Le piratage de profils de réseaux sociaux : infractions à envisager

Les réseaux sociaux[1], dont notamment Facebook, Google+, MySpace, Twitter et Linkedin offrent un espace d'échange rapide et facile entre leurs utilisateurs. Des millions de messages sont quotidiennement postés à des degrés de confidentialité différents sur des messageries internes ou sur des toiles publiques (notamment le fameux mur de Facebook).

Dans la mesure où la création de profils ou comptes d'utilisateur est particulièrement facile sur les réseaux sociaux, il arrive que des personnes ouvrent des profils sous de fausses identités. Il y a d'un côté le recours à des pseudonymes, de l'autre l'utilisation de l'identité d'autrui. C'est surtout cette deuxième hypothèse qui pose problème, en ce qu'elle peut aboutir à une véritable usurpation d'identité (I).

A côté de la création d'un profil en utilisant le nom d'autrui, on peut constater de plus en plus d'accès frauduleux au profil créé par son propriétaire légitime. Ces accès frauduleux peuvent aboutir à une véritable reprise de l'identité numérique d'autrui (II).

Dans la présente note, nous nous limitons à analyser les infractions directement liées aux créations et utilisations frauduleuses de profils de réseaux sociaux. En fonction des actes commis par l'auteur, d'autres infractions peuvent également être constituées. Nous pensons notamment aux calomnies, diffamations, injures et atteintes à la vie privée.

I. La création d'un profil au nom d'autrui

Pour pouvoir s'inscrire sur un réseau social, il faut généralement disposer d'une adresse e-mail valable. Les autres informations peuvent être librement renseignées par l'utilisateur. Ce système d'inscription – avantageux de par sa simplicité – présente l'inconvénient qu'il ne permet qu'une identification incomplète des utilisateurs. La création d'un profil frauduleux est dès lors particulièrement facile, d'autant plus que de nombreux fournisseurs proposent des adresses e-mail gratuites qui peuvent également être ouvertes très facilement.

La création d'un profil au nom d'autrui peut aller d'une simple mauvaise blague à un véritable vol d'identité. Par cette notion, on entend *« l'utilisation de données d'identification personnelles, par exemple un numéro de carte de crédit, pour commettre d'autres infractions »*[2]. Il suffit en effet de s'imaginer un profil créé au nom d'une personne qui n'utilise pas les réseaux sociaux. Au fil du temps, une véritable identité numérique se crée au sujet de cette personne sur les réseaux sociaux, sans que celle-ci ne s'en rende compte. Dans ce cas, le pirate informatique maîtrise l'identité sur les réseaux de cette personne. Il peut non seulement communiquer au nom de cette personne, mais également profiter de données confidentielles destinées à celle-ci.

[1] Les services de réseautage social peuvent être définis comme des plates-formes de communication en ligne permettant à des personnes de créer des réseaux d'utilisateurs partageant des intérêts communs ; Avis 5/2009 du groupe de travail « article 29 » sur la protection des données sur les réseaux sociaux en ligne, adopté le 12 juin 2009

[2] Communication de la Commission au Parlement européen, au Conseil et au Comité des Régions - Vers une politique générale en matière de lutte contre la cybercriminalité, COM/2007/0267 final, page 9

En droit pénal luxembourgeois, l'utilisation du nom appartenant à autrui est réprimée par l'article 231 du Code pénal[3]. Pour que l'infraction de port public de faux nom soit donnée, il faut que l'auteur prenne publiquement un nom qui ne lui appartient pas.

Le faux nom est un autre nom que celui qui figure dans l'acte de naissance. La loi punit tout changement, toute altération, toute modification du nom patronymique qui est légalement celui de l'auteur. Le port public d'un faux prénom, pris comme tel, n'est toutefois pas réprimé par l'article 231 du Code pénal[4].

La publicité exigée par l'article 231 du Code pénal existe si la prise de faux nom se réalise verbalement ou se manifeste dans un écrit ou un imprimé. *« Le législateur se contente (…) à cet égard d'une publicité relative, le port du faux nom devant se faire ostensiblement »*[5].

La jurisprudence a notamment retenu que l'utilisation du nom indiqué sur une carte de crédit volée pour effectuer des achats sur Internet tombe sous l'infraction prévue par l'article 231 du Code pénal[6]. Il en va de même pour l'inscription sous le nom d'autrui pour ouvrir des boîtes de courrier électronique[7].

A l'heure actuelle, les paramètres de confidentialité des réseaux sociaux sont configurés pour permettre une communication très large des noms attribués aux profils. Autrement dit, le nom choisi pour un profil constitue l'élément clé pour rechercher (et retrouver) celui-ci. En pratique, il y a lieu de constater que les personnes qui créent des profils au nom d'autrui en font un usage très étendu. Ils se créent notamment des listes d'amis sur Facebook et entrent ainsi en contact avec les connaissances de la personne dont ils ont pris l'identité.

Il faut en conclure que l'utilisation du nom d'autrui se fait de façon ostensible sur les réseaux sociaux, de sorte que la condition de la publicité exigée par l'article 231 du Code pénal est donnée[8].

Pour ce qui est de l'élément intentionnel, la jurisprudence retient que *« le port incriminé est punissable par le seul fait que son auteur a pris un faux nom avec l'intention de faire croire ou de laisser croire que c'était réellement le sien, quand bien même son acte serait dépourvu de toute autre intention de tromper ou de nuire »*[9]. Le mobile est indifférent[10].

II. Le piratage du profil d'autrui

Un individu peut également être amené à vouloir accéder au profil créé par son propriétaire légitime. Cette manœuvre est plus complexe, en ce qu'elle exige la connaissance du mot de passe choisi par celui-ci.

---

[3] Article 231 du Code pénal : *« Quiconque aura publiquement pris un nom qui ne lui appartient pas sera puni d'un emprisonnement de huit jours à trois mois, et d'une amende de 251 euros à 3.000 euros, ou d'une de ces peines seulement »*.

[4] CA 27 février 2007, n° 125/07 V

[5] CA 16 juin 2009, n° 312/09 V ; voir également TA Lux. 30 septembre 2004, n° 2643/2004, confirmé par CA 1er février 2005, n° 57/05 V

[6] Voir notamment : TA Lux. 5 mars 2009, n° 776/2009, LJUS 99865668 ; TA Lux. 21 juin 2012, n° 2234/2012

[7] TA Lux. 5 avril 2011, n° 1238/2011

[8] Voir notamment : TA 5 avril 2011, n° 1238/2011

[9] TA Lux. 30 septembre 2004, n° 2643/2004, confirmé par CA 1er février 2005, n° 57/05 V ; voir également TA 20 octobre 2005, n° 2837/2005, BIJ 06/2006, p. 172

[10] CA 4 juin 1956, Pas. 16, p. 488

L'accès frauduleux peut être utilisé pour consulter des informations normalement réservées au propriétaire légitime du profil (A), mais également pour créer, modifier ou effacer des informations de ce profil (B).

A. L'accès ou le maintien frauduleux à un profil

L'article 509-1, alinéa 1er du Code pénal réprime *« quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement ou de transmission automatisé de données sera puni d'un emprisonnement de deux mois à deux ans et d'une amende de 500 euros à 25.000 euros ou de l'une de ces deux peines »*.

Par des systèmes de traitement ou de transmission automatisé de données, il y a lieu d'entendre un *« ensemble composé d'une ou de plusieurs unités de traitement automatisé de mémoire, de logiciel, de données, cet ensemble étant protégé ou non par un dispositif de sécurité »*[11]. Autrement dit, l'article 509-1, alinéa 1er du Code pénal vise les systèmes informatiques. Les serveurs qui stockent des pages Internet (donc également des réseaux sociaux) tombent naturellement sous cette qualification[12].

En visant tout accès ou maintien frauduleux à des systèmes informatiques, l'article 509-1, alinéa 1er du Code pénal a un champ d'application très large. L'accès et le maintien frauduleux sont sanctionnés indépendamment du fait qu'ils ne représentent que la première phase d'une fraude plus grave ou qu'ils ne causent aucun préjudice[13]. L'infraction n'exige ni intention de lucre, ni intention de nuire[14]. L'accès doit toutefois se faire de façon volontaire[15].

Le caractère frauduleux d'un accès peut être déduit des moyens employés par l'auteur :

- un individu qui tente de deviner le mot de passe protégeant l'accès à un profil est bien conscient que cet accès est limité à son propriétaire légitime,

- il en va de même de l'emploi de techniques permettant de déceler ce mot de passe ou de contourner le système de sécurité mis en place.

  On peut notamment citer l'utilisation d'un mot de passe obtenu par hameçonnage (« phishing ») [16].

[11] M. QUEMENER, Y. CHARPENEL, Cybercriminalité – Droit pénal appliqué, Droit pénal appliqué, Economica, éd. 2010, pages 71 et 255 ; voir également Rép. pén. Dalloz, éd. mai 2009, v° Cybercriminalité, page 4, n° 6 et suivants

[12] Voir notamment TA Lux. 24 avril 2008, n° 1347/2008 ; TA Lux. 23 novembre 2009, n° 3351/2009, confirmé sur ce point par CA 14 juin 2010, n° 261/10 X, LJUS 99865656

[13] Travaux parlementaires 3493, avis du Conseil d'Etat, page 14 ; voir également TA Lux. 6 février 2001, n° 394/2001, LJUS 99820516

[14] TA Lux. 15 janvier 2009, n° 116/2009, LJUS 99864736, BIJ 04/2009, page 83

[15] Voir notamment TA Lux. 15 janvier 2009, n° 116/2009, LJUS 99864736, BIJ 04/2009, page 83

[16] Le « phishing » ou « hameçonnage » désigne *« la pratique frauduleuse qui consiste à tenter d'obtenir des informations sensibles, telles que des mots de passe ou des coordonnées de cartes de crédit, en se faisant passer pour une personne de confiance dans le cadre d'une communication électronique »* (Communication de la Commission au Parlement européen, au Conseil et au Comité des Régions - Vers une politique générale en matière de lutte contre la cybercriminalité - COM/2007/0267 final, page 3) ; pour une application pratique voir notamment : TA Lux. 23 novembre 2009, n° 3351/2009, confirmé sur ce point par CA 14 juin 2010, n° 261/10 X, LJUS 99865656

Un autre type d'accès frauduleux consiste à utiliser des données d'accès obtenues légitimement, mais de les utiliser à des fins autres que celles autorisées.

On peut notamment s'imaginer le titulaire d'un profil qui donne ses données d'accès à un ami pour effectuer un acte précis (p.ex. vérifier la messagerie interne liée au profil). L'accès au profil est alors uniquement légitime pour cet acte précis, mais devient frauduleux pour d'autres actes.

Il est encore fréquent de voir des accès frauduleux à des profils (généralement de Facebook) par un ex-conjoint, après la séparation du couple. Des données d'identification, obtenues grâce à la confiance ayant régné au sein du couple, sont alors utilisées pour surveiller ou pour nuire à l'ex-conjoint[17]. Ces accès tombent sous l'infraction de l'article 509, alinéa 1er du Code pénal.

B. La création, modification ou suppression de données du profil

L'article 509-3 du Code pénal dispose que *« quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement ou de transmission automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1.250 euros à 12.500 euros ou de l'une de ces deux peines »*.

L'article 509-3 du Code pénal vise à protéger l'intégrité des données contenues sur un système informatique. Il vise les atteintes intentionnelles aux données.

Le texte permet de réprimer la création, modification ou suppression de données sur le profil d'autrui. L'infraction est notamment donnée si ces actes se font suite à un accès frauduleux au profil au sens de l'article 509-1, alinéa 1er du Code pénal (hypothèse visée au point A. ci-dessus).

Elle l'est également si l'auteur publie des messages sur le profil qu'il a créé lui-même en utilisant l'identité d'autrui (voir l'hypothèse visée au point. I ci-dessus)[18]. Dans ce cas, l'auteur insère en effet des données dans le système informatique du réseau social au détriment des droits d'autrui.

Par la création ou l'insertion de données, on entend notamment l'envoi de messages[19], d'images, de vidéos ou d'autres contenus. On peut admettre que l'article 509-3 du Code pénal réprime toute utilisation frauduleuse d'un profil qui engendre la création de données (à notre avis, il vise également l'ajout d'amis sur un compte Facebook).

Nous tenons encore à signaler que les créations, modifications et suppressions accidentelles de données, qui résultent d'un accès frauduleux au système informatique sont également réprimées (article 509-1, alinéa 2 du Code pénal).

Max BRAUN

Version du 30/10/2012

[17] TA Lux. 3 mars 2011, n° 728/2011
[18] TA 5 avril 2011, n° 1238/2011
[19] L'envoi d'E-Mail à partir de l'adresse d'autrui a notamment été réprimé : voir : TA Lux. 3 mars 2011, n° 728/2011