

# E-réputation : se prémunir de l'usurpation d'identité numérique

publié le 20/11/2014, vu 2691 fois, Auteur : [Noé MARMONIER Avocat](#)

**L'usurpation d'identité numérique constitue l'atteinte 2.0 à la vie privée. Chaque internaute est susceptible d'être frappé, mais également les entreprises qui ne sont pas à l'abri. L'usurpation d'identité se développe, dont les réseaux sociaux constituent un terrain de chasse privilégié.**

L'usurpation d'identité se développe, dont les réseaux sociaux constituent un terrain de chasse privilégié.

Vengeance personnelle, cupidité, profiter indûment de l'image ou de la notoriété d'une personne, réalisation d'infractions derrière une fausse identité sont autant de mobiles pour les usurpateurs.

De telles atteintes peuvent avoir des effets dévastateurs sur la réputation numérique d'une personne, reflet de la réputation physique.

Il convient d'agir très rapidement, afin de limiter la forte capacité de nuisance, démultipliée par internet (ubiquité, rapidité de diffusion, etc...). Les avantages d'Internet deviennent inconvenients en matière d'usurpation numérique.

De telles atteintes peuvent avoir des effets dévastateurs sur la réputation numérique d'une personne, reflet de la réputation physique.

Les manifestations de l'usurpation d'identité sont diverses : captation de données personnelles sur les sites internet institutionnels ou sur les comptes personnels de sites marchands, création de faux profils sur les réseaux sociaux...

Nom, prénom, photos, ces données sont susceptibles d'être captées et utilisées à l'insu de l'internaute.

Il est nécessaire de connaître certaines astuces pour s'en prémunir, et de réagir efficacement en cas d'atteinte.

Tout d'abord, sur les réseaux sociaux, une astuce simple pour chaque internaute consiste à avancer masqué : l'idéal est la création d'un profil sous pseudonyme. Cela compliquera la tâche des usurpateurs qui n'auront pas accès au patronyme de leur victime potentielle.

Puis, périodiquement, il peut être utile d'exercer une veille sur son propre nom et prénom, en cherchant éventuellement des profils comportant ses données personnelles.

Il est aussi pertinent d'effectuer une veille dans Google images.

En cas d'atteinte, le premier réflexe est le signalement auprès des services d'alerte du site

internet. Chaque réseau social comporte ce type de procédure.

Le traitement est plus ou moins long, c'est pourquoi en cas d'urgence, il est opportun d'agir de manière plus ferme, et s'en remettre à un avocat peut constituer une alternative efficace.

Enfin, en cas de préjudice, notamment financier subi, le dernier réflexe consiste à déposer plainte auprès des services de police.

L'article 226-4-1 alinéa premier du Code pénal prévoit et réprime l'usurpation d'identité réalisée hors cadre numérique, et l'alinéa second prévoit et réprime l'usurpation d'identité numérique, réalisée « *à partir d'un réseau de communication au public en ligne* ».

L'usurpation d'identité constitue un délit, dont la peine encourue s'élève jusqu'à un an d'emprisonnement, et jusqu'à 15.000 Euros d'amende.

La plainte préalable de la victime n'étant pas une condition d'engagement de l'action publique.

Si un préjudice est établi, la seconde étape éventuelle, sous réserve du respect d'un cadre procédural, résidera dans une constitution de partie civile pour la victime, afin de solliciter des dommages et intérêts, en vue de la réparation du préjudice subi.