

N° 86

---

# SÉNAT

SESSION ORDINAIRE DE 2008-2009

---

---

Annexe au procès-verbal de la séance du 6 novembre 2008

## PROPOSITION DE LOI

*relative à la pénalisation de l'usurpation d'identité numérique,*

PRÉSENTÉE

Par Mme Jacqueline PANIS,

Sénatrice

*(Renvoyée à la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale, sous réserve de la constitution éventuelle d'une commission spéciale dans les conditions prévues par le Règlement.)*



## EXPOSÉ DES MOTIFS

Mesdames, Messieurs,

L'identité numérique est au cœur d'une réflexion, menée dans notre pays actuellement, visant à renforcer la confiance numérique. Le 20 octobre 2008, le secrétaire d'État auprès du Premier ministre chargé de la prospective et de l'évaluation a ainsi présenté un plan de développement de l'économie numérique, « France numérique 2012 ».

Il lui « apparaît nécessaire de renforcer la qualité et la sécurisation des titres d'identité, mais également d'offrir de nouveaux services aux citoyens en leur donnant les moyens de prouver leur identité sur Internet et de signer électroniquement ». Il s'agirait de mettre en place la carte nationale d'identité électronique « sur la base d'un standard de signature électronique fortement sécurisé, pour atteindre, à terme, un objectif de 100 % de citoyens titulaires d'une carte nationale d'identité électronique ».

Cela constituera une première réponse à un phénomène qui s'est répandu dans de grandes proportions ces dernières années, l'usurpation d'identité adaptée au support numérique, causant de réels dommages de tous ordres, notamment financiers, à nombre de particuliers, d'entreprises, voire d'administrations.

Si dans le monde réel, nul ne peut s'attribuer une identité qui ne soit pas reconnue par les autorités publiques, dans le monde du virtuel il en va tout autrement.

« L'identité numérique » échappe à toute attribution par une autorité publique, c'est-à-dire que les éléments qui la composent ne relèvent pas de l'identité juridique de la personne.

La manière la plus simple de définir une identité numérique est de considérer les données formelles que sont l'identifiant et le mot de passe.

L'identifiant fera ainsi office d'identité et le mot de passe de certificat d'authentification.

Les identifiants pour une même personne seront multiples, que l'on pourra considérer comme autant d'identités.

Avec l'évolution des réseaux internet dont ceux de convivialité et leur facilité d'accès, la multiplication des services en ligne et des opérations, notamment bancaires ou d'achats en ligne, l'impossibilité de vérifier l'identité réelle des personnes est à l'origine de nouveaux comportements, préjudiciables aux personnes et le plus souvent délictueux, difficiles à prouver.

Une pratique frauduleuse s'est développée consistant à leurrer une victime en lui faisant croire qu'elle s'adresse à un tiers en qui « elle a confiance » afin de récupérer des données personnelles sensibles.

Appelée « Phishing » ou encore « hameçonnage » dans sa traduction francophone, cette technique est de plus en plus perfectionnée et difficile à détecter. Elle peut prendre plusieurs formes dont le « pharming » (technique du hameçonnage qui en plus redirige les utilisateurs d'un site Internet authentique vers un site frauduleux semblable au site original), le « SMiShing » (un SMS, envoyé sur un téléphone mobile confirme un abonnement à l'un des services d'une entreprise, qui sera soi-disant facturé quotidiennement à défaut d'annulation de la commande sur le site Internet de l'entreprise), le « spear-phishing » ou « harponnage » (technique consistant à se faire passer pour un collègue ou l'employeur du destinataire afin de récupérer les identifiants de membres du personnel pour pouvoir accéder au système informatique de l'entreprise).

L'ampleur du phénomène, en hausse chaque année, est telle qu'une enquête faite par un cabinet privé, aux États-Unis, premier pays touché au monde, portant sur une année, entre 2006 et 2007, faisait état de 3,5 millions d'internautes piégés, pour un total de 3,2 milliards de dollars.

En France aussi, de grandes banques, des fournisseurs d'accès ou des sites de ventes et d'échanges ont été atteints par l'hameçonnage.

Ainsi captées, les données personnelles sensibles, telles que numéros de cartes de crédit, mots de passe ou autres identifiants, seront utilisées pour commettre une infraction, le préjudice étant le plus souvent matériel et financier.

Pour l'heure, gouvernements, entreprises, industrie et société civile luttent contre cette cybercriminalité chacun dans leur champ d'action, au plan national comme international.

Peu de pays se sont cependant dotés d'une législation visant spécifiquement l'usurpation d'identité.

Bien plus, parmi les états de l'Union européenne, seul le Royaume-Uni, comporte une disposition spécifique au vol d'identité en ligne. Ainsi la fraude commise en ligne est un délit distinct, depuis le 15 janvier 2007, lourdement puni (10 ans maximum de prison) aux termes du « Fraud Act ».

Dans la plupart des autres pays, elle relève de délits couverts par de nombreuses dispositions légales traitant la fraude, la falsification, l'accès illicite à des données, quand elle ne conduit pas à la commission d'infractions plus graves.

Aux États-Unis, le vol d'identité est un délit en soi, puni d'une durée d'emprisonnement renforcée en 2005 pour les voleurs d'identité numérique ayant commis une infraction.

Reste que de plus en plus de pays semblent ouverts à la proposition d'incriminer pénalement le vol d'identité comme moyen d'améliorer la lutte contre cette délinquance.

En France, l'usurpation d'identité en elle-même n'est pas un délit pénal, excepté s'il y a utilisation de fausse identité dans un acte authentique ou un document administratif destiné à l'autorité publique aux termes de l'articles 433-19 du code pénal, ou si, aux termes de l'article 781 du code pénal, un faux nom a été utilisé pour se faire établir un extrait de casier judiciaire.

L'usurpation d'identité devient un délit pénal, aux termes de l'article 434-23 du code pénal, lorsque le voleur d'identité a opéré « dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci (le tiers volé) des poursuites pénales », faisant ainsi passer le volé pour un délinquant. La peine encourue est de 5 ans d'emprisonnement et de 75 000 euros d'amende.

Le juge sanctionnera également lorsqu'il y aura fraude (escroquerie - article 313-1 du code pénal -, punie de cinq ans d'emprisonnement et de 375 000 euros d'amende) ou diffamation.

Enfin, dans l'arsenal répressif, le juge fait aussi appel aux articles 323-1 et suivants du code pénal relatifs aux atteintes aux systèmes automatisés de données, qui punissent notamment « le fait d'accéder ou de se maintenir, frauduleusement dans tout ou partie d'un système... », « le fait d'introduire frauduleusement des données dans un système de traitement automatisé... ». Les peines peuvent être assez lourdes.

Ainsi les conditions de poursuites et de sanctions de l'usurpation d'identité sont, en France, assez incertaines. Ce sont les conséquences de l'usurpation d'identité qui sont sanctionnées et non l'usurpation d'identité elle-même.

Dans ces conditions, une nouvelle infraction, l'usurpation d'identité numérique, devrait être inscrite dans le code pénal, punie d'une peine de prison d'une année et de 15 000 euros d'amende, s'ajoutant « sans possibilité de confusion, avec celles qui auront été prononcées pour l'infraction à l'occasion de laquelle l'usurpation a été commise ».

Les tentatives seront elles-mêmes punies des mêmes peines.

Tel est l'objet de la présente proposition de loi dont nous vous demandons d'adopter l'article unique qui reprend un dispositif proposé en son temps par un collègue sénateur.

## **PROPOSITION DE LOI**

### **Article unique**

I. – Il est inséré, après l'article 323-7 du code pénal, un article ainsi rédigé:

« Art. 323-8. - Est puni d'un an d'emprisonnement et de 15 000 euros d'amende, le fait d'usurper sur tout réseau informatique de communication l'identité d'un particulier, d'une entreprise ou d'une autorité publique.

« Les peines prononcées se cumulent, sans possibilité de confusion, avec celles qui auront été prononcées pour l'infraction à l'occasion de laquelle l'usurpation a été commise. »

II. – À l'article 323-7 du code pénal, après les références 323-1 à 323-3 insérer la référence 323-8.