

02-02-2010

Mag2lyon

[www.mag2lyon.com](http://www.mag2lyon.com)



## “Une nouvelle menace”

**Le 4e forum international sur la cybercriminalité s'ouvre à Lille en mars prochain. Une délinquance en pleine expansion, même s'il n'y a aucun chiffre officiel. Les explications de Mohamed Chawki, docteur en droit de l'université Lyon 3 et Président de l'association internationale de lutte contre la cybercriminalité à Paris.**

“Si les nouvelles technologies participent de manière positive au développement, elles constituent aussi de nouveaux moyens pour commettre des infractions. La pédophilie est un exemple particulièrement saisissant de criminalité qui a pris une véritable ampleur grâce au cyberspace. Les pédophiles pouvant profiter de l'anonymat d'internet pour reproduire des photos et les diffuser sans aucune limite, mais aussi pour recruter des victimes. Autre problème lié au développement d'internet : la diffusion d'œuvres protégées par le droit de la propriété intellectuelle, donc la contrefaçon, par la diffusion de copies illicites : musique, vidéo, logiciels... Les failles de type XSS qui peuvent donner la possibilité à un attaquant de voler la cession d'un internaute ou de mener des attaques de type phishing, c'est-à-dire que les cybercriminels envoient des mails frauduleux aux internautes au nom d'organismes financiers ou de grandes sociétés, pour récupérer les mots de passe de leurs comptes bancaires et leurs numéros de cartes de crédit. Il y a aussi les fausses loteries, la vente de services criminels en ligne, le cybersquattage qui consiste à enregistrer un nom de domaine correspondant à une marque, pour ensuite essayer de le revendre... La dimension globale du réseau internet permet également aux criminels de cacher leur identité pour commettre des infractions et communiquer avec d'autres criminels.

En fait, la cybercriminalité bénéficie d'un certain flou statistique car on cerne mal son ampleur et les dégâts qu'elle peut provoquer. Comme chaque phénomène criminel, une évaluation exacte de son ampleur est utopique. Selon les criminologues, seules 15 % des infractions informatiques commises sont enregistrées. Une certitude, la cybercriminalité augmente rapidement. Le Club de la Sécurité Informatique vient d'ailleurs de rendre public un bilan de la cybercriminalité pour 2009. Son objectif : dresser un état de la cybercriminalité mais aussi de la sécurité des systèmes d'information. Ce qui

permet d'avoir une vision approximative des actes délictueux commis via ou contre les systèmes informatiques, qualifiés de "nouvelle menace en pleine expansion". Selon ce bilan, les réseaux sociaux tels que Facebook peuvent servir de vecteur à de nouveaux logiciels malveillants, faciliter des escroqueries, mais surtout constituer des mines d'informations sur les individus.

Dans l'avenir, il est clair que la cybercriminalité ne peut que se développer. Et pour que la société soit capable de contrôler les risques, un cadre juridique est donc nécessaire, accompagné de dispositifs répressifs efficaces. Et même si la France est le troisième pays après l'Ukraine et la Bosnie-Herzégovine à procéder à la publication de la convention sur la Cybercriminalité de 2001, il faut aller encore plus loin.

Dans cette perspective, la lutte contre ces menaces doit d'abord être coordonnée sur le plan international pour permettre d'harmoniser les bases légales et de créer les conditions nécessaires à une coopération efficace et rapide entre les autorités judiciaires et policières de chaque pays. Ce qui est une nécessité absolue car cette cyber menace exige une coordination entre chaque Etat pour mieux détecter la cybercriminalité et lutter plus efficacement contre ce phénomène. Il est également important de promouvoir une meilleure coopération entre le secteur privé et l'administration. Le secteur privé pourrait ainsi assurer un transfert de connaissances vers l'administration. Etant donné la complexité technique des enquêtes en matière de cybercriminalité, cela permettrait de rendre plus performantes les poursuites pénales. Il est aussi important d'élaborer une procédure standard utilisable par chaque Etat pour les recherches et les enquêtes, mais aussi pour la collecte de données afin de poursuivre ces infractions et de condamner plus rapidement et plus facilement les cybercriminels."