# Le délit d’usurpation d’identité numérique, un nouveau fondement juridique pour lutter contre la cybercriminalité. Par Betty Sfez, Avocat.

Le délit d’usurpation d’identité numérique, un nouveau fondement juridique pour lutter contre la cybercriminalité. Par Betty Sfez, Avocat.

**L'usurpation d'identité numérique n'est pas un phénomène nouveau. Ce type d'escroquerie sur internet, visant à se faire passer pour un autre (entreprise, administration) pour accéder à des données ou des comptes bancaires et détourner des fonds, ou porter atteinte à la réputation d'une entreprise ou d'une personne physique s'est développé parallèlement à l'essor de l'internet. En ces périodes troublées, le détournement de comptes bancaires pour en soutirer les fonds, ou de comptes personnels sur les réseaux sociaux à des fins de propagande par exemple, est plus que jamais un phénomène d'actualité.**

Avant l'entrée en vigueur de la loi LOPPSI II, adoptée le 14 mars 2011, la victime d'une usurpation d'identité sur internet ne pouvait poursuivre l'auteur de l'infraction que sur des fondements généraux du droit pénal, tels l'escroquerie, la prise du nom d'un tiers aux fins de commission d'une infraction pénale (ex. diffamation, escroquerie), l'atteinte à un traitement automatisé de données, l'atteinte à la vie privée et l'atteinte au droit à l'image.
La LOPPSI II de 2011, qui comprend un chapitre dédié à la lutte contre la cybercriminalité, a créé une nouvelle infraction spécifique : l'usurpation d'identité numérique. [1]

La première condamnation sur le fondement de l'usurpation d'identité numérique a été prononcée par le Tribunal de grande instance de Paris le 18 décembre 2014, dans une affaire concernant la création d'un faux site web. [2]
Toutefois, la collecte des preuves, et surtout, l'identification de l'auteur du délit reste un obstacle difficile à surmonter pour la victime souhaitant engager des poursuites.
Nous analysons ci-dessous les aspects spécifiques de la notion d'usurpation d'identité numérique puis les moyens de défense dont disposent les victimes.

**1. La notion d'usurpation d'identité numérique.**

**1.1 La définition légale.**

L'usurpation d'identité est constituée quand elle porte sur l'identité même de la victime (nom, prénom, surnom, pseudonyme, identifiants électroniques) ou sur toute autre donnée de nature à l'identifier. Cette dernière expression permet de s'affranchir de la notion de données à caractère personnel, au sens de la loi Informatique et Libertés, et de rechercher tous autres éléments permettant une identification. Il est donc possible d'y inclure les adresses IP, les URL, les mots de passe, ainsi que des logos, images, voire même un avatar, tous ces éléments permettant de pointer vers une personne physique. Les juges seront amenés à interpréter et affiner cette notion et son périmètre.

L'usurpation d'identité "numérique", telle que prévue à l'article 226-4-1 al. 2 du code pénal, est commise sur un réseau de communication au public en ligne, ce qui comprend notamment les courriers électroniques, les sites web, les messages publiés en ligne et les profils en ligne sur les réseaux sociaux (Facebook, Twitter). [3]
Le préjudice effectif ou éventuel s'analyse en un trouble de la tranquillité de la personne dont l'identité est usurpée ou celle d'un tiers, ou en une atteinte à son honneur ou à sa réputation.
L'auteur de l'infraction, personne physique, encourt un an d'emprisonnement et 15.000€ d'amende. La condamnation peut atteindre 75.000€ lorsque l'auteur de l'infraction est une personne morale.

**1.2 Usurpation d'identité numérique : phishing, faux sites web et faux profils.**

L'usurpation d'identité numérique peut porter préjudice à deux catégories de victimes :
– la personne dont l'identité a été usurpée : l'auteur de l'infraction nuit à son image, à sa réputation, à sa marque ou trouble sa tranquillité ;
– le tiers trompé : l'auteur de l'infraction induit l'internaute en erreur et lui soutire des informations et/ou de l'argent.
L'usurpation d'identité numérique est généralement commise de deux manières : par la technique du phishing (ou hameçonnage), ou par la création d'un faux site web ou d'un faux profil sur un service de réseau social.

**Le phishing ou hameçonnage**

Le cyber-escroc usurpe l'identité d'un tiers, généralement une entreprise (banque, opérateur téléphonique) ou une administration, en communiquant via un faux courrier électronique et/ou via un site web contrefait. L'escroc reproduit alors les identifiants visuels et graphiques de la marque, en vue d'obtenir de la part d'internautes trompés, des informations personnelles (identifiants, mots de passe ou coordonnées bancaires). Ces informations sont ensuite utilisées pour accéder à leurs comptes et effectuer des opérations sous l'identité de l'internaute (virement, souscription d'un crédit, abonnement). [4]
Par exemple, dans un jugement rendu le 21 septembre 2005, le Tribunal de grande instance de Paris a condamné un internaute pour contrefaçon de marque et contrefaçon d'un site web. Ce dernier avait imité la page d'enregistrement du service Microsoft MSN Messenger, et sa marque figurative (le papillon MSN), pour obtenir des données personnelles des personnes au moment de leur enregistrement sur le service. [5]

**La création d'un faux site web ou d'un faux profil sous l'identité d'une tierce personne**

L'usurpation d'identité numérique est également réalisée via la création d'un faux site web, reprenant à l'identique les composants d'un site "légitime" (charte graphique, reproduction de tout ou partie du contenu, etc.). Cette technique est souvent liée à une "campagne" de phishing.
La création d'un faux site web ou d'un faux profil a pour objet ou pour effet de porter atteinte à l'honneur ou à la réputation du titulaire du site ou du profil, personne physique ou morale.

**1.3 Le jugement du 18 décembre 2014.**

Le Tribunal de grande instance de Paris a rendu un premier jugement le 18 décembre 2014 condamnant l'auteur d'une usurpation d'identité numérique sur le fondement de l'article 226-4-1 du Code pénal.
Dans cette affaire, un informaticien avait créé un faux « site officiel » de la députée-maire Rachida Dati. Le faux site reprenait la photo de Rachida Dati ainsi que la charte graphique du site officiel et permettait aux internautes de publier des commentaires sous la forme de communiqués de presse, soi-disant rédigés par Rachida Dati, mais au contenu trompeur. L'internaute se trouvait en réalité sur le site officiel, très similaire au faux site. L'auteur de cette usurpation avait utilisé une faille de sécurité du site de la députée-maire, permettant d'y injecter du code indirect (opération dite « XSS » ou cross-site scripting).

Le directeur du Cabinet de Madame Dati a déposé plainte contre X pour usurpation d'identité sur support numérique et atteinte aux systèmes de traitement automatisé de données. L'enquête, menée par la BEFTI (Brigade d'enquête sur les fraudes aux technologies de l'information), a permis d'identifier l'auteur des agissements.

Dans un jugement du 18 décembre 2014, le TGI de Paris a retenu les deux chefs d'accusation à l'encontre du prévenu. Le Tribunal considère en effet, que l'identité de Madame Rachida Dati avait été numériquement usurpée, dans la mesure où "ces mentions ["je vous offre un communiqué… » ou "merci pour ce geste citoyen "], aux côtés du nom de Madame Rachida Dati et sur un site reprenant la photographie officielle de la député-maire, sa mise en page et sa charte graphique, ne peut que conduire l'internaute à opérer une confusion avec le site officiel de celle-ci".

Par ailleurs, le Tribunal a retenu que l'auteur du faux site avait mis en place un dispositif permettant la mise en ligne par les internautes de faux communiqués au contenu sexiste et dégradant. Or, en sa qualité de modérateur du site, il avait la possibilité de fermer son site ou de désapprouver les termes des commentaires mis en ligne par les internautes.

Le prévenu a également été considéré coupable d'introduction frauduleuse de données dans un système de traitement de données, du fait d'avoir exploité la faille de sécurité du site officiel pour y introduire des instructions dans le but d'en modifier son comportement. L'ensemble de ces éléments entraînant la confusion avec le site officiel de la femme politique, l'internaute a été reconnu coupable d'usurpation d'identité numérique. Condamné à une amende de 3.000€, l'auteur du faux site a fait appel de la décision.
Le fournisseur d'hébergement a quant à lui été reconnu complice de cette infraction.

**2. Les moyens de défense à la disposition des victimes.**

**2.1 Pour la personne usurpée.**

Face à ce type d'agissement, il est possible de prendre des mesures proactives, ou en cas de constatation d'une infraction, de prendre des mesures en réaction.
Les institutions fournissent des recommandations, proactives – concernant la sécurité des comptes personnels, et réactives – concernant les mesures de retrait de contenu ou de dépôt de plainte.
L'Hadopi (Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet) fournit une série de recommandations aux fins d'éviter l'usurpation d'identité numérique. Ces recommandations, qui relèvent souvent du bon sens, consistent notamment, à utiliser des mots de passe complexes et de ne pas les communiquer à des tiers, activer les protections anti-phishing existant dans certains navigateurs web, éviter de se connecter sur des sites sensibles (sites de banques ou de vente en ligne) dans les lieux publics ou chez des tiers, ne pas répondre à des emails provenant de prétendus organismes de confiance et demandant de communiquer mots de passe ou autres coordonnées personnelles confidentielles, ne jamais cliquer sur les liens ni ouvrir les documents contenus dans ces messages, etc. [6]
Si des informations d'identification ont été publiées sans autorisation et/ou détournées, le responsable du site sur lequel ces informations ou données sont publiées doit être contacté pour en demander leur suppression. A cet effet, la CNIL (Commission nationale de l'informatique et des libertés) propose sur son site des modèles de courriers pour formuler cette demande. [7] A défaut de réponse, il conviendra alors de porter plainte en ligne via le site de la CNIL.
La Commission aide ainsi à la suppression des informations détournées et à la récupération de l'accès à sa messagerie électronique. [8]

**2.2 Les moyens de preuve à l'appui d'une action en usurpation d'identité numérique**

**La difficulté à identifier l'auteur de l'infraction.**

Il existe encore peu de décisions judiciaires condamnant ces pratiques. La victime se heurte en effet à deux difficultés majeures : l'identification des auteurs de l'escroquerie, rendue difficile notamment à cause des procédés d'anonymisation ; et la localisation de l'auteur. Lorsqu'il est possible de remonter jusqu'à l'auteur, celui-ci est souvent situé à l'étranger, rendant les poursuites difficiles et la procédure coûteuse.
Comme mentionné ci-dessus, la victime d'une usurpation d'identité numérique peut adresser une plainte à la CNIL. Elle peut également porter plainte soit auprès des forces de l'ordre (police ou gendarmerie), soit directement auprès du procureur de la République.

Afin que l'affaire ne soit pas classée sans suite, il est fortement recommandé de fournir des éléments de preuve remontant jusqu'à l'auteur de l'infraction. A cette fin, la victime peut contacter le fournisseur d'accès à internet ou le fournisseur d'hébergement afin d'obtenir la communication des données permettant d'identifier l'auteur de l'infraction.

Les moyens de preuve. Afin de faciliter l'identification des auteurs d'une infraction, la loi pour la confiance dans l'économie numérique du 21 juin 2004 (LCEN), impose aux prestataires techniques, fournisseurs d'accès à internet et hébergeurs, la conservation des données "de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles (ces personnes) sont prestataires" (article 6 II). [9]
Ainsi, à la demande de l'autorité judiciaire, FAI et hébergeurs doivent transmettre toute information en leur possession, nécessaire à la constitution du dossier, dans le respect des délais de prescription. Il est à noter cependant que, suivant les catégories de données concernées, différents délais de prescription s'appliquent. Ainsi, les données de connexion ne seront conservées que pendant un an.
Par ailleurs, il peut être utile de faire établir un constat d'huissier afin de conserver la preuve des écrans, pages web et autres éléments à l'appui des poursuites.

**Une infraction "autonome"**

Depuis la LOPPSI II, le délit d'usurpation d'identité numérique est une infraction autonome. Ainsi, le seul fait de commettre un acte de phishing, même sans accès effectif aux comptes dont les données ont été récupérées, est suffisant pour être qualifié d'acte d'usurpation d'identité numérique. Il n'est donc pas obligatoire de rapporter la preuve selon laquelle l'usurpation a été commise en vue de la réalisation d'une infraction (telle que le détournement de fonds ou l'apologie du terrorisme par exemple).
Le législateur exige cependant un dol spécial : l'accusation doit rapporter la preuve que l'usurpateur a agi en vue de troubler la tranquillité de la personne dont l'identité est usurpée ou de celle d'un tiers, ou afin de porter atteinte à son honneur ou à sa considération.
Toutefois, le législateur n'impose pas de prouver une répétition des agissements fautifs, alors que la rédaction initiale de l'article 226-4-1 al. 2 dans le projet de loi LOPPSI II avait prévu une condition de réitération.
Une infraction "instantanée". L'usurpation d'identité numérique étant un délit, la victime dispose d'un délai de prescription de trois ans pour agir. Le délit d'usurpation d'identité numérique est une infraction instantanée : le point de départ du délai de prescription se situe au jour où l'identité a été usurpée.
Cependant, comme mentionné plus haut, il convient d'agir sans attendre. En effet, selon les catégories de données concernées, différents délais de prescription peuvent avoir pour conséquence que certaines d'entre elles ne seront plus disponibles au moment de la constitution du dossier.

Betty SFEZ
Avocat au Barreau de Paris
Deleporte Wentz Avocat
*Accueil*

---



*[Notes]*
*[1] Loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.*
*[2] TGI Paris, 13e ch. corr., 18 décembre 2014, MP c/ X.*
*[3] Art. 226-4-1 du code pénal : "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."*
*[4] Les auteurs de l'escroquerie utilisent régulièrement la technique du "social engineering", ou ingénierie sociale, méthode de manipulation abusant de la crédulité de personnes, afin qu'elles divulguent des données confidentielles.*
*[5] TGI Paris, 31e ch. corr., 21 septembre 2005, Microsoft Corporation c/ Robin B.*
*[6] Fiche Hadopi relative aux moyens de sécurisation : Identité numérique//Usurpation d'identité publiée en décembre 2011, accessible à : http://www.hadopi.fr/sites/default/files/page/pdf/UsurpationIdentite.pdf.*
*[7] Accessibles sur le site de la CNIL à : http://www.cnil.fr/vos-droits/les-courriers-pour-agir/*
*[8] Voir http://www.cnil.fr/vos-droits/plainte-en-ligne/ et http://www.cnil.fr/vos-droits/la-cnil-a-vos-cotes/*
*[9] Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN).*