



AB1X10V1

**CONCOURS EXTERNE DES 18, 19 ET 20 JANVIER 2010
POUR L'EMPLOI D'INSPECTEUR STAGIAIRE DES DOUANES ET DROITS
INDIRECTS**

ÉPREUVE ÉCRITE D'ADMISSIBILITÉ N°1

(DURÉE : 4 HEURES - COEFFICIENT 6)

**RÉDACTION D'UNE NOTE DE SYNTHÈSE A PARTIR D'UN DOSSIER
RELATIF AUX QUESTIONS ÉCONOMIQUES, FINANCIÈRES ET
SOCIALES**

A partir des documents suivants, vous rédigerez une note d'environ 4 pages consacrée à la cybercriminalité.

AVERTISSEMENTS IMPORTANTS

L'usage de tout matériel autre que le matériel usuel d'écriture et de tout document autre que le support fourni est **interdit**. **Toute fraude ou tentative de fraude** constatée par la commission de surveillance **entraînera l'exclusion du concours**.

Veillez à bien indiquer sur votre copie le nombre d'intercalaires utilisés (la copie double n'est pas décomptée)

Il vous est interdit de quitter définitivement la salle d'examen **avant le terme de la première heure**.

Le présent document comporte 34 pages numérotées.

MINISTÈRE DU BUDGET
DES COMPTES PUBLICS
DE LA FONCTION PUBLIQUE
ET DE LA RÉFORME DE L'ÉTAT

Liste des documents

- Document 1 :** La cybercriminalité
Site la documentation française – dossier internet dans le monde (extrait)
- Document 2 :** La protection des données personnelles
Site la documentation française – dossier internet dans le monde (extrait)
- Document 3 :** Le droit de propriété intellectuelle
Site la documentation française – dossier internet dans le monde (extrait)
- Document 4 :** La cybercriminalité : interview du Procureur brésilien Luiz Costa
Site du ministère de la justice et des libertés
- Document 5 :** Mobilisation contre la cybercriminalité
Portail du gouvernement – 25 mars 2009
- Document 6 :** Première réflexion internationale sur la cybercriminalité
Nouvelobs.com – 25 juin 2008
- Document 7 :** Cyberdouane, un nouveau service pour lutter contre la cyberdélinquance
Portail du Gouvernement – 10 février 2009
- Document 8 :** Le Gouvernement lance une nouvelle étape de la lutte anti-cybercriminalité
Portail du Gouvernement – 15 février 2008
- Document 9 :** Royaume-Uni : le coût de la fraude bancaire sur Internet a doublé en 2008
Par ZDNet.fr, publié le 24/03/2009 - L'express.fr
- Document 10 :** Plan de lutte contre la cybercriminalité
Sources : Ministère de l'Intérieur, de l'outre-mer et des collectivités territoriales (MIOMCT)
- Document 11 :** Intervention de Michèle ALLIOT-MARIE, Ministre de l'intérieur, de l'outre-mer et des collectivités territoriales
Site defense.gouv.fr
- Document 12 :** Cybercriminalité : Michelle Alliot-Marie renforce les effectifs d'enquêteurs
Par ZDNet.fr, publié le 25/03/2009 - L'express.fr
- Document 13 :** Les eurodéputés s'engagent pour un « accès sans réserve à Internet »
Par ZDNet.fr, publié le 18/02/2009 - L'express.fr
- Document 14 :** Loppsi II - Le nouveau plan quinquennal de sécurité
Par Eric Pelletier, publié le 26/05/2009 Les échos.fr
- Document 15 :** Le gouvernement met Internet sous surveillance
CHARLES DE LAUBIER, Les Echos
- Document 16 :** La cybercriminalité et les chauffards dans le collimateur
LAURENCE ALBERT, Les Echos
- Document 17 :** Cybercriminalité : les entreprises ne sont pas assez protégées
RÉGIS MARTI, Les Echos - [19/05/09]
- Document 18 :** Internet, cybercriminalité et cybersécurité
Mise à jour le 15 07 2009 - Dossier politiques publiques – La sécurité intérieure
Site vie publique

La cybercriminalité

Si internet a permis à des millions de personnes d'accéder à d'innombrables informations, son développement a également engendré une nouvelle forme de délinquance : la cybercriminalité.

Qu'est-ce que la cybercriminalité ?

Selon la Commission européenne, le terme "cybercriminalité" englobe trois catégories d'activités criminelles :

- les formes traditionnelles de criminalité, telles que la fraude et la falsification informatiques (escroqueries, fausses cartes de paiement, etc.)
- la diffusion de contenus illicites par voie électronique (par exemple, ceux ayant trait à la violence sexuelle exercée contre des enfants ou à l'incitation à la haine raciale).
- les infractions propres aux réseaux électroniques, c'est-à-dire les attaques visant les systèmes d'information, le déni de service et le piratage.

Les acteurs économiques sont des cibles de choix pour la cybercriminalité, mais les administrations publiques ou les citoyens ne sont pas plus à l'abri. Aux Etats-Unis, le Pentagone a enregistré à lui seul, en 2001, plus de 22 000 agressions électroniques contre ses systèmes et le FBI a recensé 5 000 infrastructures "extrêmement vulnérables" à la criminalité informatique capable "de déstabiliser l'économie entière d'un pays", selon Ronald L. Dick, directeur du Centre de la protection des infrastructures nationales. Le point commun de ces catégories d'infractions est que celles-ci peuvent être commises à grande échelle et que la distance géographique entre le lieu où l'acte délictueux est effectué et ses effets, peut être considérable.

La fraude et l'escroquerie en ligne prennent de plus en plus d'ampleur. En 2001, des groupes organisés en Ukraine et Russie ont piraté plus de 40 sites américains, détournant les numéros d'au moins un million de cartes de crédit. De Moscou à Tokyo en passant par Lausanne ou Paris, la police spécialisée semble dépassée par cette criminalité galopante qui profite des failles des systèmes informatiques. D'après le Conseil de l'Europe, la fraude sur les cartes de crédit s'élève à quelque 400 millions de dollars par an et les dégâts causés par les attaques de virus à près de 12 milliards de dollars.

La lutte contre la cybercriminalité

Le caractère transfrontalier de ce nouveau type d'activités criminelles appelle à un renforcement de la coopération et de la coordination internationales.

La Convention sur la cybercriminalité

Dès le 23 novembre 2001, les pays membres du Conseil de l'Europe et leurs partenaires (Etats-Unis, Canada, Japon, Afrique du Sud) ont adopté à Budapest une Convention sur la cybercriminalité. Cette dernière, entrée en vigueur le 1er juillet 2004, constitue la première convention pénale à vocation universelle destinée à lutter contre le cybercrime. Ce texte constitue une réponse globale aux crimes commis sur et à travers les réseaux informatiques. Elle poursuit trois objectifs :

- harmoniser les législations des Etats signataires en matière de cybercriminalité : à cette fin, la Convention établit des définitions communes de certaines infractions pénales commises par le biais des réseaux informatiques.
- compléter ces législations, notamment en matière procédurale : afin d'améliorer la capacité des services de police à mener en temps réel leurs investigations et à collecter des preuves sur le territoire national avant qu'elles ne disparaissent.
- améliorer la coopération internationale, notamment en matière d'extradition et d'entraide répressive.

42 États sont signataires mais seuls 14 États ont procédé à sa ratification fin 2007.

Le protocole additionnel à la Convention sur la cybercriminalité

Ouvert à la signature en janvier 2003, le Protocole additionnel à la Convention sur la cybercriminalité demande aux Etats de criminaliser la diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques. Ce Protocole élargit donc le champ d'application de la Convention afin de couvrir également les infractions de propagande raciste ou xénophobe commises via les réseaux informatiques. Il prévoit, par ailleurs, de faciliter l'extradition des contrevenants à l'intérieur de l'espace européen, ainsi que de favoriser l'entraide judiciaire pour la répression de ces agissements.

La création de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)

L'ENISA a été établie par l'Union européenne en 2004 dans l'optique de garantir aux utilisateurs un plus haut degré de sécurité, les violations des réseaux de communication prenant de l'ampleur. Située en Crète, elle fonctionne comme un centre d'expertise pour les États membres, les institutions de l'UE et les entreprises. L'agence a pour mission de :

- prêter assistance et fournir des conseils à la Commission et aux États membres sur les questions liées à la sécurité des réseaux et de l'information ;
- recueillir et analyser les données relatives aux incidents liés à la sécurité en Europe et aux risques émergents ;
- promouvoir des activités d'évaluation et de gestion des risques afin d'améliorer la capacité de faire face aux menaces pesant sur la sécurité de l'information ;
- renforcer la coopération entre les différents acteurs du secteur de la sécurité de l'information ;
- suivre l'élaboration des normes pour les produits et services en matière de sécurité des réseaux et de l'information.

Le programme européen Safer Internet Plus

Proposé par la Commission européenne en mars 2004, le programme pluriannuel Safer Internet Plus (2005-2008), succédant au plan d'action Safer Internet (1999-2004), est doté d'un budget de 45 millions d'euros afin de lutter contre les contenus internet illicites et préjudiciables et de promouvoir une utilisation plus sûre d'internet et des nouvelles technologies en ligne, particulièrement pour les enfants. Le nouveau programme voit son champ d'application élargi à d'autres médias, comme les supports vidéos, et est explicitement conçu pour combattre le racisme et les communications électroniques commerciales non sollicitées (spam). Les activités menées au titre du programme sont réparties selon quatre lignes d'action :

- lutte contre les contenus illicites : des lignes téléphoniques d'urgence ("hotlines") ont été créées pour permettre au public de signaler les contenus illicites et transmettre les informations à l'organisme qui est en mesure d'agir (fournisseur de service internet ou police, par exemple) ;
- traitement des contenus non désirés et préjudiciables : le programme finance des mesures technologiques qui permettent aux utilisateurs de limiter le volume de ces contenus et de gérer les spams reçus, ainsi que de mettre au point de meilleurs filtres ;
- promotion d'un environnement plus sûr : afin de renforcer l'autorégulation du secteur, la Commission met à la disposition des organismes nationaux de corégulation ou d'autorégulation le "Forum pour un Internet plus sûr" pour favoriser l'échange d'expériences ;
- sensibilisation : les actions de sensibilisation visent les différentes catégories de contenus illicites, non désirés et préjudiciables et prennent également en compte les questions connexes telles que la protection des consommateurs, la protection des données et la sécurité des informations et des réseaux (virus, spams, etc.).

Site la documentation française – dossier internet dans le monde (extrait)

La protection des données personnelles

CNIL (Commission nationale de l'informatique et des libertés)

A l'origine, internet servait principalement à relier des chercheurs en informatique. La circulation des documents ne posait donc aucun problème de confidentialité et les données étaient acheminées en clair sur le réseau. Mais, l'ouverture d'internet à un usage commercial a modifié les comportements. Des informations confidentielles circulant sur les liaisons, la sécurité des communications est devenue une préoccupation importante des internautes et des entreprises. Tous cherchent à se protéger contre une utilisation frauduleuse de leurs données ou contre des intrusions malveillantes dans les systèmes informatiques.

Le vol d'informations privées

La facilité des intrusions ou divulgations de données à caractère personnel est apparue comme une menace pour la vie privée, les libertés individuelles et publiques. La question est aujourd'hui particulièrement préoccupante du fait du développement du commerce électronique qui se fonde notamment sur un "marché" des données personnelles : celles-ci sont en effet des outils de marketing permettant au commerçant de fidéliser son client en lui proposant un service sur mesure déduit de l'analyse de son comportement sur le réseau. Ainsi, les annonceurs publicitaires ont recours à des spyware ou logiciels espions, installés sur l'ordinateur à l'insu de l'utilisateur, qui collectent des informations sur l'internaute ou ses habitudes de connexion.

Un autre phénomène mettant en danger la protection des données personnelles des internautes se développe actuellement : le phishing ou hameçonnage. Il s'agit d'un courrier électronique qui persuade l'utilisateur de révéler des données personnelles sensibles par usurpation d'identité en imitant un site internet censé représenter une véritable société. Le courrier électronique non sollicité a donc cessé d'être une simple nuisance et devient peu à peu une activité de nature frauduleuse. En effet, les "polluposteurs" louent ou vendent désormais à des sociétés, aux fins de prospection, les listes d'adresses électroniques qu'ils ont récoltées.

Il n'existe pas de parade absolue garantissant l'échec des tentatives de vol d'informations sur internet mais des outils technologiques se développent comme les pare-feu, le cryptage des données, les outils de filtrage du courrier électronique ou encore les services de signalement des "pollupostages" par les internautes.

Législation et conventions internationales

Du point de vue législatif, la lutte contre la collecte et le traitement déloyaux de données à caractère personnel débute avec l'adoption par la France, de la "loi relative à l'informatique, aux fichiers et aux libertés" du 6 janvier 1978, qui institue la Commission nationale de l'informatique et des libertés

(CNIL), autorité chargée de veiller à la protection des données personnelles et de la vie privée. Dans ce cadre, la CNIL vérifie que la loi est respectée en contrôlant les applications informatiques, prononce des sanctions, établit des normes et propose au gouvernement des mesures législatives ou réglementaires de nature à adapter la protection des libertés et de la vie privée à l'évolution des techniques.

Puis en 1981, le Conseil de l'Europe élabore la "Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel" qui reste à ce jour, dans ce domaine, le seul instrument juridique contraignant sur le plan international, à vocation universelle, ouverte donc à l'adhésion de tout pays y compris non membre du Conseil de l'Europe. Cette Convention définit un certain nombre de principes pour que les données soient collectées et utilisées de façon loyale et licite. Ainsi, elles ne peuvent être collectées que dans un but précis et ne peuvent être utilisées de manière incompatible avec ce but ; elles doivent être exactes, proportionnées à cet objectif et conservées uniquement pendant le délai nécessaire à sa réalisation. Le texte établit, en outre, le droit d'accès et de rectification de la personne concernée et exige une protection spéciale pour les données sensibles (notamment celles concernant l'appartenance religieuse, les opinions politiques ainsi que les données génétiques ou médicales).

Dans le droit fil de cette Convention du Conseil de l'Europe, l'Union européenne a adopté en octobre 1995 la directive 95/46/CE qui constitue le texte de référence, au niveau européen, en matière de protection des données à caractère personnel. Celle-ci met en place un cadre réglementaire visant à établir un équilibre entre un niveau élevé de protection de la vie privée des personnes et la libre circulation des données à caractère personnel au sein de l'Union européenne. Pour ce faire, la directive fixe des limites strictes à la collecte et à l'utilisation des données à caractère personnel, et demande la création, dans chaque État membre, d'un organisme national indépendant chargé de la protection de ces données. Tous les États membres ont maintenant transposé la directive. Néanmoins, les actions entreprises au sein de l'UE restent encore insuffisantes pour faire face aux menaces que représentent le courrier électronique, les logiciels malveillants et les logiciels espions. Internet étant un réseau mondial, la Commission européenne souhaite développer le dialogue et la coopération avec les pays tiers concernant la lutte contre ces menaces et les activités criminelles qui y sont associées.

Site la documentation française – dossier internet dans le monde (extrait)

Le droit de propriété intellectuelle

La multiplication des possibilités de diffuser des contenus culturels sur internet conduit à une remise en cause généralisée du droit d'auteur. De nombreux agents économiques, notamment à travers les sites internet, les réseaux pair à pair (peer-to-peer) ou les blogs, utilisent des contenus protégés par la propriété intellectuelle en s'exonérant de toute autorisation des auteurs. Ces pratiques, de plus en plus courantes, répandent dans l'opinion publique l'idée d'une culture gratuite. Le phénomène est observable au niveau mondial et présente des risques majeurs pour les auteurs et leurs ayants droit et, plus largement, pour l'industrie culturelle.

Le pair à pair (peer-to-peer)

Depuis 1999, l'utilisation des réseaux d'échange de fichiers de pair-à-pair (P2P) est de plus en plus importante. Ces réseaux facilitent considérablement la mise en commun et le partage de ressources numérisées de toute nature (fichiers textes, audio, vidéo et logiciels) entre plusieurs individus sans transiter par un serveur central. Mais, si les réseaux P2P rendent possible la diffusion légale d'œuvres non protégées à une échelle mondiale, ils peuvent également être le vecteur de la copie et du recel illicites de contenus auxquels s'appliquent le droit d'auteur. Certains fichiers peuvent, en outre, contrevenir à des dispositions pénales (racisme, pédo-pornographie, etc...).

L'action internationale

Ce commerce de produits contrefaits et piratés se développant, l'Organisation mondiale de la propriété intellectuelle (OMPI) a mis en place, en 2004, des conférences régulières dans le cadre du Congrès mondial sur la lutte contre la contrefaçon et le piratage, en partenariat avec Interpol et l'Organisation mondiale des douanes (OMD). Ces rencontres ont pour objectif de réunir de hauts responsables du secteur public et des dirigeants d'entreprise afin de mettre en commun leurs expériences, de développer des stratégies concrètes en matière d'application des droits et d'élaborer des recommandations et des programmes internationaux pour lutter contre cette forme de criminalité qui menace le développement économique et la sécurité des consommateurs, et en réduire les effets.

Les solutions pour lutter contre la contrefaçon et le piratage

Au-delà des dispositions répressives, d'autres solutions sont à l'étude :

Le contrôle d'accès

Les systèmes numériques de gestion des droits (les Digital Right Management Systems, DRMS) permettent de distribuer des œuvres en ligne selon des usages contrôlés : achat d'un titre musical, possibilité de le copier une ou deux fois, de le lire, de le faire passer d'un ordinateur à un baladeur, de le prêter. Grâce aux DRMS peut en effet être envisagée la mise en place d'offres légales en ligne.

Le marché de la vente en ligne de musique a décollé en 2004 mais reste marginal par rapport au niveau des échanges en P2P (le volume des fichiers payants téléchargés représenterait moins de 5% du nombre des fichiers téléchargés gratuitement. Mais le droit exclusif protégé par des DMRS ne semble pas pouvoir s'imposer de manière unique dans la mesure où il ne tient pas compte des caractéristiques particulières des réseaux (systèmes d'échanges fondés sur le principe de parité et pas seulement mode de distribution).

La licence légale

La possibilité d'appliquer un système de licences légales donnant accès librement aux œuvres moyennant une compensation financière versée aux ayants droit a également été envisagée. Mais, si l'un des avantages de cette solution consiste à prendre acte d'une pratique sociale massivement répandue en la légalisant tout en assurant une rémunération aux titulaires des droits, ce modèle présente cependant de nombreux inconvénients. Quel taux de taxe envisager afin de récolter des sommes suffisantes ? Quelles catégories de contenus doivent être concernées ? Comment répartir les fonds récoltés ? Comment assurer la viabilité de telles solutions au-delà des décisions prises par quelques Etats ?

A cette solution publique difficile à mettre en pratique répondent des formes de transferts privés qui connaissent un certain succès, dans lesquelles les productions culturelles sont utilisées comme produit d'appel. C'est l'exemple d'Apple, qui, grâce à l'écoute de son site iTunes Music Store, commercialise ses baladeurs numériques Ipod.

Le libre accès

La mise à disposition gratuite d'œuvres avec le consentement de leurs auteurs répond à une logique prenant pour référence le mouvement du logiciel libre. Parce que le consentement des auteurs est requis, il s'agit de modèles très différents de ceux des réseaux ou des sites qui exploitent des contenus sans l'accord des titulaires des droits, s'exposant ainsi à des poursuites pour violation de la propriété intellectuelle. De nouveaux outils juridiques d'abord testés dans l'univers du logiciel se sont répandus dans le domaine culturel : les licences de type Creative commons constituent des tentatives pour donner aux auteurs un cadre juridique contractuel complémentaire au droit d'auteur afin de leur permettre de partager leurs œuvres sans en perdre le contrôle.

Le cas de la France, la loi DADVSI

En adoptant le 1er août 2006 la loi relative au droit d'auteur et aux droits voisins dans la société de l'information (DADVSI), la France a transposé la directive européenne du 22 mai 2001 sur le droit d'auteur. Lors du débat parlementaire, deux positions autour des pratiques de téléchargement se sont opposées : celle favorable à l'instauration d'une licence globale, qui a été rejetée par les parlementaires au grand dam de nombreux internautes, des associations de consommateurs et de certaines sociétés d'interprètes, et celle défendue avec succès par les organisations d'auteurs, de producteurs et des industriels de la culture, qui préfèrent limiter les exceptions au droit d'auteur, renforcer la protection technique et juridique des œuvres et sanctionner les pratiques illicites. Les opposants à la licence globale estiment que la rémunération issue d'un système de licence globale ne couvrirait pas les investissements réalisés et jugent donc ce système menaçant pour la création.

Ainsi, le texte légalise les dispositifs de protection anti-copie pour les auteurs et les ayants droit qui diffusent leur œuvre sur internet. Ces dispositifs sont définis comme étant "des mesures techniques efficaces (brouillage, cryptage, application d'un code d'accès, etc...) destinées à empêcher ou limiter les utilisations non autorisées par le titulaire d'un droit". Il s'agit de la légalisation des DRMS. Le

principe de l'exception pour copie privée (possibilité de copier une œuvre pour son usage personnel) est reconnu mais des sanctions sont prévues en cas de contournement des mesures techniques anti-contrefaçon. La loi prévoit la création d'une Autorité de régulation des mesures techniques (ARMT) qui sera chargée de veiller à la garantie de la copie privée et à l'interopérabilité des mesures techniques de protection, c'est-à-dire de s'assurer qu'elles n'empêchent pas de lire les œuvres légalement acquises sur différents types de support. Elle fixera également le nombre de copies privées autorisées et tranchera les litiges entre les consommateurs et les ayants droit (auteurs, interprètes, etc.). Enfin, le téléchargement et la mise à disposition de fichiers soumis au droit d'auteur depuis un logiciel d'échange "pair à pair" étaient considérés comme des contraventions dans le projet de loi et le texte prévoyait des sanctions graduées allant de 38 à 150 euros. Saisi par des députés, le Conseil constitutionnel, dans sa décision du 27 juillet 2006, les a requalifiés comme des délits de contrefaçon, ce qui autorise des peines allant jusqu'à 3 ans d'emprisonnement et 300 000 euros d'amende.

Protecteurs des créateurs et de leurs rémunérations, les droits de propriété intellectuelle dans la société de l'information sont l'objet de polémiques, pris entre l'objectif de financement de la création et de la protection de la valeur de celle-ci et l'objectif d'accès du plus grand nombre aux œuvres de l'esprit, qui prévalait dans la définition de la société de l'information.

En novembre 2007, un accord est signé en France par l'État, les professionnels de l'audiovisuel, du cinéma, de la musique et les fournisseurs d'accès à internet, sur la base du rapport de la mission confiée à Denis Olivennes, président de la FNAC. Intitulé "Le développement et la protection des oeuvres culturelles sur les nouveaux réseaux", le texte du rapport prévoit notamment l'installation d'une autorité administrative chargée de superviser la lutte contre le téléchargement pirate.

Site la documentation française – dossier internet dans le monde (extrait)

La cybercriminalité : interview du Procureur brésilien Luiz Costa

Le développement rapide d'internet et la diversification de ses usages, soulèvent de nombreuses interrogations techniques, sociologiques et surtout juridiques. En effet se pose la question de savoir comment le droit appréhende ce phénomène qui ignore les frontières.

L'une des principales règles procédurales de la Justice impose que l'action des tribunaux soit nécessairement conditionnée par un critère géographique. Or la caractéristique essentielle d'internet est justement que ce phénomène transcende les frontières. La poursuite des infractions commises en ligne est dès lors des plus délicates, posant notamment des questions pointues de compétence des tribunaux.

Certains Etats recourent à des textes spéciaux, pour encadrer des activités réelles, comme les transactions ou les publications, qui se déroulent sur un espace désormais virtuel. D'autres pays, à l'instar du Brésil, utiliseront les textes généraux qui existent en matière civile, commerciale ou pénale par la requalification des faits commis à travers internet.

A l'échelon international, des conventions et des organismes de coopération existent, afin de concerter les actions des Etats dans la poursuite des infractions commises en ligne. Des actions communes comme le « Safer internet day » ont également été organisées au sein de l'UE.

Les affaires Yahoo, en France et Google, au Brésil, sont particulièrement révélatrices de la complexité de certains litiges en la matière et des formes de criminalité susceptibles de se propager par internet.

M. Luiz Costa suit actuellement en France la formation dispensée par le master de droit de l'Internet public de l'Université Paris I Panthéon- La Sorbonne

Site ministère de la justice et des libertés

Mobilisation contre la cybercriminalité

A l'occasion, le 24 mars, du 3e forum international de Lille consacré à la cybercriminalité, Michèle Alliot-Marie a annoncé le renforcement des moyens de lutte contre ce type d'infractions.

Lors de son intervention, la ministre de l'Intérieur a rappelé les mesures adoptées pour améliorer la lutte contre la cybercriminalité :

- le nombre de cyberenquêteurs a été porté de 200 à 300 à la fin de l'année pour la police nationale, et à 214 pour la gendarmerie ;

- l'ouverture du site <http://www.internet-signalement.gouv.fr/>, permet, depuis le mois de janvier, de signaler toute malversation sur internet. Près de 450 000 connexions y ont été recensées, pour plus de 12 500 signalements ;

- la création d'un groupe dédié aux escroqueries sur internet au sein de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication de la police judiciaire.

Pour renforcer ces actions, plusieurs mesures ont été inscrites dans le projet de Loppsi, qui doit être présenté devant le Parlement :

- le renforcement de la sanction en cas d'usurpation d'identité sur internet ;

- le "blocage des contenus à caractère pédopornographique par les fournisseurs d'accès à internet" ;

- la "possibilité de captation de données numériques à distance", qui permettra aux enquêteurs, par exemple, "de saisir en temps réel des données au moment où elles s'affichent sur l'écran d'un pédophile ou d'un terroriste".

Michèle Alliot-Marie a en outre affiché sa volonté d'accroître la coopération internationale, via :

- l'adoption par le Conseil des ministres de l'Union européenne de la création d'une plateforme européenne de signalement des infractions relevées sur internet, qui sera mise en place cette année ;

- la poursuite de la coopération bilatérale, notamment avec les Etats-Unis ou la Russie.

La ministre a souhaité associer l'ensemble des acteurs de la chaîne de sécurité en favorisant les structures d'échanges et de dialogue :

un conseil de sécurité économique a été mis en place au sein du ministère de l'Intérieur en vue de "mieux travailler ensemble à l'identification des menaces". En son sein, un groupe dédié à l'insécurité économique a la charge de faire avancer la réflexion dans ce domaine ;

un Conseil national du numérique, chargé de la concertation avec les acteurs du secteur, sera créé dans le cadre du plan France numérique 2012.

Pour la question spécifique de la protection des entreprises face à l'"ingérence et l'espionnage industriel", la ministre de l'Intérieur a annoncé :

l'élaboration par chaque préfet de région d'un "plan triennal d'intelligence économique", en lien avec les services concernés, notamment la DCRI ;

la soumission des entreprises du secteur de l'intelligence économique et de leurs dirigeants à une procédure d'agrément, via l'avis d'une "commission consultative nationale", qui associera les professionnels ;

pour réduire le risque de trafics d'influence, un "délai de trois ans avant que les fonctionnaires civils et militaires ayant exercé dans un service de renseignement puissent exercer des activités privées" est instauré.

Portail du Gouvernement
25 mars 2009

Première réflexion internationale sur la cybercriminalité

Le premier forum international consacré à la "cybercriminalité" a vu le jour près de Lille, afin d'amorcer une solution contre ce nouveau type de criminalité.

Le premier forum international consacré à la "cybercriminalité" s'est déroulé jeudi 22 mars dans le nord de la France à Marcq-en-Baroeul, près de Lille. Il a réuni plus de 500 participants de nationalités diverses, qui ont un rôle dans la prévention, la répression et la sécurité, tels des policiers, gendarmes et juristes.

Lors de l'ouverture du forum, Daniel Canepa, le préfet du Nord-Pas-de-Calais, a invité ses participants "à enrayer la cybercriminalité" en cherchant des solutions de manière "décloisonnée: internationale, interministérielle et inter-services". Puisque "l'adjonction des termes cybercriminalité et international est presque redondante" a-t-il rappelé.

Un ordre public du cyberspace

Le forum avait notamment pour but de créer des bases sur lesquelles pourrait reposer un "véritable ordre public du cyberspace", afin de contrer "les nouvelles menaces dont les conséquences sont loin d'être virtuelles", a-t-il alarmé.

Les déclarations d'Esther George, membre du Crown Prosecution Service (le parquet) à Londres sont allées dans le même sens, préconisant une "solution globale". Etant donné l'absence de frontières sur la toile et par conséquent dans la cybercriminalité.

Tout au long de cette journée, les participants se sont réunis dans des ateliers de réflexion afin de travailler sur les dispositifs et la législation existants de chaque pays. Ainsi que sur la criminalité organisée et numérique, le piratage électronique et la protection des systèmes.

NOUVELOBS.COM | 25.06.2008

Cyberdouane, un nouveau service pour lutter contre la cyberdélinquance

Eric Woerth s'est rendu au siège de la Direction nationale du renseignement et des enquêtes douanières (DNRED) le 10 février pour inaugurer Cyberdouane. Ce nouveau service a pour mission de recueillir, enrichir et exploiter les renseignements permettant de lutter efficacement contre les fraudes sur internet.

Le développement du commerce sur internet s'accompagne d'une progression de la cyberdélinquance - importations de produits stupéfiants, médicaments, contrefaçons, armes et munitions, œuvres d'art et toute autre marchandise objet de trafics ou de transactions illicites.

Eric Woerth a souhaité accentuer la réponse douanière à ces fraudes commises sur internet en faisant progresser, de 4 à 15 agents, les effectifs douaniers dédiés à cette mission. Cyberdouane est composé de 8 analystes du renseignement et de 7 enquêteurs douaniers.

Les cyberdouaniers, spécialisés dans les nouvelles technologies et en particulier les protocoles de communication d'internet, ont pour mission de détecter les transactions illicites sur internet et de déclencher des contrôles douaniers ciblés ainsi que des enquêtes approfondies.

La création de Cyberdouane au sein de la DNRED est le premier volet d'un vaste plan de lutte contre la cyberdélinquance souhaité par le ministre, décliné à travers plusieurs axes stratégiques : le renforcement des moyens de contrôle ; le démantèlement des filières ; l'adaptation de l'arsenal juridique ; les coopérations inter-administrations, avec les titulaires de droits des marques, les fournisseurs d'accès internet et les sites marchands, les établissements financiers et de paiement sur internet, au niveau international et la responsabilisation des consommateurs.

Eric Woerth a indiqué qu'il souhaitait voir doubler en 2009 les résultats des services douaniers en matière de lutte contre les fraudes sur internet. Il a salué les saisies de marchandises déjà réalisées en 2008 à la suite des contrôles douaniers sur les colis postaux et le fret express : 21 tonnes de cigarettes et 148 000 articles de contrefaçon.

Eric Woerth a également insisté sur la nécessité d'accentuer toutes les formes de coopération entre services de l'Etat et acteurs du monde d'internet, afin de créer un sentiment d'insécurité pour les cyberdélinquants. Il a enfin indiqué qu'il lui paraissait important de responsabiliser les internautes afin qu'ils ne soient "ni acteurs, ni complices, ni victimes" de ce type de fraude.

PORTAIL DU GOUVERNEMENT

10.février2009

Le Gouvernement lance une nouvelle étape de la lutte anti-cybercriminalité

Michèle Alliot-Marie a dévoilé, le 14 février, le plan d'action du Gouvernement en matière de cybercriminalité. Il contient des mesures contre l'usurpation d'identité, l'escroquerie en ligne, les contenus pédopornographiques, racistes ou antisémites et les incitations au terrorisme.

La ministre souhaite tout d'abord établir une charte de bonnes pratiques avec les opérateurs de communications électroniques. Elle devra rendre possible le blocage de sites illicites "comme la Norvège, qui possède un dispositif de blocage de sites pédophiles". Une commission nationale de déontologie des services de communication au public en ligne pourra également délivrer des labels de confiance.

Un décret étendra à l'ensemble des acteurs l'obligation de conserver les données de connexion pendant un an, déjà prévue par la loi anti-terroriste de 2006. Seront concernées les bornes d'accès wi-fi, les éditeurs de messagerie électroniques et les points d'accès publics.

Des peines spécifiques pour le piratage et l'usurpation d'identité

Sous contrôle du juge, la captation à distance des données numériques se trouvant dans un ordinateur ou transitant par lui devrait figurer dans la prochaine LOPSI. "Elle permettra, par exemple, la captation de données au moment où elles s'affichent sur l'écran d'un pédophile ou d'un terroriste", a expliqué Michèle Alliot-Marie.

L'usurpation d'identité sur internet sera punie comme un délit, passible d'un an d'emprisonnement et de 15 000 euros d'amende. Parallèlement, des peines alternatives de travaux d'intérêt général pour les hackers sont prévues. "Ainsi, leurs réelles compétences en la matière pourront être nettement mieux utilisées au service de la collectivité".

Une coopération internationale plus poussée

Michèle Alliot-Marie proposera, lors de la Présidence française du Conseil de l'Union européenne, la mise en place d'accords internationaux permettant la perquisition à distance informatique "sans qu'il soit nécessaire de demander au préalable l'autorisation du pays hôte du serveur".

Enfin, la ministre veut un renforcement des dispositifs d'enquête : cela passerait par la mise en place, dès septembre 2008, d'une plate-forme de signalement automatique de toute forme de malversation, escroquerie, incitation à la haine raciale ou pédopornographie constatée sur internet. Autres moyens prévus : le doublement du nombre d'enquêteurs spécialisés en criminalité informatique, au sein de la direction centrale de la police judiciaire, et d'enquêteurs en technologie numérique de la gendarmerie ; la création de cursus à vocation technologiques au sein de la police nationale, comme il en existe dans la gendarmerie.

LE PORTAIL DU GOUVERNEMENT
15 février 2008

Royaume-Uni : le coût de la fraude bancaire sur Internet a doublé en 2008

Outre-Manche, la fraude sur la banque en ligne a progressé en 2008 de 132% à 57 millions d'euros, en raison notamment d'une hausse de 71% des attaques par phishing. En France, le préjudice est difficile à estimer.

L'association anglaise des moyens de paiement, l'Apacs, a fait ses comptes : en 2008, la fraude bancaire en ligne a coûté 52,5 millions de livres, soit pratiquement 57 millions d'euros. Au-delà de la valeur du préjudice, l'Apacs relève la forte croissance des fraudes sur Internet par rapport à l'année précédente.

En effet, en 2007, l'association avait évalué le coût de la fraude à 22,6 millions de livres. En un an, la croissance a donc été de 132%. Une explosion qui peut s'expliquer en partie par la croissance du nombre d'utilisateurs de la banque sur Internet.

Et cette pénétration dans la population de l'e-banking (ensemble des services bancaires assurés par voie électronique) a naturellement éveillé l'intérêt des cybercriminels : entre 2007 et 2008, les attaques par phishing (hameçonnage) ont notamment progressé de 71%. Le nombre de programmes malveillants conçus pour dérober des données bancaires a lui aussi augmenté sur la période.

La France représente 1,78% des attaques par phishing.

L'Apacs constate également une hausse des fraudes sur les paiements à distance (par téléphone ou Internet). Ils ont représenté en 2008 un préjudice d'un montant total de 328,4 millions de livres (355 millions d'euros), en croissance de 13% par rapport à 2007. Pour l'association, ce constat s'explique notamment par le développement du commerce sur Internet.

Si l'Europe n'est pas épargnée par le phishing, elle demeure cependant moins ciblée que les Etats-Unis. D'après le baromètre de l'Anti-Phishing Working Group (APWG), un consortium international composé d'éditeurs de sécurité et d'acteurs de l'Internet comme eBay, les Etats-Unis représentaient en février 50% des attaques de phishing.

Sur la même période, la part de la France était de seulement 1,78%, de 1,86% pour le Royaume-Uni, de 2,74% pour l'Allemagne, mais de plus de 8% pour la Suède.

Dans l'Hexagone, les principaux acteurs de la finance ont déjà été visés par le phishing au cours des dernières années comme le CIC, BNP-Paribas ou la Société Générale. Mais contrairement au Royaume-Uni, le coût de cette fraude reste difficile à estimer.

D'après le rapport 2007 de l'Observatoire de la sécurité des paiements, le taux de fraude sur les paiements à distance par Internet était de 0,281%. Cela représente un montant de 26,4 millions d'euros. Les chiffres spécifiques de la fraude sur la banque en ligne ne sont cependant pas précisés.

Par ZDNet.fr, publié le 24/03/2009 - L'express.fr

Plan de lutte contre la cybercriminalité

Michèle ALLIOT-MARIE, ministre de l'Intérieur, de l'outre-mer et des collectivités territoriales, s'est rendue le 14 février à l'Office central de lutte contre la criminalité liée aux technologies de l'information de la communication (OCLCTIC) à NANTERRE (Hauts-de-Seine) afin de se faire présenter la nouvelle plate-forme de signalement des sites Internet illicites.

En présence du général d'armée Guy PARAYRE, directeur général de la gendarmerie nationale, madame le ministre a présenté, à cette occasion, son plan de lutte contre la cybercriminalité (lié à la lutte contre le terrorisme, la pédopornographie, les escroqueries en ligne, etc.).

Dans son discours, madame ALLIOT-MARIE a mis l'accent sur la nécessité, dans une société en perpétuelle évolution, de faire preuve de réactivité, d'être toujours en avance sur la cybercriminalité et de répondre aux nouvelles technologies par des instruments en constante adaptation. Elle a également insisté sur la nécessaire adaptation de la législation et la modernisation plus globale des méthodes d'investigation.

Sources : Ministère de l'Intérieur, de l'outre-mer et des collectivités territoriales (MIOMCT)

Intervention de Michèle ALLIOT-MARIE, Ministre de l'intérieur, de l'outre-mer et des collectivités territoriales

Mesdames et Messieurs,

Internet connaît depuis vingt ans un développement spectaculaire.

Dans la vie quotidienne, Internet, c'est d'abord plus de libertés. Plus de libertés pour les individus, qui se connectent chaque jour par millions, par-delà les frontières. Plus de libertés pour les entreprises, qui peuvent accéder à des marchés mondialisés.

Internet, c'est aussi plus de menaces sur la sécurité. Escroquerie, faux mails, vols de numéros de cartes bancaires se sont rapidement répandus sur Internet. La pédopornographie et le trafic de stupéfiants y ont trouvé un moyen de propagation planétaire. Le terrorisme fait d'Internet un vecteur de propagande et un moyen de mettre sur pied des réseaux opérationnels.

L'actualité nous le rappelle régulièrement.

Dans ce domaine l'action est, je le sais, particulièrement difficile. Difficile, parce que nous sommes dans le domaine de l'immatériel. Difficile, parce que les techniques évoluent très rapidement. Je pense au développement récent de la vidéo sur Internet ou d'Internet sur nos téléphones. Difficile, parce que les sites Internet et les données auxquelles nous accédons proviennent souvent de serveurs hébergés dans d'autres pays.

Pourtant, je ne crois pas en la fatalité. Le plan d'action que je vous présente aujourd'hui marque une nouvelle étape dans la lutte contre la cybercriminalité.

Je tiens à remercier François JASPART, qui a conduit la mission "cybercriminalité et usage des technologies de la communication à des fins frauduleuses", pour sa contribution.

Mon action repose sur une conviction très forte : pour qu'il y ait de la liberté, il faut de la sécurité. Face à la cybercriminalité, nous ne garantirons le plein exercice de la liberté des usagers et des citoyens qu'en nous en donnant les moyens adaptés.

Il existe deux formes de cybercriminalité. L'une consiste dans l'atteinte aux réseaux. C'est le piratage, l'intrusion sur les sites, l'attaque d'un Système de Traitement Automatisé de Données. Nous disposons de l'arsenal législatif nécessaire à la lutte contre cette forme de cybercriminalité.

La deuxième, en fort développement, utilise le réseau comme un terrain d'action. Je pense à l'escroquerie, aux contenus pédopornographique, racistes ou antisémites de certains sites, aux atteintes à la vie privée, à la diffusion de modes d'emploi d'explosifs.

Pour nous donner les moyens d'une action plus forte et efficace, il faut d'abord améliorer notre connaissance de la cybercriminalité. Je souhaite que nous disposions rapidement d'outils statistiques fiables sur le phénomène. La mise en place d'un indicateur spécifique dans l'état 4001, sera bientôt possible, grâce au logiciel Ardoise et aux travaux menés par Alain BAUER.

Il nous faut ensuite apprendre à travailler ensemble. La lutte contre la cybercriminalité fait partie d'une chaîne, comme toute action en matière de sécurité. La police et la gendarmerie en sont des

acteurs essentiels, mais ils ne sont pas les seuls.

Je me tournerai donc vers l'ensemble des acteurs concernés par la lutte contre la cybercriminalité. Je pense en premier lieu aux fournisseurs d'accès à Internet. J'entends engager avec eux un dialogue constructif sur les actions à mener en commun contre la cybercriminalité.

Je souhaite une charte de bonnes pratiques améliorant la coopération avec les opérateurs de communications électroniques. La mission que dirige François JASPART en pilotera l'élaboration. Cette charte devra permettre le blocage des sites illicites comme la Norvège, qui possède un dispositif de blocage de sites pédophiles. Elle devra permettre l'accélération de la transmission des informations aux services de police et de gendarmerie.

Au-delà des fournisseurs d'accès, ma démarche s'adresse à l'ensemble des acteurs de la chaîne : les hébergeurs de site, les opérateurs, les associations d'utilisateurs, dont les familles.

La création d'une commission nationale de déontologie des services de communication au public en ligne est actuellement en préparation. Elle réunira les pouvoirs publics, les opérateurs et les associations d'usagers.

Elle formulera des recommandations d'ordre déontologique, afin de garantir la protection des consommateurs et en particulier des enfants. Elle délivrera des labels de confiance.

Pour que ce projet, qui concerne plusieurs ministères, voie le jour le plus vite possible, j'entends agir en liaison avec mon collègue Xavier BERTRAND.

Pour réussir, nous devons être pragmatiques, utiliser tous les moyens nationaux comme internationaux. Nous avons aussi l'obligation de moderniser les moyens de la police et de la gendarmerie.

La société évolue, la criminalité aussi. Nous devons faire preuve de réactivité, être toujours en avance sur la cybercriminalité. Il faut répondre aux nouvelles technologies par des instruments en constante adaptation.

Je veux tout d'abord adapter notre législation aux pratiques contemporaines de la cybercriminalité.

L'adaptation de notre législation passera d'abord par une modernisation plus globale de nos méthodes d'investigation.

L'identification des utilisateurs d'Internet doit être facilitée. Je souhaite nous donner les moyens techniques et juridiques de le faire. Il faudra en particulier évoluer, dans le cadre de procédures judiciaires, vers la géolocalisation des utilisateurs d'Internet.

Je souhaite donc établir les règles de coopération des acteurs de l'Internet avec les services concernés par la lutte contre la cybercriminalité.

La loi anti-terrorisme de 2006 prévoit pour les cybercafés, entre autres, l'obligation de conserver à la disposition des autorités judiciaires les données de connexion pendant un an. Il faut clarifier cette disposition pour qu'elle puisse être applicable à l'ensemble des acteurs de l'Internet. Un décret détaillera pour chacun de ces acteurs la liste des catégories de données à conserver. Cette obligation pourra alors s'appliquer aux bornes d'accès Wifi, aux éditeurs de messagerie électronique, aux points d'accès dans les lieux publics.

Par ailleurs, il convient d'autoriser sous contrôle du juge la captation à distance de données numériques se trouvant dans un ordinateur ou transitant par lui. Cette procédure concernera la criminalité organisée et figurera dans la future LOPSI. Elle permettra, par exemple, la captation de données au moment où elles s'affichent sur l'écran d'un pédophile ou d'un terroriste.

L'adaptation du droit passera aussi par la création de nouvelles formes d'incrimination.

Il est aujourd'hui possible d'utiliser à des fins malveillantes l'identité d'une personne physique ou morale sur Internet pour ouvrir des comptes de messagerie, pour accéder à un site, pour créer un site, pour envoyer des spams.

Je veux que l'usurpation d'identité sur Internet soit punie par la loi comme un délit, passible d'un an d'emprisonnement et de 15 000 euros d'amende. Cette disposition sera intégrée, elle aussi, à la LOPSI.

En outre, le piratage doit faire l'objet de sanctions spécifiques. C'est pourquoi je proposerai la création de peines alternatives de travaux d'intérêt général pour les "hackers" condamnés.

Ainsi, leurs réelles compétences en la matière pourront être nettement mieux utilisées au service de la collectivité.

Cela passera aussi par la mise en oeuvre d'une meilleure coopération internationale.

La cybercriminalité ne connaît pas de frontières. Notre action ne peut se passer d'une coopération internationale approfondie.

Prenons l'exemple de l'investigation en ligne. Souvent les pédophiles stockent des images illicites non pas sur leur propre ordinateur, mais sur des sites de stockage hébergés dans un autre pays. La perquisition à distance est donc devenue un instrument incontournable de sécurisation d'Internet. La coopération avec nos partenaires nous permettra d'élargir son champ d'application.

La loi pour la sécurité intérieure de 2003 autorise les perquisitions sur un réseau informatique, tant que les systèmes informatiques concernés se trouvent situés sur le territoire national.

L'exécution des commissions rogatoires internationales peuvent prendre beaucoup de temps.

Assez pour que les données visées par l'enquête soient effacées. Je proposerai donc, lors de la présidence française de l'Union Européenne, la mise en place d'accords internationaux permettant la perquisition à distance informatique sans qu'il soit nécessaire de demander au préalable l'autorisation du pays hôte du serveur. Bien évidemment, comme toute perquisition, cette procédure s'effectuera sous contrôle du juge.

Nous savons en outre que, sans vouloir stigmatiser quiconque et à titre d'exemple, de nombreux sites illicites sont domiciliés aux Etats-Unis, en Russie ou en Chine. Cela tient soit à la législation des pays, soit au fait que le nombre de sites hébergés dans ces pays est beaucoup plus élevé qu'en France.

La Russie accepte maintenant plus volontiers de répondre à nos sollicitations, lorsque nous leur signalons des sites pédophiles, par exemple. Pour les Etats-Unis, avec qui nos relations sont permanentes sur ce sujet, la quantité de sites hébergés nécessite une procédure plus directe d'échanges d'informations. Je me rendrai prochainement aux Etats-Unis pour examiner les possibilités d'une coopération bilatérale avec nos partenaires américains.

Pour lutter contre la délinquance en général et la cybercriminalité en particulier, les policiers et les gendarmes doivent être au moins au niveau technique des délinquants et, j'oserais dire, meilleurs que les hackers dont je parlais à l'instant.

Il est donc impératif de faire évoluer en permanence les moyens humains et techniques dont nous disposons dans trois directions : la mutualisation, la formation, l'amélioration du signalement des sites illicites.

Première direction, la mutualisation.

J'insiste sur la nécessité, dans la lutte contre la cybercriminalité, de mutualiser les efforts des services de la police et de gendarmerie. L'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication regroupe policiers et gendarmes. Je veux renforcer son action, en créant en son sein un groupe dédié aux escroqueries sur Internet. Il permettra une centralisation opérationnelle.

Ces escroqueries relèvent d'un mode opératoire techniquement de plus en plus élaboré. Leur résolution nécessite une forte compétence technique. L'expertise de ses agents permettra une action ciblée et un travail de concert avec les pays touchés par ce type de criminalité.

La Grande Bretagne, par exemple, refuse de traiter des dossiers d'escroquerie sur Internet endessous d'un seuil de quelques milliers d'euros. Une coopération accrue avec nos amis britanniques permettra de mettre en évidence l'existence de réseaux organisés, responsables de préjudices globaux, et donc de traiter l'affaire.

Plus généralement, il faut mutualiser les expériences et les savoirs-faires acquis par chacun des services impliqués dans cette lutte. Je pense, au sein de la police nationale, à la Brigade d'Enquête sur les Fraudes aux Technologies de l'Information (BEFTI) et à la Brigade de Faux Moyens de Paiement (BFMP) pour la Préfecture de Police, ou aux brigades spécialisées des directions interrégionales de police judiciaire.

Au sein de la gendarmerie nationale, la lutte contre la cybercriminalité associe l'Institut de Recherche Criminelle de la Gendarmerie Nationale (IRCGN), le Service Technique de Recherches Judiciaires et de Documentation (STRJD), et les sections territoriales de recherche de la gendarmerie nationale. Ces services effectuent déjà un travail remarquable. Je les en félicite. Nous irons encore plus loin en partageant au mieux les expériences acquises par chacun.

Deuxième direction, la formation.

- Je veux augmenter le nombre des personnels formés à la lutte contre la cybercriminalité.

Je veux doubler le nombre de nos cyber-enquêteurs. Nous formerons deux fois plus d'Enquêteurs Spécialisés en Criminalité Informatique (ESCI) au sein de la Direction Centrale de la Police Judiciaire et d'enquêteurs en technologie numérique de la gendarmerie (N'TECH). Ces enquêteurs, qu'ils soient issus de la police ou de la gendarmerie, recevront une formation commune du plus haut niveau.

Je souhaite en outre que nos Attachés de Sécurité Intérieure (ASI) soient sensibilisés à la lutte contre la cybercriminalité par le biais d'une formation spécifique. Nous pourrions ainsi établir un lien permanent avec les Etats qui font face au même problème. Nous pourrions également sensibiliser les Etats qui ne se sont pas encore dotés d'une législation adaptée.

La formation ne se réduit pas à mes yeux à une question de quantité. Elle est aussi une question de qualité.

La formation à la lutte contre la cybercriminalité devra être encore plus pointue. J'établirai des partenariats avec les organismes de recherche publique et l'industrie française.

Je veux accentuer l'implication de la police et de la gendarmerie dans les programmes de recherche et dans les pôles de recherche et de développement de l'industrie française. Dès juin 2008, je mettrai en place un réseau d'experts au sein de nos services pour définir des axes de recherche au profit des services opérationnels. Des cursus à vocation technologique seront créés au sein de la police nationale en partenariat avec l'université, comme il en existe déjà dans la gendarmerie.

Troisième direction, l'amélioration du signalement des sites illicites.

Les dispositifs de signalement de ces sites doivent mieux associer prévention et signalement.

Nous disposons déjà d'une plate-forme automatisée pour le signalement des sites pédopornographique. Le signalement des autres types de sites illicites se fait pour l'instant de manière non automatisée.

Ce dispositif a donné des résultats prometteurs. La plate-forme de signalement de l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication compte aujourd'hui 8 policiers et gendarmes. Elle a traité près de 15 000 signalements. Elle en a orienté 308 vers des services de Police, de Gendarmerie et des Douanes, et 1552 vers Interpol. Elle a permis d'élucider un certain nombre de délits et facilité l'arrestation de plusieurs pédophiles violeurs.

Je veux renforcer ce dispositif. Je vais créer en 2008 un site Internet de conseils et de prévention contre les contenus illicites d'Internet pour sensibiliser les utilisateurs d'Internet aux dangers de la cybercriminalité.

Il donnera en outre aux internautes les moyens de signaler automatiquement toute forme de malversation constatée sur Internet : l'escroquerie sur Internet, mais aussi les sites pédopornographiques, l'apologie du terrorisme, l'incitation à la haine raciale.

Le traitement des signalements se fera en temps réel. La police transmettra ensuite à la justice lorsque les faits seront caractérisés. Cette plate-forme sera opérationnelle dès septembre 2008.

Je veux compléter ce dispositif national par un dispositif européen de signalement.

Je souhaite que soit rapidement mise en place une plate-forme européenne de signalement des sites illicites. 17 pays d'Europe sont aujourd'hui dotés de systèmes de plate-forme de contenus illicites sur Internet. Chaque pays ayant sa propre législation, les systèmes sont tous différents. Je souhaite qu'une plate-forme européenne d'échanges d'informations sur la cybercriminalité soit mise en oeuvre

dans le cadre d'Europol. Je profiterai là aussi de la présidence française de l'Union Européenne pour y parvenir.

Mesdames, Messieurs,

Les progrès accomplis par la cybercriminalité mettent à l'épreuve notre réactivité. Vous l'avez compris, mon action sera ferme et résolue. Elle se fera en concertation avec l'ensemble des ministères concernés par la lutte contre la cybercriminalité. Je proposerai la création d'un comité interministériel d'investigations en matière de technologies de l'information et de la communication. La lutte contre la délinquance classique, comme la lutte contre la cybercriminalité, ne supporte aucune faiblesse. Mais, dans notre lutte contre la cybercriminalité, comme dans celle contre la délinquance ordinaire, nous ne saurions empiéter sur les libertés individuelles.

Il ne s'agit pas de surveiller à la "Big Brother". Il s'agit de protéger les utilisateurs d'Internet.

Mon ambition est de garantir aux internautes et à l'ensemble de nos concitoyens la pleine jouissance de leur droit à la sécurité. Cette liberté fondamentale est la condition de toutes les autres. Mon ambition est de donner à la police et de la gendarmerie tous les moyens pour faire face au défi de la cybercriminalité. Mon ambition est, en somme, de ne jamais laisser le dernier mot aux trafiquants, aux pédophiles et aux terroristes.

Nous ferons usage de toutes nos armes contre ce fléau qu'est la cybercriminalité. Il en va de la sécurité des Français et, je le crois, des intérêts vitaux de la Nation.

Je vous remercie.

Site defense.gouv.fr

Cybercriminalité : Michelle Alliot-Marie renforce les effectifs d'enquêteurs

Fin 2009, police et gendarmerie disposeront de plus de 500 cyber-enquêteurs selon la ministre de l'Intérieur. Ils seront aussi dotés de nouveaux moyens d'investigation, comme la captation à distance de données numériques.

A l'occasion du Forum international sur la cybercriminalité (qui s'est tenu à Lille le 24 mars), la ministre de l'Intérieur Michèle Alliot-Marie a annoncé l'augmentation du nombre d'enquêteurs affectés à la lutte contre les crimes et délits liés aux nouvelles technologies.

A la fin de l'année 2009, ils seront 300 dans la police (soit 100 de plus) et 214 dans la gendarmerie. En trois ans, les effectifs des cyber-enquêteurs en France auront ainsi doublé. Le patron du CERTA (Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques), le colonel Stanislas de Maupeou, regrette toutefois le manque de centres d'alerte informatique en France : 5 CERT contre 18 en Allemagne et 17 au Royaume-Uni.

La captation à distance par la police de nouveau évoquée

La ministre a également vanté les premiers résultats du dispositif de signalement sur Internet : internet-signalement.gouv.fr. Le site Web, qui permet d'informer les services de police d'actes illégaux relatifs notamment à des escroqueries, de la pédopornographie ou des incitations à la haine raciale, a enregistré 12 500 signalements en moins de trois mois.

Michèle Alliot-Marie a rappelé aussi que la future loi d'orientation pour la sécurité intérieure (Lopsi 2) doterait les autorités de nouveaux moyens de lutte contre la cybercriminalité. Il s'agira notamment, comme elle avait déjà évoqué en 2008, de la captation de données numériques à distance par les policiers.

Les modalités de ces perquisitions ou écoutes à distance doivent toujours être précisées. Plusieurs pistes sont explorées en France, mais aussi en Europe : autorisation préalable ou non par un juge, installation de programmes espions physiques ou logiciels, interceptions d'échanges numériques, ...

Par ZDNet.fr, publié le 25/03/2009 - L'express.fr

Les eurodéputés s'engagent pour un « accès sans réserve à Internet »

Le rapport d'un député visant à garantir aux citoyens le « droit d'accéder à l'ordinateur et à l'Internet » a été adopté par la commission des libertés civiles du Parlement européen. Une nouvelle expression du refus de voir notamment s'appliquer la riposte graduée.

Une nouvelle fois, les eurodéputés expriment leur vigilance et leur désaccord face aux projets de lois de certains Etats de l'UE tentés de limiter l'accès à Internet.

La commission des Libertés civiles, de la Justice et des Affaires intérieures a adopté à l'unanimité de ses 44 membres un rapport du député grec Stavros Lambridinis (groupe PSE). Il vise à garantir aux citoyens européens « un accès à Internet sans réserve et sûr », à renforcer « l'engagement résolu de lutter contre la cybercriminalité », mais aussi à porter « une attention constante à la protection absolue et à la promotion renforcée des libertés fondamentales sur Internet ».

Ce rapport servira de base pour des recommandations au conseil de l'Europe et devra encore faire l'objet d'un vote du Parlement en assemblée plénière.

Ouvrir la voie à une surveillance massive

Dans l'exposé des motifs, le député Lambridinis met en garde contre les tentations sécuritaires de certains Etats de l'UE en matière de surveillance des réseaux : « Internet peut également renforcer considérablement nos droits fondamentaux, tels que la liberté d'expression, d'action politique et d'association - mais il peut également les affaiblir. Un exemple récent en a été fourni par l'initiative législative concernant la surveillance des discours sur Internet visant à prévenir les attaques terroristes. Il s'agit d'un exemple classique d'une législation qui, si elle n'est pas étroitement ajustée à ces objectifs, pourrait ouvrir la voie à une surveillance massive, paralysant ainsi le discours politique des individus - qui est au coeur d'une société démocratique. »

Il précise aussi qu'« il ne fait aucun doute qu'Internet offre aux auteurs de crimes ou de délits de nouveaux instruments puissants, et il faut bien évidemment empêcher les terroristes d'utiliser Internet pour planifier et exécuter des attaques. De la même façon, nos sociétés exigent à juste titre que nous empêchions d'agir les auteurs de pornographie infantile sur Internet. Les délits constituent des menaces tangibles, ce qui porte les citoyens à opposer une moindre résistance aux appels des services de police en faveur de l'exercice d'une large surveillance sur Internet - qui, par nature est "intangibile". Nous devons lutter contre cette tendance. »

Pas de refus à l'accès internet comme sanction

Enfin, l'eurodéputé demande aux différentes institutions européennes de garantir « le droit à l'éducation et le droit à l'accès à Internet », considérant qu'ils peuvent être menacés « dans le contexte de la lutte contre la criminalité sur Internet » ; il ajoute que « cet accès ne doit pas être refusé en tant que sanction ». La référence au projet de loi français Création et Internet et à

l'instauration de la future Hadopi (Haute Autorité pour la Diffusion des Oeuvres et la Protection des Droits sur Internet) ne peut être plus claire.

En septembre 2008 déjà, le Parlement européen avait voté un amendement au projet de directives dit Paquet Telecom. Il rendait caduc le projet de loi français en exigeant qu'une suspension de l'accès à Internet ne puisse être prononcée que suite à une décision de justice. Si le vote de cet amendement avait été suivi par la Commission européenne en novembre 2008, les ministres des Télécoms des états membres de l'UE l'aurait supprimé du texte final du Paquet Télécom quelques jours plus tard.

On peut donc craindre le même sort pour le rapport de l'eurodéputé Lambridinis, même s'il il sera voté en réunion plénière du Parlement européen et transcrit sous forme de loi ou de directive.

Par ZDNet.fr, publié le 18/02/2009 - L'express.fr

Loppsi II

Le nouveau plan quinquennal de sécurité

La nouvelle loi de programmation sur la sécurité intérieure (Loppsi II), présentée mercredi en Conseil des ministres, pourrait changer la vie quotidienne de millions de Français. Le gouvernement veut reprendre l'initiative en matière de sécurité.

Sécurité routière, espionnage, vidéoprotection, intelligence économique: Michèle Alliot-Marie présente mercredi en conseil des ministres son projet de Loi d'orientation et de programmation pour la performance de la Sécurité intérieure (Loppsi), deuxième du genre, qui s'étend de 2009 à 2013. Ce texte, dont la première mouture remonte à l'automne 2007, a été maintes fois reporté, au profit de projets de loi d'ordre économique et social. Il doit permettre au gouvernement de reprendre l'initiative en matière de la sécurité. Une exigence du chef de l'Etat.

La Loppsi II prévoit de dégager 2,5 milliards d'euros pour l'Intérieur, sécurité civile comprise, et pourrait être présentée à l'Assemblée nationale courant juillet.

Selon la ministre de l'Intérieur, elle vise à "s'adapter aux évolutions de la délinquance" ainsi qu'à "prévenir les nouvelles menaces". A la lecture, la cohérence du texte ne saute pourtant pas aux yeux. Mais, si la Loppsi est adoptée en l'état, elle changera la vie quotidienne de millions de Français. Revue de détails.

1. Sécurité routière

Confiscation obligatoire du véhicule en cas de récidive

En cas de conduite sans permis ou en cas de récidive dans certains cas (alcoolémie; consommation de stupéfiants; accidents ayant entraîné des blessures; grands excès de vitesse, soit plus de 50 km/h au-delà de la vitesse autorisée), le véhicule sera confisqué. Le juge pourra déroger à cette "peine plancher", à condition de motiver sa décision - par exemple, par le risque de perte d'emploi.

Une peine complémentaire d'interdiction de conduire un véhicule non équipé d'un dispositif d'anti-démarrage par éthylotest est créé.

Trafic de points

Le gouvernement veut lutter contre le trafic de points qui se développe sur Internet ou par le biais de petites annonces dans les revues spécialisées. Une incrimination spécifique est créée, punie d'une peine allant jusqu'à 6 mois d'emprisonnement et 15 000 euros d'amende. L'"échange" de points au sein d'une famille restera en revanche difficile à matérialiser, convient-on place Beauvau.

2. Informatique et Internet

Lutte contre la cybercriminalité

Une nouvelle incrimination sera créée: l'"usurpation d'identité électronique" - elle peut notamment s'appliquer en cas de fausse inscription sur un réseau social en ligne comme Facebook.

Lutte contre la pédopornographie sur Internet

L'Intérieur dressera une "liste noire" des sites que ses services transmettront aux fournisseurs d'accès. Ceux-ci se sont engagés à en bloquer l'accès. Selon la place Beauvau, le système permettra de rendre inopérants certains sites hébergés à l'étranger, auparavant à l'abri de la législation française.

Captation de données à distance

Les services d'enquête judiciaires seront autorisés à "pénétrer" l'ordinateur d'un suspect et à y lire les informations qu'il contient ou qui s'affichent à l'écran. Cette possibilité d'intrusion informatique, qui doit être validée par un magistrat, sera réservée à la lutte antiterroriste et contre la grande criminalité. En pratique, le recours à des logiciels espions sera donc légalisé à des fins judiciaires.

Vidéoprotection

Une durée minimale de conservation des images de vidéosurveillance, modulable selon les lieux et selon les préfetures, est créée - la durée maximale de conservation reste fixée à un mois. Les agents de sociétés privées de gardiennage sont autorisés à visionner en direct les images, afin de détecter d'éventuels flagrants délits, mais ils ne peuvent consulter les enregistrements.

3. Intelligence économique et Renseignement

Moralisation de la profession

Devant la multiplication des affaires de barbouzerie, la place Beauvau veut moraliser les agences et les cabinets d'intelligence économique. Une procédure d'agrément préfectoral, et non plus une simple déclaration, sera obligatoire pour l'organisme et pour ses dirigeants. En outre, policiers et gendarmes ayant travaillé dans le domaine du renseignement ne pourront intégrer de telles structures moins de trois ans après leur cessation d'activité.

Protection des agents de renseignement

Les agents de renseignement pourront témoigner sous leur fausse identité en cas de procédure judiciaire. En cas de révélation de leur véritable identité, les sanctions sont durcies.

4. Préfets délégués à la sécurité

Des pouvoirs renforcés

En matière de maintien de l'ordre, les préfets chargés de la sécurité auront désormais des responsabilités de coordination à l'échelle régionale ou, en tous cas, dans des zones situées à la périphérie des grandes agglomérations, à Paris, Lyon ou Marseille. En coulisse, cette disposition a fait l'objet de vives tensions entre le préfet de police de Paris - militant pour l'élargissement de ses compétences aux Hauts-de-Seine, à la Seine-Saint-Denis et au Val-de-Marne - et la Direction générale de la police nationale - qui plaidait pour le maintien du statu quo.

5. Violences dans les stades

Pour la place Beauvau, les interdictions de stades actuellement en vigueur ne sont "pas suffisamment dissuasives". Les interdictions administratives seront doublées (jusqu'à un an) et une peine d'emprisonnement d'un an pourra être prononcée en cas de non-respect de ces obligations.

Par Eric Pelletier, publié le 26/05/2009 Les échos.fr

Le gouvernement met Internet sous surveillance

La ministre de l'Intérieur a inscrit trois mesures anti-cybercriminalité dans le projet loi Loppsi 2, dont le filtrage de sites Web, qui pourrait faire débat.

La loi Loppsi 2 est à la ministre de l'Intérieur ce que la loi Hadopi est à la ministre de la Culture. Le projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure présenté aujourd'hui en Conseil des ministres comprend en effet un volet Internet qui donne les coudées franches aux cyberenquêteurs dans leur lutte contre la cybercriminalité. La ministre de l'Intérieur, Michèle Alliot-Marie, a fait inscrire dans le texte législatif des mesures qui permettront aux services de l'Etat de surveiller le Web ou de prendre en flagrant délit des internautes malfaiteurs. L'une d'elle, bien que circonscrite aux contenus en ligne à caractère pédopornographique, pourrait faire débat : le filtrage de sites Web. En effet, l'article 6 du projet de loi prévoit que les fournisseurs d'accès à Internet (FAI) « empêchent sans délai l'accès aux contenus dont les adresses électroniques sont désignées par arrêté du ministre de l'Intérieur » - sous peine d'un an d'emprisonnement et de 75.000 euros d'amende. Souvent hébergés à l'étranger, ces contenus répréhensibles identifiés dans une « liste noire » devront être bloqués en France pour protéger les enfants. Les FAI ont adhéré à ce dispositif. Il ne s'agit pas, a priori, d'une obligation généralisée de l'Internet. Reste à savoir ce que prévoira le décret d'application en termes de techniques de filtrage et de prise en compte des coûts supportés par les FAI.

Captation de données

Selon nos informations, la Commission supérieure du service public des postes et des communications électroniques (CSSPCE) a rendu un « avis favorable » le 12 mars dernier en demandant à ce que le filtrage n'intervienne qu'en « second ressort » après l'« échec » des hébergeurs de sites Web déjà responsabilisés par la loi « Confiance dans l'économie numérique » de 2004.

Autre mesure électronique de la Loppsi 2 : la captation à distance de données numériques telles qu'elles s'affichent à l'écran de l'ordinateur. Lors du Forum international de la cybercriminalité, le 24 mars dernier, Michèle Alliot-Marie avait précisé que cela visait aussi bien les pédophiles que les terroristes. Enfin, la lutte contre l'usurpation d'identité sur Internet - y compris sur les réseaux sociaux comme Facebook - sera passible de poursuite. Reste à savoir si le gouvernement divulguera l'avis que la CNIL lui a rendu le 16 avril. Pour la loi Hadopi, elle avait émis des réserves...

CHARLES DE LAUBIER, Les Echos

La cybercriminalité et les chauffards dans le collimateur

Alors que le gouvernement remet l'accent sur la sécurité, la ministre de l'Intérieur présente aujourd'hui en Conseil des ministres sa deuxième loi d'orientation et de programmation dotée d'un budget de 2,5 milliards d'euros.

Deux ans. C'est le temps qu'il aura fallu à la deuxième loi d'orientation et de programmation pour la performance de la sécurité intérieure (Loppsi 2) pour passer des bureaux du ministère de l'Intérieur à ceux de l'Elysée. Alors que le gouvernement remet les questions de la sécurité sur le devant de la scène depuis quelques jours, la ministre de l'Intérieur Michèle Alliot-Marie présente aujourd'hui en Conseil des ministres son texte visant à « apporter une réponse immédiate aux nouvelles réalités de la délinquance ». La réforme, qui pour la première fois concerne la sécurité civile, couvre un champ très vaste, allant de la cybercriminalité à la vidéo-surveillance en passant par le terrorisme, la violence dans les stades et les automobilistes dangereux. Pour la mettre en musique, le gouvernement a prévu une coquette enveloppe de 2,5 milliards d'euros pour la période 2009-2013. Il a déjà distribué 187 millions dans le budget 2009. La dotation grimpera en flèche chaque année pour atteindre 836 millions d'euros dans le budget 2013.

Vidéo-surveillance

Bon nombre de mesures contenues dans ce projet étaient déjà connues. Dès 2007, Michèle Alliot-Marie avait dévoilé son intention de sévir contre les « sorties de route » des chauffards. Le texte prévoit que les auteurs des infractions les plus graves (conduite sans permis, excès de vitesse supérieur à 50km/heure, récidive en cas de conduite sous emprise de l'alcool) verront obligatoirement leur véhicule confisqué. Le trafic de points sera plus sévèrement sanctionné. Autre mesure « grand public », annoncée dès 2008 dans la foulée des incidents survenus dans des stades (banderole injurieuse déployée par le PSG...), les supporters délinquants pourront se voir interdire plus longtemps l'accès aux stades.

Au-delà des sanctions, le texte vise aussi à améliorer concrètement l'organisation de la lutte contre la délinquance. Il crée une nouvelle police d'agglomération placée sous un commandement unique en Ile-de-France, à Lille, Lyon et Marseille, étend les pouvoirs de la police scientifique et technologique (notamment pour le recueil d'empreintes génétiques) et favorise le développement de la vidéo-surveillance dans le secteur privé « pour prévenir les atteintes à la sécurité des personnes et des biens dans les lieux particulièrement exposés ». En 2007, 340.000 caméras avaient été autorisées, pour la plupart dans des lieux publics. Enfin, d'autres mesures sont prévues pour réglementer le sort des sociétés d'intelligence économique et des fonctionnaires ayant exercé des activités de renseignement.

LAURENCE ALBERT, Les Echos

Cybercriminalité : les entreprises ne sont pas assez protégées

La cybercriminalité ne connaît pas la crise. Elle aurait même tendance à en tirer un nouveau dynamisme selon les spécialistes du secteur. Plusieurs enquêtes récentes ont mis en évidence une recrudescence inquiétante des fraudes et attaques de logiciels malveillants à la faveur de la dégradation des conditions économiques. Selon une étude menée par le cabinet KPMG International en collaboration avec la société britannique AKJ Associates, spécialisée dans la sécurité et la gestion du risque, la majorité des professionnels du secteur souligne que les mesures engagées contre des risques, pourtant en nette augmentation, sont encore largement insuffisantes. De l'enquête menée auprès de spécialistes de la sécurité et de la fraude, majoritairement européens, il ressort que 50 % des responsables estiment que les entreprises ne sont pas protégées de manière efficace contre les « malwares » (logiciels malveillants tels que virus, cheval de Troie...). Ces mêmes responsables constatent à 45 % que le nombre d'attaques sur leurs réseaux connaît une forte augmentation et 66 % d'entre eux estiment même que certains informaticiens susceptibles d'être licenciés du fait de la crise pourraient mettre leurs compétences au service de l'économie cybercriminelle !

Ce tableau inquiétant est largement corroboré par les professionnels du secteur - éditeurs de logiciels de sécurité en tête - ainsi que par les récentes attaques dont ont été la cible plusieurs sites communautaires très populaires. Ainsi, selon Symantec, le nombre de virus a progressé de quelque 165 % entre 2007 et 2008 et affiche une progression exponentielle depuis les dernières années. La société russe Kaspersky notait récemment pour sa part que 74 % des programmes malveillants découverts au troisième trimestre 2008 provenaient de sites infectés, favorisant ainsi le téléchargement d'applications malicieuses à l'insu de l'utilisateur. Dans son rapport annuel, Trend Micro pointait de son côté l'émergence de nouvelles menaces liées au développement du « cloud computing » ainsi qu'une recrudescence des détournements de sites redirigeant les utilisateurs vers des serveurs tiers malveillants. Le spam, le hameçonnage (« phishing »), les botnets (réseaux d'ordinateurs « zombies »), l'usurpation d'identité et le développement de la cybercriminalité financière sont également en plein essor à la faveur de la crise. La situation économique actuelle tend à rendre florissante une économie souterraine, qui se chiffre désormais en milliards de dollars.

Le développement du « monde virtuel » attire également les cybercriminels qui trouvent dans les sites communautaires et les réseaux sociaux le moyen de toucher aisément une large audience. Ainsi, après une première alerte début mai, Facebook a de nouveau été contraint, en fin de semaine dernière, de mobiliser ses experts sécurité face à de nouvelles opérations de « phishing » détournant les utilisateurs de la plate-forme communautaire vers des sites leurre, via des imitations de sa page d'accueil.

RÉGIS MARTI, Les Echos
[19/05/09]

Internet, cybercriminalité et cybersécurité

Au préalable, il convient de distinguer entre cyberterrorisme et cybercriminalité.

Guerre informatique, "hactivisme" et cyberterrorisme sont les expressions les plus fréquemment utilisées par les experts pour désigner des agressions à caractère politique commises sur ou à l'aide des réseaux informatiques. Toutefois, les contours de leurs définitions respectives restent difficiles à cerner.

Le cyberterrorisme se traduit par des attaques préméditées et à connotation politique contre des systèmes ou des programmes informatiques, voire contre des données, visant des cibles civiles et proférées par des groupes nationaux ou clandestins. En France, la loi du 1er décembre 2008, qui prolonge l'application des articles 3, 6 et 9 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, comporte un dispositif de réquisition administrative des données relatives aux communications électroniques et l'accès des services de lutte contre le terrorisme à certains fichiers administratifs. En pratique, le travail de veille pour parer aux attaques informatiques est assuré au sein du Secrétariat général de la défense nationale (SGDN) par le centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques (CERTA). Rattaché à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) au sein du SGDN, le CERTA est chargé d'assister les organismes de l'administration à mettre en place des moyens de protection et à résoudre les incidents ou les agressions informatiques dont ils sont victimes. Il constitue le complément indispensable aux actions préventives déjà assurées par la ANSSI et qui se situent plus en amont dans la démarche de sécurisation des systèmes d'information.

Les motivations des cybercriminels sont, quant à elles, essentiellement financières. La cybercriminalité est le fait de réseaux criminels générant des spams, des attaques de phishing, des programmes ou ensemble de programmes permettant à un tiers de maintenir – dans le temps – un accès frauduleux à un système informatique.

Dans la lutte contre la cybercriminalité, différentes mesures ont été adoptées : augmentation du nombre de cyberenquêteurs (de 200 à 300 pour la police nationale et à 214 pour la gendarmerie) et ouverture d'un site permettant de signaler toute malversation sur internet (www.internet-signalement.gouv.fr). L'arrêté du 16 juin 2009 précise que les signalements sont traités par des policiers et gendarmes affectés à la Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (Pharos), elle-même intégrée à l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC).

Pour renforcer la lutte contre la cybercriminalité, plusieurs mesures ont été inscrites dans le projet de LOPPSI, présenté en conseil des ministres le 27 mai 2009, notamment :

la possibilité, sur commission rogatoire d'un juge, de capter à distance et en temps réel (grâce à l'installation d'un logiciel espion), toutes les informations contenues sur les disques durs de l'ordinateur mais aussi celles apparaissant à l'écran. Ce dispositif doit permettre de contrôler également les données enregistrées sur des matériels périphériques comme les clés USB, cartes

mémoires et disques optiques. Cette forme de surveillance devrait être réservée aux affaires liées au terrorisme ou à la "grande criminalité" ;

la création d'un délit d'usurpation d'identité sur internet qui pourra être réprimé pour préjudice moral même en l'absence de dommage financier.

Afin de favoriser des structures d'échanges et de dialogue entre l'ensemble des acteurs concernés par la sécurité, un conseil de sécurité économique a été mis en place au sein du ministère de l'Intérieur en vue de "mieux travailler ensemble à l'identification des menaces". Il est également prévu la création d'un conseil national du numérique, chargé de la concertation avec les acteurs du secteur, dans le cadre du plan France numérique 2012.

S'agissant de la protection des entreprises face à des formes d'ingérence et d'espionnage industriel, trois types de mesures sont également prévues :

- l'élaboration par chaque préfet de région d'un "plan triennal d'intelligence économique", en lien avec les services concernés, notamment la DCRI (Direction Centrale du Renseignement Intérieur) ;
- la soumission des entreprises du secteur de l'intelligence économique et de leurs dirigeants à une procédure d'agrément, via l'avis d'une "commission consultative nationale", qui associera les professionnels ;
- pour réduire le risque de trafics d'influence, un "délai de trois ans avant que les fonctionnaires civils et militaires ayant exercé dans un service de renseignements puissent exercer des activités privées" est instauré.

Mise à jour le 15 07 2009

Dossier politiques publiques – La sécurité intérieure

Site vie publique