

LOPPSI 2 : Le grand bazar – Le point sur quelques moyens de lutte contre la criminalité (cyber ou pas)

La LOPPSI 2 (loi d'orientation et de programmation pour la performance de la sécurité intérieure) fixe les grandes orientations en matière de sécurité pour cinq ans (2009-2013) et définit des objectifs opérationnels prioritaires concernant les menaces terroristes, les mouvements et actes qui nuisent à la cohésion nationale, la criminalité organisée, les violences intrafamiliales, la délinquance routière, les crises de santé publique ou environnementale et la lutte contre la cybercriminalité. Ce texte, dont l'examen a débuté il y a plus d'un an, a été adopté en Commission Mixte Paritaire le 8 février 2011.

Nous avons choisi de nous intéresser plus particulièrement à trois initiatives destinées à lutter contre la cybercriminalité.

1. Création d'une infraction d'usurpation d'identité en ligne

L'article 2 de la loi LOPPSI 2 prévoit la création d'un article 226-4-1 dans le code pénal disposant que « **le fait d'usurper l'identité d'un tiers ou une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur, à sa considération ou à ses intérêts, est puni de deux ans d'emprisonnement et de 20.000 euros d'amende. Cette infraction est sanctionnée des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne** ».

La création d'un délit d'usurpation d'identité est un projet de longue date. Elle avait été annoncée, le 20 mars 2008 lors du Forum international de la cybercriminalité,

par le ministre de l'Intérieur de l'époque, Michèle Alliot-Marie¹.

M. le député Patrice CALMEJANE a énoncé lors des débats parlementaires de la LOPPSI 2 devant l'Assemblée Nationale, le 11 février 2010, que « *chaque année en France, plus de 210 000 personnes, soit 4,2 % de la population majeure au cours des dix dernières années, seraient confrontés à cette criminalité* » qui « *représente un phénomène plus important que les cambriolages à domicile – 150 000 – et que les vols de véhicules – 130 000* », et qui connaît « *une croissance de 40 % par an* »².

Jusqu'alors, une action pour usurpation d'identité ne pouvait être intentée que si cet usage provoquait des poursuites pénales à l'encontre de la personne dont l'identité est usurpée. Ainsi, l'article 434-23 du code pénal dispose que « *le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales, est puni de cinq ans d'emprisonnement et de 75000 euros d'amende* ». Or, ce texte ne permet pas de sanctionner les multiples atteintes à l'identité qui peuvent être réalisées par le biais des nouvelles technologies.

Le nouvel article 226-4-1 du code pénal a donc vocation de sanctionner toutes les atteintes qui peuvent être portées à l'identité d'un individu et devrait aussi permettre de protéger les personnes

¹

http://www.interieur.gouv.fr/sections/le_ministre/interventions/archives-mam/forum-cybercriminalite

²

http://www.nosdeputes.fr/seance/3310#inter_dadf627de99edc709a689c0a3e035812

morales. En effet, dans le cadre des débats parlementaires, le rapporteur du projet de loi, M. Eric CIOTTI, a précisé que les dispositions de l'article 2 de la loi « *s'appliquent aussi bien aux personnes morales qu'aux personnes physiques* »³.

L'élément intentionnel de l'infraction est constitué par la volonté de prendre les identifiants et données d'une personne dans le but de porter atteinte à ses intérêts, sa tranquillité, ou à celle d'autrui, à son honneur et à sa réputation.

La rédaction des dispositions instituant ce délit est assez large pour sanctionner de nombreux comportements : utilisation des données bancaires (carte ou compte) d'un tiers afin de réaliser des opérations à son insu, utilisation des données de connexion d'un tiers afin d'accéder à des informations ou réaliser des opérations qui lui sont réservées, ou utiliser le pseudo d'un internaute dans des conditions nuisibles à sa réputation, utiliser le nom d'un individu pour diffamer ou injurier un tiers. Lors de son second examen à l'Assemblée Nationale en décembre 2010, le champ d'application du délit d'usurpation d'identité a été élargi aux fait « *portant atteintes (aux) intérêts* » de la victime afin de pouvoir intégrer les pratiques de phishing ou d'hameçonnage.

Les notions d'identité et de données permettant l'identification trouvent de nombreuses applications : adresse IP, pseudonyme, adresse email, compte sur un site de réseau social comme Facebook. De plus, tous les éléments utilisés pour rendre le profil usurpé plus réaliste sont prohibés, tels que les photographies et vidéos.

A défaut de précision du législateur, il appartiendra au juge d'en limiter le

domaine de définition et de régler les nombreux problèmes juridiques qui ne manqueront pas d'apparaître. Par exemple, la création d'un compte du type « nom.prénom » chez un prestataire de service reprenant les nom et prénom d'une personne existante ayant un compte chez un autre prestataire pourrait-elle constituer une usurpation d'identité ? Idem pour la reprise de la dénomination sociale d'une entreprise, des comptes comme « edouard.leclerc » ou « le.figaro » pourraient-ils être déclaré illégal ?

Il appartiendra également au juge de se prononcer sur le point de savoir si, pour les personnes morales en particulier, cette nouvelle incrimination viendra ou non se cumuler avec la notion de contrefaçon ?

En tout état de cause, nous vous conseillons vivement de ne pas faire de plaisanterie à vos connaissances en ouvrant, par exemple, sous leur nom un faux profil Facebook. Vous pourriez le payer très cher... jusqu'à 20.000 euros pour être exact !

2. Logiciels mouchards : la captation de données à distance

L'article 23 de la loi prévoit que « *lorsque les nécessités de l'information concernant un crime ou un délit entrant dans le champ d'application de l'article 706-73 l'exigent, le juge d'instruction peut, après avis du procureur de la République, autoriser par ordonnance motivée les officiers et agents de police judiciaire commis sur commission rogatoire à mettre en place un dispositif technique ayant pour objet, sans le consentement des intéressés, d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre, telles qu'elles s'affichent sur un écran pour l'utilisateur d'un système de traitement automatisé de données ou telles qu'il les y introduit par*

³ <http://www.assemblee-nationale.fr/13/cri/2009-2010/20100129.asp>

saisie de caractères. Ces opérations sont effectuées sous l'autorité et le contrôle du juge d'instruction » (futur article 706-102-1 du code de procédure pénale).

L'article 706-73 du code de procédure pénale concerne uniquement les crimes et délits les plus graves (meurtre commis en bande organisée, trafic de stupéfiants, enlèvement, proxénétisme, terrorisme, fausse monnaie, blanchiment en liens avec les infractions susmentionnées, etc.). Afin de pouvoir constater et/ou prévenir ces crimes et délits, la police est autorisée à utiliser des logiciels mouchards, tel que le keylogger (enregistreur de frappes au clavier) ou des programmes enregistrant les captures d'écran.

Ces dispositifs pourront être installés pour une durée allant jusqu'à 8 mois sur un ordinateur mais aussi sur un téléphone portable ou une tablette puisque la surveillance peut concerner les données informatiques « *telles qu'elles s'affichent sur un écran* ». Toutes les infractions enregistrées pourront être utilisées par les services de police même si elles n'ont pas de liens avec le crime/délit ayant justifié la mesure de surveillance puisque « *le fait que ces opérations révèlent des infractions autres que celles visées dans ces décisions ne constitue pas une cause de nullité des procédures incidentes* » (futur article 706-102-4 du code de procédure pénale).

Ainsi, contrairement à ce que l'on a pu lire dans la presse, l'utilisation de cette faculté d'écoute est strictement encadrée et limitée. Il ne s'agit pas là de l'arrivée de Big Brother venant espionner vos moindres faits et gestes informatiques annoncé par certains médias alarmistes. Cette surveillance ne pourra s'appliquer que dans quelques cas bien précis liés au grand banditisme et les entreprises ne devraient pas être concernées par cette mesure.

Toutefois, les éditeurs de solutions de sécurité risquent d'être confrontés à de nombreuses difficultés avec ce nouveau dispositif légal. On peut se demander en premier lieu s'ils devront laisser une porte ouverte aux spywares policiers dans le cadre des logiciels de sécurité qu'ils proposent. Dans ce cas, un éditeur qui distribue un logiciel au niveau mondial devra le modifier spécialement pour le marché français afin d'y intégrer les fonctionnalités permettant de ne pas signaler à l'utilisateur la présence des spyware policiers. Comment, dès lors, contraindre les éditeurs de logiciels qui ne sont pas localisés en France et qui propose la fourniture de leurs services uniquement sur Internet ?

De plus, lors d'un audit, les prestataires de services informatiques pourront repérer sur les serveurs de l'entreprise des spywares policiers. Or, au vu du silence de la LOPPSI sur ce point et à défaut de précisions législatives ou réglementaires, le prestataire se trouvera dans une position délicate. Il devra choisir entre garder sous silence la présence de spywares policiers à condition qu'ils puissent les identifier comme tels et ainsi rompre le lien de confiance qui le lie à l'entreprise qui l'a engagé ou en avertir cette dernière et risquer de compromettre une enquête de police.

La mise en œuvre de ces dispositions risque donc de créer des difficultés.

3. Neutralisation des sites à caractère pornographique

L'article 4 de la loi dispose que « *lorsque les nécessités de la lutte contre la diffusion des images ou des représentations de mineurs relevant de l'article 227-23 du code pénal le justifient, l'autorité administrative notifie aux Fournisseurs*

d'Accès Internet (« FAI ») les adresses électroniques des services de communication au public en ligne contrevenant aux dispositions de cet article, auxquelles ils doivent empêcher l'accès sans délai ».

L'OCLCTIC (Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication), autorité administrative dépendant du Ministère de l'Intérieur, sera chargé de mener le processus de blocage des sites pédopornographique. Cette autorité pourra demander le blocage des sites aux FAI, par le biais de notification d'arrêté du Ministère de l'Intérieur, sans avoir à recourir à une autorisation judiciaire préalable.

Malgré plusieurs amendements imposant un contrôle judiciaire préalable à toute mesure de blocage, le texte prévoit que le processus de neutralisation d'un site ne fera pas l'objet d'une instruction judiciaire en amont.

Dans son rapport du 28 septembre 2010, le rapporteur de la commission des lois de l'Assemblée Nationale, Eric CIOTTI, expliquait que l'article 4 de la LOPPSI mettait en place « *un système de police administrative* » et que « *faire prononcer la mesure d'interdiction d'accès par un juge est donc contraire à la philosophie de ce système et à son efficacité* »⁴. Il justifiait sa position par la décision du Conseil constitutionnel relative à la loi Hadopi qui avait érigé l'accès à internet en une composante du principe de la liberté d'expression. En effet, selon lui, « *le recours au juge judiciaire n'est pas nécessaire en droit puisque nous ne sommes pas dans le cas de figure déjà*

examiné par le Conseil constitutionnel, dans lequel c'était l'accès à l'ensemble d'Internet qui est en cause » et ce d'autant plus que « *l'appréciation que l'autorité administrative portera sur le caractère réellement pornographique d'un contenu sera placée sous le contrôle du juge administratif, compétent pour connaître de tout recours formé contre la décision du ministre de l'Intérieur* ».

Des voix s'élèvent pour contester les dérives possibles du système de blocage des sites. La lutte contre la pédopornographie justifie bien que des mesures soient prises en urgence mais, comme le fait remarquer Maître Christiane Féral-Schuhl, le dauphin du Bâtonnier de Paris, « *il est à craindre que l'automaticité de la sanction ne s'étende à d'autres crimes et délits, et s'écarte progressivement du contrôle d'un juge indépendant* »⁵.

De plus, ces dispositions ne prennent pas en compte le constat d'échec de nos voisins allemands. En effet, en juin 2009, le Parlement allemand avait adopté une loi sur la censure d'Internet aux fins de lutte contre les sites pédopornographiques similaire aux dispositions mises en place dans la LOPPSI 2. Cependant, neuf mois plus tard, le gouvernement allemand a décidé d'abandonner ce système en raison des risques d'atteinte aux libertés publiques et des difficultés pratiques de mise en œuvre.

Dans un email adressé à l'un de ses membres, l'Association française des Fournisseurs d'Accès (AFA), explique la suppression de ce dispositif. Ainsi, « *d'après les études menées en Allemagne, sur 8000 URLs contenues dans les listes*

⁴ http://www.assemblee-nationale.fr/13/pdf/amendements_commissions/cloi/2780-01.pdf

⁵ http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/loppsi-2-les-points-qui-fachent-28-09-2010-1242300_56.php

noires présumées de la police, seuls 110 sites web contenaient des images d'abus sexuels sur mineurs et des images érotiques de mineurs, et après notification à l'hébergeur, seulement 7% de ces contenus illégaux, hébergés dans des pays non-membres d'INHOPE, étaient encore en ligne après 14 jours (alors que la plupart des contenus notifiés ont été supprimés dans les 48h après notification) »⁶.

Ainsi, alors que les fichiers de police recensaient 8000 noms de domaine qui auraient pu être potentiellement bloqués en application de la loi sur la censure d'Internet, seuls 110 adresses renvoyaient véritablement vers des sites pédophiles, soit un ratio de 1,37 %.

Cela illustre les risques d'inefficacité du système de blocage des sites et de dérive dénoncées par de nombreux interlocuteurs dont la Commission de la défense nationale et des forces armées qui dans un rapport parlementaire signé Marc Joulaud avait estimé que « *si (le système de blocage) semble opportun, l'étude d'impact correspondante n'en démontre pas l'efficacité, ni n'évalue précisément son coût global, tant en termes de compensation pour les FAI que de moyens pour les services de l'État* »⁷.

Aux vues des études mentionnées par l'AFA, il semble plus efficace de contacter directement l'hébergeur des contenus pédophiles pour lui demander de les supprimer plutôt que de procéder au blocage du site. D'une part, cette démarche évite de porter atteinte à la neutralité des réseaux et permet d'économiser des dépenses dont le coût n'a pas été déterminé mais qui seront a fortiori élevés. D'autre

part, cela permet d'utiliser un système juridique qui existe déjà et qui, à l'évidence, fonctionne efficacement. En effet, l'article 6 de la Loi sur la confiance dans l'économie numérique du 21 juin 2004 impose aux hébergeurs de supprimer tous les contenus manifestement illicites dès la première notification à défaut de quoi leur responsabilité peut être engagée.

Ainsi, dans les études mentionnées par l'AFA, après notification à l'hébergeur, 93 % des sites pédophiles ont été supprimés dans un délai de deux semaines. La procédure préexistante de notification à l'hébergeur est beaucoup plus efficace et moins coûteuse que la création et la mise en place de services de police entièrement dédiés au filtrage de sites pédophiles dont l'exemple allemand illustre l'inefficacité et les délais de procédure. Enfin, il est beaucoup plus simple de contacter directement un hébergeur pour lui demander de supprimer des contenus que d'adresser des demandes aux FAI pour qu'elles opèrent le blocage de certains sites à partir des connexions françaises.

Les dispositions controversées de cette loi ont conduits à la saisine du Conseil Constitutionnel le 15 février 2011, après adoption du texte par une commission paritaire le 8 février dernier.

Le 11 mars 2011, les Sages du Conseil Constitutionnel ont statué sur la LOPPSSI 2. Qualifiée de « revers cinglant pour le gouvernement et pour le chef de l'état », cette décision fait droit aux griefs invoqués par les requérants et vient censurer plus de treize dispositions clé de la loi (peine plancher, vidéosurveillance, modification du statut de certains policiers municipaux, etc.). La saisine ne portait pas sur les articles 2 et 23 et ces dispositions peuvent donc entrer en vigueur inchangées. Par ailleurs, la mesure relative au filtrage des contenus pédopornographiques prévue par

⁶ <http://www.pcinpact.com/actu/news/53750-loppssi-afa-fai-allemande-blocage.htm>

⁷ <http://www.assemblee-nationale.fr/13/pdf/rapports/r2271.pdf>

l'article 4 de la loi n'a pas été censurée. Pour le Conseil Constitutionnel, « *l'article 4 assure entre la sauvegarde de l'ordre public et la liberté de communication une conciliation qui n'est pas disproportionnée* ». Les Sages considèrent ainsi que la possibilité pour les FAI de contester la décision de l'autorité administrative associé au fait que le pouvoir de filtrage soit limité à la poursuite d'un objectif bien défini constituent des garanties suffisantes pour justifier la censure des sites qui diffusent des images pornographiques infantiles.

Cette loi a vocation à diriger la politique gouvernementale en matière de cybercriminalité jusqu'en 2013. Elle rogne quelques libertés publiques et posera inévitablement des problèmes d'application mais, aux yeux du gouvernement, la cybersécurité est à ce prix. C'est la « cyberlutte » finale !

Le 17 Mars 2011

Une synthèse de Annabelle RICHARD Avocat à la Cour - Attorney at Law(New York Bar) et de Oriane ZUBCEVIC, Département TMT du Cabinet Ichay & Mullenex Avocats.

Le cabinet Ichay & Mullenex Avocats est spécialisé dans la gestion des problématiques juridiques liées à l'activité des entreprises de nouvelles technologies et de développement durable. Il conseille ainsi de nombreux acteurs du e-commerce, de l'informatique, des médias, des télécoms et de la recherche dans la gestion de leurs affaires au quotidien, pour leurs projets de croissance interne ou externe et leur développement à l'international. L'ensemble des avocats du cabinet Ichay & Mullenex Avocats a reçu une double formation en complétant leur formation française soit par une formation à l'étranger soit par une formation en école de commerce. Chacun d'entre eux est tourné vers la nouvelle économie et la mondialisation des échanges accompagnant leurs clients avec une vision pragmatique de la vie des affaires.

5, rue de Monceau 75008 Paris - France
Tel : +33 1 42 89 19 80
Fax : + 33 1 42 89 14 99
www.ichay-mullenex.fr