Le traitement judiciaire de la cybercriminalité

Guide méthodologique

Mai 2002

Direction des affaires
criminelles et des grâces

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA JUSTICE


WWW


Pén
de

MINISTÈRE DE LA JUSTICE

DIRECTION DES AFFAIRES CRIMINELLES ET DES GRÂCES

13, place Vendôme 75042 Paris Cedex 01

Conception : SICOM - Illustrations : Sophie ZAGURY - Imprimerie TRAIT D'UNION Le Mans - Mai 2002

Le Conseil de sécurité Intérieure du 13 novembre 2000 consacré aux atteintes sexuelles sur mineurs a fixé de nouvelles orientations pour mieux connaître, signaler ces faits et mieux prendre en charge les victimes en assurant une répression plus sévère de ces agissements. Le Gouvernement a par ailleurs dressé un bilan de l'application de la loi du 17 juin 1998, relative à la prévention et à la répression des infractions sexuelles et à la protection des mineurs.

La Chancellerie a été désignée pour piloter un groupe de travail interministériel relatif à la problématique "Internet et pédophilie".

Les atteintes sexuelles à l'égard des mineurs s'appuient de plus en plus souvent sur des réseaux à caractère pédophile ayant recours à l'Internet. Or le développement des nouvelles technologies rend plus complexe le traitement judiciaire des infractions de toute nature, certains faits pouvant être commis hors du territoire national ou s'inscrivant dans un contexte plus large de criminalité organisée ce qui rend parfois difficile l'identification des auteurs.
La réflexion du groupe interministériel s'est étendue ensuite à l'ensemble des atteintes à la dignité humaine.

Le groupe a abouti à l'élaboration du présent document relatif à un domaine appelé à connaître de nombreuses évolutions sur le plan technique, législatif et jurisprudentiel. Ce guide doit donc être appréhendé en tenant compte de ces changements probables.

Les enjeux liés à l'Internet sont multiples : protection des droits fondamentaux et des libertés individuelles, responsabilités des intermédiaires techniques, compétence et loi applicable au regard du droit international.

◗ La protection des droits et des libertés

Certains ont souhaité qu'Internet constitue un espace de liberté totale non soumis au droit. En réalité, le monde virtuel n'est pas un espace de non droit et pour l'essentiel, les lois existantes suffisent à assurer cette protection.
C'est ainsi qu'un message raciste ou révisionniste sera sanctionné qu'il soit diffusé sur l'Internet ou à la radio. Il en va de même s'agissant d'une diffusion diffamatoire ou violant des droits d'auteur.
Internet est également protégé par le droit. C'est ainsi qu'une correspondance échangée par le biais d'un courrier électronique sera, selon la jurisprudence, protégée par le secret, comme une lettre envoyée par la poste.

◗ Responsabilité des intermédiaires techniques

Il faut distinguer les fournisseurs d'hébergement et les fournisseurs d'accès. Les premiers, offrent d'héberger, en général contre rémunération, des pages web sur leurs serveurs. Les seconds sont des sociétés donnant accès à Internet moyennant un abonnement payant ou gratuit.

Transposant partiellement la directive européenne sur le commerce électronique qui pose le principe de l'absence de responsabilité pour les prestataires et intermédiaires assurant le simple transport des informations, la loi du 1er août 2000, modifiant la loi du 30 septembre 1986 sur la liberté de communication, crée pour les fournisseurs d'hébergement un régime spécifique de responsabilité.

Le projet de loi sur la Société de l'information adopté en conseil des ministres le 13 juin 2001 prévoit leur irresponsabilité sous certaines conditions, à raison des contenus qu'ils transmettent.

Ce projet de loi complète la transposition de la directive européenne sur le commerce électronique et celle concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications.

◗ ***Droit international :*** *compétence et loi applicable*

Par nature, l'Internet est un réseau international ; plusieurs législations nationales sont donc susceptibles de s'appliquer. Lorsqu'un litige survient, même relatif à l'Internet, l'impact est localisé géographiquement. Le conflit concerne en premier lieu la compétence : la juridiction française est-elle compétente ? Par exemple, dans certains pays anglo-saxons, les discours d'incitation à la haine raciale sont tolérés au nom de la liberté d'expression et poursuivis en France car attentatoire à la dignité humaine. Le conflit concerne en second lieu la loi applicable : la juridiction doit-elle appliquer la loi française ou une loi étrangère ? Il faut garder à l'esprit qu'une fois réglés les différents conflits de lois, la décision française devra en principe faire l'objet d'une procédure d'exequatur à l'étranger pour recevoir force obligatoire.
Plusieurs questions se posent lorsque l'on évoque le réseau des réseaux :

- *Peux-t-on éviter l'écueil de la plurilocalisation d'Internet en déclarant le droit d'un seul Etat applicable ?*
- *Le risque n'est-il pas réel de voir des prestataires délocaliser leur établissement de manière à échapper à un système pénal trop sévère dans le pays où ils étaient implantés initialement ?*

En facilitant les communications et la diffusion d'informations, Internet favorise la commission d'infractions et apparaît comme le vecteur d'une nouvelle forme de délinquance contre laquelle l'application du droit pénal se heurte à la difficulté d'identifier les auteurs, eu égard à cette dimension internationale.

La protection des transactions sur l'Internet exige de détecter les agissements illicites et de réprimer efficacement leurs auteurs.
L'article 43-9 de la loi du 1er août 2000 oblige les prestataires d'hébergement (de sites ou de contenu)s à détenir ou à conserver "les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont (ils) sont prestataires".
L'article 29 de la loi relative à la sécurité quotidienne *impose une obligation de conservation de données techniques aux opérations de télécommunications dans leurs activités de fournisseurs d'accès à l'Internet, pour les besoins de la recherche et de la poursuite des infractions pénales.*

L'Internet, qui n'est autre qu'un réseau mondial informatique, est utilisé à de multiples fins telles que la recherche d'informations, mais également le courrier électronique, le transfert de fichiers informatiques, la participation à des groupes de discussion, et également à des fins illégales telles que la diffusion de pornographie enfantine.

*• **Les sites Web** ou http (hyper text transfert protocole) auxquels accèdent les internautes en utilisant des moteurs de recherche leur permettent de télécharger des photos via un site contenant par exemple des images de mineurs à caractère pornographique. Cette technique pour diffuser des photographies est de moins en moins utilisée car un site est facilement identifiable contrairement à d'autres services offerts par Internet.*
Cette technique est cependant la seule utilisée lorsque la diffusion de pornographie enfantine a un côté commercial (sites payants soit directement soit par l'utilisation de bandeaux publicitaires parfois mensongers pour attirer le client sur un site payant).

*• **Le courrier électronique** (e-mail) permet de joindre aux messages des fichiers, facilitant ainsi la mise en place de réseaux d'échanges de photographies qui peuvent avoir un caractère pédophile. Un courrier avec fichier attaché peut être envoyé dans des espaces de discussion publique. Il revêtira alors un caractère public.*

*• **Les news groups ou forums de discussion** sont fédérés par thèmes et constituent des réservoirs d'informations sur des sujets variés. A l'intérieur de ces forums circulent des photos et toute personne se connectant sur ces derniers forums de discussion peut télécharger ce type de photographies. Certains sont ouverts à tous, d'autres sont réservés à des membres, selon la configuration déterminée par le gestionnaire du forum.*

*• **L'IRC (Internet Relay Chat)** est un protocole qui permet à plusieurs internautes de communiquer en direct, dans les forums privés. Ce système est le plus utilisé par les pédophiles. Les communications se font en temps réel, tous les utilisateurs connectés à un canal pouvant interréagir simultanément.*

Annexes

I - LES INFRACTIONS POUVANT ÊTRE COMMISES VIA INTERNET

La cybercriminalité correspond à deux catégories d'infractions pénales qui peuvent poser des problèmes identiques dans leur traitement judiciaire, à savoir :

- Les infractions où l'informatique est l'objet même du crime ou du délit.
- Les infractions où l'informatique est le moyen de commission d'un crime ou d'un délit.

A. Les infractions pénales relevant de la criminalité informatique :

1- La loi "informatique et libertés" du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés vise notamment à combattre la création de fichiers nominatifs clandestins et réprime plusieurs infractions portant atteinte aux droits de la personne résultant des fichiers ou des traitements informatiques.

Infractions	Texte	Peine (maximale)
Le fait, "y compris par négligence", de procéder ou de faire procéder à des traitements automatisés d'informations nominatives sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi.	art. 226-16 du Code pénal	• amende de 45 000 € • emprisonnement de 3 ans
Le fait de procéder ou de faire procéder à des traitements automatisés d'informations sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés.	art. 226-17 du Code pénal	• amende de 300 000 € • emprisonnement de 5 ans

Infractions	Texte	Peine (maximale)
Le fait de collecter des données par un moyen frauduleux, déloyal ou illicite, ou de procéder à un traitement d'informations nominatives concernant une personne physique s'y opposant pour des raisons légitimes.	art. 226-18 du Code pénal	• amende de 300 000 € • emprisonnement de 5 ans
Le fait de mettre ou de conserver en mémoire informatisée sans l'accord expresse de l'intéressé des données nominatives qui, directement ou indirectement, font apparaître les origines raciales ou les opinions politiques, philosophiques, religieuses ou les appartenances syndicales ou les mœurs des personnes.	art. 226-19 du Code pénal	• amende de 300 000 € • emprisonnement de 5 ans

2- La loi du 5 janvier 1988 dite "loi Godfrain" vise à assurer la sécurité des systèmes d'information. Au sens de la décision du Conseil de l'Europe du 31 mars 1992, "la sécurité des systèmes d'information est reconnue comme une qualité partout nécessaire dans une société moderne". La récente convention du Conseil de l'Europe sur la cybercriminalité invite à incriminer les comportements portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des données et systèmes informatiques.

Infractions	Texte	Peine (maximale)
Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système.	art. 323-1 du Code pénal art. 323-1 al 2 du Code pénal	• amende de 15 000 € • emprisonnement d' 1 an • amende de 30 000 € • emprisonnement de 2 ans
Le fait d'introduire frauduleusement des données dans un système de traitement informatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient.	art. 323-3 du Code pénal	• amende de 45 000 € • emprisonnement de 3 ans
La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3 du Code pénal.	art. 323-4 du Code pénal	• peine prévue pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée

B. Les infractions pénales "classiques" commises au moyen d'Internet

1 - Les infractions relatives aux atteintes à la dignité humaine

• 1.1 Infractions prévues par le Code pénal

◗ Les atteintes à la personnalité :

Infractions	Texte	Peine (maximale)
• La menace de commettre un crime ou un délit contre les personnes dont la tentative est punissable lorsqu'elle est soit réitérée, soit matérialisée par un écrit, une image ou tout autre objet.	art. 222-17 al 1 du Code pénal	• amende de 7 500 € • emprisonnement de 6 mois
Si menace de mort.	art. 222-17 al 2 du Code pénal	• amende de 45 000 € • emprisonnement de 3 ans
• La menace de commettre un crime ou un délit contre les personnes lorsqu'elle est faite avec ordre de remplir une condition.		
Si menace de mort avec ordre de remplir une condition.	art. 222-18 al 2 du Code pénal	• amende de 75 000 € • emprisonnement de 5 ans
Atteintes à la vie privée, sans le consentement de l'interessé, par colportation, enregistrement ou transmission des paroles prononcées à titre privé ou confidentiel ou en fixant, enregistrant ou transmettant l'image d'une personne se trouvant dans un lieu privé.	art. 226-1 du Code pénal	• amende de 45 000 € • emprisonnement d'1 an

Infractions	Texte	Peine (maximale)
Le fait de solliciter, d'accepter ou d'obtenir, en échange d'une rémunération, des relations de nature sexuelle de la part d'un mineur qui se livre à la prostitution, y compris de façon occasionnelle.	art. 225-12-1 du Code pénal	• amende de 45 000 € • emprisonnement de 3 ans
1° Lorsque l'infraction est commise de façon habituelle ou à l'égard de plusieurs mineurs ; 2° Lorsque le mineur a été mis 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 communication.	art. 225-12-2 du Code pénal	• amende de 75 000 € • emprisonnement de 5 ans
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. Le fait 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.	art. 227-23 du Code pénal	• amende de 45 000 € • emprisonnement de 3 ans
Si utilisation pour la diffusion de l'image ou de la représentation du mineur à destination d'un public non déterminé, un réseau de télécommunication (intranet par exemple).	art. 227-23 al 2 du Code pénal	• amende de 75 000 € • emprisonnement de 5 ans

Infractions	Texte	Peine (maximale)
Le fait soit de fabriquer, de transporter, de diffuser par quelque moyen que se 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, lorsque ce message est susceptible d'être vu ou perçu par un mineur.	art. 227-24 du Code pénal	• amende de 75 000 € • emprisonnement de 3 ans
Le fait de détenir une telle image ou représentation.	art. 227-23 al. 4 du Code pénal	• amende de 30 000 € • emprisonnement de 2 ans
Le fait, pour un majeur d'exercer sous violence, contrainte, menace où surprise une atteinte sexuelle sur la personne d'un mineur de 15 ans.	art. 227-25 du Code pénal	• amende de 75 000 € • emprisonnement de 5 ans
L'infraction définie à l'article 227-25 est aggravée : 1° lorsqu'elle est commise par un ascendant légitime, naturel ou adoptif ou par tout autre personne ayant autorité sur la victime ; 2° lorsqu'elle est commise par une personne qui abuse de l'autorité que lui confie ses fonctions ; 3° lorsqu'elle est commise par plusieurs personnes agissant en qualité d'auteur ou de complice ; 4° lorsqu'elle s'accompagne du versement d'une rémunération (prostitution) ; 5° lorsque le mineur a été mis 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 télécommunication.	art. 227-26 du Code pénal	• amende de 150 000 € • emprisonnement de 10 ans

Infractions	Texte	Peine (maximale)
Corruption de mineurs • Le fait de favoriser ou de tenter de favoriser la corruption d'un mineur ; • Circonstance aggravante lorsque le mineur à moins de 15 ans.	art. 227-22 du Code pénal	• amende de 75 000 € • emprisonnement de 5 ans • amende de 100 000 € • emprisonnement de 7 ans
Tout acte de pénétration sexuelle, de quelque nature qu'il soit, commis sur la personne d'autrui par violence, contrainte, est un viol. Circonstance aggravante • Si commis sur un mineur ; • 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.	art. 222-23 du Code pénal	• 20 ans de réclusion criminelle
Les faits d'agressions sexuelles autres que le viol sont aggravés 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 déterminé, d'un réseau de télécommunications.	art. 222-28 du Code pénal	• amende de 100 000 € • emprisonnement de 7 ans

• 1.2. prévues par des textes spécifiques :

◗ Infractions à la loi sur la presse (loi du 29 juillet 1881) :

Infractions	Texte	Peine (maximale)
Refus d'insertion ou de rectification dans un imprimé.	art. 13 de la loi 29/07/1881 relative à la liberté de la presse	• amende de 3 750 € • emprisonnement de 3 mois si refus d'insertion après jugement
Contestation de crimes contre l'humanité tels que définis par l'article 6 du statut du tribunal militaire de Nuremberg annexé à l'accord de Londres du 8/08/1945.	art. 24 bis de la loi de 1881	• amende de 45 000 € • emprisonnement de 1 an
Provocation aux atteintes volontaires à la vie, à l'intégrité de la personne, aux agressions sexuelles.	art. 24 al.1-1° de la loi de 1881	• amende de 45 000 € • emprisonnement de 5 ans
Provocation au vol, extorsion, destructions, dégradations, détériorations volontaires dangereuses pour les personnes.	art. 24 al.1-2° de la loi de 1881	• amende de 45 000 € • emprisonnement de 5 ans
Provocation aux crimes et délits portant atteinte aux intérêts fondamentaux de la nation.	art. 24 al. 2 de la loi de 1881	• amende de 45 000 € • emprisonnement de 5 ans
Apologie des crimes portant atteinte volontaire à la vie, à l'intégrité de la personne et agressions sexuelles.	art. 24 al. 3 de la loi de 1881	• amende de 45 000 € • emprisonnement de 5 ans

Infractions	Texte	Peine (maximale)
Apologie des crimes de guerre, crimes contre l'humanité ou des crimes ou délits de collaboration avec l'ennemi.	art. 24 al. 3 de la loi de 1881	• amende de 45 000 € • emprisonnement de 5 ans
Provocation ou apologie des actes de terrorisme.	art. 24 al. 4 de la loi de 1881	• amende de 45 000 € • emprisonnement de 5 ans
Provocation à la discrimination, à la haine ou à la violence raciale, à raison de l'origine ou de l'appartenance ou non appartenance à une ethnie, une nation, une race ou une religion.	art. 24 al. 6 de la loi de 1881	• amende de 45 000 € • emprisonnement de 1 an
Fausses nouvelles, pièces fabriquées, falsifiées ou mensongèrement attribuées à des tiers.	art. 27 de la loi de 1881	• amende de 45 000 €
Diffamation publique commise envers les cours et tribunaux, les armées les corps constitués et les administrations publiques.	art. 30 de la loi de 1881	• amende de 45 000 €
Diffamation publique commise envers les magistrats, jurés, témoins, fonctionnaires publics, envers un parlementaire national, un citoyen chargé d'un mandat public, un ministre.	art. 31 de la loi 1881	• amende de 45 000 €
Diffamation publique commise envers les particuliers concernant la vie privée.	art. 32 al. 1er de la loi 1881	• amende de 12 000 €

Infractions	Texte	Peine (maximale)
Diffamation raciale à raison de l'origine ou de l'appartenance ou non appartenance à une ethnie, une nation, une race ou une religion.	art. 32 al. 2 de la loi de 1881	• amende de 45 000 € • emprisonnement de 1 an
Injure publique.	art. 33 al. 1er et 2 de la loi de 1881	• amende de 12 000 €
Injure publique à raison de l'origine ou de l'appartenance ou non appartenance à une ethnie, une nation, une race ou une religion.	art. 33 de la loi de 1881	• amende de 22 500 € • emprisonnement de 6 mois
Diffusion, sans l'accord de l'intéressé, de l'image d'une personne menottée ou entravée ou placée en détention provisoire.	art. 35 ter de la loi de 1881	• amende 15 000 €
• **Réalisation, publication ou diffusion, ou commentaire de sondage portant sur la culpabilité** d'une personne mise en cause ou sur la peine susceptible d'être prononcée à son encontre ; • **publication d'indications** permettant d'avoir accès à de telles sondages.	art. 35 ter de la loi de 1881	• amende 15 000 €
Diffusion de l'image des circonstances d'un crime ou d'un délit, portant gravement atteinte à la dignité d'une victime, sans l'accord de celle-ci.	art. 35 quater de la loi de 1881	• amende 15 000 €

Infractions	Texte	Peine (maximale)
Publication des actes d'accusation et tous autres actes de procédure criminelle ou correctionnelle avant leur lecture en audience publique - sauf demande écrite du juge d'instruction (ex: pour la publication de portraits robots).	art. 38 al. 1er (abrogé) de la loi du 29/07/1881	• amende de 3 750 €
Publication d'informations relative aux travaux et délibération du Conseil Supérieur de la Magistrature, à l'exception des informations et audiences publiques rendues en matières disciplinaire à l'encontre des magistrats.	art. 38 al. 2 de la loi du 29/07/1881	• amende de 3 750 €
Diffusion des informations relatives à l'identité ou permettant l'identification : • d'un mineur ayant quitté ses parents, son tuteur, la personne ou l'institution qui était chargée de sa garde ou à laquelle il était confié ; • d'un mineur délaissé ou qui s'est suicidé ; • d'un mineur victime d'une infraction. *Sauf demande des personnes ayant la garde du mineur ou des autorités administratives ou judiciaires.*	art. 39 bis de la loi de 1881 art. 227-1 et 227-2 du Code pénal	• amende 15 000 €

Infractions	Texte	Peine (maximale)
Diffusion de renseignements concernant l'identité d'une victime d'une agression ou d'une atteinte sexuelles ou **l'image** de cette victime lorsqu'elle est identifiable, et sans son accord écrit.	art. 39 quinquies de la loi de 1881	• amende 15 000 €
Publication avant décision judiciaire de toutes informations relative à des constitutions de partie civile ayant mise en mouvement l'action publique.	art. 2 loi du 2 juillet 1931	• amende 18 000 €
Publication du compte rendu des débats des tribunaux pour enfants. **Publication de texte ou illustration** concernant l'identité et la personnalité de mineurs délinquants.	art. 14 al. 4 de l'Ordonnance du 2/02/1945	• amende de 6 000 € • emprisonnement de 2 ans, si récidive
Publication du jugement des tribunaux pour enfants mentionnant le nom ou l'identité du mineur.	art. 14 al. 5 de l'ordonnance du 2 février 1945	• amende de 3 750 €
Publication du jugement des tribunaux pour enfants mentionnant le nom ou l'identité du mineur.	art. 14 al. 5 de l'ordonnance du 2 février 1945	• amende de 3 750 €
Discrédit porté sur une décision de justice, portant atteinte à l'autorité judiciaire ou son indépendance (sauf commentaires techniques visant à réformer ou réviser la décision).	art. 434-25 du Code pénal	• amende de 7 500 € • emprisonnement de 6 mois

❒ Le point sur la prescription en matière de presse

La Cour de cassation a clarifié sa jurisprudence dans deux arrêts des 16 octobre 2001 et 27 novembre 2001 dans lesquels elle réaffirme que le délai de prescription de l'action publique court, pour les infractions de presse commises sur l'Internet, à partir du jour où *"le message a été mis en place pour la première fois à la disposition des utilisateurs"*.

Ces arrêts posent toutefois plusieurs interrogations.

◗ *Les notions de réseau et de site*

La Cour de cassation ne distingue pas les deux notions. Or d'un point de vue technique, les notions de mise en ligne sur un réseau et mise en ligne sur un site ne se confondent pas.

Il est en effet possible de supposer qu'une information diffamatoire mise en ligne pendant plusieurs mois sur un site, sans que les représentants de celui-ci n'aient été inquiétés, soit reprise par un autre site plus de trois mois après la première mise à disposition.

Dès lors si l'on retient la date de mise en ligne sur le réseau Internet comme point de départ de la prescription, une poursuite pénale contre les responsables du second site paraît impossible. Il résulte de ces décisions que la prescription peut-être acquise sans que l'écrit litigieux soit définitivement retiré du serveur.

◗ *La notion de réédition*

La chambre criminelle de la Cour de cassation, depuis un arrêt du 16 décembre 1910, rappelé dans un arrêt du 8 janvier 1991, estime que la réédition d'un ouvrage constitue un nouvel acte de publication.

Par ailleurs, la cour d'appel de Paris, dans un arrêt définitif du 15 décembre 1999 a, d'une part considéré que la diffusion sur Internet était un acte de publication continue, et, d'autre part, estimé que la modification de l'adresse du site constituait une nouvelle mise à disposition du public, point de départ d'un nouveau délai de prescription.

Ainsi il semblerait possible, dans le cadre de l'exemple ci-dessus proposé, d'envisager des poursuites à l'égard du second site, sans que puisse être opposée l'exception de prescription.

Les décisions du 16 octobre 2001 et 27 novembre 2001 considèrent que les infractions commises sur Internet ne dérogent en rien à la législation et à la jurisprudence de la Cour de cassation en matière d'infractions de presse.

Par jugement en date du 26 février 2002, le tribunal correctionnel de Paris (17ème chambre) confirme cette analyse, en précisant que *"chaque mise à jour du site constitue une infraction nouvelle", "chaque nouvelle mise à disposition d'objets aux internautes, fait courir un nouveau délai de prescription".*
(Décision disponible sur le site http = //www.foruminternet.org).

Ainsi, tous faits tels que les provocations à la haine raciale, à la discrimination, la contestation de l'existence des crimes contre l'humanité, l'apologie de ces crimes, et plus généralement l'ensemble des infractions de presse, à partir du moment où ils auront pour support Internet, seront soumis à la prescription trimestrielle.

NB : La jurisprudence est susceptible d'évoluer en ce domaine.

2 - Les infractions contre les biens :

• 2.1 prévues par le Code pénal :

Infractions	Texte	Peine (maximale)
L'escroquerie est le fait, soit par l'usage d'un passe nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres fraduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice dun tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge.	art. 313-1 du Code pénal	• amende 375 000 € • emprisonnement de 5 ans
La menace de commettre une des infractions, une dégradation ou une détérioration "dangereuse" pour les personnes.	art. 322-12 du Code pénal	• amende 7 500 € • emprisonnement de 6 mois


WWW

II - QUELLES SONT LES JURIDICTIONS COMPÉTENTES ?

A) - La compétence des juridictions nationales

L'article 113-1 du Code pénal prévoit que la loi française est applicable aux infractions commises sur le territoire de la République.
Aux termes de l'article 113-2 du Code pénal, est réputée commise sur ce territoire l'infraction dont l'un des éléments constitutifs a eu lieu en France. Il convient donc qu'un élément constitutif de l'infraction commise lors de la connexion à des informations illicites se situe en France. A cet égard, par jugement en date du 26 février 2002, le tribunal de grande instance de Paris (17e chambre) a rappelé que "le juge français est compétent dans la mesure où les messages ou le contenu du site sont rendus accessibles, par l'Internet, sur le territoire français".
Comme l'a rappelé le rapport du Conseil d'Etat "*l'Internet et les réseaux numériques*[1], il résulte de ces dispositions que la loi pénale française s'appliquera clairement dans le cas d'un message litigieux disponible sur le réseau Internet, quel que soit sa source dans le monde, et accessible de France, dès lors que la réception par l'utilisateur sur le territoire français est bien un élément constitutif de l'infraction en application de l'article 113-2 du Code Pénal. Par exemple, le lieu d'émission des sites litigieux qui peut correspondre au domicile de l'internaute signalant est un critère qui peut être retenu, de même que le lieu de localisation du serveur véhiculant le site litigieux.
Les règles de compétence édictées notamment par l'article 18 du Code de procédure pénale s'appliquent en la matière et les investigations en préliminaire sont vite bloquées en raison de leur poursuite souvent hors ressort qui nécessite l'ouverture d'une information judiciaire.

Il convient cependant de souligner que la jurisprudence en la matière n'est pas stabilisée et suceptible d'évolution.

[1] - *La documentation française 1998 page 171*

B) - La compétence territoriale du parquet

Il convient de rappeler qu'en matière d'infractions commises via Internet, il n'existe pas de parquet à compétence nationale, les critères de compétence territoriale de droit commun demeurent.

En principe est compétent :

- Le parquet du lieu de commission de l'infraction, avec par ordre de priorité :
  - celui du lieu où la personne a physiquement agi pour commettre l'infraction (exemples : personne recelant, stockant ou proposant des images ou des textes illicites, personne ayant accédé illégalement à un traitement automatisé de données) ;
  - celui du lieu où l'internaute a constaté l'existence d'un site à caractère illicite ou a reçu des images ou des textes de nature illicite. Il est utile de connaître l'identité ou l'adresse de la personne ayant dénoncé l'infraction.
  - celui du lieu du serveur hébergeant le site s'il apparaît, après les premières vérifications, qu'il est en France.

- Le parquet du domicile du mis en cause ;

- Le parquet du lieu d'arrestation du mis en cause.

Exceptions : en raison de la nature des infractions commises ou susceptibles de l'être, la saisine d'un parquet spécialisé doit être privilégiée.

Exemple : découverte d'un site à caractère terroriste dont le serveur se trouve en province ; dans ce cas, un service central spécialisé pourra être saisi par le parquet de Paris disposant d'une compétence particulière en matière de terrorisme.

En cas de procédures multiples initiées dans plusieurs parquets, il est préconisé un regroupement de celles-ci.

Si l'information transversale des juridictions apparaît indispensable en ce domaine, force est de constater qu'en l'état, un éparpillement des procédures nuit à leur traitement.

III - L'APPRÉHENSION NÉCESSAIREMENT INTERNATIONALE DU TRAITEMENT JUDICIAIRE DES INFRACTIONS COMMISES VIA INTERNET

Dans la mesure où l'Internet bouleverse les règles classiques de compétence, que les infractions peuvent être commises simultanément dans plusieurs pays, que des investigations doivent souvent être effectuées à l'étranger, il est nécessaire, d'une part, de présenter les services compétents en la matière et, d'autre part, de fournir des éléments pour améliorer le traitement des procédures lorsque les enquêtes doivent se poursuivre à l'étranger.

A. Les services compétents

1. Interpol

Organisation Internationale de Police criminelle (OIPC) créée en 1929, Interpol vise à améliorer la coopération policière dans le monde grâce à des bureaux dans 178 pays membres (BCN). Ces bureaux sont des services de police permanents composés de policiers agissant dans le cadre de leur législation nationale.

Ils constituent le relais national aux opérations de police sollicitées par les autres Etats membres. Le BCN-France, antenne d'Interpol, est rattaché à la Direction centrale de la Police Judiciaire au sein de la sous Direction des ressources et liaison dans la Division des relations internationales (Point de contact unique EUROPOL – SCHENGEN)

Mission :

Le rôle d'Interpol est de faciliter pour ses membres la lutte contre le trafic de stupéfiants, le terrorisme, la criminalité informatique ou économique. Interpol dispose d'un système de communication informatique commun à tous les pays membres et d'une base de données criminelles internationales.

Moyens :

Interpol porte à la connaissance des services de police nationaux les BSN certains renseignements relatifs à des infractions, des délinquants et des victimes. A cet égard, il est procédé à l'établissement des notices signalétiques internationales individuelles relatives aux disparitions des personnes et notamment des mineurs et aux délinquants susceptibles de récidiver.

Les infractions collectées entrent directement en procédure.

Depuis juillet 1999, Interpol a développé un site Web à deux niveaux d'accès public et restreint, afin de donner une plus large diffusion aux notices avec l'autorisation BCN. Interpol réalise des opérations de police judiciaire d'envergure tels l'opération "Cathédrale" par exemple, lancée en 1998, qui a permis le démantèlement d'un réseau diffusant plus de 750 000 clichés de pornographie enfantine et qui s'est traduite par l'arrestation de 107 personnes dans 12 pays.

Il convient de souligner les efforts d'Interpol en vue de constituer une base de données d'images pédophiles, grâce au logiciel excalibur d'analyse et de comparaison automatique par le contenu (www.excalib.com).

2. Europol

Mission :

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

Le mandat d'Europol ainsi défini a été progressivement élargi. Initialement limité au soutien des activités de répression dans les domaines du trafic de stupéfiants, de véhicules volés, de matières nucléaires et radioactives, les filières d'immigration, le faux monnayage et la falsification d'autres moyens de paiement, la traite des êtres humains - y compris la pornographie enfantine -, le terrorisme, le blanchiment d'argent lié à ces formes de criminalité, il est aujourd'hui compétent pour tout ce qui concerne les atteintes à la vie, à l'intégrité physique et à la liberté, les atteintes au patrimoine, aux biens publics, au commerce illégal ainsi que les atteintes à l'environnement.

Toutefois, les infractions doivent impliquer une structure ou une organisation criminelle et deux Etats membres ou plus, doivent être affectés. Europol est donc compétent dans la lutte contre la criminalité informatique ou pour les formes de criminalité dont la commission est facilitée par Internet.

Europol intervient en :

- facilitant l'échange d'informations, conformément aux dispositions nationales ;
- fournissant des analyses opérationnelles pour les opérations menées par les Etats membres ;
- fournissant des rapports de type stratégique et des analyses d'activité criminelles réalisées à partir d'informations et de renseignements communiqués par les Etats membres, recueillis par Europol ou issus d'autres sources ;
- apportant son expertise et son assistance technique aux enquêtes et aux opérations menées au sein de l'UE.

Moyens :

La liaison entre Europol et la France est assurée par l'Unité nationale Europol. Elle est implantée au sein du ministère de l'intérieur à la direction centrale de la police judiciaire (D.C.P.J. 11rue des Saussaies 75008 PARIS). Elle peut-être touchée par le point de contact unique (01 40 97 88 00). La mission justice est placée dans les mêmes locaux ; de plus, la gendarmerie, la douane et l'INSEE participent à cette structure.

La convention Europol demande qu'EUROPOL installe et gère un système informatisé permettant l'introduction, l'accès et l'analyse des données. Celui-ci est donc composé des systèmes d'informations, d'analyse et d'index.

Il peut stocker et utiliser les données nécessaires à l'accomplissement des fonctions d'Europol. Les données introduites sont relatives aux personnes mises en cause pour avoir commis ou participé à une infraction relevant de la compétence d'Europol conformément à l'article 2 de la convention Europol.

Le système d'analyse intègre les fichiers de travail à des fins d'analyse qui ont pour objet d'assister les services compétents des Etats membres dans la répression et la lutte contre les formes de criminalité comprises dans le mandat d'Europol.

Les informations susceptibles d'être collectées proviennent de sources ouvertes accessibles aux analystes d'Europol, mais également d'informations transmises par les services d'enquêtes des Etats membres.
Le système d'index indique à chaque officier de liaison des Etats membres que des données concernant son Etat membre d'origine ont été intégrées dans un fichier d'analyse clairement identifié.

B . SCHENGEN[1]

Seuls les articles de la convention des accords de Schengen susceptibles d'avoir un lien avec une affaires de criminalité sur Internet seront évoqués.

1. Le système d'information SCHENGEN ou S.I.S.

La suppression des contrôles aux frontières intérieures de l'espace SCHENGEN a conduit à la création d'un système d'information commun dénommé "système d'information SCHENGEN" et au renforcement de la coopération policière entre les forces de sécurités des parties contractantes.

Le système d'information SCHENGEN permet l'échange d'informations entre les Etats signataires et la consultation automatisée de données sur les personnes, les véhicules terrestres et les objets signalés.
Il participe ainsi à la préservation de l'ordre et la sécurité publics, y compris la sûreté de l'Etat, et facilite l'application des dispositions de la convention relative à la circulation des personnes sur le territoire des Etats membres. Dans chaque Etat, est mis en place à coté du N.SIS un organisme chargé d'assurer 24 heures sur 24 un point de contact unique et permanent à la disposition des forces de l'Etat considéré et des autres partenaires européens.

[1] *Pays membres de l'Espace SCHENGEN (15) : France, Espagne, Portugal, Italie, Grèce, Autriche, Belgique, Allemagne, Luxembourg, Pays-Bas, Danemark, Norvège, Suède, Finlande, Islande*

Le SIRENE FRANCE (supplément d'information requis à l'entrée nationale) est le point de contact national unique mis à la disposition des autres partenaires de l'espace Schengen pour assurer les échanges d'informations et les documents avec les autres SIRENE. Il s'agit d'un service interministériel qui associe des policiers, gendarmes et magistrats.
Il répond au n° 01 40 97 88 00. Son adresse postale est : D.C.P.J./DRI 11, rue des Saussaies 75008 PARIS.

2. La coopération policière dans l'espace SCHENGEN

La coopération entre les polices des Etats de l'Union ayant signé et ratifié la convention s'exerce grâce à un échange d'informations et se traduit par plusieurs mesures novatrices.
Elle prévoit notamment l'assistance mutuelle aux fins de la prévention et de la recherche de faits punissables, l'intensification de la coopération policière dans les régions frontalières (article 39 de la convention).
Cet article concerne la coopération policière et judiciaire, en facilitant l'assistance mutuelle des services de police et de gendarmerie, en permettant l'échange d'informations ou d'éléments de procédure par le biais de l'unité centrale de coopération policière internationale (UCCPI).

Pour l'application de l'article 39-5 de la convention un modèle interministériel de convention de coopération transfrontalière policière et douanière a été mis au point.
Il fixe, d'une part, les principes de la coopération judiciaire directe entre unités opérationnelles situées dans la zone frontalière définie par l'accord et prévoit, d'autre part, la création de centres de coopération policière et douanière (CCPD) à proximité des frontières.

Dans une même structure, sont rassemblés policiers, gendarmes et douaniers, mis à disposition de l'ensemble des services chargés de missions de police et de douane, afin notamment de lutter contre "l'immigration irrégulière, la délinquance frontalière, les menaces à l'ordre public et les trafics illicite".
Une convention a été signée avec l'Allemagne, l'Italie et l'Espagne. Deux autres conventions sont en cours de signature avec la Belgique et le Luxembourg. Deux CCPD fonctionnent actuellement. Il s'agit d'Offenbourg et Modane. Vintimille devrait prochainement être ouvert.

- Le droit d'observation (article 40) est une possibilité offerte à un enquêteur de poursuivre selon certaines modalités qui sont différentes selon les Etats, une filature sur un Etat voisin. Les magistrats du parquet et de l'instruction peuvent faire procéder d'initiative à ces observations.
- L'article 41 permet aux services enquêteurs de poursuivre une personne prise en flagrant délit de participation ou de commission d'une infraction prévue par la convention, sans autorisation préalable au-delà de la frontière lorsque cette personne prend la fuite vers un Etat voisin et si l'avis n'a pu être donné à temps par l'Etat requis. Les règles de la poursuite varie selon les Etats.
- L'entraide répressive entre les Etats Schengen relève des articles 48 à 53 de la convention.
  Le domaine de l'entraide est étendu aux faits constituant une infraction administrative, aux procédures liées à des poursuites pénales, à la notification de communications judiciaires, aux modalités d'exécution des peines et aux infractions fiscales.
  Celle-ci peut toutefois être refusée lorsque le montant des droits trop peu perçus ou non perçus est inférieur à 25 000 €. Il en est de même si la valeur des marchandises exportées ou importées illégalement ne dépasse pas 10 000 €.
- La convention Schengen assouplit également les conditions de l'entraide en matière de perquisitions et de saisies.

L'article 51 prévoit comme seule condition à l'exécution d'une perquisition et d'une saisie, outre sa compatibilité avec la législation de la partie requise, que l'infraction soit passible soit d'une peine d'emprisonnement ou d'une mesure de sûreté d'au moins six mois sur le territoire des deux Etats, soit d'une sanction équivalente sur le territoire d'une partie et qu'elle constitue dans la législation de l'autre partie une infraction administrative susceptible de donner lieu à recours devant une juridiction compétente notamment en matière pénale.

De plus, les demandes d'entraide pourront être adressées directement aux autorités judiciaires compétentes et renvoyées par la même voie. En France, les commissions rogatoires internationales, les demandes d'entraide ainsi que les pièces d'exécution doivent transiter par le parquet général territorialement compétent.

Enfin, la convention a introduit la possibilité facultative de transmettre à son destinataire par voie postale avec accusé de réception la notification des actes judiciaires[2].

Pour des éléments d'informations complémentaires, il est recommandé de se référer à la circulaire NOR JUSA95000149C du 23 juin 1995 du Ministère de la Justice. La mission Justice placée auprès du D.C.P.J. peut-être contactée (01 40 97 84 85), ainsi que le BEPI à la D.AC.G. qui dispose d'un site Intranet.(01.44.86.14.00)

Le point de contact déjà cité peut-être utilement joint ainsi que les magistrats, policiers et gendarmes du SIRENE France (01 40 97 88 00). Ce numéro fonctionne 24h/24.

Cas particuliers

Grande-Bretagne

"L'accord d'Amsterdam signé en 1997 reconnaît l'efficacité de l'accord signé à Schengen en 1985 jusqu'alors pratiqué au sein d'une sorte de Club et le consacre comme un outil de l'Union Européenne. Désormais, tous les Etats membres de l'Union Européenne doivent satisfaire aux exigences de l'accord. Ainsi, le Royaume Uni et l'Irlande qui avaient refusé jusqu'à présent d'adhérer à l'accord de Schengen préparent leur intégration à l'horizon 2002. Toutefois, ces deux pays bénéficieront d'un régime dérogatoire les autorisant à conserver les contrôles à leurs frontières".

[2] *Les actes de procédure susceptible d'être notifiés par voie postale concerne : Les convocations devant le juge d'instruction (victime, témoin, mis en examen), citation à témoin partie civile, victime ou prévenu, notification d'expertise, ordonnance (à caractère juridictionnel du juge d'instruction, du président du tribunal de police), jugement du tribunal de police ou du tribunal correctionnel, arrêt de la chambre d'accusation, de la chambre des appels correctionnels.*

La situation spécifique de la Suisse

En raison de l'absence de la Suisse des instances de coopération SCHENGEN, et pour assurer une meilleure sécurité de l'espace SCHENGEN un accord de coopération policière judiciaire et douanière a été signé entre la France et la Suisse en mars 1998.
Son contenu est proche de celui de la convention d'application. A ce titre, l'accord reprend certaines modalités de coopération introduites par la convention d'application des accords de SCHENGEN. Il s'agit notamment de l'assistance sur demande, et l'échange d'informations pour lutter contre la délinquance dans la zone frontalière, prévenir l'immigration illégale et les trafics illicites, sauvegarder l'ordre et la sécurité publics et recueillir et échanger des informations en matière policière et douanière.

L'accord précise également les conditions d'échange d'informations effectué entre les services compétents des deux parties, notamment au regard du respect des dispositions nationales en matière de protection des données à caractère personnel.
A ce titre, la commission des communautés européennes a constaté dans une décision du 26 juillet 2000 le caractère adéquat de la protection des données à caractère personnel en Suisse conformément à la directive 95/46/CE du parlement européen et du conseil.
Un centre de coopération policière et douanière (CCPD) prévu dans l'accord franco-suisse devrait donc être créé pour améliorer la circulation de l'information entre les différents corps de sécurité dans la région "des trois frontières".

C. Les instruments internationaux

1. Au niveau de l'ONU

- Convention relative aux droits de l'enfant de New-York du 26 janvier 1990.
- Protocole additionnel à la Convention de Palerme des Nations Unies contre la criminalité transnationale organisée visant à prévenir, réprimer et punir la traite des personnes, en particulier des femmes et des enfants.

2. Au niveau du Conseil de l'Europe

- Recommandation 91-11 sur l'exploitation sexuelle, la pornographie, la prostitution, le trafic d'enfants et de jeunes adultes.
- Pour améliorer et renforcer ce texte, un projet de nouvelle recommandation a été élaborée (PC-SE(2000) 18 Révisé afin d'appréhender l'exploitation sexuelle dans un but non lucratif, non prise en compte dans le texte de 1991.
- Recommandation sur la lutte contre la traite des êtres humains aux fins d'exploitation sexuelle adoptée par le Comité des Ministres en mai 2000.

La convention sur la cybercriminalité constitue le premier traité international sur les infractions pénales commises contre les réseaux informatiques ou à l'aide de ceux -ci. Ce texte permet un traitement efficace des agissements des auteurs d'infractions commises sur la toile (document disponible sur le site du conseil de l'Europe).

Ce texte, signé le 23 novembre 2001 par 30 pays dont la France, vise à harmoniser les législations nationales pour mieux lutter contre la cybercriminalité. Le traité entrera en vigueur dès que les parlements de cinq Etats, dont trois membres du Conseil de l'Europe, initiateur du texte, l'auront ratifié.

De nouvelles procédures

La convention fixe le droit commun des mesures d'enquêtes pénales sur les réseaux et est basée sur le maintien de la compétence exclusivement nationale des autorités en charge de lutte contre la cybercriminalité.

Les pouvoirs d'investigations définis dans la Convention visent à permettre l'obtention et la collecte de données informatiques dans le cadre d'enquêtes pénales en cours.

La convention reconnaît aux données numériques une valeur juridique et des effets probants identiques aux éléments matériels existant dans le monde hors ligne.

- Le titre 2, définit la notion de “conservation rapide des données stockées". Les modalités de mise en œuvre de cette mesure varieront selon les États. Il s’agit de préserver l’intégrité des seules données utiles à l’enquête en cours. L’article 17 de la convention vise à assurer la traçabilité de la communication, quel que soit le nombre de fournisseurs ayant participé à la transmission du message.
- Le titre 3, dans son article 18, prévoît le cas des “injonctions de produire des données”. Cette mesure devrait constituer le fondement juridique permettant la remise aux autorités compétentes de certaines données.
- Le titre 3, dans son article 19 vise les "perquisitions informatiques à distance”. Les données perquisitionnées peuvent être soit conservées sur un support de stockage ou stockées dans un autre système informatique si celui-ci demeure dans les limites territoriales de l’état perquisitionneur. En revanche, cet article n’autorise pas à perquisitionner des données stockées à l’étranger, même si elles sont accessibles via le réseau.

Ces dispositions sont soumises aux conditions légales des pays signataires mais doivent garantir le respect des droits de l’homme et l’application du principe de proportionnalité. En particulier, les procédures ne pourront être engagées que sous certaines conditions, tel que, selon le cas, l’autorisation préalable d’un magistrat ou d’une autre autorité indépendante.

Les règles de la coopération internationale

A côté des formes traditionnelles de coopération pénale internationale prévues notamment par les conventions européennes d’extradition et d’entraide judiciaire en matière pénale, la nouvelle convention exigera des formes d’entraide correspondant aux pouvoirs définis préalablement par la convention et, en conséquence, que les autorités judiciaires et services de police d’un Etat puissent agir pour le compte d’un autre pays dans la recherche de preuves électroniques, sans toutefois mener d’enquêtes ni de perquisitions transfrontalières. Les informations obtenues devront être rapidement communiquées.

La compétence

Chaque pays doit établir sa compétence lorsque l'infraction est commise sur son territoire, à bord d'un bateau ou d'un avion immatriculé chez lui ou lorsque l'un de ses ressortissants en est l'auteur si l'infraction ne relève de la compétence territoriale d'aucun autre Etat.
Par ailleurs, un projet de protocole additionnel sur l'incrimination des actes racistes ou xénophobes via les réseaux informatiques a été rendu public en février 2002. Ce protocole aura pour conséquence d'élargir le champ d'application de la convention.

3. Au niveau de l'Union Européenne

- Résolutions du Parlement européen en 1996, 1997 et 1998.
- La décision 276/1999CE du parlement Européen et du Conseil du 25 janvier 1999 adopte un plan d'action communautaire pluriannuel visant à promouvoir une utilisation plus sûre d'Internet par la lutte contre les messages à contenus illicites et préjudiciables diffusé sur les réseaux mondiaux. Sont ainsi encouragés l'auto réglementation de l'industrie d'Internet, le développement de dispositifs de filtrage et enfin la création d'un réseau européen de hotlines.
- Conférence internationale sur la lutte contre la pédopornographie sur Internet (Vienne, 29 septembre - 1er octobre 1999).
- Décision du Conseil relative à la lutte contre la pédopornographie sur Internet du 29 mai 2000.


Code
Pén
al

Annexes

ANNEXE 1 : LE GLOSSAIRE RÉDUIT DU LANGAGE INFORMATIQUE

Adresse électronique *e-mail*	Chaque internaute dispose de sa propre adresse électronique. Par exemple : untel@fournisseur.fr, "untel" correspondant au login de l'internaute (son identifiant). Le symbole "@" (appelé arobace) s'obtient en enfonçant les touches Alt Gr et 8 (en haut du clavier). Le ".fr" signifie que le fournisseur est localisé en France, ce serait "ca" au Canada ou "be" en Belgique.
Adresse IP	Numéro unique d'identification donné à chaque ordinateur connecté à Internet. Un numéro IP est un groupe de 4 nombres (de 0 à 255) séparés par des points. Cette adresse peut être fixe (pour les connexions par ADSL ou câble) ou dynamique (elle change à chaque connexion en cas d'utilisation d'un modem téléphonique). Chaque fois qu'un ordinateur se connecte à Internet, il est repéré par l'adresse IP d'origine qui indique son emplacement sur le réseau. A une demande d'identification, peuvent correspondre plusieurs adresses IP. L'adresse IP destinataire correspond à la machine sur laquelle l'Internaute désire se connecter.
Adresse URL	C'est ce que vous tapez sur votre clavier pour indiquer l'endroit où vous souhaitez aller sur Internet. Elle identifie un site ou une page Web.
AFNIC	Association française pour le nommage Internet en coopération. C'est l'organisme chargé de fédérer en France, l'obtention des noms de domaine auprès des sociétés habilitées à les vendre.
AFPI *AFA*	Association française des providers internet (AFPI), des fournisseurs d'accès (AFA). Organismes qui regroupent plusieurs fournisseurs d'accès pour favoriser le développement de l'Internet en France.

Arobace *@*	Caractère d'imprimerie utilisé dans le domaine de l'Internet pour séparer le nom de l'utilisateur du service qui héberge sa boîte aux lettres. user@mail
CD-R *Compact Disc Recordable*	Disque compact enregistrable une seule fois. Sur ce type de CD, les fichiers enregistrés ne peuvent plus être effacés. Il est surtout utilisé pour la production personnelle de CD-Rom et de CD audio, ainsi que pour l'archivage des données.
CD-Rom *Compact Disc Read Only Memory*	Apparemment identique à un disque compact audio, il n'est lisible que sur micro. Par extension, on nomme aussi CD-Rom (ou cédérom) les programmes multimédias vendus sur ce support.
CD-RW *Compact Disc Read Write*	Disque compact permettant d'enregistrer et effacer des données autant de fois qu'on le souhaite, comme sur une disquette.
Compression	Opération visant à réduire la taille d'un fichier ou d'un groupe de fichiers. Elle s'effectue au moyen d'un logiciel de compression (Winzip, Stuffit…) dont le rôle est de coder les informations numériques. Elle est souvent utilisée pour des photographies qui utilisent de la mémoire.
Courrier électronique	Ce service majeur d'Internet permet aux usagers munis d'une adresse électronique de s'envoyer instantanément des messages à travers le monde. Autre terme e-mail.
Domaine	Adresse d'un site Internet unique sur la planète. Pour être avalisé, ce nom doit être déposé et enregistré avant la mise en service du site Web.
Editeur HTML *Hyper Text Markup Language*	Langage de programmation adopté dans le monde entier, utilisé pour créer des documents hypertextes et construire des pages Web. C'est également un logiciel de communication rapide.

FAI	Fournisseur d'accès Internet
FAQ *Frequently Asked Questions*	Terme qui désigne un ensemble d'informations pratiques se rapportant à un groupe de discussion, à un site Web ou à un logiciel. Les FAQ sont censées répondre aux interrogations les plus fréquentes. En français, se traduit par la Foire aux questions.
Forum de discussions *Newsgroups*	Espace de discussion sur Internet, les forums sont des " places virtuelles " où chacun peut venir poser des questions, lancer un débat ou répondre aux contributions des internautes. Il en existe des milliers.
Fournisseur d'accès Internet *ISP (Internet Service Provider) (FAI)*	Abréviation de Fournisseur d'Accès à Internet ou Provider. C'est un prestataire de service qui permet de se connecter sur Internet. Fournisseur d'accès à l'Internet, nommé aussi Provider ou IAP (Internet Access Provider).Souvent les FAI ont un contrat avec leurs clients comportant une clause permettant aux FAI d'interdire l'accès à des informations illicites (ex : pornographie infantile).
Fournisseur de services Internet *Service provider ou Hébergeur*	Société qui offre des services complémentaires aux services de base : l'hébergement et la diffusion de pages web. On parle plus précisément de fournisseur d'hébergement pour la construction de pages web "personnelles", la gestion de sites Web et/ou de serveurs de news propres au client.
FTP *File Transfert Protocol*	Protocole informatique standard dédié à Internet permettant le téléchargement de fichiers situés sur ordinateurs distants vers votre poste de travail local et inversement. Un serveur FTP est un ordinateur du réseau Internet ou intranet qui vous propose un choix de fichiers et de répertoires dans lequel se trouve l'information susceptible d'être copié sur son propre ordinateur personnel.

Hébergeur	Société prestataire de services qui installe les serveurs web de ses clients sur des machines reliées au réseau Internet. En matière de commerce électronique, le métier d'hébergeur est rendu plus complexe compte tenu de la diversité des technologies nécessaires : paiement en ligne, conception de sites web marchand avec ses composants spécifiques (catalogue), promotion de site.
HTML *HyperText Markup Language*	Le HTML est le langage de programmation adopté dans le monde entier, utilisé pour créer des documents hypertextes et construire des pages Web. Il utilise une liste déterminée de balises qui décrivent la structure d'un texte (caractères, couleurs) ou l'emplacement d'éléments incorporés à la page (photos, graphiques, applets). Par exemple, la phrase : "Micro Hebdo présente son petit dictionnaire" s'écrit en HTML : <html> <body> Micro Hebdo présente son petit dictionnaire </body> </html>. Aujourd'hui, de nombreux logiciels permettent de créer des pages HTML sans connaître un seul mot de ce langage. La programmation en HTML n'est pas nécessaire quand on utilise un programme, un assistant ou un éditeur HTML (Frontpage par exemple). Ce format peut être traduit directement par des logiciels tels qu'Internet Explorer, Netscape Communicator ou même Word.
HTTP *Hyper Text Transfer Protocol*	Protocole technique utilisé sur le Web pour transférer des fichiers au cours d'une séance entre le serveur et l'utilisateur. La première partie des adresses Web (URL) commence ainsi généralement par http://. Ce qui indique au navigateur que l'utilisateur tente d'accéder à un site Web.
Internet	Réseau informatique mondial constitué d'un ensemble de réseaux nationaux, régionaux et privés, qui sont relié par le protocole de communication TCP/IP et qui coopèrent dans le but d'offrir une interface unique. Internet est divisé par ailleurs en plusieurs sous ensembles, utilisant des protocoles de communication différents : le Worl Wide Web (ou Web) qui regroupe les sites à consulter ; la messagerie électronique (ou e-mail) et les forums de discussion (news-groups).

InterNIC *Internet Network Information Centre*	C'est l'équivalent de l'Afnic, à l'échelon international (Voir Afnic) Il propose des statistiques sur l'utilisation d'Internet et attribue des noms de domaine dans son pays.
IP *Internet Protocol*	Protocole (ensemble de règles, code et signaux servant à établir un échange de données) utilisé sur Internet pour le transfert des données par paquets, qui permet de traverser de multiples réseaux hétérogènes, c'est à dire constitués de machines et de systèmes d'exploitation différents. L'adresse IP correspond à l'adresse électronique de l'ordinateur.
IRC *Internet Relay Chat*	Ce logiciel permet d'entretenir une discussion en direct avec des internautes du monde entier en envoyant et recevant des messages par le biais du réseau. On peut discuter en groupe ou avoir une conversation privée avec seulement une personne. (Mirc 32 = logiciel d'IRC) Réseau mondial de discussion en ligne. Tout ce qui est écrit est envoyé immédiatement à tous les participants. Il se divise en canaux de conversations où le pire côtoie le meilleur. C'est sur ce type de protocole que se fait le plus souvent les offres et demandes à caractère pédophile.
Jpeg *Joint photographic experts group*	Format de fichier très répandu pour les images numériques, qui autorise une compression variables des images. Une forte compression permet d'obtenir des fichiers plus petits, et de faire circuler ces images plus rapidement sur Internet.
Les sites portails	Ils sont de plus en plus nombreux sur Internet. Ils offrent une porte d'entrée vers une série d'hyperliens sur différents domaines, activités et rubriques particulières. Afin d'enrichir leur offre, ces sites spécialisés mettent à disposition des outils complémentaires, gratuits pour l'utilisateur, comme par exemple un compte e-mail, des inscriptions aux news, le vote sur des sujets ciblés et bien d'autres produits.

Lien hypertexte	Il relie un mot, une expression ou une image d'un document à une autre partie du document. Sur une page Web, le soulignement de couleur signale l'existence d'un lien avec une autre page Web. Il suffit de cliquer dessus pour aller vers cette autre page. Lors de la consultation d'une page Web, lorsque l'on promène le curseur sur le contenu, il peut prendre la forme d'une main. A ce moment il s'agit d'un lien et si on clique dessus, le nouveau document est mis en ligne.
Mot de passe	Chaîne de caractères alpha, numériques ou alphanumériques, à saisir en majuscules et/ou en minuscules pour accéder à un document ou à un système.
Moteur de recherches	Site Web spécialisé dans la recherche et le classement d'informations. Les moteurs de recherches regroupent dans des bases de données les noms, les adresses et les descriptions des sites qu'ils ont indexés. Pour faire une recherche, il suffit de taper un ou plusieurs mots clefs et d'utiliser éventuellement les opérateurs booléens ou de consulter les catégories proposées. Les moteurs de recherches les plus utilisés ont pour nom : Altavista, Excite, Hot-Bot, Infoseek, Lycos et Webcrawler.
Napster	A la fois moteur de recherches et gestionnaire de téléchargement, ce logiciel est en effet, l'un des premiers responsables du piratage d'œuvres musicales, décrié par les maisons de disques. Son principe de fonctionnement est simple. Une fois téléchargé et installé, le logiciel crée un dossier spécial sur votre disque dur, dans lequel il est possible de stocker tous les MP3 que l'on souhaite partager avec les autres utilisateurs de Napster. Lorsque le logiciel est lancé, celui-ci se connecte à Internet et les fichiers s'inscrivent dans la base de données du site de la société Napster. Tout internaute utilisateur du logiciel Napster peut alors télécharger les morceaux "publiés" sur L'ordinateur émetteur.

Navigateur ou logiciel de navigation *Browser*	Logiciel permettant d'avoir accès aux sites Internet et de visualiser les pages HTML et de se promener de site Web en site Web au moyen des liens hypertextes. Parmi les navigateurs les plus répandus on trouve NCSA Mosaic, Netscape navigator ou Microsoft Internet Explorer. Ils permettent aussi d'écrire des messages électroniques et d'accéder à des forums de discussion. Les principaux navigateurs connus : Internet Explorer 5.0 (www.microsoft.fr) Netscape Navigator 4.08 (www.netscape.fr) Amaya (www.w3.org/amaya) Browser 2000 (www.ftppro.com) Neoplanet (http://ftp.neoplanet.com/pub/neosetupfull.exe) Opera (www.opera.no/o361e32.exe)
Naviguer ou surfer	Il s'agit sur Internet, de passer d'une information à une autre. On utilise pour cela des liens hypertextes, qui permettent de passer directement de pages en pages et de sites en sites.
NEWS	Les News sont des forums où chacun dépose des courriers (articles) par thème. Ces courriers sont conservés quelques jours et donnent lieu à des discussions.
News group Groupe de discussion	Discussion en temps différé sur Internet. Les groupes de discussion sont constitués de forums sur lesquels il est possibles de débattre d'un grand nombre de sujets. Leur approche s'apparente au fonctionnement d'une liste de diffusion : on poste des messages, semblables à des e-mails, et l'on consulte les réponse en se connectant de nouveau sur le forum. Contrairement à une liste de diffusion, les messages postés n'arrivent pas directement dans la boîte aux lettres. Il est nécessaire de se connecter à un serveur, dit serveur de news, pour télécharger les réponses ou les nouveaux messages.

Tout le monde peut poster des messages dans n'importe quel groupe.
Certains groupes sont dits modérés. Avant qu'un message soit publié, l'accord du modérateur est nécessaire. Il s'agit généralement d'une vérification du contenu du message, le modérateur étant libre de supprimer ce qu'il veut. En pratique, cette "censure" est opérée sur des points précis, décrits dans une charte. On trouve également des robots qui excluent automatiquement les messages non sollicités (spam).

Les hiérarchies principales :

Il existe un certain nombre de hiérarchies qui ne sont pas liées à un pays d'origine. Il s'agit de préfixes génériques qui décrivent un thème global. On retrouve ces préfixes en tête des dénominations des groupes. A l'intérieur de chaque hiérarchie coexiste un grand nombre de groupes.
Comp : informatique
misc : divers
rec : récréatif
sci : sciences
soc : société
talk : discussions
alt : sujets dits alternatifs
Ces grandes catégories sont parfois reprises telles quelles, sans traduction, dans les hiérarchies nationales.
Exemple : depuis un serveur de news francophone, on accède aussi bien à comp.sys.mac qu'à l'excellent fr.comp.sys.mac, pendant francophone du premier groupe.

	Rechercher dans les news : Pour retrouver des informations sur un thème donné sans connaître le forum qui traite de ce sujet, il s'avère intéressant d'effectuer des recherches sur les groupe de discussion. Le volume d'articles généré chaque jour étant colossal, archiver tous les groupes devient vite difficile. Certains site comme Dejanews.com, proposent des recherches dans les hiérarchies principales, ainsi que dans leurs archives. *Pertinence de l'information :* Mieux vaut ne pas se départir d'une certaine prudence face aux informations présentes sur certains forums. Toutefois, la plupart du temps les newsgroups des communautés véhiculent des informations de qualité. *Les logiciels :* Forte Free Agent pour télécharger des messages et les lire une fois déconnecté. Editeur : Forté Inc / version 1.21 / adresse : www.forteinc.com Autopix pour télécharger des images sur les groupes de discussion. Editeur : Ken E. Browning / version : 99.1212 / adresse : kenbrow.simplenet.com
Password	Mot de passe accompagnant le nom d'utilisateur (login) et permettant d'assurer la confidentialité d'un compte. Il est personnel et confidentiel (comme un numéro de carte bleue). Le mot de passe lié à l'identifiant est requis au moment de la connexion à Internet et aussi, parfois, pour accéder à une boîte à lettres électronique.
Patch	Logiciel qui modifie ou optimise les fonctions d'un programme ou d'un matériel.

Peer to peer *P to p* *P2P* *PtoP*	Le peer to peer repose sur une idée simple : tous les chaînons d'un réseau agissent d'égal à égal. Alors que les réseaux traditionnels disposent d'une machine serveur sur laquelle se connectent des machines clientes, ceux du P2P ne connaissent pas de hiérarchie : toutes les machines sont à la fois clientes et serveur.
PGP *Pretty Good Privacy*	Se traduit par "assez bonne confidentialité". Il s'agit d'un programme de cryptage de courrier électronique. Logiciel d'encodage de données pour Email, afin d'assurer la confidentialité des messages.
POP *(Point Of Présence)*	Point d'accès internet pour un usager. Protocole d'envoi et de récupération des messages entre le serveur et le client dont la troisième version POP3, est utilisée entre les serveurs de messagerie. Un fournisseur d'accès possède généralement de nombreux POP, ce qui permet la connexion à Internet au tarif local.
Port	Lors d'une connexion à un ordinateur hôte, il est nécessaire de spécifier son adresse mais aussi sont numéro de port qui indique le type de communication utilisé. Celui d'une communication en HTTP est 80. Numéro précédé du symbole : dans certaines adresses. Cet artifice permet de mettre plusieurs serveurs sur une même adresse avec une différenciation par le numéro de port. Les ports sur une machine sont des entrées qui permettent d'échanger des informations dans un sens ou dans un autre avec une autre machine. Chaque port a ses caractéristiques, l'un permet de lire le courrier, l'autre permet de communiquer par ICQ, un autre permet de télécharger des fichiers... Il existe plusieurs centaines de ports différents sur une machine. C'est donc par eux qu'un hacker va pouvoir s'introduire sur un PC. A titre d'exemple, le port 21 est celui du FTP, le port 23 est aussi assez connu puisque c'est celui du telnet et aussi l'entrée favorite de la majorité des troyens (d'où le nom socket 23), le port 25 appelé SMTP permet d'envoyer le courrier et le port 110 (POP) permet de relever celui-ci.

Protocole	Convention précisant un ensemble de règles et de spécifications techniques à respecter dans le domaine des télécommunications. Un protocole est le langage utilisé par les ordinateurs pour communiquer entre eux). Le mot protocole désigne en général les messages échangés entre deux machines. L'intérêt d'un protocole est de définir des méthodes d'échange d'information, indépendantes des matériels. Ainsi une fois le protocole défini, chaque terminal, ou client ou serveur implémente ce protocole sans se soucier des autres ordinateurs.
Provider *(FAI)*	En français : Fournisseur d'accès Internet. Société permettant à des particuliers ou à des entreprise d'utiliser son système de communication pour se connecter et naviguer dans le réseau Internet.
PROXIES *PROXY*	Un grand nombre de prestataires Internet fournissent un accès au réseau par l'intermédiaire d'un serveur proxy. Celui-ci enregistre localement les données souvent appelées sur le réseau afin d'éviter de les rechercher systématiquement sur Internet. Le mode de fonctionnement est relativement simple : le proxy intercepte toutes les demandes du serveur réseau et vérifie si les données recherchées ne se trouvent pas déjà sur son disque dur. Si c'est le cas, il expédie sa propre copie sur l'ordinateur de l'Internaute. S'il ne dispose pas de cette page, il va la rechercher sur le réseau. Il s'agit du proxy cache. Ce dispositif permet d'économiser de la bande passante pour réduire la quantité de données reçues d'Internet. Par ce moyen, il y a une amélioration théorique de la vitesse de transfert. De plus des fournisseurs d'accès ont configuré leur système de telle sorte qu'un accès au réseau n'est possible que par l'intermédiaire d'un proxy. Si celui-ci n'est pas mentionné dans le logiciel de navigation, il ne sera pas possible d'accéder à la page demandée. Dans ce cas, on peut considérer le proxy comme un "serveur relais". Concrètement, le fournisseur d'accès envoie la requête à un serveur Proxy qui la route vers le site demandé.

	Mais dans ce cas, à l'instar de l'utilisation par l'internaute d'un proxy anomyme, le serveur hébergeant le site demandé enregistre les données techniques du proxy qui sont différentes de celles de l'internaute ayant émis la requête initiale, notamment l'adresse IP d'origine. Au reste certains fournisseurs d'accès utilisent un proxy pour effectuer des statistiques très précises sur les habitudes de navigation des Internautes. Les informations obtenues sont alors revendues à des sociétés de marketing. L'inconvénient majeur du proxy réside dans sa capacité à masquer l'adresse IP d'origine des internaute afin de diluer les traces pouvant être recueillies et exploitées par les services d'enquête lorsque le réseau est utilisé à des fins criminelles. Pour rendre anonyme sa présence sur le réseau, l'internaute devra choisir un proxy dont il indiquera les références dans la zone ad hoc du logiciel de navigation. Or, plusieurs milliers de proxies sont disponibles dans le monde. Leur liste est diffusée librement sur Internet. Au reste, le proxy peut être utilisé pour contourner l'éventuel filtrage de l'accès à un site au niveau de l'adresse IP. En matière de sécurité, un proxy peut également protéger contre les intrusions.
Pseudo	Abréviation de pseudonyme. Surnom choisi par l'internaute pour figurer par exemple dans une discussion (" chat ") sur un serveur IRC.
Réexpéditeur anonyme *Anonymat*	Lorsqu'une personne envoie des informations par l'intermédiaire de composants Internet tels que le courrier électronique ou la "grande toile", il est généralement possible d'en identifier la provenance et la destination. Toutefois, les personnes qui postent des images pornographiques aux Newsgroups d'Usenet ou qui envoient directement du matériel d'un ordinateur à un autre ont de plus en plus tendance à accéder à Internet au moyen de certains ordinateurs paramétrés de façon à préserver l'anonymat de l'expéditeur.

	A l'heure actuelle, l'ordinateur le plus utilisé à cette fin est situé en Finlande et répond à l'adresse internet "anon.penet.fi". Il est géré par une personne qui propose ce service gratuitement sur Internet. Toute personne souhaitant dissimuler son identité électronique envoie les informations au réexpéditeur, qui efface l'identité de l'ordinateur d'origine et les expédie à leur destination finale, qui peut être un "groupe de discussion" ou un ordinateur individuel. A la réception, l'adresse d'origine se présente par exemple comme suit : "1234@anon.penet.fi". Le numéro "1234", cité ici à titre d'exemple, correspond au numéro affecté par l'ordinateur réexpéditeur, grâce auquel il devient impossible d'identifier l'ordinateur d'origine. Toutefois, à l'aide du numéro en question, il est possible de renvoyer des informations à l'ordinateur anonyme sans en connaître la position géographique.
Remailer	Serveur spécialisé dans l'expédition anonyme de courriers électroniques et permettant d'envoyer ses messages électroniques sans être identifié.
RNIS *Réseau Numérique à Intégration de Service*	Réseau numérique permettant le transport de services voix, données, images sur la même infrastructure.
Roms	Terme employé pour désigner les jeux de consoles du genre Super nintendo, Nintendo, Game boy, Nintendo 64. Souvent proposé au téléchargement sur Internet sous deux formes de fichiers, les émulateurs et les roms. Les roms sont les fichiers contenus dans les cartouches de jeux, les émulateurs, eux, peuvent lire les roms. Sous l'appellation "ROMS" on désigne ainsi la copie d'un jeu original protégé par les droits des marques et des auteurs.

Serveur	Ordinateur principal d'un réseau hébergeant des ressources (Informations, images, logiciels…) mises à la disposition d'autres ordinateurs par l'intermédiaire d'un réseau. Sur Internet, on trouve des serveurs de tous types : serveurs Web, serveurs FTP, serveurs de noms…) Ils hébergent les données accessibles aux utilisateurs depuis leurs ordinateurs. Ils sont chargés de répondre aux demandes d'autres ordinateurs auxquels ils sont reliés.
Serveur de mail	Serveur spécialisé dans la gestion du courrier électronique. Il abrite les "boîtes aux lettres" des internautes contenant leurs messages. Le serveur de mail d'un internaute est souvent géré par son fournisseur d'accès.
Serveur de news	Ordinateur qui héberge et distribue les newsgroups (forums). Reliés entre eux au moyen du protocole NNTP (Net News Transfer Protocol), les serveurs de news expédient entre eux les nouvelles contributions qui leur parviennent, afin que celles-ci soient visibles de tous, sur tous les serveurs.
Serveur proxy	Assure le stockage des pages Web les plus consultées.
Serveurs de nom DNS *Domain Naming System / Domain Name Server*	Serveurs formant une base de données mondiale destinée au transcodage des adresses de type de type URL (adresses texte) en adresse IP destinataire (adresses numériques).
Serveurs IRC *Internet Relay Chat*	Serveur permettant aux internautes de discuter en direct. Les serveurs IRC comportent des "canaux" thématiques traitant des sujets les plus variés. Les dialogues s'y font exclusivement par l'intermédiaire du clavier. Les serveurs de "chat" sont l'équivalent international des messageries du Minitel.

Signature électronique	Elle fait appel à deux clés. La première est stockée par l'internaute sur un disque dur ou une carte à puce, la seconde est détenue par un tiers de confiance. Pour "signer" un courrier, l'internaute clique sur une icône affichée dans la barre d'outils de sa messagerie.
Site	Serveur ou plusieurs pages Web développées par un particulier, une entreprise, un Etat ou une organisation quelconque puis mis en ligne.
Site Web	Désigne un endroit d'Internet où sont rassemblées des informations (textes, images fixes ou animées, logiciels, etc.) souvent dans un ensemble de pages mises en ligne par un fournisseur de contenu (une entreprise par exemple ou un particulier) sur un serveur et consultables sur l'écran d'un micro via Internet. On se connecte à un site en tapant son adresse (par exemple : yahoo.fr). Le site contient des informations (images, sons, textes) que l'on peut télécharger, c'est à dire installer dans la mémoire de son ordinateur pour les consulter ultérieurement en étant déconnecté.
Smileys	Les Smileys sont des expressions réalisées avec les signes du clavier, pour marquer l'intonation. Par exemple le signe suivant ressemble au visage de quelqu'un qui vous fait un sourire et un clin d'œil ;-) si vous penchez la tête vers la gauche. L'expression de sourieur ou de binette est en vogue au Québec. Les smileys sont employés dans les e-mails, les forums de discussion et les chats.
Spamming ou Spam *Pollution Spam*	Terme anglais qui désigne la pollution des boîtes aux lettres électroniques par des courriers indésirables, généralement publicitaires.

Stéganographie	La stéganographie étudie les techniques pour communiquer de l'information de façon cachée afin de : • contourner la censure et la surveillance ; • protéger ses communications privées là où l'utilisation de la crytographie n'est normalement pas permise ou soulèverait des suspicions ; • contrebalancer toutes les législations ou barrières possibles empêchant l'usage de la cryptographie ; • publier des informations ouvertement mais à l'insu de tous des informations qui pourront ensuite être révélées et dont l'antériorité sera incontestable et vérifiable par tous. La stéganographie vous permettra de cacher un vrai message dans un message anodin ayant pour support un texte, un son, une image un autre support.
Taux de tranfert	Vitesse à laquelle les informations voyagent d'un périphérique de stockage (disque dur, lecteur de CR-Rom ou disquette) vers la mémoire centrale du micro. Il est souvent exprimé en méga-octets par seconde.
TCP/IP *Transmission Control Protocol-Internet*	Il s'agit du couple de protocoles de base le plus important pour Internet. C'est le protocole utilisé pour transmettre les données sur Internet. Ce protocole universel définit le format des données transmises sur Internet ainsi que l'adressage hiérarchique des ordinateurs. Ce protocole permet également de contrôler que les données transmises soient toutes bien reçues par le destinataire. TCP/IP est le nom de la partie cachée de l'Internet. Il existe plusieurs protocoles réseau (Netware, LanManager…). TCP/IP est le plus propice aux interconnexions de réseaux. Il existe beaucoup de réseaux TCP/IP qui ne sont pas reliés à l'Internet.

Téléchargement *Download*	Transfert de fichiers puisés sur un serveur pour être enregistrés sur un ordinateur par l'intermédiaire d'un modem.
URL *Uniform Resource Locator*	Il s'agit de l'adresse spécifique d'un site sur le Web comportant essentiellement le protocole pour l'atteindre, le chemin du répertoire où il se trouve, ainsi que le nom du document. Chaque adresse est unique au monde. La syntaxe d'une URL est : protocole://www.serveur.dns:port/répertoires/fichier?paramètres. • Protocole : nom de la méthode d'accès identifiant le serveur ; • http : pour les URL servis par les serveurs http ; • ftp : pour les fichiers à transférer ; • news : pour les forums de discussion ; • telnet : pour les sessions interactives ; • gopher : pour les serveurs gopher ; • wais : pour les interrogations des bases de données Wais. :// : délimiteur qui est interprété en fonction de la méthode d'accès www. : réservé aux serveurs Web (bien qu'il ne soit pas obligatoire, l'usage veut que les noms des serveurs Web commencent par ces trois lettres). Serveur.dns : identifie le serveur qui contient le document ainsi que le réseau dans lequel se trouve l'ordinateur. Exemple : yaourt.fr désigne le nom du serveur "yaourt" qui se trouve dans le réseau ou DNS fr, c'est à dire en France. Port : c'est un nombre qui caractérise chaque protocole dans le serveur. Par défaut, le nombre 80 est réservé au port du Web. En port standard, vous n'avez pas à l'écrire. Répertoire : c'est le chemin d'accès au document que vous cherchez dans un serveur, comme sur votre ordinateur.

Fichier : est ne nom du document ou de l'application à ouvrir.

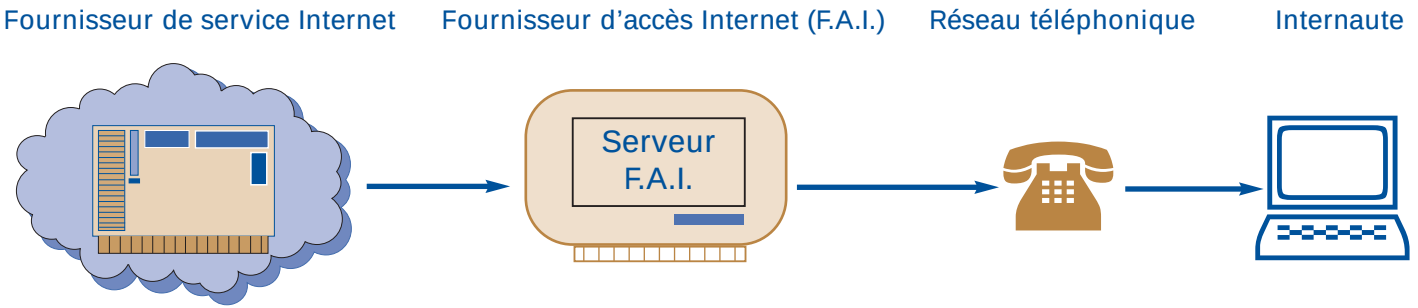
Paramètres : paramètres qui peuvent être passés au serveur Web par le navigateur.
Exemple : imaginez que vous souhaitiez accéder à un document s'appelant "carabosse", écrit en langage HTML, se trouvant sur le répertoire "fee" d'un serveur nommé "recettes" situé en Angleterre.
serveur Web : http://www.
Nom du serveur : recettes.uk
Répertoire : /fee
Fichier : /carabosse.html
Ainsi pour trouver les meilleures recettes de la fée carabosse sur Internet il vous suffit de taper l'URL suivante :
http://www.recettes.uk/fee/carabosse.html

D'autres codes sont également utlisés pour les adresses de personnes morales, tels que :
- co : entreprise
- com : organisme à caractère commercial
- org : organisation
- gov : réseau appartenant aux administrations
- mil : réseau militaire
- edu : institution à caractère éducatif
- ac : institution universitaire
- net : ressources réseaux
- fr : France

Usenet *Users Network*	Sous-ensemble d'Internet, ce réseau est dédié exclusivement aux forums de discussions. C'est le réseau d'échanges des données propre aux groupes de discussions (forums, news-groups). Utilisant le protocole NNTP, le réseau Usenet réunit l'ensemble des serveurs de news disséminés dans le monde.
Virus	Petit logiciel parasite, créer par jeu ou pour saboter. Il se transmet par disquette, CD-Rom, Internet et infecte les programmes ou les fichiers informatiques. Un virus reste indétectable par l'utilisateur tant qu'il n'a pas pas produit son effet, par exemple altérer le fonctionnement d'un logiciel. Certains d'entre eux empêchent même carrément l'ordinateur de fonctionner, alors que d'autres se contentent d'afficher des gags. Voir logiciel antivirus.
Warez	Sites proposant des logiciels piratés ou contrefaits en téléchargement.
Wave	Format de fichier le plus commun sur PC équipés de Windows pour les extraits audio (extension : wav).
Web *World Wide Web*	C'est la partie la plus connue d'Internet. Elle se caractérise par ses serveurs d'informations, consultables au moyen de pages reliées entre elles par des liens hypertextes. Ces pages, appelées pages Web, se composent de textes d'images, de sons, de séquences vidéos, etc. On les consulte par le biais d'un logiciel de navigation.
Whois	Cette commande permet de rechercher des informations à partir d'un numéro de réseau 125.144.78.15, d'un nom de domaine Altern.org, d'un nom de personne LACAMBRE Valentin, dans un des annuaires présent sur le réseau Internet. Cette fonction particulière, disponible en interrogation sur le serveur de l'AFNIC (Association Française de Nommage Internet en Coopération), donne accès aux renseignements minimums mis à la disposition de tous les internautes.

Source : Ministère de la Défense – gendarmerie nationale

SHÉMA TYPE D'UN PROCESSUS D'IDENTIFICATION DE L'AUTEUR D'UNE INFRACTION SUR INTERNET



[1] Ces indications ne sont pertinentes que dans le cas d'un F.A.I. payant ; pour les F.A.I. gratuits, aucune vérification n'étant effectuée lors de la souscription, les renseignements fournis en ligne par l'abonné sont souvent fantaisistes – En tout état de cause, il est nécessaire de croiser les éléments relatifs à l'abonné fourni par le F.A.I. et ceux concernant l'abonné à la ligne téléphonique, la connexion pouvant être effectuée, avec un ordinateur portable par exemple, depuis n'importe quelle ligne téléphonique (pour les connexions par modem).

Source : Ministère de l'Intérieur O.C.L.C.T.I.C.

ANNEXE 2 : L'INTERVENTION DU MINISTÈRE PUBLIC DANS LES PROCÈS CIVILS RELATIFS À INTERNET

1. Le cadre de l'intervention

Ces dernières années, de très nombreuses affaires liées à l'Internet, donnant lieu à une jurisprudence inédite, ont été portées devant le juge civil, en particulier devant le juge des référés. D'où l'intérêt pour le ministère public d'intervenir par les deux voies qui lui sont offertes par le Code de procédure civile.

Le ministère public peut intervenir comme **partie jointe** dans un procès déjà engagé entre les parties pour faire connaître son avis sur l'application de la loi et indiquer au tribunal la solution que, selon lui, devrait recevoir le procès. Le ministère public est partie jointe s'agissant des affaires dont il doit avoir communication (articles 424 et 425 du nouveau Code de procédure civile mais il peut également prendre communication de celles des autres affaires dans lesquelles il estime devoir intervenir (article 426 du nouveau Code de procédure civile). Le parquet présente oralement ses réquisitions à la fin de l'audience ou peut le faire uniquement par écrit en produisant des conclusions.

Le ministère public peut également intervenir comme **partie principale** en déclenchant le procès en tant que demandeur. L'article 423 du nouveau Code de procédure civile lui offre le pouvoir d'intervenir "pour la défense de l'ordre public à l'occasion des faits qui portent atteinte à celui-ci".

L'intervention du parquet, qu'il agisse comme partie jointe ou comme partie principale, peut être justifiée tout particulièrement dans des affaires qui mettent en jeu la dignité de la personne humaine (racisme, antisémitisme, négationnisme, etc).

2. La jurisprudence Yahoo

Tribunal de grande instance de Paris, ordonnance de référé, 20 novembre 2000 : Licra, Union des étudiants juifs de France contre Société Yahoo! Inc. et Société Yahoo France.
L'affaire Yahoo! a opposé plusieurs associations de protection des droits de l'homme aux sociétés Yahoo! Inc. et Yahoo France. Il était reproché à Yahoo ! Inc. de permettre la vente d'objets et d'insignes à la gloire du Troisième *Reich* sur son site d'enchères en ligne. Il lui était également reproché d'héberger différentes pages antisémites issues notamment de *Mein Kampf*.

Par ordonnance du 22 mai 2000, le juge, après avoir relevé que "*l'exposition en vue de leur vente d'objet nazis constituent une contravention à la loi française"* (article 645-2 du Code pénal), ainsi qu'une "*offense à la mémoire collective du pays*" s'est déclaré compétent pour connaître du litige.

Le 20 novembre 2000, le juge des référés du tribunal de grande instance de Paris a rendu une ordonnance enjoignant à l'entreprise américaine 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.*"

L'ordonnance a été rendue sur la base d'un rapport portant sur les possibilités techniques de filtrer l'accès au contenu litigieux pour le public français. Rédigé par trois experts, ce document évoquait plusieurs mesures d'identification de la nationalité des visiteurs dont le taux d'efficacité pouvait varier entre 70 et 90% (ordonnance du 11 août 2000).

ANNEXE 3 : JURISPRUDENCE EN MATIÈRE DE CONTENUS ET COMPORTEMENTS ILLICITES SUR INTERNET

- *Tribunal de Grande Instance de Puteaux, 28 septembre 1999*
  Axa conseil Iard et AXA Conseil Vie contre C.MCS et Société infonie
  Diffamation, responsabilité éditoriale - responsabilité de l'hébergeur (non) - loi du 29 juillet 1881.

- *Cour d'appel de Paris, 11ème chambre, 10 novembre 1999*
  Monsieur D .J contre FCO Fiduciaire
  Diffamation- loi applicable.

- *Tribunal de Grande Instance de Paris, ordonnance de référé, 22 mai 2000*
  Affaire Yahoo ! : licra, Uejf contre société Yahoo !Inc et Société Yahoo France.
  Contenus illicites - négationnisme - loi applicable - juridiction compétente - responsabilité -mesures techniques.

- *Tribunal de Grande Instance de Paris, ordonnance de référé, 20 septembre 2000*
  Sarl One Tel contre SA Multimania
  Diffamation-responsabilité civile -- loi du 1er août 2000 - identification - responsabilité de l'hébergeur (non).

- *Tribunal de Grande Instance de Paris (17ème chambre) 12 octobre 2000*
  Alain B-C Associés-Vienne-Informatique - Internet-hébergeur - Responsablilité (non) Forum de discussion -
  diffusion de messages - site WEB - valeurs juridiques des règles éthiques - Gaz.Pal 14 au 16 octobre 2001 page 56. s

- *Tribunal de Grande Instance de Paris, ordonnance de référé, 20 novembre 2000*
  Affaire Yahoo ! : Licra, UEJF contre société Yahoo ! Inc et société Yahoo France
  Contenus illicites - négationnisme - loi applicable - juridiction compétente - mesures techniques

- *Tribunal de Grande Instance de Paris, ordonnance de référé, 6 février 2001*

  SA Ciriel contre SA Free
  Contrefaçon de marques- diffamation-responsabilité de l'hébergeur.

  Cour de cassation, chambre criminelle, 30 janvier 2001
  Madame A.R. contre Monsieur A.B.
  Diffamation - délai de prescription des délits de presse

- *Cour de cassation, chambre criminelle, 16 octobre 2001*

  Affaire "Marianne" : T.G contre G.B et R.R.
  Diffamation - délai de prescription des délits de presse.

- *Tribunal de Grande Instance de Paris, ordonnance de référé, 30 octobre 2001*

  affaire j'Accuse et a. contre l'AFA, Monsieur D et a.
  contenus illicites - négationnisme-racisme - responsabilité - hébergement étranger - filtrage.

- *Tribunal de Grande Instance de Paris, (17ème chambre) ordonnance de référé, 26 février 2002*

  affaire Yahoo ! Timothy K, Société Yahoo ! Inc contre amicale des déportés d'Auschwitz et des camps de haute Silésie et MRAP - loi applicable - contenus illicites - négationnisme - délais de prescription.

- *Consultation des décisions judiciaires sur les sites suivants :*

  Légifrance.
  http://www.legalis.net

ANNEXE 4 : LES APPORTS DE LA LOI SUR LA SÉCURITÉ QUOTIDIENNE (LSQ) DANS LE TRAITEMENT DES INFRACTIONS JUDICIAIRES COMMISES SUR L'INTERNET

L'article 29 insère dans le Code des postes et télécommunications les articles L 32-3-1 et L 32-3-2 qui disposent que les opérateurs de télécommunications ont une obligation d'effacer ou de rendre anonyme toute donnée technique relative à une communication. Ce principe général connaît deux exceptions qui concernent :
- d'une part, les données techniques nécessaires à la facturation et aux paiement des prestations de télécommunications, permettant la conservation facultative dans la limite de un an qui correspond au délai de prescription prévu par l'article 126 du code des postes et télécommunications ;
- d'autre part, les données techniques susceptibles d'être utilisées pour la recherche, la constatation et la poursuite des infractions pénales, pour une durée maximale d'un an. Elles ne pourront en aucun cas porter sur le contenu des correspondances échangées ou des informations consultée, sous quelque forme que ce soit.

S'agissant de l'Internet cette obligation d'effacement et ses dérogations s'appliquent aux fournisseurs d'accès à l'Internet, sachant que les prestataires d'hébergement sont assujettis, en application de l'article 43-9 de la loi du 30 septembre 1986, dans sa rédaction issue de la loi du 1er août 2000, à l'obligation de détenir et de conserver "les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont (ils) sont prestataires".

Les données techniques concernées au titre de ces deux lois font l'objet d'une définition précise par décret en conseil d'Etat en cours d'élaboration, pris après avis de la CNIL.

L'article 30 introduit dans le Code de procédure pénale les articles 230-1 à 230-5.

Ces articles prévoient la possibilité de mise au clair de données chiffrées nécessaires à la manifestation de la vérité dans le cadre d'une poursuite judiciaire. Il peut ainsi être fait appel aux moyens de déchiffrement de l'Etat couverts par le secret de la défense nationale lorsque la peine encourue est supérieure à deux ans d'emprisonnement. La saisine par l'autorité judiciaire devra être adressée à l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, qui la transmet à un centre technique d'assistance placé sous l'autorité du ministère de l'intérieur (direction de la surveillance du territoire) et qui se charge d'adresser en retour les résultats obtenus à l'autorité judiciaire.

L'article 31 introduit une disposition nouvelle dans la loi de 1991 relative à l'interception des correspondances émises par la voie des télécommunications (art 11-1) et dans le Code pénal (art 434-15-2).
Ces articles prévoient l'obligation de remise des clés de déchiffrement ou leur mise en œuvre d'une part aux agents habilités agissant dans le cadre d'interceptions administratives , d'autre part à l'autorité judiciaire lorsque un moyen de cryptologie est susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit. Cet article fixe les peines encourues en cas de refus de remplir cette obligation.
Les dispositions prévues par les articles 29, 30 et 31 sont applicables et transitoires jusqu'au 31 décembre 2003.

L'article 40 introduit dans le Code monétaire et financier les articles L 163-4-1 et L 163-4-2 qui permettent de poursuivre pénalement certains agissement frauduleux et relatifs aux chèques et aux cartes de paiement commis ou préparés par le biais de l'Internet. Il s'agit de la fabrication, l'acquisition, la détention, la cession, l'offre, la mise à disposition notamment de logiciels permettant de contrefaire ou de falsifier des chèques ou des cartes de paiement. La tentative de commettre ces délits est par ailleurs réprimée et punie des mêmes peines.

ANNEXE 5 : INTERNET, CASINO VIRTUEL ET BLANCHIMENT D'ARGENT[1]

Exemple 1 : Un casino "virtuel" sert à blanchir des fonds générés par un groupe criminel organisé

Les forces de police nationale d'un pays européen (Pays A) enquêtent actuellement sur un casino virtuel sur l'Internet découvert par un service d'étude des services douaniers nationaux ; dans le même temps, l'agence de renseignement financier du pays a reçu une déclaration d'opération suspecte d'une banque qui a fait état de mouvements de fonds importants associés à ce casino virtuel. L'enquête préliminaire a montré que cette activité était gérée par une société du Pays A. Les règles du jeu de ce casino virtuel stipulent qu'il est possible de miser directement en fournissant simplement les coordonnées d'une carte de crédit.

Le site Web du casino virtuel est installé sur un serveur tenu dans la région caraïbe. Pour avoir accès aux services de jeu sur ce site, l'utilisateur doit télécharger une application relais à partir d'un fournisseur d'accès à l'Internet du Pays A. Ce site appartient également à une entreprise du Pays A dont le siège est établi dans la partie méridionale du pays. La personne responsable de la société a effectué un investissement dans une autre société située dans un territoire différent des Caraïbes. Par l'intermédiaire de cette deuxième société, cette personne a acheté un nom de domaine "GAME.COM". Elle a ensuite cédé la propriété de ce nom à une autre entreprise encore établie en Extrême-Orient.

Les services douaniers et la cellule de renseignement financier du Pays A ont mis à jour des mouvements de fonds impliquant plusieurs sociétés et leurs dirigeants. Des mouvements d'espèces sont apparus dans un bureau de change et un centre commercial du Pays A, ainsi que dans plusieurs sociétés d'Extrême-Orient, de la région caraïbe et d'un pays européen voisin (le Pays B). Les liens entre ces diverses entreprises restent néanmoins à établir.

La personne responsable du bureau de change était connue des services de police pour des infractions à la réglementation sur les jeux ; un actionnaire avait été accusé d'avoir participé à une attaque de banque. La société située dans le Pays B faisait aussi l'objet d'une enquête sur les jeux de la part des autorités locales. Selon ces dernières, les casinos virtuels représentent l'une des méthodes de blanchiment de fonds provenant d'activités criminelles dans le Pays B.

[1] *Source : Rapport du GAFI-XII sur les typologies du blanchiment de capitaux (2000-2001)*

A partir de ces renseignements, il a été possible de procéder à une enquête qui a mis en évidence deux opérations illégales au sein de la même société.
La première de ces opérations consistait à produire des composants (cartes-mères) pour exploiter des machines à sou, ce qui est interdit par la législation du Pays A. Les bénéfices générés par cette activité (ventes dans le Pays B) ont été estimées à USD 739 400 pour 1998 d'après les documents saisis dans le Pays A ; les chiffres correspondants n'ont pas été retrouvés dans les documents comptables de la société du Pays B.
La seconde opération, également interdite par la législation du Pays A, était liée à la préparation, la création et l'exploitation d'un casino virtuel sur un site Web dans le Pays et hébergé par un fournisseur d'accès également établi sur son territoire.

Les services douaniers ont mis en évidence cette activité de jeu durant une brève période de 56 jours à la fin de 1998. L'enquête menée par les services de police nationaux du Pays A n'ont pas fait apparaître de période plus longue en raison du transfert du casino vers d'autres sites Web qui n'ont pas été retrouvés.

Au cours de cette période de fonctionnement, 23 joueurs ont pu être identifiés. Ils venaient d'Europe, d'Amérique du Nord et d'Afrique. Il y a eu 170 connexions pour USD 40 300 de mises. L'autorisation de jouer intervenait après vérification de la carte de crédit. Une ligne de crédit était ouverte pour un montant défini.

Les fonds crédités à une société d'un troisième pays européens étaient transférés en Extrême-Orient avant d'être rapatriés dans le Pays A (bureau de change et magasins).

Toutefois, les mouvements de fonds se sont avérés plus importants que ceux qui auraient été générés simplement par des opérations identifiées de jeu. En effet, des fonds sans justification (fausses factures) ont été régulièrement transférés vers le compte d'une autre société encore du Pays A à concurrence de USD 94 000. Un transfert de USD 268 500 au compte du bureau de change a été retransmis en dernier ressort au compte personnel du directeur.

Exemple 2 : USD 178 millions blanchis par un mécanisme de jeux sur l'Internet

Une enquête conjointe des brigades criminelle et financière de la police nationale du Pays C s'est intéressée à un service de pronostics sportifs (SPS) proposant des services de paris au moyen de l'Internet. Ce SPC servait également de fournisseur d'accès à l'Internet (FAI). Le SPS collectait, réunissait et analysais des informations statistiques ou autres ayant trait à des manifestations sportives, avant de vendre ces informations à des abonnés à charge pour eux de les prendre en compte dans leurs paris. Le SPS/FAI visé a développé ses services pour intégrer deux exploitations de jeu extraterritoriales dans la région caraïbe, qui acceptaient des mises via l'Internet ou des numéros de téléphone gratuits. Les agents des brigades ont réussi à infiltrer ce mécanisme.

Pour blanchir le produit de leurs activités illégales de jeu sur l'Internet, les personnes ayant fait l'objet de l'enquête employaient les services d'un avocat. Celui-ci avait mis au point un dispositif complexe dans lequel le SPS louait ses services à ces personnes pour une certaine somme. Les produits étaient également blanchis par l'intermédiaire d'une série de comptes bancaires dans la zone des Caraïbes pour être finalement rapatriés vers des établissements bancaires du Pays C. Les enquêteurs estiment que près de USD 178 millions ont été misés annuellement par l'intermédiaire du SPS/FAI.

Il est prévu que les personnes ayant fait l'objet de l'enquête soient accusés de jeux illégaux, blanchiment de capitaux, fraude fiscale et autres infractions relatives à la criminalité organisée.

Exemple 3 : Utilisation d'une proche ressemblance pour dissimuler une opération de blanchiment

L'expérience de la cellule de renseignement financier du Pays D montre que le mécanisme suivant est fréquemment utilisé par des criminels opérant dans ce pays.

Un individu du Pays D déclare une société de jeu, la "Gamblerz.com" dans le Pays E où le nom de la société est très voisin de celui d'une société de jeu du Pays F - "Gamblers.com" qui opère légalement et qui a obtenu une licence d'exploitation. Par la suite, un site Web destiné à diffuser des informations sur le jeu est créé dans le Pays G sous le nom de "Gambler.com" qui est lui-même un raccourci et qui est commun aux deux sociétés. Un compte est ensuite ouvert dans le Pays H et des milliers de personnes du Pays J transfèrent des sommes sur ce compte. Le criminel peut opérer avec les fonds détenus sur ledit compte à l'aide d'un modem.

Grâce à son modem, l'individu retire USD 1 million du compte qu'il détient auprès de la banque RECORD. Les activités se poursuivent durant plusieurs mois, mais aucune licence n'est délivrée. Dès que la banque commence à s'interroger sur les transactions, l'individu qui a monté l'opération (un homme) contacte la banque par téléphone. Plus tard, une autre personne (une femme) fournit les documents demandés par la banque ; toutefois, ces documents ne semblent pas authentiques et on peut y déceler des marques de contrefaçon.

La banque gèle le compte et fait une déclaration à la cellule de renseignement financier qui prend les mesures nécessaires pour préparer la documentation à l'intention de la police. Comme la détermination du pays dans lequel l'infraction pénale a été commise pose un problème, le Pays J ouvre une procédure pénale et lance une enquête pénale pour protéger ses propres ressortissants qui semblent être victimes de l'opération.

ANNEXE 6 : INTERNET ET SECTE

Internet peut être utilisé par les groupes sectaires pour exercer des pressions sur leurs adeptes ou détracteurs.

1.- Par ce moyen moderne, ils captent l'internaute, en lui offrant différents produits, services afin d'améliorer son bien-être spirituel, physique ou autres...
En outre, les causes humanitaires, la lutte contre la toxicomanie, l'écologie... valeurs reconnues par tous, sont un outil de propagande pour les groupes scectaires, facilitant le recrutement d'un adepte.

2.- des réseaux de mobilisation, des groupes de discussion ont été initiés également par les sectes, afin notammment de dénoncer la politique de l'État en matière de lutte contre les agissements des mouvements sectaires.
À ce titre, il peut être relevé un nombre croissant d'actions en diffamation, via le net.
Des procédures des chefs d'escroqueries, fraude informatique et publicité mensongère. Ils ont déjà été initiées.

3.- Les associations de défense contre les sectes ainsi que certains de leurs membres, voire d'ex-adeptes ont réagi en créant leur propre site, afin de dénoncer la nocivité des mouvements sectaires.

Contact à la Direction des Affaires criminelles et des grâces chargée de mission des questions relatives aux sectes :
Mme Marie-Josée AUBE-LOTTE tél : 01 44 77 60 60

MILS
Mission Interministérielle de Lutte contre les Sectes
66, rue de Bellechasse 75007 Paris
Téléphone : 01 42 75 76 08

ANNEXE 7 : PROCÈS VERBAL

DESTINATAIRE

PARQUET DE PARIS

REFERENCE DU DESTINATAIRE

REMPLIR AU DESTINATAIRE

REPUBLIQUE FRANCAISE

PREFECTURE DE POLICE

DIRECTION
de la
JUDICIAIRE

Brigade de Protection des Mineurs
12 quai de Gesvres
75004 PARIS

Réa N°

PROCES - VERBAL

L'an deux mille un

Le

à heures

Nous,

Capitaine de Police

Officier de Police Judiciaire en fonction à Paris,
— Etant en service, —
— Poursuivant l'enquête préliminaire, —
— Vu les articles 14, 75 et suivants du modifié CPP, —
— Vu l'article 43-9 de la loi du 30/9/86 modifiée par la loi du 01/08/2000, —
— PRIONS et au besoin REQUERONS Monsieur le directeur de « nom du fournisseur d'accès ou de services » de bien vouloir nous communiquer tous renseignements permettant d'identifier :
- le titulaire de l'adresse électronique xxx@yyy.fr
ou
- l'abonné qui était connecté à Internet le (date et heure précise) avec l'adresse IP 195.123.56.187
ou
- l'abonné ayant mis en ligne le site situé à l'adresse universelle http://xxx.yyy.fr
et notamment :

Pour un fournisseur de service (adresse électronique, hébergement)
- formulaire d'inscription en ligne rempli par l'abonné
- adresse IP date et heure d'envoi de ce formulaire
- adresse IP, date et heure de chaque accès au service (logs de connexion pour une adresse électronique, logs FTP pour site Web)
- moyens de paiement éventuels

Pour un fournisseur d'accès à internet
- nom, prénom, adresse, téléphone déclaré et tout autre renseignement d'état-civil en sa possession
- login, date et heure du début et de fin de connexion (nécessaire en cas de recherche France télécom pour retrouver le numéro appelant en cas de connexion RTC)
- numéro appelant pour cette session (s'il n'a pas été caché par l'abonné : 3651 en secret permanent)
- adresses électroniques, pages web personnelles associées à ce login
- moyen de paiement éventuels

Vu l'urgence, il conviendra de nous faire la réponse au .... ou nous l'envoyer par courrier électronique à l'adresse ....
— Dont procès-verbal, —

Le Capitaine de Police

VU et TRANSMIS

Le

Le Commissaire de Police

Chef de Service

ANNEXE 9 : FORMATIONS ECOLE NATIONALE DE LA MAGISTRATURE

◗ Théorie et pratique de l'Internet

Ce module doit permettre aux magistrats d'allier l'approche théorique et la pratique personnelle de l'Internet : des ateliers entrecouperont les exposés-discussions et permettront une découverte concrète de cette nouvelle technique de communication. A la fin du stage, le magistrat aura la capacité d'utiliser personnellement l'Internet de manière pertinente.

Deux sessions sont organisées : une d'initiation, l'autre de perfectionnement.

• Initiation

Cette session est destinée aux magistrats qui n'ont aucune pratique de l'Internet ou débutent sur le réseau.

Elle nécessite, pour être efficace, que le magistrat soit déjà connecté à l'Internet ou en voie de l'être dans les deux mois qui suivent le stage. Elle commence par une approche de la connaissance et de la maîtrise du système d'exploitation Windows (version 95 ou 98). Les participants apprendront les bases essentielles de la navigation sur les sites Web, des téléchargements, de la messagerie électronique. Ils appréhenderont les notions indispensables aux premières connexions. Une démonstration complète de l'Intranet du ministère de la Justice est également au programme du stage. Enfin, sera présenté l'apport d'une autre nouvelle technologie : la dictée électronique.

Sur le plan méthodologique, cette formation associe les exercices pratiques et les conférences théoriques. Elle permet à chaque participant d'expérimenter lui-même sur ordinateur les informations données.

Lieu : E.N.M Bordeaux
Dates : 8 demi-journées du 11 au 15 février
Public : 22 magistrats souhaitant s'initier à l'Internet et disposant d'un micro-ordinateur connecté à l'Internet.

• Perfectionnement

Ce stage est destiné aux magistrats qui ont une connaissance correcte de Windows et des bases Internet et qui souhaitent renforcer leurs maîtrises sur logiciels de l'Internet (paramétrages, techniques de recherche documentaire, recours aux logiciels d'initiation à la conception d'un site Web).

Comme le stage d'initiation, il alterne les exercices pratiques et les conférences théoriques, permet de mieux cerner les enjeux organisationnels,, sécuritaires et sociaux de l'Internet.

Lieu : E.N.M Bordeaux
Dates : 8 demi-journées
Public : 22 magistrats, connaissant déjà l'Internet et voulant se perfectionner.

◗ Formation de référents Internet

Sans prétendre créer une nouvelle fonction au sein des juridictions, ce stage est destiné à des utilisateurs aguerris de l'Internet, volontaires et suffisamment disponibles pour faire profiter leur environnement professionnel de leur expérience et de leurs compétences.

Il comportera une réflexion en commun étayée de l'expérience d'un spécialiste de la pédagogie, sur les techniques à mettre en oeuvre pour former des utilisateurs à l'Internet, les aider à configurer leurs ordinateurs et leurs logiciels, les assister en cas de "plantage", les soutenir dans leur apprentissage personnel.

Il se propose en second lieu de fournir les bases pour concevoir, réaliser et assurer la maintenance de petits sites web locaux.

Il proposera enfin un approfondissement de la réflexion et un effort d'anticipation sur l'évolution de la communication électronique de groupe au sein des juridictions, à l'échelon local, régional ou national et ses répercussions sur l'organisation du travail juridictionnel.

Des outils logiciels et documentaires seront fournis aux stagiaires.

Lieu : Nantes (dans les locaux du casier judiciaire)
Date : 25 au 29 mars
Public : 7 magistrats, 7 fonctionnaires, passionnés et utilisateurs confirmés d'Internet.

◗ Criminalité organisée et évolution de ses manifestations : blanchiment, immigration clandestine, cybercriminalité

On constate, depuis plusieurs années, la spectaculaire montée en puissance des principaux groupes relevant de la criminalité transnationale dans le monde (mafias d'origine italienne, cartels colombiens, yakusas japonais, triades chinoises, "mafias" russes, pour ne citer que les plus importantes).

Les profits réalisés par ces groupes, notamment grâce au trafic de stupéfiants, constituent un instrument particulièrement puissant de criminalisation de l'économie et de corruption. Les profits réalisés sont tels qu'ils permettent de mettre en place d'importants dispositifs de corruption tant au niveau d'appareils institutionnels que de décideurs privés.

Cette session devrait permettre :

- de mieux appréhender ces phénomènes et leurs conséquences sur le plan national et international,
- d'envisager les réponses possibles, à la fois en termes de prévention et de répression : incriminations spécifiques (dispositifs législatifs ou conventionnels), mécanismes institutionnels de lutte (coopération policière et judiciaire...).

Lieu : Saint-Cyr au Mont d'Or (ENSP)
Dates : 11 au 15 mars
Public : spécialisé - 50 participants : 20 E.N.M - 20 commissaires de police, 10 officiers de gendarmerie

Internet et les atteintes à la dignité humaine

Le développement de l'Internet contribue à faciliter la commission d'infractions portant atteinte à la dignité humaine, tels les faits de pédophilie, les réseaux de prostitution, les manifestations de racisme ou bien encore la proposition de vente d'objets dont le commerce est normalement interdit ou strictement réglementé. L'anonymat, le caractère international de ces nouvelles technologies a favorisé l'éclosion de pratiques répréhensibles. Mais la rapidité avec laquelle les "réseaux Internet" se sont constitués puis développés, souvent selon des modalités difficilement contrôlables rend difficile le travail des officiers de police et des magistrats.

La session proposera une présentation des différentes techniques pour améliorer le traitement des procédures dans un domaine où la conduite des enquêtes est souvent complexe à mener en raison notamment de leur caractère international. Une présentation de la législation tant nationale qu'européenne sera effectuée associant des professionnels de l'Internet, des représentants de l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, d'Interpol et d'Europol.

Lieu : E.N.M Paris
Durée : 10 au 13 septembre 2002
Public : 50 participants (20 magistrats, 12 policiers, 13 gendarmes, 5 ENG).

Annexe 10 : Le site gouvernemental de signalement des sites illicites

Ce site, https://www.internet-mineurs.gouv.fr, mis en ligne en novembre 2001, propose aux internautes un formulaire de signalement en ligne et une adresse e-mail.
L'Office Central de lutte contre la criminalité liée aux technologies de l'information et de la communication est chargée de la gestion de la base de données alimentée par les signalements transmis en ligne par l'intermédiaire de ce site.

Grâce à un partenariat interministériel associant avec les ministères de la justice, de l'intérieur, de la défense et du ministère délégué à la famille, ce point de contact a été mis en œuvre par arrêté ministériel le 8 novembre 2001. Il a pour finalité de recevoir les signalements émanant de particuliers qui auraient détectés des sites, des forums ou des chats dont le contenu à un caractère pédopornographique.

Un groupe de l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication gère la base de données des signalements, procède aux premières vérifications et adresse le dossier technique soit au bureau central national d'Interpol du lieu ou l'infraction est censée avoir été commise soit aux autorités judiciaires françaises localement compétentes à charge pour elles de saisir un service d'enquête de la police ou de la gendarmerie nationales afin de poursuivre les investigations.

Tout internaute qui trouve sur un site Internet ou un service en ligne (e-mails, news-groupes…) des contenus ayant un caractère pédophile peut désormais le faire savoir immédiatement en remplissant un formulaire en ligne (l'anonymat pouvant être conservé).

Ce site propose en outre :

- Des conseils aux parents et aux enfants sur l'utilisation d'Internet ;
- Une information sur l'ensemble des législations française et internationale en matière de crimes et délits à caractère sexuel sur mineurs par le réseau Internet ;
- Une présentation des différents organismes nationaux et internationaux de protection de l'enfance.

ANNEXE 11 : SITES D'INFORMATIONS RELATIFS AU DROIT ET NOUVELLES TECHNOLOGIES

- Commission nationale de l'informatique et des libertés CNIL
  http://www.cnil.fr
- Forum des droits sur l'Internet
  http://www.foruminternet.org
- Agence pour les technologies de l'information et de la communication dans l'administration – ATICA
  http://www.atica.pm.gouv.fr
- Direction centrale de la sécurité des systèmes d'information – Secrétariat général de la défense nationale – SCSSI
  http://www.ssi.gouv.fr
- Direction du développement des médias
  site portail de l'action gouvernemental pour la société de l'information
  http://www.internet.gouv.fr
- Mission interministérielle pour l'accès public à la micro-informatique, à l'internet et au multimédia
  http://www.accespublics.premier-ministre.gouv.fr
- Juriscom.net
  http://www.juriscom.net
- Conseil de l'Europe
  http://www.coe.int

Ce guide a été réalisé par la Direction des Affaires criminelles et des Grâces

- *Sous Direction de la justice Pénale générale*
  - *Bureau des politiques pénales et de la protection des libertés individuelles :*
    Madame Myriam Quemener, chef du bureau,
    Monsieur Matthieu Bourrette, MACJ,
- *Sous Direction de la justice Pénale spécialisée*
  Monsieur Gilles Sorba, lieutenant Colonel de gendarmerie, cadre spécialisé (D.A.C.G.) ;

et le service de l'Information et de la Communication du ministère de la Justice (SICOM)

avec la collaboration :

- *des Officiers de liaison Intérieur et défense : Madame Lilianne Leymarie, Commissaire divisionnaire et Monsieur le Colonel de gendarmerie Richard Alexandre ;*
- *du Service des Affaires Européennes et Internationales (SAEI) : Madame Sonya Djemni -Wagner, magistrat en charge des questions liées aux nouvelles technologies de l'information et de la communication ;*
- *de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la Communication : Madame Catherine Chambon, chef de service. Monsieur Daniel Bertinet adjoint au chef de service ; Monsieur Joël Ferry, Lieutenant-colonel, chargé de mission à (L'OCLCLTIC),*
- *Institut de Recherches Criminelles de la Gendarmerie Nationale : Capitaine Eric Freyssinet*
- *du Service Technique de Recherches Judiciaire et de Documentation de la Direction Générale de la Gendarmerie Nationale : adjudant Toussaint ;*
- *Monsieur Bruno Nedellec, magistrat détaché au Ministère des Affaires Etrangères ;*
- *de Madame Nicole Tricart, commissaire Divisionnaire, responsable de la brigade des Mineurs de Paris ;*
- *de Monsieur Fabrice Gauthier, capitaine de police, Brigade des Mineurs de Paris ;*
- *de la Direction de la Protection Judiciaire de la Jeunesse.(Bureau K2) ;*
- *de Monsieur Christian Boucard, Directeur adjoint des Douanes, cadre spécialisé ;*
- *de Madame Marie-José Aube-Lotte, chargée de mission pour les questions relatives aux sectes (D.A.C.G.) ;*
- *de Monsieur Rodolphe Uguen, rédacteur au Bureau de la criminalité (D.A.C.G.).*