



La cybercriminalité:Aspects législatifs et jurisprudentiels

publié le **30/04/2013**, vu **10454 fois**, Auteur : [maitre imen nasri](#)

Face à l'ampleur du danger que représente la cybercriminalité pour la sécurité des réseaux informatiques et des cybers citoyens, il est apparu nécessaire de faire un état des lieux de la stratégie de prévention et de répression de la cybercriminalité .

L'Internet offre aujourd'hui une multitude de services aux gens mais les dérapages restent possibles en raison des failles facilement détectables par les escrocs du net.

Le terme de cybercriminalité est une notion large qui regroupe l'ensemble des infractions pénales commises via les réseaux informatiques, notamment sur le réseau Internet.

Il s'agit donc d'une nouvelle forme de criminalité et de délinquance qui se distingue des formes traditionnelles en ce qu'elle se situe dans un espace virtuel,selon l'Organisation des Nations unies, la cybercriminalité peut être définie comme « **tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent** ».

La Convention de Budapest du 23 novembre 2001 définit la Cybercriminalité ainsi : « L'ensemble des infractions pénales spécifiques liées aux technologies de l'information et de la communication, ainsi que celles dont la commission est facilitée ou liée à l'utilisation de ces technologies».

La cybercriminalité englobe trois catégories d'activités criminelles :

- Les infractions propres aux réseaux électroniques (piratage)?.
- Les formes traditionnelles de criminalité facilitées par les technologies de l'information et de la communication(escroquerie, vols de données,fausses cartes de paiement ,)?
- Les infractions liées aux technologies de l'information et de la communication:La diffusion de contenus illicites.

Les aspects les plus répandus de la cybercriminalité sont :

- Le Carding ;
- Le Skimming ;
- Le Phishing
- Les escroqueries à la téléphonie

Le dispositif législatif et réglementaire français

La cybercriminalité est prise juridiquement en compte depuis la [loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978](#).

La Loi Godfrain du 5 février 1988 relative à la fraude informatique a introduit les articles 323-1 et suivants dans le [Code pénal](#), concernant notamment la suppression ou modification de données (art 323-1 al 1), ou encore la tentative d'infraction sur un STAD (323-7).

La [loi du 15 novembre 2001 relative à la sécurité quotidienne](#)

La loi du 18 mars 2003 pour la sécurité intérieure

La loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité

La [loi pour la confiance dans l'économie numérique](#) du 21 juin 2004, qui a modifié les articles 323-1 et suivant du [Code pénal](#). Cette loi a, en outre, modifié l'article 94 du [Code de procédure pénale](#) relatif à l'inclusion des données informatiques dans la liste des pièces susceptibles d'être saisies lors des [perquisitions](#) réalisées en [flagrant délit](#) ou au cours d'une [instruction](#). (Ces perquisitions sont aussi régies par les art. 56 et 97 du [Code de procédure pénale](#)).

La loi du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle.

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.

La loi du 5 mars 2007 relative à la prévention de la délinquance

Par ailleurs de nombreux textes réglementaires ont été adoptés. On peut citer pour exemple le décret du 24 mars 2006 sur la conservation des données de trafic prévu par la loi relative à la sécurité quotidienne.

La lutte contre la cybercriminalité est en pleine évolution et elle fait l'objet de nombreuses réflexions en France.