



YVES DENOYELLE

*Chaque semaine
M^e Alain Bensoussan,
avocat à la cour
d'appel de Paris
et spécialiste
en droit de
l'informatique, vous
informe de vos droits.*

Les limites du droit de la criminalité informatique sur le Web 2.0

En France, ces règles ont pris corps avec la loi du 21 juin 2004 (dite LCEN) qui a complété le dispositif pénal classique de lutte contre les infractions informatiques pour l'étendre à la cybercriminalité. On pourrait donc estimer qu'avec un tel ensemble de règles,

les infractions du monde « Web 2.0 » sont couvertes. C'est loin d'être le cas car la fraude informatique et la cybercriminalité sont fondées sur deux notions (l'intrusion dans un système et l'altération de ce système) qui échappent au Web 2.0. La plupart des

infractions commises ne relèvent d'aucune de ces deux notions ou sont manifestement incompatibles. Par exemple, la notion d'espace collaboratif ouvert ne fait pas bon ménage avec la notion d'intrusion. De même, les « Bots Nets » (réseau de zombies)

permettent de commettre des dommages majeurs par « rebond », mais n'altèrent pas nécessairement les ordinateurs infectés à l'insu de l'internaute. Il existe même des services du Web 2.0 qui sont par nature criminogènes, comme les services permettant à n'importe quel internaute de

donner à un autre la possibilité de prendre à distance la main sur l'ordinateur pour le déboguer. Cela fait de chaque utilisateur une victime et une menace potentielle. L'internaute devient ainsi l'élément déterminant de la sécurité du monde Web 2.0...