CHANTIER SUR LA LUTTE

CONTRE LA

CYBERCRIMINALITE

Rapport présenté par Thierry BRETON

Remis à Monsieur le Ministre de l'Intérieur,

de la Sécurité intérieure et des Libertés Locales

le 25 février 2005

Suite à une lettre de mission en date

du 29 juin 2004

Le développement des nouvelles technologies de l'information ouvre un nouvel espace. L'espace "informationnel" vient désormais s'ajouter aux espaces terrestre, maritime et aérien, dont la protection et la sécurité entrent naturellement dans le champ des compétences régaliennes de l'Etat. Espace virtuel, par sa structure et la nature même des informations qu'il véhicule, le cyberespace a des incidences concrètes sur la vie quotidienne, notamment en ce qui concerne l'accès à la connaissance, les communications entre les personnes, le commerce, l'exercice de la citoyenneté (vote électronique), l'administration ou le travail en ligne.
Toute activité, toute invention humaine porteuse de progrès, peut être aussi génératrice de comportements illicites. La cybercriminalité est l'une des nouvelles formes de criminalité et de délinquance, dont les conséquences peuvent être particulièrement graves pour notre sécurité collective, pour notre économie et, bien sûr, pour les citoyens qui peuvent être personnellement atteints, dans leur personne, dans leur dignité et dans leur patrimoine. Le caractère virtuel des échanges qui débutent sur Internet favorise le franchissement des barrières de l'illégalité, les internautes ayant le sentiment que les bornes morales ou légales de la vie réelle ne s'appliquent pas au cyberespace, ce dernier leur paraissant totalement "désincarné".

La cybercriminalité est un nouveau domaine pour le droit pénal et la procédure pénale. Elle recouvre deux grandes catégories d'infractions :

⇨ les infractions directement liées aux technologies de l'information et de la communication ;
⇨ celles dont la commission a été facilitée ou liée à l'utilisation de ces technologies.

La première catégorie comprend :

⇨ les atteintes aux systèmes de traitement automatisé de données (S.T.A.D) ;
⇨ la diffusion de programmes permettant de commettre une atteinte à un S.T.A.D ;
⇨ les infractions à la loi Informatique et liberté sur la protection des données personnelles ;
⇨ les infractions aux cartes de paiements, dont la diffusion de programmes permettant de fabriquer de fausses cartes de paiement ;
⇨ les infractions à la législation sur la cryptologie.

La seconde catégorie recouvre :

⇨ la diffusion de contenus illicites (pédopornographie, racisme, antisémitisme, etc.) ;

⇨ les escroqueries par utilisation frauduleuse de numéro de carte bancaire pour une transaction en ligne ;

⇨ les escroqueries par fausse vente sur un site d'enchères en ligne ;

⇨ les contrefaçons de logiciels ou d'œuvres audiovisuelles.

Dans cette deuxième catégorie il faut mentionner les infractions sexuelles, et plus particulièrement pédophiles, pour lesquelles Internet permet aux agresseurs « prédateurs » de rentrer en contact avec leurs victimes et de les « séduire » : corruption de mineurs, agressions sexuelles, atteintes sexuelles sur mineur, voire viol ou proxénétisme. Il s'agit d'ailleurs d'infractions pénales pour lesquelles Internet est une circonstance aggravante[1].

Le tableau annexé récapitule les principales infractions énoncées ci-dessus.

L'émergence d'un corpus législatif et réglementaire

Depuis la loi Informatique et libertés (1978), la législation française a pris en compte la problématique de la cybercriminalité avec la loi du 5 janvier 1988[2], dite « loi Godfrain », la loi du 15 novembre 2001[3] relative à la sécurité quotidienne, la loi du 18 mars 2003[4] pour la sécurité intérieure, la loi du 9 mars 2004[5] portant adaptation de la justice aux évolutions de la criminalité et, très récemment, la loi du 21 juin 2004[6] pour la confiance dans l'économie numérique et la loi du 9 juillet 2004[7] relative aux communications électroniques et aux services de communication audiovisuelle. Cet important dispositif législatif est complété par des textes réglementaires en cours d'élaboration, qu'il s'agisse du projet de décret sur la conservation des données de communications électroniques[8] ou du projet de décret sur la conservation des données relatives aux contenus des services en ligne[9].

La dimension internationale de la cybercriminalité

La communauté internationale a pris conscience des enjeux liés au développement des technologies numériques, notamment au travers de la Convention du Conseil de l'Europe sur la cybercriminalité (23 novembre 2001) et de son protocole additionnel (7 novembre 2002[10]), en cours d'approbation par

---

[1] Art. 227-22, 227-5, 227-26, 227-28, 227-24, 225-12-1 et 2 du code pénal.

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

[3] Loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne.

[4] Loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure.

[5] Loi n°2004-204 du 3 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.

[6] Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

[7] Loi n°2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle.

[8] En application de l'art. 29 de la loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, devenu art. 34 de loi n°2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle.

[9] En application de l'art.6 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

[10] Protocole additionnel à la convention sur la cybercriminalité relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques.

le Parlement[11]. Les dispositions contenues dans ces deux textes sont déjà intégrées dans le droit français. Il en est de même de la directive européenne 2000/31 du 8 juin 2000[12] relative au commerce électronique, transposée en droit français par la loi pour la confiance dans l'économie numérique, et qui précise notamment la responsabilité des hébergeurs. Il convient aussi d'ajouter les travaux accomplis au sein du G8, d'EUROPOL ou du groupe de travail sur la criminalité liée aux technologies de l'information d'INTERPOL. Un projet de décision cadre a été déposé le 28 avril 2004 par la France ainsi que par l'Irlande, la Suède et le Royaume-Uni sur la rétention des données de trafic[13].
Les sources internationales du droit soulignent bien la nécessité d'une approche transfrontalière de la cybercriminalité qui, par construction, ne connaît pas de frontières.

La prise en compte de la cybercriminalité par la police et la gendarmerie

La France n'est pas restée inactive, tant sur la scène internationale où elle joue un rôle moteur que sur le plan interne. La police et la gendarmerie ont pris conscience des nouvelles menaces liées au cyberespace. Pour ces deux institutions, la cybercriminalité constitue déjà aujourd'hui et sera demain davantage encore un champ d'action renouvelé et ouvert. Hier, marginale dans ses manifestations, elle représente la nouvelle forme de criminalité du XXIe siècle. Elle a joué un rôle déterminant dans les derniers attentats terroristes les plus meurtriers, comme celui de Madrid.
En mai 2000, l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC) a été créé au sein la Direction centrale de la Police judiciaire au ministère de l'intérieur afin de mieux lutter contre cette criminalité. Ce service de police judiciaire à vocation interministérielle comprend des policiers et des gendarmes qui mettent en commun leurs compétences pour lutter contre ce fléau. La Direction de la surveillance du territoire, compétente pour diligenter des enquêtes judiciaires relatives à des actes de piratage sur les systèmes informatiques des établissements à régime restrictif ou des données classifiées de défense, intervient de manière complémentaire à l'action de l'OCLCTIC. La Division nationale de répression des atteintes aux personnes et aux biens (DNRAPB) a pris en charge depuis 1997 le traitement des atteintes aux mineurs victimes et des infractions à la loi sur la presse liées au cyberespace. Dès 1998, la gendarmerie a créé le département de lutte contre la cybercriminalité au sein du service technique de recherches judiciaires et de documentation (STRJD).
La police technique et scientifique a développé son savoir-faire, du côté de la police comme de la gendarmerie, ainsi qu'en témoignent les capacités que mettent en œuvre la division criminalistique "ingénierie et numérique" de l'Institut de recherche criminelle de la gendarmerie (IRCGN) et les services de la

[11] Trois membres du groupe de travail ont été entendus, le 24 novembre 2004, par M. NESME, député, rapporteur du projet de loi.
[12] Directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur.
[13] Texte n° E 2616.

sous-direction de la police technique et scientifique de la police judiciaire basés à Ecully.
Des enquêteurs spécialisés ont été formés, des services ou unités ont acquis une solide expérience et obtenu des résultats tangibles. C'est le cas notamment du groupe Internet de la Brigade de Protection des Mineurs (BPM) et de la Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI) de la Préfecture de police de Paris, des directions interrégionales de police judiciaire (DIPJ) ou bien encore des sections et brigades de recherches de gendarmerie dotées progressivement d'enquêteurs spécialisés. Une veille des contenus illicites véhiculés sur Internet a été mise en œuvre au Service technique de recherche judiciaire et de documentation de la gendarmerie (STRJD) ou au sein de la police nationale.
La riposte s'est construite par touches successives, parfois de façon empirique, souvent de manière accélérée au gré de l'utilisation des technologies numériques par la criminalité organisée ou pour la commission d'actes terroristes. Il faut désormais prendre acte de la révolution technologique en changeant d'échelle dans l'organisation, les moyens, les modes d'action.
Concevoir et mettre en œuvre une posture plus offensive, c'est d'abord mieux organiser les synergies entre la police, la gendarmerie et les autres composantes de la sécurité intérieure. C'est aussi développer les coopérations techniques, juridiques avec toutes les institutions, les entreprises, les organismes publics ou privés qui agissent, chacun dans son domaine, contre la cybercriminalité. S'ajoute, bien évidemment, la coopération internationale, car les technologies numériques ne connaissent pas de frontière.
Le contenu du chantier est complexe au regard des technologies concernées, de la pluralité des intervenants publics ou privés, nationaux ou internationaux, et des aspects juridiques qui lui sont propres.
Le ministre de l'intérieur, de la sécurité intérieure et des libertés locales a validé les six premières propositions émises par le groupe de travail[14], lors d'un déplacement au sein des services spécialisés la police et de la gendarmerie, le 7 septembre 2004. Ce rapport en rappelle le dispositif et contient de nouvelles propositions.

1. Une meilleure connaissance statistique de la cybercriminalité

Les chiffres présentés ci-après sont le fruit d'une collecte effectuée par l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) auprès des services de police et de gendarmerie. Plus que leur volume brut, c'est leur forte variation qui souligne les enjeux.

[14] Propositions 1à 5 et 6.1

Infractions spécifiques aux technologies de l'information et de la communication

	2003	Variation N-1
Atteintes au système (piratage)	1280	+ 9%
Diffusions de programmes informatiques permettant de fabriquer de fausses cartes bancaires	792	+ 149 %
Infractions "informatique et liberté"	37	+ 48 %
Falsifications et usages de cartes de crédits[15]	50138	+10,64%

source OCLCTIC

Infractions dont la commission est facilitée par l'utilisation des technologies de l'information et de la communication

	2003	Variation N-1
Escroqueries par utilisation de numéro de carte bancaire	12214	+ 34,6 %
Diffusion d'images de pédopornographie sur Internet	464	+ 22,4 %
Infractions à la loi sur la presse (incitation à la haine raciale, diffamation, négationnisme) sur Internet	156	+ 6 %

Source OCLCTIC

Cette délinquance ne fait pas l'objet d'une analyse précise : le "chiffre noir" (infractions commises mais non portées à la connaissance des forces de police ou de gendarmerie) est particulièrement important et les outils statistiques utilisés ne sont toujours pas adaptés.

⇨Le "chiffre noir" demeure important car nombre de victimes ne se font pas connaître, soit parce qu'elles n'ont pas pris conscience du préjudice subi, soit parce qu'elles craignent que la dénonciation auprès des services de police ou de gendarmerie ait des effets négatifs sur leur image (cas des entreprises victimes de piratage de leurs réseaux).

⇨La nomenclature des infractions (état "4001") retrace les crimes et délits constatés par la police et la gendarmerie. Elle comporte 107 index. Les index 106 (autres délits économiques et financiers) et 107 (autres délits) intègrent indistinctement ces délits nouveaux. Certaines infractions sont bien identifiées dans l'état 4001, mais l'utilisation de technologies numériques pour leur commission n'est pas mise en évidence dans les statistiques (par exemple, escroqueries, fraudes). Les évolutions dans les moyens d'opérer[16], quant à elles, ne figurent pas dans les rubriques de l'état 4001.

Pour mieux agir, il est impératif de mieux identifier les contours quantitatifs de la cybercriminalité.

[15] Extraction de l'index 90 de l'état 4001.

[16] À l'exception de l'index 90 regroupant la falsification et l'usage de cartes de crédit.

Les grandes applications informatiques que développent actuellement la police nationale (STIC-Ardoise) et la gendarmerie nationale (PULSAR) permettront prochainement une connaissance précise de la cybercriminalité constatée par leurs unités et services. Conformément aux décisions annoncées par M. de VILLEPIN, le 14 janvier 2005, le rapprochement de STIC et de JUDEX se fera à l'horizon 2006 sous forme d'un portail commun de consultation de ces deux bases.
Sans attendre, les mesures suivantes sont prises depuis le 1er janvier 2005 :

- la gendarmerie place dans les messages d'information statistique (MIS) un nouvel indicateur de lieu, dénommé "cyberespace", qui est indexé lorsqu'une infraction est directement liée aux technologies de l'information et de la communication, dont Internet ; cette technique permet d'identifier dans l'état 4001 les infractions relevant de la cybercriminalité par tri sur le lieu ; la base MIJ (message d'information judiciaire) permet un éclairage plus précis pour les affaires présentant un caractère particulier ;
- la police nationale s'appuie sur l'enrichissement des procédures effectué sur la base opérationnelle du STIC, à partir d'une table de concordance entre un thesaurus d'infractions et les index de l'état 4001. L'extraction se fait par requête spécifique, grâce au logiciel "*Business Object*" ; cette méthode permet une remontée des données statistiques par nature d'infraction ; il est ensuite possible de reconstituer la part de la cybercriminalité dans chacun des 107 index concernés ; chaque semestre, la DCPJ produira des statistiques communes.

En concertation avec l'Observatoire national de la délinquance (OND), des questions relatives à la cybercriminalité seront introduites dans l'enquête de victimation "2006" que cet organisme est chargé de concevoir.

Ainsi, pourra-t-on à court terme, mieux connaître la « cartographie » de la cybercriminalité.

2. Un doublement des capacités d'investigation spécialisées des services de police et des unités de gendarmerie

2.1. le renforcement de l'OCLCTIC

Le renforcement des effectifs spécialisés concerne tout d'abord l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC). Ce service de police judiciaire, au centre du dispositif, est le point de contact national en matière de lutte contre la cybercriminalité. Composé actuellement de 32 fonctionnaires de police et de 3 militaires de la gendarmerie, cet office central de police judiciaire verra son effectif doubler d'ici à 2008, avec une participation plus importante de la gendarmerie. La création en son sein d'un pôle unique de signalement (voir infra proposition n° 6.2), composé de manière paritaire de policiers et de gendarmes, s'ajoute à ce renforcement déjà annoncé.

2.2. Le doublement du nombre des enquêteurs spécialisés

L'objectif est de disposer de 310 enquêteurs hautement spécialisés d'ici à 2007. Les capacités d'investigation des services et unités spécialisées seront également accrues. Cette mesure concerne également les services spécialisés de la DST et la DNRAPB.
Les groupes d'enquêteurs spécialisés en criminalité informatique au sein de chaque direction régionale et interrégionale de la Police Judiciaire seront dotés en personnels supplémentaires.
De son côté, la gendarmerie renforcera par une vingtaine de spécialistes ses services dédiés à la lutte contre la cybercriminalité au sein de l'Institut de recherche criminelle (IRCGN) et du Service technique de recherche judiciaire et de documentation (STRJD). Les sections de recherche de gendarmerie verront également augmenter leur nombre d'enquêteurs spécialisés, certaines d'entre elles ayant un rôle plus marqué dans la lutte contre la cybercriminalité.

2.3. La mise en place de référents

Les enquêteurs de terrain devront pouvoir bénéficier de conseils et d'assistance de « proximité » afin d'obtenir une aide technique pour leurs constatations, la préservation des preuves, les actes à accomplir.
A cette fin, des policiers référents seront formés au sein de chaque sûreté départementale de la sécurité publique. Ils pourront traiter les enquêtes et bénéficier en cas de besoin de l'aide de fonctionnaires plus spécialisés.
Des personnels spécialisés, affectés au sein des brigades départementales de recherche et d'investigation judiciaire de la gendarmerie (BDRIJ), assisteront les enquêteurs des brigades territoriales et des unités de recherches dans la conduite des enquêtes impliquant l'utilisation de technologies numériques.

Au total, les effectifs spécialisés dans la lutte contre la cybercriminalité passeront de 300 environ (situation actuelle) à plus de 600 au terme de la LOPSI (loi d'orientation et de programmation pour la sécurité intérieure 2003-2007).

3. Le développement d'actions de formation communes

Les actions communes de formation continue et d'information des enquêteurs spécialisés de la police et de la gendarmerie, déjà initiées, seront développées pour favoriser les partages d'expériences. Cette formation hautement spécialisée fera notamment appel à des intervenants extérieurs, en particulier aux fournisseurs d'accès à Internet.

3.1. Un séminaire annuel commun

Pérennisant les initiatives passées, un séminaire, animé conjointement par la police judiciaire et la gendarmerie nationale, réunira chaque année une centaine d'enquêteurs spécialisés (ESCI et N-TECH). Ce séminaire (le prochain organisé à la fin du mois de juin 2005) reposera sur des ateliers pratiques et interactifs au travers de "scènes de crime informatique". A cette occasion, les opérateurs et fournisseurs d'accès seront sollicités pour présenter leur organisation, leurs matériels de communication et leur dispositif en matière de sécurité et de systèmes d'exploitation.

3.2. L’organisation de journées thématiques

Des journées thématiques de haut niveau seront organisées pour les enquêteurs spécialisés par l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), le Centre national de formation de la police judiciaire (CNFPJ) et l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN). Il s'agira d'approfondir des sujets particuliers : problématique des liaisons sans fil, connaissances juridiques sur les communications électroniques, etc.

3.3. Un Forum commun aux enquêteurs

Un forum Internet commun aux enquêteurs spécialisés de la police et de la gendarmerie sera opérationnel au deuxième trimestre 2005. Ce Forum sécurisé sera une enceinte de partage des informations techniques et de diffusion de l'information juridique. Réservé dans un premier temps aux enquêteurs spécialisés de la police et de la gendarmerie, il sera progressivement élargi aux référents de la Direction centrale de la sécurité publique. Il pourra être ouvert à d'autres administrations, comme la douane.

3.4. Une sensibilisation de tous les policiers et gendarmes

Plus généralement, les policiers et les gendarmes bénéficieront, dès leur formation initiale et tout au long de leur parcours professionnel, d'une sensibilisation à la cybercriminalité. En effet, la lutte contre la cybercriminalité ne doit pas être un champ d'action réservé à des spécialistes. Elle concerne l'ensemble des policiers et gendarmes. Dans ce but, il convient de développer les connaissances techniques et juridiques des enquêteurs sur les aspects législatifs récents et sur l'évolution des technologies en particulier en termes d'usage, d'introduire dans la formation des modules de techniques élémentaires pour traiter les infractions classiques et préciser les conduites à tenir, de la prise de plainte aux premières investigations, pour les infractions plus spécifiques liées à la criminalité informatique.

3.5. Des outils pédagogiques communs

Des documents pédagogiques communs seront réalisés. Au cours du troisième trimestre 2005, sera diffusé un CD-ROM interactif contenant des textes et des scènes de mise en situation sous forme de vidéo ou d'images en ligne et sera mis en ligne un guide méthodologique. L'arborescence sera conçue pour une utilisation intuitive et souple afin d'en faciliter l'accès à des utilisateurs non-spécialistes.

4. Un renforcement des capacités juridiques d'investigation

Internet est devenu un haut lieu d'échange d'images pédopornographiques et cette activité délictueuse est en pleine croissance. Le vecteur Internet favorise ces échanges en toute confidentialité. Il convient d'insécuriser les pédophiles.

Pour faciliter les recherches, le projet de loi pour la prévention de la violence contiendra des dispositions autorisant l'utilisation de moyens particuliers d'investigation en matière de lutte contre les contenus illégaux qui visent les mineurs.
La caractérisation des éléments constitutifs des infractions, commises par un moyen de communication publique en ligne et dont sont victimes les mineurs, est souvent difficile à mettre en œuvre en raison des problèmes liés à la recherche de la preuve. Ceci est particulièrement vrai pour les faits de corruption de mineurs, diffusion de contenus pédopornographiques, d'incitation à commettre des crimes ou des délits. Les enquêteurs, après la commission des faits, doivent solliciter les fournisseurs d'accès ou les hébergeurs pour qu'ils retrouvent les données techniques permettant d'incriminer les auteurs. Cette intervention en temps différé est insatisfaisante et n'assure pas une protection des mineurs.
Pour dissuader les auteurs de ces messages ciblant les mineurs, certains officiers et agents de police judiciaire travaillant dans des services spécialisés ou des brigades de mineurs et spécialement habilités par l'autorité judiciaire, doivent pouvoir, en toute légalité, assurer une veille du réseau sur les contenus dont sont victimes les mineurs. Ils pourront, dans ces conditions, agir en temps réel et capter en direct toutes les caractéristiques techniques des échanges.
Les enquêteurs doivent pouvoir entrer et participer aux échanges électroniques en ligne sur messagerie électronique, éventuellement en se faisant passer pour mineur ou pour pédophile.
Ces moyens d'investigations seraient limités à certaines infractions particulièrement graves.

Le projet de loi ajoutera au code pénal un article 227-27-2 ainsi rédigé :

« Pour rechercher les infractions visées aux articles 227-18 à 227-24 du code pénal lorsqu'elles sont commises par un moyen de communication publique en

ligne, les officiers ou agents de police judiciaire spécialement habilités peuvent, sans être pénalement responsables de ces actes :

- *participer sous un nom d'emprunt aux échanges électroniques,*
- *être en contact par ce moyen avec les personnes susceptibles d'être les auteurs de ces infractions.,*
- *stocker des contenus illicites dans des conditions fixées par décret.*

« Lorsqu'un site contient des informations illicites constituant une des infractions visées au premier alinéa, aucun paiement ne peut être exigé des services d'investigations qui visitent ces sites pour la recherche de ces infractions ».
« A peine de nullité, ces actes ne peuvent constituer une incitation à commettre ces infractions. »

5. Un renforcement de la veille technologique et de la recherche et développement (R&D).

Les technologies de l'information occupent une position duale au sein de la criminalité, à la fois en tant qu'objectif et moyen, constituant une cible pour les délinquants ou leur fournissant un outil efficace pour l'accomplissement de leurs méfaits. Les progrès constants que connaissent ces technologies sont autant d'occasions pour la cybercriminalité d'échapper aux forces de l'ordre. En effet, la vitesse d'exécution des crimes et délits est augmentée, avec une dissimulation des traces. Les services de police et de gendarmerie ne doivent pas se laisser distancer dans la course aux technologies de plus en plus performantes et sophistiquées. Ils doivent au moins s'adapter aux évolutions de la cybercriminalité, au mieux devancer les éventuels détournements ou usages déviants de ces technologies.
A cet effet, deux principes doivent être respectés : disponibilité et primeur de l'information. La somme des connaissances requises pour résoudre certains problèmes techniques ne peut être maîtrisée en permanence par tous les enquêteurs, ce qui implique un nécessaire partage de l'information technique. Par ailleurs, les services de police et de gendarmerie doivent être informés de l'état de l'art, à la fois pour bénéficier des dernières avancées et pour devancer d'éventuelles menaces à venir.
Il s'agit donc de renforcer le savoir-faire technique des services d'investigation dans le domaine des technologies de pointe et de faciliter ainsi leurs recherches, notamment grâce à une coopération entre les services opérationnels et la division "Recherche et Développement" de France Télécom, forte de 3500 chercheurs. Cette coopération n'est pas exclusive de celle pouvant être établie avec le ministère de la défense (DGA en particulier), avec des centres de recherches universitaires ou avec d'autres laboratoires privés.
Le dispositif s'appuie sur la mise en place d'un réseau mixte public/privé d'experts et sur l'identification d'axes de recherche correspondant aux priorités des services opérationnels.

Le réseau d'experts devrait rassembler dans un premier temps une douzaine de spécialistes de la police, de la gendarmerie et de France Télécom, reliés par des outils de travail coopératifs. La sécurité des réseaux, la téléphonie et les accès à Internet seront, dans l'immédiat, les principaux domaines explorés. Un forum de discussion, créé au sein de la police et de la gendarmerie, relaiera et prolongera les échanges du réseau d'experts au sein des services concernés des deux forces.
De cet échange pourront découler des projets de recherche portant sur le développement d'outils à la disposition des enquêteurs. Les experts se réuniront régulièrement sous forme d'un collège pour examiner les thèmes à développer.

Les logiciels développés par la police et la gendarmerie feront l'objet d'une mise à disposition mutuelle, sans formalité administrative. C'est également ensemble que la police et la gendarmerie nationales rechercheront les matériels les mieux adaptés à leurs missions de veille et d'investigation, dans le cadre des travaux du Conseil de l'équipement et de la logistique et en liaison avec le Centre technique de sécurité intérieure.

6. Un meilleur contrôle des contenus illicites véhiculés par Internet

La problématique des contenus illicites véhiculés par Internet a été étudiée sous deux angles afin de fixer la meilleure solution de gestion et d'exploitation de la veille et des signalements sur Internet. Avant d'exposer les propositions, il convient de préciser ce qui distingue « veille » et « signalement ».
↳ **La veille** est un travail d'initiative qui a pour but de rechercher de manière pro-active les infractions en surveillant l'espace public par les « patrouilles du Net ». C'est une forme de recherche de renseignements utiles à de futures enquêtes. La veille s'accompagne d'une liberté d'action et de réaction de l'enquêteur qui peut sélectionner les éléments qui méritent d'être travaillés, exploités. C'est une approche ciblée, ciselée.
↳ **Le signalement**, *a contrario*, émane d'une tierce personne, physique ou morale (associations, groupements professionnels, administrations) et s'impose à l'enquêteur qui doit, systématiquement, le vérifier, l'exploiter, dans une finalité judiciaire. Le traitement des signalements est un traitement de masse (20 millions d'internautes en 2004 en France). Sa démarche étant officialisée, le signalant est en droit d'obtenir une réponse. Cette réponse se fera en tant que de besoin en lien avec le procureur de la République. Il s'agit, dès le début, d'une enquête judiciaire dont le but est d'identifier l'auteur de l'infraction et ses victimes.

6.1. Un renforcement de la veille des contenus illicites

Internet est un espace de liberté. Mais cette liberté ne saurait être absolue, dès lors que des contenus peuvent porter atteinte à la sécurité et, notamment, à la dignité ou à l'intégrité physique des personnes.
Il importe donc, prolongeant dans l'espace informationnel l'action des services de police et de gendarmerie sur l'espace public traditionnel, de veiller sur les

contenus véhiculés par Internet et de détecter ceux que la loi interdit afin de déférer leurs auteurs devant la Justice.
Cette veille, déjà organisée dans les services de la police et de la gendarmerie, peut être accrue en identifiant des pôles de compétence pour des domaines essentiels :
- le pôle de veille de la police nationale sera plus particulièrement chargé de la veille des contenus à connotation raciste, antisémite ou xénophobe[17], de ceux liés au terrorisme[18] et de ceux relatifs au piratage informatique ;
- le pôle de la gendarmerie nationale sera, quant à lui, plus particulièrement chargé de la veille des contenus pédopornographiques ; des liens fonctionnels sont établis avec le Centre national d'analyse des images pédopornographiques (CNAIP)[19] et avec la base des sites pédopornographiques (GESSIP) tenue par l'OCLCTIC.
Ces pôles devront être renforcés en moyens humains et techniques. Ils agiront en étroite synergie par des échanges réguliers d'information. Ils seront reliés entre eux par le réseau ADER et seront dotés de boites aux lettres électroniques fonctionnelles. Ils pourront ainsi échanger les informations sur les domaines relevant de leurs compétences respectives.
Les deux centres de veille auront pour mission :

- de veiller les contenus sur les sites, les canaux de discussion ("*chats*"), les forums et les réseaux d'échange de fichiers (" *peer to peer")* ;
- de trier les informations recueillies ;
- de transmettre les informations pertinentes aux services d'enquête ; les éléments fournis aux services par les opérateurs devront permettre une localisation de l'origine des faits, sans que celui-ci puisse exiger la production d'une réquisition judiciaire, s'agissant de la mise en œuvre d'une obligation légale de signalement ; les modalités de cette transmission seront définies en concertation avec le ministère de la Justice ;
- d'assister à leur demande les services d'enquête, notamment pour procéder à des investigations ciblées.

La veille des contenus s'exercera en collaboration étroite avec les opérateurs et les fournisseurs d'accès.

6.2. Une centralisation des signalements

Le traitement du signalement engage une réponse opérationnelle, réactive, dans un cadre judiciaire pénal ou de coopération internationale.
Il convient de traiter le signalement par des enquêteurs spécialistes en informatique, mais aussi de la procédure pénale. Ces signalements devront être rapidement orientés vers l'autorité judiciaire compétente s'ils ont été jugés fondés.

[17] La lutte contre le racisme et l'antisémitisme est l'objet d'un des six chantiers, dont la présidence a été confiée à Jean-Christophe RUFIN.
[18] . Cette proposition vient en appui des travaux du chantier « lutte contre le terrorisme »
[19]. Ce centre, composé de policiers et de gendarmes, est situé à Rosny-sous-Bois, au sein du STRJD.

Le traitement du signalement doit être au plus proche des canaux internationaux, très nombreux s'agissant de l'Internet. Il apparaît en effet souhaitable :

- de rapprocher les informations issues du signalement avec les celles émanant des pays étrangers via les canaux de coopération policière ;
- d'émettre les demandes d'identification vers les pays étrangers via Interpol, sans intermédiaire.

La création d'un point d'accès unique est souhaitée par les fournisseurs d'accès à Internet (F.A.I.), les fournisseurs de services Internet (F.S.I.) et les associations rencontrés par le groupe de travail. Elle doit, pour les premiers, faciliter la tâche de leurs collaborateurs et les obliger à remplir leurs obligations légales. Ainsi le pôle de signalement unique offrira aux professionnels une entrée simple, claire, facile.

L'ensemble des services prendra part au fonctionnement du système mis en place. Une base de données consultable par l'ensemble des acteurs sera adossée à ce pôle de traitement des signalements.

Ce pôle, composé de manière paritaire par des policiers et de gendarmes spécialistes, sera placé auprès de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. Il assurera la liaison constante avec les pôles de compétence veille sur Internet, comme c'est le cas aujourd'hui pour la pédopornographie sur Internet.

Ce pôle pourra être contacté par le public par un canal différencié de celui réservé aux « professionnels ».

La mise en place de ce pôle de signalement interministériel, placé sous l'autorité du ministre de l'intérieur, répond aux demandes exposées dans plusieurs chantiers lancés par le ministre (protection des mineurs, lutte contre le racisme et l'antisémitisme, lutte contre la cybercriminalité).

7. Une meilleure protection des mineurs

La prévention des agressions sexuelles à l'égard de mineurs doit être pertinente et efficace. Pour renforcer leur protection, il est proposé d'inscrire dans le projet de loi de pour la prévention de la délinquance une infraction spécifique relative aux propositions sexuelles adressées par Internet à des mineurs.

Les moyens de communication au public en ligne peuvent mettre directement en relation des enfants et des pédophiles, à l'insu des adultes chargés de l'autorité parentale ou ayant une obligation de surveillance sur les mineurs.

Il n'existe pas actuellement d'incrimination spécifique pour sanctionner les propositions sexuelles adressées à des mineurs, notamment via l'Internet. Les « prédateurs » communiquent avec les mineurs, soit par messages électroniques, soit par « chat » ou conversations en direct, services proposés par des sites Web dédiés aux enfants ou aux adolescents.

La création d'une incrimination spécifique permettra de dissuader et de sanctionner les pédophiles qui font des offres à caractère sexuel à des mineurs à l'aide de ce vecteur qui échappe souvent à la vigilance des parents.

Le code pénal comprend un article qui sanctionne le fait de favoriser ou de tenter de favoriser la corruption de mineurs (article 227-22) mais la portée de cet article ne permet pas de sanctionner les personnes qui font des propositions sexuelles à des mineurs ou à des personnes se faisant passer pour mineurs.
La rédaction proposée ci-dessous implique que les services d'enquêtes n'auront pas à établir la réalité de la minorité de la personne destinataire des propositions. Elle permettra de réprimer les auteurs de ces propositions dès lors qu'elles auront été formulées et adressées. Cette incrimination créera une insécurité pour les pédophiles qui hésiteront à adresser des messages de cette nature sur Internet.
L'article suivant sera inscrit dans le projet de loi pour la prévention de la délinquance :
Après l'article 227-22-du code pénal, il est inséré un article 227-22-1 :
« Le fait pour une personne majeure de proposer des échanges de nature sexuelle à un mineur de quinze ans à l'aide d'un moyen de communication au public en ligne est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.
« Les peines encourues sont portées à cinq d'emprisonnement et 75 000 euros d'amende lorsque ces propositions ont été suivies d'une rencontre physique »

8. Une politique de prévention

Cette politique s'appuiera sur des opérations de communication à l'égard du grand public et des professionnels, avec des campagnes de sensibilisation sur les dangers du Net et sur les règles qui doivent s'y appliquer. Parmi les bénéficiaires de cette action figurent bien évidemment les jeunes, notamment les mineurs, dont la sécurité est un des objectifs prioritaires du ministre de l'intérieur, comme en témoigne le chantier sur la "sécurité des mineurs" qu'il a confié à Marie-Thérèse HERMANGE. Dans le cadre du protocole établi entre le ministre de l'intérieur et le ministre de l'éducation nationale, les services de police et de gendarmerie pourront également sensibiliser les élèves aux règles de bonne conduite sur Internet.
Des contenus pédagogiques communs à la police et à la gendarmerie seront conçus pour sensibiliser les acteurs publics et privés aux risques en matière de cybercriminalité.
La prévention sera également le fruit d'actions communes avec les opérateurs et les fournisseurs d'accès désireux de mieux informer les internautes, en particulier grâce à des mailings, des SMS, des encarts sur les factures, des espaces sur les portails.
S'ajoutent également les actions avec les associations qui se sont constituées afin de mieux sensibiliser le public. Des campagnes d'information sur les peines réprimant la détention et la diffusion d'images pédophiles seront également menées, eu égard à l'ampleur démesurée du phénomène.

9. La définition d'un certificat "citoyen" des fournisseurs de services de l'Internet

La lutte contre la cybercriminalité n'est pas le monopole de l'Etat. Elle concerne l'ensemble des acteurs publics et privés, les entreprises comme les particuliers qui doivent avoir une démarche citoyenne.

S'agissant des fournisseurs de service Internet, la loi, tout en limitant leur responsabilité pénale[20], leur crée des obligations, notamment en ce qui concerne la lutte contre la pédopornographie, l'apologie des crimes contre l'humanité ou l'incitation à la haine raciale. Les fournisseurs de services sont tenus à conserver les données de trafic[21] et de contenu[22] pour répondre aux réquisitions des autorités judiciaires.

Les prestataires de services d'hébergement en ligne et d'accès à Internet sont conscients de leurs responsabilités. L'Association des Fournisseurs d'Accès et de Services Internet (AFA) a signé, le 14 juin 2004, une charte qui précise les dispositifs de signalement et la mise en œuvre d'outils de contrôle parental, les diligences auprès des autorités publiques compétentes et le règles de coopération avec les autorités judiciaires. Dans cet esprit, elle a créé un label[23].

Pour tenir compte des efforts déployés par certains fournisseurs d'accès et de services Internet, il est proposé d'instituer une régulation souple en créant un certificat[24] « citoyen » attribué aux fournisseurs d'accès ou de services sur Internet et s'appuyant sur un système volontaire et déclaratif. Ce certificat s'inscrirait dans le cadre de la responsabilité sociétale d'entreprise. Il impliquerait les trois parties prenantes : fournisseurs de services sur Internet (FSI), utilisateurs et Etat. Il mesurerait l'effort et l'efficacité de la politique de lutte contre la cybercriminalité des FSI, ainsi que leur contribution au développement de la civilité du cyberespace.

Le principe ayant reçu un accueil favorable des organismes consultés (AFA, Forum des droits sur Internet), il est proposé de mettre en place un groupe de travail réunissant les parties prenantes. Ce groupe pourrait être piloté par le Forum des droits sur Internet et devrait préciser les critères pertinents, la procédure d'attribution du certificat, l'organisme qui pourrait en être le porteur.

[20] Art. 6 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

[21] Art. 34 de la loi n°2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle.

[22] Art. 6 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

[23] Label = mot anglais, marque élaborée par un syndicat professionnel et imposé par ses adhérents sur un produit pour en attester l'origine et la qualité des conditions de fabrication.

[24] Certificat = attestation écrite émanant d'une autorité compétente et garantissant un fait.

Conclusion

La réflexion sur la cybercriminalité ne peut s'arrêter avec la remise de ce rapport qui marque une étape et non un terme.
Il est proposé de pérenniser les travaux du chantier en approfondissant ses réflexions dans les trois domaines suivants :

- L'extension de l'espace Schengen à la cybercriminalité
La cohérence du dispositif national étant réalisée, il convient de renforcer notre action de coopération et de proposer à nos partenaires européens la simplification des procédures d'identification des traces numériques indispensable à la résolution des enquêtes. Un groupe de travail définira les contours de cette coopération et proposera les mesures susceptibles d'être inscrites à l'ordre du jour d'un conseil JAI.

- Le développement de la coopération entre les acteurs publics et privés
La diversité des acteurs publics et privés qui interviennent dans la lutte contre la cybercriminalité rend nécessaire une meilleure organisation des échanges. Il est proposé de constituer un Forum État/industrie rassemblant, chaque trimestre, sur la base du volontariat, l'ensemble des intervenants pour des séances d'information, d'échanges de vues ou de travail sur des thèmes particuliers. Seraient concernés pour l'Etat les représentants du ministère de l'intérieur, du ministère de la défense, du ministère de l'économie, des finances et de l'industrie, et du ministère de la Justice. La participation du Forum des droits de l'Internet serait également souhaitable. Du côté de l'industrie, l'AFA et France Télécom seraient, en particulier, les interlocuteurs privilégiés. Cette réflexion devrait déboucher sur un protocole fixant les relations entre les différents partenaires, comme l'a souhaité l'AFA lors de sa réception au ministère de l'intérieur.

- La conception et la planification des actions de prévention, évoquées dans la proposition n°8.

RESUME DES MESURES PROPOSEES

1. Une meilleure connaissance statistique de la cybercriminalité.
Depuis le 1er janvier 2005, les services de police et de gendarmerie ont pris des dispositions pour que les infractions relatives à la cybercriminalité soient mieux connues. Il est également souhaité qu'une enquête de victimation soit conduite par l'OND en 2006.

2. Un doublement des capacités opérationnelles des services de police et de gendarmerie.
Ce doublement devrait concerner les organismes centraux et les services et unités spécialisés.

3. Un développement d'actions de formation communes.
Cette formation devrait s'adresser aux enquêteurs spécialisés de la police et de la gendarmerie. Elle bénéficierait à l'ensemble des policiers et gendarmes, dès leur formation initiale et tout au long de leur carrière.

4. Un renforcement des capacités juridiques d'investigation.
Un article facilitant les investigations pourrait être inséré dans le projet de loi sur la prévention de la délinquance :
« Pour rechercher les infractions visées aux articles 227-18 à 227-24 du code pénal lorsqu'elles sont commises par un moyen de communication publique en ligne, les officiers ou agents de police judiciaire spécialement habilités peuvent, sans être pénalement responsables de ces actes :

- *participer sous un nom d'emprunt aux échanges électroniques,*
- *être en contact par ce moyen avec les personnes susceptibles d'être les auteurs de ces infractions.,*
- *stocker des contenus illicites dans des conditions fixées par décret.*

« Lorsqu'un site contient des informations illicites constituant une des infractions visées au premier alinéa, aucun paiement ne peut être exigé des services d'investigations qui visitent ces sites pour la recherche de ces infractions ».

5. Un renforcement de la veille technologique et de la recherche & développement.
Un réseau d'experts rassemblera des spécialistes de la police, de la gendarmerie et de France Télécom, reliés par des outils de travail coopératifs. Un forum de discussion, créé au sein de la police et de la gendarmerie, pourrait utilement relayer et prolonger les échanges du réseau d'experts au sein des services concernés des deux forces.
Les logiciels développés par la police et la gendarmerie feront l'objet d'une mise à disposition mutuelle. Police et la gendarmerie nationales rechercheront les matériels les mieux adaptés à leurs missions de veille et d'investigation.

6. Un meilleur contrôle des contenus illicites

6.1 Un renforcement de la veille des contenus illicites.

Un pôle de veille sur les contenus à caractère pédophile sera développé au sein de la gendarmerie nationale. Le pôle de la police nationale sera chargé de la veille des sites à caractère raciste ou antisémite, relatifs au terrorisme ou au piratage informatique.

6.2 Un centre unique de signalement.

Un pôle unique de signalement des sites à contenus illicites pourrait être constitué au sein de l'OCLCTIC avec une participation paritaire de la police et de la gendarmerie. Ce pôle, saisi par les particuliers ou les associations, dénoncerait aux autorités judiciaires les infractions constituées.

7. Un renforcement de la protection des mineurs.

Pour dissuader les pédophiles, il est proposé d'insérer dans le code pénal un article 227-22-1 ainsi rédigé :

« Le fait pour une personne majeure de proposer des échanges de nature sexuelle à un mineur de quinze ans à l'aide d'un moyen de communication au public en ligne est puni de deux ans d'emprisonnement et de 30 000 euros d'amende.

« Les peines encourues sont portées à cinq d'emprisonnement et 75 000 euros d'amende lorsque ces propositions ont été suivies d'une rencontre physique »

8. Le développement d'une politique de prévention.

Il est suggéré que des opérations de communication soient conduites à l'égard du grand public et des professionnels, avec des campagnes de sensibilisation sur les dangers du Net et sur les règles qui doivent s'y appliquer.

9. La création d'un certificat "citoyen".

Pour tenir compte des efforts déployés par certains fournisseurs d'accès et de services Internet, il est proposé d'instituer une régulation souple en créant un certificat[25] « citoyen » attribué aux fournisseurs d'accès ou de services sur Internet et s'appuyant sur un système volontaire et déclaratif.

[25] Certificat = attestation écrite émanant d'une autorité compétente et garantissant un fait.

ANNEXE

Les bases légales de la "CYBERCRIMINALITE'

1. Les infractions spécifiques aux technologies de l'information et de la communication

Catégorie	*Libellés des infractions*	*Texte de loi*	*Codification*	*Peines*	*Observations*
Atteintes aux Systèmes de Traitement Automatisé de Données (S.T.A.D.)	Suppression/Modification de données	Loi Godfrain 05 I 1998	Code Pénal Art. 323 al. 1	1 an d'emprisonnement 15 000 € d'amende	
	Altération de fonctionnement		Art. 323-1 al.2	2 ans d'emprisonnement 30 000 € d'amende	
	Entrave au fonctionnement		Art. 323-2	3 ans d'emprisonnement 45 000 € d'amende	
	Introduction, suppression, modification de données		Art. 323-3	3 ans d'emprisonnement 45 000 € d'amende	
	Groupement de pirates		Art. 323-4	Idem à la plus sévère des infractions	
	Tentative d'infraction sur un STAD		Art. 323-7	Même peine que l'infraction visée	
	- Importation - Détention - Offre - Cession - Mise à disposition d'équipement, instrument ou programme informatique conçus ou adaptés pour commettre des infractions aux STAD	LCEN au 9 IV 2004 art. 34	Code Pénal Art. 323-3-1	Même peine que l'infraction au STAD visée	
Traitements automatisés de données personnelles	Traitement sans formalités CNIL	Loi Informatique et Libertés 06 I 1978	Code Pénal Art. 226-16	3 ans d'emprisonnement 45 000 € d'amende	
	Base de données non sécurisée		Art. 226-17	5 ans d'emprisonnement 300 000 € d'amende	
	Collecte déloyale ou malgré opposition		Art. 226-18	5 ans d'emprisonnement 300 000 € d'amende	
	Conservation des données "sensibles"		Art. 226-19	5 ans d'emprisonnement 300 000 € d'amende	
	Conservation supérieure à la déclaration préalable – (sauf à fins historiques, scientifiques, statistiques)		Art. 226-20	3 ans d'emprisonnement 45 000 € d'amende	
	Détournement des fins		Art. 226-21	5 ans d'emprisonnement 300 000 € d'amende	
	Cession des informations personnelles		Art. 226-22	1 an d'emprisonnement 15 000 € d'amende	
	- Non anonymisation des données dans certains cas - Non conservation des données techniques - Fabrication	LSQ 15 XI 2001 - art. 29	Code des P&T Art. L. 39-3 1	1 an d'emprisonnement 75 000 € d'amende	
Les infractions aux cartes bancaires		LSQ 15 XI 2001 Art. 35-39 et 40	Code monétaire et Financier	7 ans d'emprisonnement	
Les chiffrements non autorisés ou non déclarés	Utilisation non-autorisée de clé de chiffrement	L. Télécom 29 XII 1990 +	Code Pénal Art. 434-15-2 al. 1er	3 ans d'emprisonnement 45 000 € d'amende	
	Refus de répondre à réquisition pour remise de clé de chiffrement	art. 11 L. 10 VII 1991 mod.		2 ans d'emprisonnement	

	Refus de fournir une clé qui aurait pu éviter/limiter un crime ou un délit	par L.S.Q. – art. 31	Art. 434-15-2 al. 2	30 000 € d'amende 5 ans d'emprisonnement 75 000 € d'amende	
Interceptions	Régime des interceptions des correspondances émises par voie de télécommunication	Loi Perben II	Code de Procédure Pénale Art. 706-95	Autorisées par le juge des libertés, à la requête du Procureur, pour une durée de 15 jours renouvelables une fois	**Interceptions en enquête préliminaire possible**
	Violation de correspondance (interception illégale)	Ordonnance n° 2000-916 du 19/9/2000	Code Pénal Art. 226-15 et 432-9	1 an d'emprisonnement et 15 000 € d'amende (3 ans et 45 000 € si auteur dépositaire autorité publique ou exploitant de réseau de télécom)	Circonstance aggravante si auteur dépositaire de l'autorité publique

2. Les infractions liées aux technologies de l'information et de la communication

Catégorie	*Libelles des infractions*	*Texte de loi*	*Codification*	*Peines*	*Observations*
Pédo-pornographie	Fixation en vue de diffusion Enregistrement en vue de diffusion		Code Pénal Art.227-23	3 ans d'emprisonnement 45.000€ d'amende	La loi Perben II (art.47) ***incrimine*** la fixation et l'enregistrement en vue de sa diffusion ainsi que la transmission d'images pédophiles en *bande organisée*
	Diffusion sur un réseau d'images pédo-pornographiques		Art.227-23 al.3	***Diffusion en ligne*** 5 ans d'emprisonnement 75.000€ d'amende	
	Détention d'image pédo-pornographique	L.04 III 2002	Art.227-23 al.4	***En bande organisée*** 10 ans d'emprisonnement 500.000€ d'amende	
	Diffusion d'images pornographiques susceptibles d'être vues par un mineur		Code Pénal Art.227-24	3 ans d'emprisonnement 75.000€ d'amende	
Terrorisme, haine raciale...	Provocation aux crimes et aux délits	L.29 VII 1881	Art.23 et 24	5 ans et 45.000€ d'amende	
	Apologie de crime de guerre Provocation au terrorisme		Art.24, al.3&4	5 ans et 45.000€ d'amende	
	Provocation à la haine raciale		Art.24 al.6	1 an et 45.000€ d'amende	
	Contestation de crimes contre l'humanité		Art.24 bis	1 an et 45.000€ d'amende	
	Diffamation (raciale)		Art.29 à 32	12.000€ d'amende (1 an de prison et 45.000€ d'amende)	
	Injure (raciale)		art.29 à 33	12.000€ d'amende (6 mois de prison et 22.500€ d'amende)	
Atteintes aux personnes	Usurpation d'identité		Code Pénal Art.434-23	5 ans d'emprisonnement 75.000€ d'amende	Usurpation d'identité ou d'identifiant (adresse mail par ex.)
	Menaces et menaces de mort		Art.222-17	6 mois à 3 ans d'emprisonnement 45.000€ à75.000€ d'amende	
	Atteintes à la vie privée		Art.226 al.1&2	1 an et 45.000€ d'amende	
	Atteintes à la représentation de la personne		Art.226-8	1 an et 45.000€ d'amende	
	Dénonciations calomnieuses		Art.226-10	5 ans et 45.000€ d'amende	

	Atteintes au secret professionnel		Art.226-13	1 an et 45.000€ d'amende	
Atteintes aux biens	Menaces de commettre une destruction, une dégradation ou une détérioration		Code Pénal Art.322-12	6 mois d'emprisonnement 7.500€ d'amende	

3. les infractions facilitées par les technologies de l'information et de la communication

Catégorie	*Libellés des infractions*	*Texte de loi*	*Codification*	*Peines*	*Observations*
Escroquerie en ligne	L'escroquerie par utilisation frauduleuse de numéro de carte de paiement sur internet et les escroqueries en général.		Code Pénal Art.313-1	5 ans d'emprisonnement 375.000€ d'amende	
Propriété intellectuelle	Toute contrefaçon d'une oeuvre de l'esprit y compris logiciels, marques, dessins ou modèles. Récidive ou si le délinquant est lié à la victime.	Loi Perben II 09 III 2004	Code de la Propriété intellectuelle Art. L.335-1 et 335-3 Art.L.335-9 Art. L.521-4 Art. L.716-9 et suivants	3 ans d'emprisonnement 300.000€ d'amende ***En bande organisée*** 5 ans d'emprisonnement 375.000€ d'amende En cas de récidive, les peines sont portées au double (art.335-9)	La loi Perben II a modifié le quantum des peines applicables en matière de contrefaçon
Jeux de hasard	Participation à la tenue d'une maison de jeux de hasard.	Art.1er – L 12VII 1983 mod.l. Perben II		3ans d'emprisonnement 45.000€ d'amende ***En bande organisée*** 7 ans d'emprisonnement 100.000€ d'amende	Modification de la loi PerbenII
	Publicité en faveur d'une telle loterie	L. Perben II art.23		4.500€ d'amende	