

## Compte-rendu de la conférence du 17 mars 2011

### **LOPPSI 2 : un nouvel arsenal contre la cybercriminalité**

**Master 2 Professionnel Droit du Multimédia et de l'Informatique  
Université Panthéon-Assas Paris 2**

**En partenariat avec l'association française des juristes d'entreprise et juriscom.net**



### **LE NOUVEAU DÉLIT D'USURPATION D'IDENTITÉ EN LIGNE**

**Par Lucien CASTEX, ATER en droit privé et sciences criminelles, Conseil en technologies de l'information**



L'usurpation d'identité suppose tout d'abord de définir l'identité. L'identité c'est la conscience qu'une personne a d'elle-même, la qualité qui fait qu'une chose est la même qu'une autre, c'est l'ensemble des données de fait et de droit permettant d'individualiser quelqu'un. On voit une double approche : ce qui rapproche les éléments pour constituer une unité et ce qui les différencie par rapport à d'autres unités. Dans le droit français, nous n'avons pas de définition explicite de l'identité,

mais un ensemble d'informations regardant l'état civil et un encadrement par le décret de 1955 qui précisent les éléments d'identité : nom, prénom, sexe, domicile...

L'appréciation par le droit de la notion d'identité peut être double. On voit une approche subjective de l'identité : l'identité est un attribut de la personnalité, de même que l'on peut la rapprocher du droit de propriété. On le voit notamment concernant les analyses faites sur les noms de domaine et la protection du nom patronymique. Ainsi, la notion d'identité se caractérise le plus souvent par la formulation d'un nom qui peut être associé à un patronyme, un pseudonyme.

Conférence du 17 mars 2011

LOPPSI 2 : un nouvel arsenal contre la cybercriminalité

Master 2 Droit du Multimédia et de l'Informatique – [www.m2dmi.com](http://www.m2dmi.com)

Quant à l'usurpation, elle s'entend du fait de s'emparer de l'identité de quelqu'un. Le numérique démultiplie les risques d'usurpation bien qu'une étude récente de l'OCDE montre que la plupart des usurpations d'identité avaient comme point de départ le monde physique, c'est-à-dire un nombre de documents récupérés par les pirates dans les poubelles des différents usurpés et les documents trouvables dans le monde réel. Par ailleurs, en terme de chiffres, l'usurpation a été évaluée aux États-Unis à 32 milliards de dollars de perte pour l'industrie tandis que le CREDOC l'évalue en France en 2009 à 4 milliards d'euros. Il estime également à 210000 le nombre d'usurpations d'identité en 2009 et considère que 32 % des ménages franciliens avaient des poubelles comportant des documents permettant d'usurper leur identité (relevés bancaires, lettres administratives...)

### Les principes et techniques utilisés pour usurper l'identité :

On distingue deux techniques pour usurper l'identité : les logiciels malveillants, dits « malware » consistant à infiltrer l'ordinateur ou les serveurs d'institutions afin de récupérer des données personnelles et de construire un profil permettant d'usurper l'identité. Il y a ensuite l'hameçonnage, ou le phishing, qui participe d'une technique plus compliquée mettant en œuvre des méthodes d'ingénierie sociale permettant de tromper l'utilisateur néophyte afin de lui soutirer des informations confidentielles. L'une des méthodes les plus couramment employées est un lien envoyé par courrier électronique sur lequel on clique, qui nous dirige vers un site web qui ressemble à un site officiel, qui reproduit les logos et informations paraissant authentiques. Dans ce site web, il est demandé de rentrer des informations personnelles sous couvert de sécurité ou de faux avantages que l'on pourrait tirer de ce service, mais ces informations sont envoyées aux pirates. De telles techniques jouent sur la crédibilité et la non-connaissance par les néophytes des techniques qui permettent d'usurper l'identité. Ces techniques parfois couplées avec des logiciels malveillants deviennent plus redoutables : par exemple, le détournement des serveurs DNS permettant d'arriver sur un site contrefait en hackant le serveur par lequel le site officiel est redirigé et permettant de créer un site pirate. L'association des deux techniques permet de récupérer des profils, des numéros de cartes bleues, d'où les pertes importantes qui peuvent être le fait de l'usurpation d'identité.

### L'encadrement juridique :

- Avant la loi LOPPSI 2 :

L'usurpation d'identité était le plus souvent traitée de manière connexe c'est-à-dire en lien avec une autre infraction : l'abus de confiance, ou encore l'escroquerie. Par ailleurs, il existe l'article 434-23 du Code pénal qui encadre déjà de manière connexe l'usurpation d'identité et qui précise qu'elle se définit comme "le fait de prendre le nom d'un tiers dans des circonstances qui ont déterminé ou auront pu déterminer contre celui-ci des poursuites pénales". On voit dans la rédaction même du texte, la nécessité de poursuites corollaires pour pouvoir condamner l'usurpation d'identité. Donc deux conditions sont à réunir. Tout d'abord, il faut constater la prise du nom d'un tiers, ce qui peut connaître un certain nombre de limites. Ce nom doit être celui d'une personne existante. La seule utilisation d'un

pseudonyme sans lien avec une personne réelle fait que l'on retombe sur l'article 781 du Code de procédure pénale qui prohibe le fait de fournir des renseignements erronés ou imaginaires au service de police. Ensuite, il est nécessaire que les circonstances d'une infraction pénale soient réunies. Ainsi, si les éléments constitutifs de l'infraction pénale ne sont pas remplis, l'usurpation d'identité ne peut pas être retenue. Ce qui est une limite importante qui nous apprend que l'usurpation d'identité n'est pas condamnée en tant que telle.

Il y a des atteintes voisines à l'usurpation d'identité : l'article 434-23 alinéa 3 du Code pénal punit la fausse déclaration. De même, un certain nombre de textes dans le Code de la route et dans le Code des marchés publics encadrent les fausses déclarations qui peuvent être fournies sur l'identité.

Il existait et demeure également des protections en amont de l'usurpation d'identité. Tout d'abord, regardons la phase de collecte d'informations personnelles. L'article 226-18 du Code pénal modifié par la loi du 6 août 2004 prohibe la collecte illicite par un moyen frauduleux, déloyal ou illicite de données à caractère personnel. Le phishing s'analyserait tout à fait comme un tel moyen frauduleux. Là encore, ce n'est pas l'usurpation d'identité qui est directement réprimée, mais les moyens de la collecte des éléments qui permettent cette usurpation. Par ailleurs existent des mesures réprimant la transmission de connaissances visant à collecter frauduleusement des données ou à s'introduire dans un système de traitement automatisé de données. Ainsi par exemple, il est interdit d'apprendre aux néophytes à pirater un site internet pour réaliser des actes de phishing. La limite est l'internationalisation de l'internet et les serveurs qui peuvent se trouver au Canada, en Chine, en Suède, au Danemark...

L'usurpation d'identité s'analyse ici comme une infraction connexe. Un arrêt du 29 mars 2006 de la chambre criminelle de la Cour de cassation dans lequel étaient combinées une usurpation d'identité et une diffamation, et dans lequel les éléments de diffamation n'ont pas été réunis, a occasionné le fait que l'usurpation d'identité n'a pas trouvé d'écho juridique pour sa condamnation. Pour être condamnée, l'usurpation d'identité nécessitait de retenir la commission d'une infraction. Puisqu'il y avait usurpation d'identité, la Cour de cassation a considéré qu'une personne ne pouvait se diffamer elle-même, il n'y avait pas de victime.

Le deuxième point important est le caractère protéiforme de la notion même de l'identité. Elle peut être définie eu égard à l'état civil, mais cela est dépassé par le texte et la rédaction de la loi LOPPSI et des analyses jurisprudentielles et doctrinales préalables.

La notion d'identité numérique peut être divisée en trois types d'identités principales : tout d'abord l'identité numérique définie au sens strict, c'est-à-dire l'ensemble des données techniques permettant de recomposer le parcours d'un individu sur internet (données de connexion et adresse IP). Par ailleurs, on a l'identité numérisée composée des données relatives à la personne physique en tant qu'elle est transposée dans le cyberspace (les photographies, textes publiés, billets mis en ligne sur son blog, identifiants de connexion qui relie une personne à son service de courriel... sachant qu'un certain nombre de médias sociaux invitent à divulguer le plus grand nombre d'informations possible). Et enfin,

troisième type d'identité : l'identité immatérielle faisant référence aux avatars que l'on retrouve dans le monde numérique, les jeux vidéo (par exemple World of Warcraft où des problématiques d'identité se sont posées et où un certain nombre de ressources sont monnayées pour des sommes réelles).

Il faudrait y ajouter la protection des noms de domaine : l'encadrement des noms de domaine protège le nom patronymique. Ainsi, l'article R 20-44-46 du Code des postes et des communications électroniques condamne l'usage frauduleux du nom patronymique d'autrui pour en tirer un bénéfice indu. Dans un jugement du TGI de Paris du 22 mai 2007, un candidat à une élection politique a été condamné car il usurpait le nom d'un de ses opposants pour rediriger les personnes vers son propre site.

En dehors de la difficulté de saisir l'identité, demeurent des questions relatives à l'adresse IP en tant que telle. L'identité numérique au sens strict présente une première difficulté : elle est changeante. On peut changer d'adresse IP, usurper l'adresse IP d'autrui, utiliser l'adresse IP de ses parents, utiliser l'adresse IP de l'Université Paris 2 pour se connecter à des services illicites et donc se cacher derrière l'adresse IP d'institutions comme l'employeur pour commettre un certain nombre d'infractions. L'adresse IP s'analyse comme une donnée de connexion, mais peut-elle s'analyser comme une donnée à caractère personnel ? Le G29 et la CNIL prônent une analyse de l'adresse IP comme une donnée à caractère personnel et une proposition de loi du Sénat adoptée le 23 mars 2010 et transmise à l'Assemblée nationale propose d'intégrer tout numéro identifiant le titulaire d'un accès des services de communication au public dans le champ des données à caractère personnel. La question serait d'office résolue.

Dernier point sur le délit d'usurpation d'identité. La Cour de cassation, dans un arrêt rendu le 16 février 1999 par la Chambre criminelle, a précisé que ce délit d'usurpation est un délit instantané et qu'ainsi la prescription ne commence à courir qu'au jour où l'identité est usurpée dans des circonstances de nature à déterminer des poursuites pénales. Un certain nombre d'auteurs en doctrine ont pu donner une analyse de l'usurpation d'identité comme une infraction continue, dès lors ce délai de prescription courrait à partir de la découverte de l'infraction. C'est une analyse qui rendrait plus aisée la condamnation de telles usurpations.

- Le cadre législatif de la LOPPSI 2

La notion d'usurpation d'identité et la volonté de l'encadrer ont été formulées en 2005 à l'initiative du sénateur Dreyfus-Schmidt qui regrettait l'absence d'infraction propre et mettait en cause le caractère connexe de l'usurpation d'identité. Des projets voient le jour, et notamment en 2008 à l'initiative de Michelle Alliot-Marie qui présente le projet de loi LOPPSI. Il faut savoir qu'un certain nombre de propositions de loi avaient déjà été préparées et ont été largement reprises par les rédacteurs de la LOPPSI. Le premier projet, déposé le 27 mai 2009, faisait référence à une infraction qui devait être réitérée. Cette réitération a disparu du texte car elle posait des problèmes : la simple usurpation n'était pas en tant que telle sanctionnée et il fallait définir la réitération. Des moutures ont vu le jour pour enfin arriver au texte proposé et validé en commission mixte paritaire le 8 février 2011. Ce texte précise que "le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs

Conférence du 17 mars 2011

*LOPPSI 2 : un nouvel arsenal contre la cybercriminalité*

Master 2 Droit du Multimédia et de l'Informatique – [www.m2dmi.com](http://www.m2dmi.com)

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 ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende" et le second alinéa précise que "cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne." On peut s'étonner de ce second alinéa. Était-il nécessaire de le préciser alors qu'il est déjà appréhendé par le premier alinéa ? On peut considérer que ce second alinéa serait source de problème dans l'interprétation qui pourrait être faite des limites de l'usurpation d'identité. Faut-il un alinéa spécifique pour chaque nouvelle technologie et donc une interprétation restrictive des dispositions de la LOPPSI 2 ?

### Perspectives :

"Une ou plusieurs données de nature à permettre d'identifier". Le texte est large, dépassant les notions simples de nom patronymique, pseudonyme, le prénom et état civil. Ce sont des photos, vidéos utilisées par autrui qui pourraient entrer sous le coup d'un tel article. En pratique, l'usurpateur n'a-t-il pas tendance, dans le cadre par exemple d'un profil Facebook usurpé, à remplir le profil d'un maximum d'informations, de vidéos, images pour le rendre plus crédible ? Chacun de ces actes doit être incriminé eu égard à la loi LOPPSI. C'est donc un champ d'application qui dépasse les simples informations de l'état civil. La formulation du 1er alinéa permet d'envisager que de futures techniques de piratage seraient appréhendables par le texte dans sa rédaction actuelle.

Par ailleurs, l'usurpation d'identité concerne l'usurpation en ligne et l'usurpation dans la sphère réelle. Dans ce sens, on peut s'interroger sur l'utilité du second alinéa. Pour finir, qu'est-ce qu'une information permettant d'identifier une personne ? La difficulté se présentera. Jusqu'à quel point peut-on définir une information identifiant une personne ? Le cas le plus aisé serait celui de l'usurpation d'un pseudonyme ne renvoyant pas directement à une identité réelle. Peut-on parler d'usurpation d'identité si le pseudonyme n'a pas de lien avec l'identité réelle. Une affaire de 2007 mettant en cause le blogueur Maître Eolas n'avait pas permis la condamnation pour usurpation d'identité.

Enfin, sur la notion de tranquillité : qu'est-ce que troubler la tranquillité d'autrui ? Deux approches peuvent être présentées. La tranquillité serait un élément automatique découlant de l'usurpation d'identité ou elle découlerait d'une usurpation et d'une atteinte à la vie privée (cf. « *the right to be left alone* »). Les difficultés relèvent de la délimitation qui sera faite de la notion de tranquillité et du lien entre l'identité réelle et l'identité usurpée. Si un tel lien ne peut être réalisé, une telle usurpation pourra-t-elle être condamnée sur le fondement de la loi LOPPSI ?

## LE FILTRAGE DES SITES INTERNET : DANGER !

Par Jérémie ZIMMERMANN, Co-fondateur et Porte-parole, LA QUADRATURE DU NET



La Quadrature du Net est particulièrement intéressée par l'article 4 de la LOPSSI 2 visant à mettre en œuvre le filtrage de site pornographique. Mais il faut reconnaître tout d'abord que la stratégie du Gouvernement a parfaitement fonctionné : dans cet univers que représente la LOPSSI la stratégie était d'agiter quelques chiffons rouges qui allaient être lâchés au niveau du Conseil constitutionnel afin de s'assurer que tout le reste passe, et en l'occurrence l'article 4.

### Le mode de fonctionnement de l'article 4 et pourquoi ce filtrage est inefficace et inadapté par rapport aux objectifs recherchés

Personne ne s'oppose à cet objectif noble qu'est la lutte contre la pédopornographie sur internet. Il s'agit bien de représentation de scènes de crimes. La diffusion et ces représentations sont évidemment abjectes et nécessitent d'être combattue. Le dispositif mis en œuvre par le Gouvernement, déjà expérimenté dans certains pays européens avec plus ou moins de succès, consiste à bloquer l'accès à ces sites dits pédopornographiques et il semble difficile de s'y opposer à première vue. Mais il convient de mettre la lumière sur quelques aspects techniques pour comprendre comment fonctionne le filtrage. Il ne s'agit pas de retirer les contenus des serveurs qui se trouvent quelque part sur internet, mais simplement d'en bloquer l'accès. Concrètement, on a une autorité administrative qui dépend du ministère de l'Intérieur qui va recevoir des signalements, des liens vers ces contenus pédopornographiques, puis va constituer une liste noire de ces ressources, les transmettre aux opérateurs, obligation étant faite aux opérateurs de rendre ces sources inaccessibles pour leurs utilisateurs. Cela peut sembler une bonne idée, mais le problème c'est que la nature même d'internet fait que l'ensemble du dispositif est dépassé technologiquement car l'article 4 ne s'attaque qu'à des sites web c'est-à-dire publics sur internet. Il faut être naïf pour croire que les personnes qui diffusent ces contenus, qui s'exposent à des peines de prison de l'ordre de 10 à 20 ans utilisent des sites publics. La vaste majorité de ces contenus sont diffusés au travers de réseaux privés, de réseaux chiffrés, de réseaux peer to peer... Bref des modes de distribution qui sont totalement hors d'atteinte de cet article.

Ensuite, penser que les gens qui s'adonnent à ces contenus sont naïfs au point de ne pas savoir à quoi ils s'exposent et penser qu'ils pourraient accéder à ces contenus de la même manière qu'ils consultent leur messagerie ou qu'ils font des recherches sur Google est encore méconnaître sinon la psychologie de ces individus, en tout cas leur méthode.

La Quadrature du net a beaucoup travaillé avec l'association L'ange bleu (association d'information sur la pédophilie qui traite à la fois des victimes et des pédophiles). Ils sont

confrontés à des situations difficiles tous les jours. L'association nous a rapporté que la vaste majorité de ces personnes utilisent déjà pour se rendre plus discret dans leur consommation de ces contenus des outils qui contourneront le filtrage le jour où il sera mis en place.

En pratique les mesures de filtrage de l'article 4 consistent à mettre la main devant les yeux de la personne qui regarde le problème pour conclure que le problème a été réglé. Les outils de chiffrements (les proxys, les VPN...), permettant de contourner l'HADOPI : en deux clics, qui sont consubstantiels d'internet et de ses protocoles, qui sont indispensables à l'administration du réseau et des réseaux interconnectés, indispensables au télétravail existent déjà et sont largement utilisés afin de soit contourner la censure dans certains pays, soit de s'émanciper des contraintes types HADOPI...

La perspective de voir l'ensemble des concitoyens se tourner vers des dispositifs de chiffrement pour des raisons diverses et variées risque probablement de compliquer les travaux des renseignements humains.

C'est donc un fonctionnement sous forme de liste noire foncièrement administrative dépendant du Gouvernement. Au passage, le contrôle de l'autorité judiciaire qui avait pourtant été voté en première lecture a été supprimé en seconde lecture.

Ce dispositif est dépassé techniquement et technologiquement puisque la réelle distribution de ce contenu passe par d'autres moyens que le web public, un dispositif très largement contournable fait se poser alors la question de la nécessité du dispositif et surtout de son adaptation à l'objectif. Lorsqu'on parle de la lutte contre la pédopornographie sur internet on pourrait se demander un instant quels sont les outils efficaces, s'il y en a. Qu'aurait pu faire le Gouvernement pour lutter réellement contre la pédopornographie, sa distribution et son commerce ? Faire enlever les contenus des serveurs et faire disparaître à tout jamais ces sites est la seule solution, le seul moyen efficace de lutter contre la pédopornographie et son commerce. Ce à quoi on entend immédiatement comme réponse : lorsque le site est situé ailleurs en Europe ou même hors d'Europe, comment faire ? Il existe un traité de lutte contre la cybercriminalité ratifié par environ 150 pays, il existe déjà des règles de coopération internationale en la matière et en pratique le pays où la plupart du temps sont hébergés ces contenus en dehors d'Europe c'est les États-Unis et lorsqu'on envoie une requête pour enlever les contenus, la plupart du temps c'est lettre morte. Il faudrait un peu plus taper du poing pour que le retrait des contenus soit fait. Donc il faut des moyens politiques, des moyens humains, renforcer les moyens des enquêteurs pour leur permettre de faire leur travail. Plutôt que de s'attaquer aux symptômes et à la représentation des scènes de crime, il faudrait remonter les filières, comme on le fait dans la lutte contre le terrorisme ou dans la lutte de trafics de stupéfiants, pour remonter à la source. Ces moyens efficaces de remonter à la source qui impliquent des moyens financiers et humains ne figurent pas dans l'arsenal de la LOPPSI. Il n'y a plus qu'à attendre la LOPPSI 3.

### Un dispositif dangereux et disproportionné

Ce dispositif est profondément dangereux et disproportionné. En plus d'être inefficace, il peut se révéler contreproductif parce que la liste noire compilée par le ministère de l'Intérieur va inévitablement fuiter (comme dans nombre de pays où l'expérience a été

réalisée). Cette liste deviendra donc une compilation des contenus pédopornographiques qui pourra faire l'objet d'une offre commerciale. Contreproductif également parce que le filtrage pourrait servir de désincitation pour les enquêteurs qui travaillent avec très peu de ressources, énormément de dossiers, des objectifs chiffrés donc lorsqu'il s'agira en un clic de prétendre avoir réglé un problème plutôt qu'à investir plus de ressources à infiltrer les réseaux, comprenez bien que cliquer au lieu d'enquêter permettra d'économiser des ressources.

Ce dispositif est aussi dangereux car il aboutit au surblocage ou à la censure collatérale. Dans l'étude d'impact du Gouvernement annexé à la LOPPSI, le Gouvernement lui-même admet que ce risque est inévitable quel que soit le dispositif de filtrage employé. Par surblocage on entend bloquer en même temps qu'un site pédopornographie un ou plusieurs sites parfaitement licites, sans contenu pédopornographique mais situés dans le même espace logique du réseau.

Quelque soit le dispositif de filtrage mis en œuvre, le risque est grand, quasiment inévitable, qu'en essayant de filtrer une image ou un site il y ait d'autres sites légitimes qui passent à l'as. Un exemple s'est produit en Grande-Bretagne où le dispositif de filtrage n'est pas imposé par la loi, mais un dispositif volontaire reposant sur l'association de protection de l'enfance. Une pochette de disque d'un album de 1976 du groupe Scorpions "Virgin Killers" représentant une petite fille nue avec un éclat de verre sur ses parties génitales qui avait fait couler beaucoup d'encre à l'époque figurait en haut de la page Wikipédia décrivant cet album. Pendant deux jours, dans toute la Grande-Bretagne l'ensemble de Wikipédia s'est retrouvé inaccessible. Il a fallu peu de temps pour s'en apercevoir et en 48 heures seulement le site a pu sortir de cette liste noire. Cependant, on peut imaginer ce que peut donner la mise dans une liste noire d'un site d'un parti politique proposant des sondages sortis des urnes à 24 heures d'une élection. On imagine encore le calvaire que peut représenter le surblocage lorsque l'on n'est pas la Wikimedia foundation et ses millions de connexions par jour, mais un petit site de commerce de Biélorussie qui pour une raison ou une autre se trouve dans une liste noire par hasard dans un pays européen. Ce risque de surblocage est le danger majeur causé par ce dispositif, une atteinte manifeste à la liberté d'expression et, selon l'aveu même du Gouvernement, un risque inévitable.

Le deuxième risque majeur plus prospectif est que ce dispositif soit généralisé, que l'on puisse considérer que bloquer l'accès à un site, quel qu'il soit et pour quelque motif que ce soit, puisse être une bonne idée. Par exemple on se souvient des vidéos de blagues sur les Auvergnats et la ruée des ministres qui avaient demandé le droit à l'oubli ou bien l'affaire Wikileaks où Eric Besson a clamé qu'il devait être interdit en France car ne correspondait pas à cette notion de l'internet civilisé. On a tous en tête cette notion d'internet civilisé et on imagine ce que cette tentation du filtrage pourrait donner surtout lorsque l'on sait que les moyens pour mettre en œuvre ces dispositifs sont les mêmes techniquement que ceux déployés en Tunisie, en Iran, ou en Chine...

Sur cette note d'optimisme et pour conclure : on a un remarquable exemple, avec cet article 4 de la loi LOPSSI 2, d'un coup politique où on a instrumentalisé un prétexte émotionnel au sujet duquel il est extrêmement difficile de débattre sereinement, on a pris

une mesure profondément attentatoire aux libertés individuelles que l'on camoufle par sa complexité technique en un dispositif efficace, on noie le tout dans une foire-à-tout-sécuritaire qu'est la LOPSSI 2, on tient son Parlement en main, on laisse mijoter quelques lectures et la France entre dans l'ère de la censure administrative de l'internet.

**Question : Le dispositif installé par la LOPSSI 2 est-il un cheval de Troie futur pour l'HADOPI ?** Un cheval de Troie oui. Que les industries du divertissement demandent des dispositions similaires est un fait. Cette question n'est pas nouvelle et remonte à la loi DADVSI. Dans son article 10, il était prévu la possibilité d'expérimenter des dispositifs de filtrage par l'HADOPI.

**Intervention d'Antoine Chéron :** Aujourd'hui, le législateur a voulu tester techniquement ce que pouvait être le blocage de l'accès d'un site et on le voit depuis la loi sur les jeux d'argents où on a montré qu'on était capable de bloquer un site avec la jurisprudence StanJames. Il y a un combat amusant entre les FAI et l'ARJEL qui aboutit à la même décision à chaque fois : le blocage. Depuis août 2010, l'aspect technique est apparu avec ce problème de surblocage. On l'a vu aux États-Unis avec ces 82 sites qui ont été bloqués et qui ont entraîné 52 000 blocages de sites en surblocage. Avec la LOPSSI, techniquement le législateur a besoin de voir les conséquences de ces blocages. La jurisprudence commence à vouloir ce filtrage. On l'a vu avec l'affaire Scarlett (voir notamment une décision de la Cour d'appel de Bruxelles du 28 janvier 2010 : Scarlet c/ Sabam et Autres) qui a effectivement été validée par la Cour européenne. Techniquement, tout le monde était d'accord pour dire que l'on n'était pas capable de filtrer, mais juridiquement et judiciairement on l'était. Une décision en référé du TGI Montpellier a été rendue le 16 mars 2011 concernant des contenus portant atteinte à une ancienne actrice de pornographie reconvertie en institutrice. Ce qui est intéressant c'est le fondement juridique retenu par le TGI qui se focalise sur l'atteinte à la vie privée et sur l'utilisation de données à caractère personnel. Le fondement n'est pas très précis, mais cela montre que la jurisprudence prend le pas sur l'aspect législatif.

**Réponse de Jérémie Zimmermann :** Il y a un phénomène connu sur internet, l'effet Streisand où Barbara Streisand avait tenté de faire interdire la présence de la photo de sa maison sur internet ce qui avait produit l'effet inverse, sa photo s'étant retrouvée copiée des millions de fois sur internet. Le filtrage conduit fréquemment à cet effet Streisand. On se souvient de l'affaire Arrgh où le site est réapparu sur une dizaine de points du net. Dans l'affaire Stanjames : le site stanjames.com a été bloqué, mais un site au nom de domaine similaire développé par le même éditeur avec le même contenu n'a pas été bloqué. La décision Stanjames (TGI Paris, 6 août 2010) a fait froid dans le dos car elle représente une obligation de résultat et le juge dans cette décision évoque les moyens à mettre en œuvre à la charge des opérateurs devant rendre ce site inaccessible : "il appartient donc aux fournisseurs d'accès à internet de prendre toutes mesures de nature à permettre l'arrêt de l'accès au service en cause, soit toute mesure de filtrage, pouvant être obtenu [...] par blocage du nom de domaine, de l'adresse IP connue, de l'URL, ou par analyse du contenu des messages". L'inspection du contenu des paquets signifie que l'on regarde tout ce qui circule sur internet, toutes les données consultées par les utilisateurs pour voir si le contenu est licite ou non. C'est la technique la plus élaborée de filtrage tellement intrusive qu'elle porte inévitablement atteinte au secret des correspondances privées. Mais le juge français va

jusqu'à invoquer cette intrusion massive dans la vie privée au nom d'une lutte contre le jeu de poker qui ne payerait pas leur TVA.

## LA PERQUISITION À DISTANCE PAR L'INTRODUCTION DE MOUCHARDS INFORMATIQUES

Par David ZNATY, Expert en Informatique, Président honoraire des experts agréés auprès de la Cour de cassation



Je voudrais tout d'abord rappeler le rôle de l'expert judiciaire : Il agit principalement sur mission d'un magistrat, réquisition d'un service de police ou assistance d'un huissier. C'est un technicien à la disposition de la Justice.

### La preuve numérique, domaines d'interventions :

Nous sommes dans un monde où l'échange se fait en temps réel, en permanence et en réplication. La notion de réplication fait que l'on peut être un instant donné à Paris et les informations peuvent se dupliquer en un temps record, en quelques secondes, dans n'importe quel endroit du monde. Le but est de capturer des données, mais il faut aussi démontrer que ces données représentent une preuve qui ne peut être contestée. Elles peuvent transiter sur des réseaux locaux ou globaux, être des données de traitement, des données statiques (données stockées à un instant donné quelque part) et des données dynamiques (les données sont parfois volatiles).

Les données capturées ne sont pas uniquement des données de texte, il peut s'agir de données de son (on peut vous écouter sur Skype), des images, des vidéos. C'est un monde de multimédia et, en tant qu'experts, nous travaillons sur ces différents types de données.

La technique de perquisition à distance n'est pas nouvelle. On a d'abord les écoutes téléphoniques qui sont devenues difficiles depuis que l'on a intégré le monde digital, avec l'écoute du Minitel il suffisait de mettre un enregistreur derrière le Minitel pour relire les messages sur un autre Minitel. Les missions d'experts incluent la possibilité dans certains cas d'accéder à la boîte mail de la personne en cassant le mot de passe et login (avec l'autorisation du magistrat). Il faut pour cela aller voir l'opérateur de messagerie qui donnera l'accès au compte. Enfin, il y a l'écoute digitale et spyware.

La capture de données n'est pas suffisante. Une fois obtenue, il faut démontrer que ces données sont des preuves certaines. À ce titre, il existe trois types de preuves :

- La preuve démonstrative ou structurée : on est capable de répéter la preuve devant la personne sans qu'il y ait une contestation possible
- La preuve semi-démonstrative ou semi-structurée : la collecte des informations et la démonstration de la preuve qui va se répéter chez le magistrat fait que cette personne ne peut pas contester ce qui a été obtenu

- La preuve non démonstrative ou non structurée : c'est la conviction qui l'emporte, ce qui peut amener à faire des erreurs d'appréciation.

### Un univers complexe :

Nous sommes dans des systèmes ouverts, globalement répartis. Donc lorsqu'il y a une action à faire on ne peut pas se limiter à un endroit. Ensuite, on a une combinatoire de réseaux et de systèmes avec des interfaces complexes. Le nombre de gens qui savent construire des systèmes pour des routeurs en télécommunications est extrêmement restreint. Ensuite il y a le cryptage. La haute délinquance utilise des techniques de cryptage difficiles à casser. De plus, le principe du cryptage est que celui qui a décrypté ne le dira jamais, comment donc démontrer que ce qui a été décrypté est bien ce qui était chiffré. Enfin, on a des applications hétérogènes avec des interfaces complexes et avec des informations éphémères.

### Problématique du filtrage et de l'écoute du net :

Le trafic global est émis ou reçu par de nombreux canaux ainsi qu'au sein même du réseau propre à chaque opérateur. On ne peut pas dire qu'un opérateur est unique, lui-même en tant qu'opérateur reçoit des contenus qu'il ne maîtrise pas.

Le problème du filtrage est complexe. Je crois beaucoup plus à l'utilisation des moteurs de recherche qu'au filtrage en terme d'efficacité.

Il existe des techniques de contournement à la fois du côté de l'éditeur et du côté de l'utilisateur. On trouve aussi les surcharges de systèmes, la surveillance et le suivi du fonctionnement d'une URL qui nécessitent des tables au niveau des routeurs et entraîneront nécessairement des saturations comme pour une surveillance par DNS. On peut utiliser le proxy, le cryptage des données, la collaboration Opérateurs avec les redirections et la localisation géographique et l'identification.

### Techniques d'investigation et utilisation du spyware et progiciel de FORENSIC :

La loi autorise aujourd'hui l'installation des logiciels, cookies sur une station à l'insu de l'utilisateur (téléchargement, ver, cookie) qui contrôlent l'accès de l'ordinateur, mais qui n'agissent pas lorsque la personne utilise elle-même son ordinateur. Le ver existe depuis les années 80. Comment démontrer que quelqu'un est auteur d'un ver ? Le seul moyen est de constater les sources chez la personne qui pourrait être l'auteur (arme du crime).

On rencontre aussi une problématique relative à la collecte de l'information si on est hors réseau. Ensuite il y a les copies des mémoires de masse. D'autre part, malgré la loi sur le cryptage, l'utilisateur peut chiffrer son disque dur, les personnes peuvent créer des méthodes de cryptage dures à casser. L'autre problème c'est que les gens utilisent maintenant des outils de nettoyage systématique des mémoires et de détection des spywares. Mais dans le cas où les policiers mettront des spywares dans le cadre de la loi LOPPSI, le logiciel ne se verra pas.

En ce qui concerne le P2P, la loi a parlé de techniques d'infiltration. Elles existaient avant la technique. Mais la loi LOPSSI va permettre l'infiltration de certains réseaux. Le problème qui va se poser ici c'est l'identité de la personne puisqu'on ne sait pas qui a été l'utilisateur de l'ordinateur (dans une même maison, plusieurs personnes peuvent utiliser l'ordinateur). Enfin, est important le choix des traces et des indices. Parce que, par le choix des traces et des indices, on peut annuler ou renforcer la preuve. Les agents, les fonctionnaires vont augmenter leur niveau de technologie.

Abordons le cas du FORENSIC : l'expert est utile ici. On peut constater les choses, à un moment donné il y a une intervention pour saisir les documents et mettre sous scellé les téléphones, disques durs... Les techniques de FORENSIC permettent de créer ce qu'on appelle de la convergence de faisceaux et d'informations permettant aux magistrats et aux policiers de recouper les informations. Le FORENSIC contient des outils d'analyse des systèmes, des outils de crack, des problèmes de filtrage forts que les services arrivent à casser et du matériel d'analyse hardware qui permet d'analyser les mémoires.

Indépendamment de l'arsenal juridique qui ne relève pas du rôle de l'expert technicien, les moyens techniques contre la cybercriminalité impliquent une collaboration internationale afin de disposer d'outils efficaces de surveillance et de capture des données.

Pour l'expert, l'exécution de sa mission dans le « tout numérique » se fera avec un haut de degré de technicité et de pédagogie pour expliquer aux magistrats son rapport. Il devra être perspicace dans le choix des tests, prendre connaissance de tous les documents, maîtriser les réseaux. Dans un environnement géographique international, l'information sera multimédia et les systèmes de plus en plus intégrés. Le « tout numérique » le mènera à mener une investigation sur des systèmes complexes (traitements et télécommunications). Le tout va être extrêmement complexe. Il y a un élément important : pour 6 mois d'écoute internet avec des DPI il faut 10 millions d'euros donc la reconstitution de l'environnement de test et de la preuve va être un élément critique. Ils sont donc formés tous les 3 mois.

**Question : en France où en est l'application des technologies en matière de vote électronique ?** Sur le vote, on avait dit qu'un rayonnement avait faussé les votes. En réalité, il n'y a pas eu de rayonnement. C'est simplement que la collecte s'est faite lentement. La vidéo a ainsi été collectée, il a fallu expertiser les boîtiers et on a pu constater que certains boîtiers n'avaient pas été lus.

**Question : Vous avez dit que vous ne croyiez pas trop au filtrage et qu'il serait plus efficace d'aller vers les moteurs de recherche, pourquoi ?** Il est plus efficace d'aller vers les moteurs de recherche. L'objectif est d'essayer de filtrer au maximum. Or, les moteurs de recherche ont la capacité de balayer tout l'internet. Donc si on veut bloquer un contenu il est plus efficace de passer par les moteurs de recherche qui sont plus adaptés. Il faudra cependant faire attention à ce que les moteurs de recherche ne les utilisent pas dans leur propre intérêt.

## LE POINT DE VUE DU MAGISTRAT

Par Myriam QUÉMÈNER, Magistrat au service criminel de la Cour d'appel de Versailles,  
Experte pour le Conseil de l'Europe en matière de cybercriminalité



L'institution judiciaire a toute sa place dans ce débat même si les magistrats, notamment en matière pénale sont encore parfois encore en retrait par rapport aux enjeux de la cybercriminalité.

La LOPPSI 2 est une loi contestée comme la loi DADVSI ou la loi HADOPI. Ainsi, on trouve des pétitions contre les articles 4 et 32 de la loi LOPPSI 2, des caricatures. Il y a des points communs entre toutes ces réformes. On a besoin d'outils pour mieux lutter contre la cybercriminalité tout en respectant les libertés individuelles. Cela ne choque pas que les enquêteurs utilisent les mêmes outils que les cyberdélinquants. Bien sûr, on est attaché à la protection des libertés individuelles, mais il faut savoir mesurer les enjeux et lutter efficacement contre la cybercriminalité. Au niveau des juridictions, en l'état, il n'y a que le parquet de Paris qui a mentionné cette notion de cybercriminalité dans son organigramme. Autrement, la cybercriminalité est dispersée dans les sections économiques et financières, les sections générales et les sections relatives aux mineurs. Il va donc falloir à moyen terme revoir les organisations pour mieux appréhender ce phénomène.

Pourquoi une telle virulence par rapport à la LOPPSI 2 ? Internet est basé sur le principe de la liberté absolue. La liberté numérique n'est-elle pas le dernier refuge de l'homme moderne ? Tout contrôle d'internet est perçu comme une atteinte intolérable aux libertés individuelles. Les réactions sont souvent irrationnelles sans véritablement connaître les textes critiqués et le domaine de la cybercriminalité. En fait, c'est un peu simpliste de dire que tous ces textes aboutissent à la censure du net.

### Cybercriminalité et contexte législatif :

Depuis 2001, on assiste à une accélération du processus législatif pour renforcer la lutte contre un phénomène encore mal défini. La notion de cybercriminalité n'est pas codifiée de façon lisible dans le Code pénal. C'est d'ailleurs l'une des préconisations que plusieurs personnes auditionnées dans le cadre d'une mission parlementaire sur la révolution numérique et la protection des droits ont faites. On a trouvé un vecteur dans la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité où on aurait pu inclure la cybercriminalité dans la criminalité organisée. On doit faire face à une évolution technologique et une course contre la montre s'est engagée pour faire de la veille juridique et essayer de suivre l'actualité. Cette actualité s'est accélérée ces derniers temps, on l'a vu en attendant quasiment 6 ans le décret sur la conservation des données. On est dans un décalage entre le droit et la technique. La cybercriminalité est une délinquance transversale qui va appréhender l'ensemble des contentieux. C'est extrêmement pratique pour les

cyberdélinquants d'utiliser internet en raison de sa volatilité, la possibilité de prendre des alias et ils peuvent se jouer des frontières puisque le droit pénal est établi en fonction des souverainetés étatiques. La cyberdélinquance est mondiale et on essaye de colmater les brèches et d'apporter des réponses quasiment naïves ou alors qui appréhendent qu'imparfaitement le phénomène.

On assiste à un empilement de lois. Or il faudrait mieux utiliser l'existant avant de créer de nouveaux textes. Ainsi si on prend l'exemple de la contrefaçon, on compte 70 infractions qui appréhendent la contrefaçon or seulement 5 articles sont réellement utilisés. En matière de cybercriminalité on a simplement 4 articles, la création de la procédure de captation de données à distance, un calage du droit processuel (infiltration, interception) et concernant les infractions qui nous concernent aujourd'hui, toutes les infractions à l'exception de la vente de billet sur internet ont été validées par le Conseil Constitutionnel. Il est important de refixer les choses.

On a un peu près 10 000 infractions et seulement 4 900 infractions selon le rapport Léger qui donnent lieu à condamnation. Faut-il vraiment continuer à produire des lois ? Par exemple, suite à la diffusion de films violents par les jeunes via les téléphones portables, on a créé l'incrimination d'happy slapping. Or cette dernière ne donne lieu qu'à seulement quatre condamnations par an. Le cyberdélinquant n'est pas perçu comme un délinquant ordinaire, parce qu'on considère que c'est lointain, virtuel. On a tendance à penser que ce n'est pas grave, mais cela a des incidences énormes et on n'a aucune étude gouvernementale permettant de cerner le phénomène. Les seuls repères que l'on possède proviennent des entreprises privées qui font des études sur la cybercriminalité, mais ces sociétés commercialisent elles-mêmes des logiciels de protection donc elles ont tout intérêt à dire que la cybercriminalité explose. La gendarmerie est en train de faire une étude sur la cybercriminalité qui est en cours de finalisation.

On constate aussi une sous-utilisation de certaines infractions dont les infractions issues de la loi Godfrain. Actuellement, on n'a qu'une centaine de condamnations par an ce qui est assez peu, mais le nombre augmente.

#### Les infractions et circonstances aggravantes prévues par la LOPPSI 2 :

La loi LOPPSI 2 crée un délit d'usurpation d'identité en ligne puni d'une peine d'un an d'emprisonnement et 15 000 euros d'amende. Particulièrement en phase avec le développement des réseaux sociaux, cette nouvelle incrimination vise aussi à punir l'utilisation de données permettant d'identifier une personne en vue de porter atteinte à son honneur ou à sa considération, comme par exemple publier une photo un peu trop personnelle. Les conditions d'application de cet article ne sont pas encore clairement définies.

Après l'article 226-4 du Code pénal, il est inséré un article 226-4-1 ainsi rédigé : "Le fait d'usurper l'identité d'un tiers ou de faire usage d'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 ou à sa considération, est puni d'un an d'emprisonnement et de

15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne".

Il faudrait tout d'abord définir la notion d'identité numérique permettant de réprimer des cas d'usurpation sans préjudice.

Les termes d'atteinte à l'honneur ou à la considération sont directement inspirés de la loi du 29 juillet 1881 sur la liberté de la presse, laquelle vise notamment le délit de diffamation. Ne va-t-on pas contourner la courte prescription de la diffamation, qui est de trois mois, à partir de la mise en ligne du contenu ? En effet, il est vrai qu'en matière de diffamation on constate que les victimes de diffamation saisissent les tribunaux alors que les faits sont prescrits. Donc ne va-t-on pas utiliser l'infraction d'usurpation d'identité comme une sorte de détournement de la procédure de diffamation ? La notion d'"identité d'un tiers" peut laisser entendre que constituerait une infraction pénale le fait d'usurper (pseudo/mots de passe) d'une personne en vue de troubler sa tranquillité ou de porter atteinte à son honneur.

L'extension des peines aggravantes a aussi été soulignée. Les douanes insistent depuis longtemps pour aggraver les peines en matière de contrefaçon commise en ligne. L'article 3 de la LOPPSI 2 a ainsi porté à dix ans d'emprisonnement et 10 000 euros d'amende le délit de contrefaçon de carte bancaire et de chèque lorsque ces délits sont commis en bande organisée ou par l'intermédiaire d'un réseau de communication au public en ligne. De même, le texte prévoit une aggravation des peines relatives à certaines atteintes à la propriété intellectuelle lorsqu'elles sont commises en bande organisée ou par l'usage d'internet. Cependant, on assimile le fait de mettre en ligne à la bande organisée.

#### Le blocage des sites :

L'article 6 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique se trouve modifié par l'article 4 de la loi LOPSSI 2. Ainsi sont insérés deux nouveaux alinéas qui disposent 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 personnes mentionnées au 1 du présent 9 les adresses électroniques des services de communication au public en ligne contrevenant aux dispositions de cet article, auxquelles ces personnes doivent empêcher l'accès sans délai.

"Un décret fixe les modalités d'application de l'alinéa précédent, notamment celles dont lesquelles sont compensés, s'il y a lieu, les surcoûts résultant des obligations mises à la charge des opérateurs."

Actuellement, il est déjà possible de demander à un juge d'imposer à l'hébergeur de supprimer un contenu ou de fermer un site. Ce dispositif de blocage vise à lutter contre les sites hébergés à l'étranger en mettant les FAI en première ligne du dispositif. Cependant, la pertinence est faible d'autant qu'il y a longtemps que les pédophiles n'agissent plus sur les réseaux publics et passent par des forums de discussion ou les réseaux sociaux. Ce sont les premiers à suivre l'actualité judiciaire. Cette disposition rassure plus la population qu'autre chose. Ce type de législation est déjà en vigueur au Danemark, en Grande-Bretagne, en

Norvège, aux Pays-Bas et en Suède avec des résultats plus ou moins probants en raison des difficultés techniques liées à un tel blocage.

Concernant, le renforcement de la protection des mineurs, le dispositif législatif est complété et modifié tous les ans suite aux faits divers. Ainsi par exemple l'article 5 de la loi LOPPSI 2 modifie l'article 227-24 du Code pénal en y incriminant le fait d'inciter "des mineurs à se livrer à des jeux les mettant physiquement en danger". Cette disposition a ainsi permis de réprimer le jeu du foulard par exemple.

#### Les moyens d'investigation :

Il faut que les services d'enquêtes spécialisés disposent de moyens pour combattre la cybercriminalité. On assiste à une extension de l'infiltration tout à fait adaptée à l'univers numérique. De plus, il y a un rallongement des délais en matière d'interception des appels téléphoniques transposables au numérique avec un contrôle des magistrats garantissant les libertés individuelles. Le domaine est très défini : terrorisme et criminalité organisée.

#### La captation de données :

La captation des données à distance est un outil complétant un dispositif devant être mis à la disposition des services d'enquête spécialisés.

Ainsi un nouvel article 706-102-1 du Code de procédure pénale dispose 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 saisis 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 saisie de caractères. Ces opérations sont effectuées sous l'autorité et le contrôle du juge d'instruction". Cette procédure de « cyberpatrouille » nécessite des officiers de police judiciaire spécialement formés. De plus, on constate que seulement une vingtaine de procédures ont eu recours à la procédure de cyberpatrouille. On dénote un manque de moyens au niveau des services d'enquêtes.

De plus se posent des difficultés en matière de données à caractère personnel. Malgré les précautions prises concernant notamment la limitation des données enregistrées aux seuls éléments utiles à la manifestation de la vérité et aux séquences liées aux infractions, la CNIL relève que le projet LOPPSI 2 prévoit l'utilisation de ces outils de captation des données informatiques à l'insu des intéressés dans les points publics d'accès à internet.

Or, une telle mesure a pour conséquence, par exemple, de placer l'ensemble des postes informatiques d'un cybercafé sous surveillance. Le recours à cette possibilité doit donc revêtir un caractère exceptionnel, ainsi qu'une traçabilité des accès et utilisation de ces outils de captation afin de garantir les citoyens contre toute dérive. À ce titre, la CNIL

souhaite que ces mesures techniques de traçabilité soient fixées par des dispositions réglementaires prises après son avis.

#### Les fichiers de police et la vidéoprotection :

- *Fichiers d'analyse sérielle :*

En ce qui concerne les fichiers d'analyse sérielle (ANACRIM et SALVAC), la loi LOPPSI 2 a abaissé le seuil des peines des crimes et délits, à savoir au moins 5 ans, pour lesquels ces traitements peuvent être mis en œuvre.

Ces fichiers pourront désormais traiter des vols aggravés prévus par l'article 311-4 du Code pénal, des vols à l'encontre des personnes particulièrement vulnérables ou encore des vols accompagnés d'actes de destruction ou de détérioration, dont les peines seront ramenées à cinq ans d'emprisonnement.

Il faut noter que ces applications peuvent enregistrer des données à caractère personnel faisant apparaître les origines raciales ou ethniques, les opinions politiques, religieuses... ou qui sont relatives à la santé ou la vie sexuelle, dans la stricte mesure nécessaire aux finalités de recherche criminelle assignées auxdits traitements. Un décret en Conseil d'État pris après avis de la CNIL sera donc nécessaire pour en fixer les modalités.

- *Les logiciels de rapprochement judiciaire :*

Afin de faciliter le rassemblement des preuves des infractions et l'identification des auteurs, les services de police nationale et de la gendarmerie nationale chargés d'une mission de police judiciaire pourront mettre en œuvre, sous le contrôle de l'autorité judiciaire, des logiciels destinés à faciliter l'exploitation et le rapprochement d'informations qu'ils détiennent sur les modes opératoires.

Les données à caractère personnel, éventuellement révélées par l'exploitation des enquêtes et investigations, rapprochées par ces logiciels seront effacées à la clôture de l'enquête et, en tout état de cause, à l'expiration d'un délai de trois ans après le dernier acte d'enregistrement.

Ces logiciels devront également être autorisés par décret en Conseil d'État pris après avis de la CNIL

- *La vidéoprotection :*

La loi LOPSSI 2 étend les finalités, pour lesquelles la loi du 21 janvier 1995 autorise la vidéoprotection de la voie publique par les autorités publiques, à la régulation des flux de transport, la prévention de lieux particulièrement exposés au trafic de stupéfiants ou de trafics illicites, et la prévention des risques naturels ou technologiques.

Elle précise également que les personnes morales de droit privé sont autorisées à installer, après information du maire et autorisation du préfet, des systèmes de vidéosurveillance sur la voie publique afin de protéger les abords de leurs bâtiments dans les lieux susceptibles d'être exposés à des actes de terrorisme ou particulièrement exposés à des risques d'agression ou de vol.

Le projet de loi LOPPSI 2 donnait aussi la possibilité aux autorités publiques ou personnes morales de déléguer à des opérateurs publics ou privés l'exploitation de leur système de vidéosurveillance. On va vers un État de plus en plus sécuritaire et curieusement on délègue à des opérateurs privés des fonctions devant rester à la sphère étatique ce qui n'a pas échappé au Conseil constitutionnel qui a émis des réserves d'interprétation.

Conclusion : plutôt que de faire un empilement de textes en matière pénale, il faudrait plutôt aller vers une définition d'ensemble de la politique pénale. On voit beaucoup d'instructions, de circulaires qui sont des paraphrases des textes. Mais il n'y a aucune orientation globale de politique pénale sur la notion même de cybercriminalité, mais des commentaires au cas par cas. C'est gênant car des problèmes se posent en matière de compétence territoriale. Il faudrait clarifier les critères. On a aussi des problèmes car certains contentieux nécessitent la mise en place de stratégie procédurale (notamment avec Interpol et Europol où il faut faire des réunions en amont). Il faut connaître les prestataires techniques, coopérer avec les entreprises privées, renforcer les moyens et la formation spécialisée en la matière et enfin améliorer la coopération internationale plutôt que de faire des nouveaux textes. On a des textes complètement en conformité avec la Convention de Budapest sur la lutte contre la cybercriminalité que la France a ratifié, mais certains ne l'ont pas ratifié, on a des conventions bilatérales, mais dans certains pays où la cybercriminalité se développent, l'arsenal pénal est encore faible ou inexistant et il faut aider ces pays ce que fait le Conseil de l'Europe.

## CLÔTURE DE LA MATINÉE

Par Jérôme HUET, Professeur à l'Université Panthéon-Assas Paris 2, Directeur du CEJEM et du Master 2 Professionnel Droit du Multimédia et de l'Informatique (M2 DMI)



Avant de commencer, il faut remercier les étudiants qui se sont tellement dévoués pour que cette conférence manifestement attendue ait lieu. Je vais faire un ensemble de réflexions, deux principalement, précédées de quelques remarques.

La première remarque c'est nous avons pris ces derniers temps, l'habitude de dénommer des lois par un sigle, un peu pour faire passer par ce raccourci l'abondance de textes que l'on pourrait désigner d'harcèlement textuel. Ce qui amène à la seconde réflexion. On en est à la LOPPSI 2, pourquoi pas la LOPPSI 3 et après la LOPPSI le retour ? C'est comme au cinéma. Dans ce harcèlement textuel, la Communauté européenne et le

législateur français feraient bien de se méfier des problèmes de conflits de lois dans le temps que tout ceci va inévitablement poser.

Sur l'usurpation d'identité, on s'est trompé. Cette disposition devrait être dans le Code civil. « Chacun a le droit au respect de son identité ». Chose que j'ai apprise dans ma carrière c'est que dans le Code civil, il n'y a pas de sanction pénale. Cependant, ce serait mieux de supprimer l'usurpation d'identité à des fins de causer une infraction et de balancer le texte que l'on vient d'adopter, qui encourt tous les griefs, qui va être censuré par le Conseil constitutionnel. On a fait une infraction pénale sur la tranquillité et la considération. Mais qu'est-ce que la tranquillité ? C'est une notion imprécise contraire à la légalité des délits et des peines. On devrait uniquement insérer un article disposant "l'usurpation d'identité est punie". On ferait du nettoyage et ça irait dans le sens de la dépénalisation que l'on souhaite aujourd'hui. Nous sommes en plein paradoxe, on fait la LOPPSI 2 à une époque où on cherche à dépénaliser la diffamation. Dépénaliser la diffamation est aberrant parce que lorsqu'il n'y aura plus de sanction pénale, n'importe qui diffamera n'importe qui.

De plus, je suis tout à fait d'accord avec Jérémie Zimmermann. On suit un siècle où il y a eu deux guerres mondiales, un holocauste, une guerre en Irak... Les États ne sont pas bons, ils prennent les bons prétextes (la cyberpornographie en l'occurrence) pour faire passer leur dispositif. On aurait pu s'interroger pour savoir s'il y avait d'autres solutions. N'avez-vous pas remarqué que dans l'article 1er sur l'usurpation d'identité il n'y a pas de filtrage, mais pour la pédopornographie le filtrage existe. Pourquoi ? Parce que dans un cas on veut avoir l'air respectable et dans l'autre cas on s'en fout. Cette infraction ne va jamais jouer car aucun juge ne dira que quelqu'un a troublé la tranquillité d'autrui pour lui mettre une amende de 15 000 €. Donc, il serait plus utile d'agir en responsabilité ça suffit. On n'a donc pas besoin de filtrer. Comme d'habitude, on est bon en faire savoir, mais en savoir-faire on est nul.