations présentées doivent être accompagnées des outils juridiques pour les mettre en œuvre.

La Convention prévoit dans sa section 2, l'harmonisation des procédures pénales entre les Etats signataires. Cette harmonisation a été effectuée dans le souci de conserver les prérogatives territoriales des Etats en matière de recherche de preuves par la définition de méthodes et pouvoirs d'investigation, tout en conservant le caractère national des services répressifs.

Chaque Etat membre disposera de ses compétences territoriales mais devra cependant mettre les pouvoirs minimaux d'investigation imposés.

La Convention tient compte du caractère volatile de la preuve numérique et elle définit donc les dispositions qui doivent être mises en place selon trois axes principaux :

-
- la conservation rapide de données informatiques stockées et l'injonction de produire : il s'agit de créer une obligation légale pour les opérateurs privés de conserver les données susceptibles de constituer des preuves en matière pénale, notamment en terme de données de connexion pour les fournisseurs d'accès et les hébergeurs de sites web ;
 - la perquisition et saisie de données informatiques stockées : il s'agit de définir les conditions de la perquisitions en milieu informatique, ainsi que le formalisme de leur saisie, notamment en reconnaissant l'existence de la preuve numérique. Cette disposition définit également les conditions de perquisition physique par un agent qui se déplace sur les lieux de l'opération, afin de faire face aux problèmes posés par la perquisition à distance ;
 - la collecte en temps réel de données informatiques : cette disposition traite la question des interceptions de données, notamment en environnement Internet ou de télécommunications.

Concernant l'entraide judiciaire, la Convention indique que les services d'enquêtes des Etats doivent coopérer et communiquer aux Etats demandeurs les résultats des enquêtes. Il pourra de plus être effectué une perquisition et saisie pour le compte d'un autre Etat dans le cadre de la recherche de preuves numériques, sans toutefois mener d'enquêtes transfrontalières. Les informations obtenues devront être communiquées rapidement.

CHAPITRE DEUXIEME : CAS DE CYBERCRIMINALITE ET TRAITEMENTS AU NIVEAU INTERNATIONAL

Section première: le cas des courriels non sollicités

Paragraphe premier : définition générale d'un courriel non sollicité

L'envoi d'un courriel non sollicité⁵³ désigne l'envoi massif de messages commerciaux ou à diffusion générale sous forme de courriels personnalisés. Généralement, l'intérêt pour l'expéditeur est que le destinataire lise son message, et que dans certains cas il finisse par passer commande.

Les émetteurs de ce type de courriels étant très nombreux et très actifs, chaque destinataire reçoit de grandes quantités de courriels non sollicités.

Cette technique d'attaque peut donc provoquer une indisponibilité de la messagerie, par un dépassement de capacité des boîtes de messagerie. De plus, le problème de courriel non sollicité a aussi pour conséquence une perte du temps, puisque des courriels importants noyés dans la masse devront être triés.

Cette technique est aussi utilisée dans le cadre des attaques permettant de propager des virus ou des chevaux de Troie.

Paragraphe deuxième : les difficultés de la lutte contre l'envoi de courriels non sollicités

La lutte contre ce phénomène se heurte à plusieurs difficultés, à la fois techniques mais aussi juridiques.

La première difficulté est l'identification des émetteurs, car les courriels non sollicités sont souvent envoyés à partir d'adresses mails créées à cet effet sous un faux nom, ou à partir d'adresses détournées voire inexistantes.

La deuxième difficulté réside dans les nouvelles formes que prend ce type de messages. Ils ne se limitent plus à des courriels électroniques de prospection commerciale, d'autres types de messages ayant fait leur apparition : messages de propagande politique, appels au don, etc.

Malgré la loi américaine « Can-Spam Act » de 2003⁵⁴ et la LCEN en France tendant à réprimer essentiellement l'envoi de ce courriels non sollicités commerciaux, il n'existe pas de réglementation internationale en matière de lutte contre l'envoi de ce type de message.

⁵³ Appelé aussi « spam »

⁵⁴ Voir le site <http://www.ftc.gov/bcp/online/pubs/buspubs/canspam.shtml>

De plus, il est souvent difficile de faire la différence entre un courriel non sollicité et un courriel légitime, par exemple dans le cas d'une publicité souhaitée ou d'une publicité diffusée dans le contexte de relations commerciales existantes.

Devant l'absence de réglementation internationale, il s'avère donc nécessaire de développer une coopération internationale, qui s'avère insuffisante aujourd'hui.

Les émetteurs ne sont pas toujours du même pays que le destinataire, ce qui nécessite une collaboration des autorités des pays concernés pour identifier, appréhender et poursuivre l'émetteur de ces courriels.

Par ailleurs, cette coopération doit s'accompagner d'une mise en garde du public contre cette pratique, par des campagnes d'information sur les sites Internet des FAI par exemple, mais aussi par une sensibilisation du public qui doit se voir invité à s'équiper de systèmes de filtrage et d'anti-virus, ainsi qu'à suivre les règles élémentaires de prudence.

Section deuxième: le cas de la pédo-pornographie

Paragraphe premier : définition générale de la pédo-pornographie

La possession et la diffusion de textes et illustrations pornographiques mettant en jeu des enfants sont devenues très problématiques aujourd'hui.

Il semble que cette problématique ne soit pas prête de cesser, le nombre de cas augmente, et l'expansion d'Internet, notamment dans les pays de l'Europe de l'Est ne fera qu'accroître le problème.

Par ailleurs l'anonymat d'Internet pourrait encourager l'afflux de groupes relevant de la criminalité organisée et favoriser notamment l'apparition de réseaux pédophiles mieux structurés.

La décision – cadre du Conseil de l'Union Européenne du 22 décembre 2003⁵⁵ relative à la lutte contre l'exploitation sexuelle des enfants et la pédo-pornographie définit la pédo-pornographie comme la représentation visuelle « *d'un enfant réel* », « *une personne réelle qui paraît un enfant* », ou « *des images réalistes d'un enfant qui n'existe pas* » « *participant à un comportement sexuellement explicite ou s'y livrant, y compris l'exhibition lascive des parties génitales ou de la région pubienne* ».

⁵⁵ <http://www.droitsenfant.com/decisioncadreeurope.htm>

Paragraphe deuxième : les difficultés de la lutte contre la pédo-pornographie

La plupart des sites illicites diffusant des contenus pédo-pornographique ne se situent pas en France mais à l'étranger. Ce point est d'ailleurs confirmé par Mme Catherine Chambon, chef de l'OCLCTIC⁵⁶. En 2004, le point de signalement interministériel a permis à l'OCLCTIC de transmettre 800 signalements auprès d'autorités étrangères et seulement 7 signalements auprès de parquets français.

Les sites pédo-pornographiques sont extrêmement mobiles et susceptibles, lorsqu'ils sont identifiés par les services de police et de gendarmerie, de changer très rapidement de serveur d'hébergement et d'adresse.

En effet, les contenus illicites rencontrés sur les sites web ne représentent que la partie visible d'un ensemble plus vaste d'images échangées. L'utilisation des applications et les protocoles propres au réseau Internet est en constante évolution dans le cadre de la diffusion des contenus pédo-pornographiques.

Les applications d'échanges « point à point » (appelés aussi « P2P »), de « discussion relayée par Internet » (appelée aussi « IRC »), les forums de discussion ou l'échange de mails, et l'usage des techniques de chiffrement lors des échanges, constituent aujourd'hui une partie non négligeable de cette diffusion illicite, rendant le contenu difficilement visible.

Il ressort de ces quelques exemples que ce n'est donc pas uniquement dans d'éventuelles carences existantes de la législation des Etats qu'il convient de rechercher les causes de l'accroissement de la diffusion de contenus pédo-pornographiques

⁵⁶ Office Centrale de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication

CONCLUSION

Les technologies de l'information se retrouvent dans la plupart des activités des individus. L'ordinateur, ainsi qu'Internet, est aujourd'hui accessible à n'importe quelle personne, et, de ce fait, le « cyber-délinquant » peut être « n'importe qui ». La cybercriminalité tend ainsi à se généraliser et devient d'autant plus dangereuse.

Les systèmes informatiques et les réseaux deviennent de plus en plus complexes, et sont des outils de travail incontournables pour notre société. Ce même outil, qui est utilisé pour faire transiter des informations commerciales ou administratives, peut aussi être utilisé pour le transfert de contenus illicites, tels que des fichiers pédo-pornographiques.

Le caractère international de l'Internet est incontestablement un des facteurs de propagation de la cybercriminalité aujourd'hui, et nous pensons que cette expansion sera difficilement maîtrisée.

Le caractère décentralisé d'Internet, sans véritable structure de contrôle, ne permet pas de détecter facilement les échanges de contenus illicites. En effet, un fichier contenant une photo pornographique représentant un mineur, peut être envoyé par Internet à des millions d'internautes, via les logiciels d'échange de fichiers « pair à pair ».

De même, une attaque par l'envoi de courriels non sollicités (appelés aussi « *spams* ») qui est perpétrée dans un pays outre atlantique peut toucher des millions de personnes de l'autre côté de la planète. Cette attaque peut même porter atteinte aux données des personnes et capter frauduleusement ces mêmes données lorsque ces courriels sont porteurs de virus ou Chevaux de Troie. L'accès à un contenu illicite peut s'effectuer à partir de quel n'importe pays, et, si le serveur est installé dans un « cyber-paradis », l'hébergeur de contenu sera hors d'atteinte.

Face à ces menaces planétaires, nous pensons donc que la sécurité des systèmes informatiques et des réseaux, et la prévention qui doit en être faite autour des individus, est un défi majeur pour la société de l'information aujourd'hui.

En matière de répression, les investigations informatiques par les services spécialisés sont parfois laborieuses et longues. Le « cyber-délinquant » utilisera tous les moyens pour se rendre anonyme ou bien pour crypter les contenus qu'il diffuse.

Nous pensons que l'expertise judiciaire de matériel informatique saisi va tendre à se complexifier très sérieusement avec ces nouvelles techniques de cryptage introduites maintenant de façon standard sur les nouveaux systèmes d'exploitation tels que Windows Vista ou Mac OS X. Le « cyberdélinquant » pourra alors crypter les données qu'il souhaite, sans aucune connaissance particulière en informatique, et aura « oublier » le mot de passe de cryptage lors de son interrogatoire pendant l'enquête, rendant alors impossible la lecture des données.

Il est donc essentiel de disposer d'un système efficace de droit pénal permettant d'enquêter sur ces nouveaux types de délits et de poursuivre leurs auteurs. Nous pensons à ce sujet que le système pénal français est doté d'un cadre légal suffisamment riche pour pouvoir réprimer la plupart des crimes que l'on peut rencontrer sur Internet. De plus, il évolue

régulièrement pour faire face aux lacunes rencontrées dans les différentes affaires liées à l'Internet. La récente loi du 5 mars 2007⁵⁷ modifiant l'article 227-23 du Code pénal afin de rajouter une incrimination concernant la consultation des sites dont le contenu est à caractère pédo-pornographique en est un exemple.

Au niveau international, les efforts réalisés ces dernières années, et notamment les dispositions prises avec la Convention sur la cybercriminalité du Conseil de l'Europe, doivent être poursuivis. En effet, les systèmes traditionnels de droit pénal se fondent sur l'idée de la souveraineté nationale, et les décisions générées portent sur le territoire national du pays en question. Or Internet est un système universel et les données peuvent transiter d'un pays à l'autre, peu importe les frontières. Il nous paraît donc important que les différents droits des Etats s'harmonisent afin d'améliorer les procédures de coopération.

⁵⁷ Loi n° 2007-297 du 5 mars 2007 réformant la protection de l'enfance

BIBLIOGRAPHIE

Ouvrages :

VERON M., *Droit pénal spécial*, Sirey, 2006

LARGIER J., LARGUIER A.M., *Droit pénal spécial*, Dalloz, 2005

RASSAT M.L., *Droit pénal spécial, Infractions des et contre les particuliers*, Dalloz, 2006

PRADEL J., *Droit pénal général*, Cujas, 2006

LARGUIER J., *Droit pénal général*, Dalloz, 2005

FILIOL E., RICHARD P., *Cybercriminalité: Enquête sur les médias qui envahissent le web*, Dunod, 2006

MIGNARD J.P., *Cybercriminalité*, Dalloz, 2006

FERAL-SCHUHL C., *Cyberdroit – le droit à l'épreuve de l'Internet*, Dalloz, 2006

Conseil de l'Europe, *Criminalité organisée en Europe – la menace de la cybercriminalité*, avril 2006

Articles :

www.zataz.com , *Les cyber-flics, les nouveaux E-Sherlocks*, 2/01/2006

HAAS G., *Conservation des logs : un décret inquiétant pour le respect des libertés individuelles*, Le Journal du net, 22/05/2007

LEVY M., ESKINAZI E., *Les fournisseurs d'accès et d'hébergement face à la cybercriminalité*, La Gazette du Palais n°109 p.33, 19/04/2005

BARBRY E., ROUILLE-MIRZA S., *La responsabilité des acteurs de l'Internet quant à la protection des mineurs*, La Gazette du Palais, 20/04/2006

MAYAUD Y., *L'élément moral du délit de diffusion de messages à caractère violent ou pornographique*, Revue de science criminelle p.642, 2004

JAHAN G., *Personal Data Privacy and Security Act : combattre le détournement des données personnelles sur Internet*, La Gazette du Palais n°293 p.23, 20/10/2005

AMAUDRIC DU CHAFFAUT B., LIMOUZIN-LAMOTHE T., *Une nouvelle forme de criminalité informatique à l'épreuve de la loi : le phishing*, Expertise p.140, avril 2005

PERE D., FOREST D., *L'arsenal répressif du phishing*, Recueil Dalloz p.2666, 2006

BELLOIR P., *L'application des règles de procédure pénale aux infractions commises sur le réseau Internet (1^{ère} partie)*, Expertises p.256-260, juillet 2002

NORMANDEAU A., *Conseil de l'Europe, Criminalité organisée en Europe*, Revue de science criminelle p.207, 2007

FORGERON JF., *Le projet de loi portant approbation de la Convention sur la cybercriminalité*, La Gazette du Palais n°22 p.8, 22/01/2004

BOURRE P., *Internet et la lutte contre la cybercriminalité*, La Gazette du Palais n°23 p.19, 23/01/2003

Rapports :

CLUSIF, Panorama de la cybercriminalité, 2006

Thierry BRETON, Chantier sur la lutte contre la cybercriminalité

Le Forum des droits de l'Internet – Recommandation – Les enfants du Net – II – Pédo-pornographie et pédophilie sur l'Internet, janvier 2005

Journaux :

Revue Experts

Revue Expertises

Revue Gend'Info – La cybercriminalité, août – septembre 2005

Site Internet :

www.legalis.net

www.foruminternet.org

www.legifrance.gouv.fr

www.caprioli-avocats.com

www.ladocumentationfrancaise.fr

<http://conventions.coe.int>

<u>ANNEXES</u>
