# L’usurpation d’identité sur internet

**Actualité législative** publié le **16/10/2019**, vu **4269 fois**, Auteur : Droit de la sécurité informatique

**Il s’agit là d’un phénomène qui est en pleine expansion. De fait, les modes d’usurpation d’identité sur internet sont nombreux. Quelles solutions juridiques et techniques de lutte contre cette infraction peuvent être envisagées ?**

INTRODUCTION

Depuis la naissance de l’écriture, les faux documents existent, mais c’est véritablement au XX$^{e}$ siècle, avec le progrès de l’imprimerie « moderne » et le développement de l’Administration et des services publics, que la fraude documentaire a gagné en importance.

C’est après la Seconde Guerre mondiale que de nombreux Gouvernements ont pris conscience que les risques de fraude sur l’état civil devaient être envisagés à l’échelon international. Ils ont alors décidé de définir un cadre permettant une normalisation des pratiques et des contrôles. Cela a pu être réalisé par, notamment, la mise en place de la Commission internationale de l’état civil (CIEC), une organisation intergouvernementale fondée en 1949, dont le but était de promouvoir la coopération internationale en matière d’état civil. Cette commission a contribué, par ses recommandations, à harmoniser, mais aussi à actualiser, les procédures de contrôle et les législations relatives aux documents d’identité. Ces mesures ont été efficaces tant que les déplacements internationaux sont restés limités, et jusqu’à ce que les techniques d’impression numérique fassent leur apparition massive. La situation a alors beaucoup changé, et l’augmentation des flux migratoires a contribué à renouveler la fraude documentaire sur les titres de voyage. En 2003, Interpol estimait à plus de 35 millions le nombre de faux documents d’identité circulant dans le monde.

Avec l’essor du commerce électronique, la fraude numérique a réalisé une poussée notable dans l’environnement quotidien. D’abord en raison de la croissance de la relation à distance. Internet et les réseaux numériques permettent à un ensemble de services marchands de se libérer des contraintes et des coûts d’une implantation physique. Il ne s’agit pas seulement du transfert du flux traité par des employés vers des automates, mais de la transformation d’une grande partie des magasins ou agences en simples points d’appui, de conseils et de logistique à une relation qui devient peu à peu une relation à distance. Les agences de voyages ont quasiment disparu de nos centres commerciaux, les banques adoptent des modèles directs, en ligne, sur un ordinateur ou un téléphone portable, les supermarchés livrent les courses à domicile sur simple commande *via* internet.

Ensuite vient l'importance que prennent les données personnelles, qui tendent à devenir la forme presque exclusive d'échange et de reconnaissance. En France, c'est le début de la Commission nationale de l'informatique et des libertés. Cette haute autorité administrative a la lourde tâche de superviser la protection des données. Les entreprises doivent respecter des obligations déclaratives concernant les fichiers et leur traitement. Par exemple, le responsable du fichier ou du traitement de données personnelles a le devoir d'informer les personnes concernées des objectifs de ce traitement, de l'identité des destinataires de ces informations et des droits d'accès et de rectification dont disposent les titulaires des données.

Enfin, la fraude numérique connaît un essor important avec l'émergence de l'internet et des usages marchands sur la Toile. Les informations d'accès (code, mot de passe, identifiant), les informations de navigation (courriel, adresse IP, URL, *cookie*), les données nominatives et les renseignements postés sur les réseaux sociaux deviennent des informations susceptibles de désigner des cibles potentielles et de rapporter de l'argent. Elles attirent une nouvelle catégorie de fraudeurs : les cybercriminels.

Dans son dernier rapport sur les statistiques de vol d'identité, le groupe de recherche Gartner affirme que près de 60 millions d'Américains ont déclaré avoir reçu un courriel d'hameçonnage, que 1,7 million de personnes ont été victimes de vol d'identité, et que les banques et les sociétés de cartes de crédit estiment les pertes à 1,2 milliard de dollars.

Dans ce contexte, il convient d'examiner l'usurpation d'identité en tant que phénomène en développement (I), et les différents modes d'usurpation d'identité sur internet (II), avant d'envisager les solutions juridiques et techniques de lutte contre cette infraction (III).

## I. - L'USURPATION D'IDENTITÉ : UN PHÉNOMÈNE EN DÉVELOPPEMENT

Le vol d'identité est considéré par beaucoup de pays comme un des risques majeurs auxquels s'exposent les consommateurs et utilisateurs dans l'environnement numérique actuel. Les services de paiement électronique et de banque électronique souffrent considérablement de cette méfiance. Au Royaume-Uni, par exemple, on estime que 3,4 millions de personnes, en mesure d'utiliser internet, ne veulent pas faire d'achats en ligne par manque de confiance ou par crainte pour leur sécurité personnelle (UK OFT, 2007, p. 6). De nombreux pays européens ont constaté ce problème et pris des mesures destinées à contribuer à une protection adéquate des consommateurs et utilisateurs contre le vol d'identité. Ces mesures comprennent diverses actions et dispositions telles que des campagnes de sensibilisation des consommateurs et utilisateurs, la mise en place de cadres légaux nouveaux ou adaptés, des partenariats public-privé et des initiatives de l'industrie visant à mettre en place des mesures de prévention techniques et des réponses à cette menace.

Dans cette première partie, notre étude s'attache à l'utilisation des données volées par les fraudeurs (A) et aux victimes concernées (B).

### A. - L'utilisation des données volées par les fraudeurs

Une fois que les voleurs d'identité ont obtenu les informations personnelles de leurs victimes, ils les exploitent de diverses façons. Dans l'édition 2012 de son *Identity Theft Survey Report*, la *Federal Trade Commission* (FTC) des États-Unis classe les actes de vol d'identité en trois grandes catégories : i) ouverture de nouveaux comptes (cartes de crédit, comptes bancaires ou emprunts) et autres types de fraude (par exemple, bénéficier de soins médicaux) ; ii) utilisation illicite de comptes sans carte de crédit ; ou iii) utilisation illicite de cartes de crédit seules. Les formes d'utilisation illicite des données volées sont les suivantes (FTC, États-Unis, 2012, p. 21) :

cartes de crédit (20 %) ;

autres (23 %) ;

services téléphoniques (15 %) ;

comptes chèques ou comptes d'épargne (6,5 %) ;

prêts bancaires (4 %) ;

assurances médicales (2,2 %) ;

courrier électronique et autres comptes internet (2,1 %).

Nous pouvons remarquer que la fraude à la carte de crédit est la forme la plus répandue d'utilisation illicite de comptes existants. Cette forme de vol d'identité est réalisée lorsque l'usurpateur obtient la carte de crédit elle-même, les numéros associés au compte, ou l'information tirée de la bande magnétique au dos de la carte. Les cartes de crédit pouvant être utilisées à distance, par exemple par le biais de l'internet, les voleurs d'identité ont souvent la possibilité de commettre des fraudes sans être en possession matérielle de la carte de crédit de la victime. Les voleurs d'identité se livrent également à un autre type de fraude : ils utilisent les informations personnelles des victimes pour ouvrir à leur insu un nouveau compte, dépenser de fortes sommes et disparaître. Souvent, les victimes ne découvrent le vol d'identité et l'escroquerie qu'au moment où un agent de recouvrement les contacte, ou lorsqu'elles se voient refuser un emploi, un prêt, une voiture ou une prestation à cause de renseignements négatifs sur leur solvabilité. Dans certains cas, les voleurs d'identité déposent des chèques volés ou contrefaits, ou des chèques sans provision et retirent des espèces, causant des dommages financiers immédiats généralement de grande ampleur. Bien que cette forme de vol d'identité soit moins fréquente, elle peut entraîner, pour la victime, davantage de dommages financiers, il y a moins de chances qu'on la découvre rapidement et la récupération est plus longue pour les victimes. En fait, d'après l'édition 2006 du *ID Theft Survey Report* de la FTC, 24 % des victimes d'ouverture frauduleuse de nouveaux comptes ou d'autres types de fraude similaires ne se sont rendu compte de l'utilisation illicite de leurs informations personnelles qu'après un délai de six mois, contre 3 % des victimes d'utilisation frauduleuse de cartes de crédit seules et de comptes sans carte de crédit existante. Dans cette seconde catégorie de victimes, le délai moyen de constatation de la fraude variait d'une semaine à un mois, contre un délai moyen de un à deux mois chez les victimes d'ouverture frauduleuse de nouveaux comptes ou autres types de fraude.

Certains sites internet spécialisés dans la fraude à la carte bancaire organisent un trafic de données de cartes de crédit volées à l'échelle mondiale.

Les voleurs d'identité peuvent également utiliser les informations personnelles de leurs victimes pour faire du « courtage de données ». Certains sites internet spécialisés dans la fraude à la carte bancaire organisent un trafic de données de cartes de crédit volées à l'échelle mondiale. Les services secrets des États-Unis estiment que les deux plus importants sites de ce type possèdent ensemble près de 20 000 « comptes ».

### B. - Les victimes concernées

D'après des recherches conduites par le Forum sur la prévention de la fraude, l'impact du vol d'identité au Canada s'étend à des victimes de tout âge, et de tout niveau de revenus ou d'éducation (GTBFTFMM, 2004, p. 4). En mai 2006, plus de 20 000 plaintes en matière d'hameçonnage ont été déposées au Canada par des particuliers, soit une augmentation de plus de 34 % par rapport à l'année précédente.

Aux États-Unis, le rapport de la *Consumer Sentinel* de la FTC de 2012, intitulé *Consumer Fraud and Identity Theft Complaint Data*, confirme ces constatations. Parmi les personnes qui ont indiqué leur âge dans leur plainte relative à un vol d'identité, les jeunes de 20 à 29 ans représentent la catégorie la plus tou chée par le vol d'identité (23 %) en 2011, suivie par la catégorie des 30 à 39 ans (21 %), puis des 40 à 49 ans (18 %), 50 à 59 ans (15 %), 60 à 69 ans (9 %), moins de 19 ans (8 %) et finalement celle des plus de 70 ans (6 %).

Ces données, reposant sur les plaintes de victimes, ne concernent que les cas signalés et elles ne rendent pas compte du fait que, en réalité, le concept de victime est plus complexe. Par exemple, les données reposant sur les plaintes n'intègrent pas toujours la notion que les entreprises et autres institutions peuvent également être victimes de vol d'identité. Dans certains cas, les voleurs d'identité peuvent faire une utilisation illicite du compte bancaire d'un client ou bien utiliser le nom d'une banque dans une attaque d'hameçonnage pour voler l'un de ses clients, auquel cas la banque sera également victime du vol d'identité dans la mesure où elle devra rembourser à son client la somme qui aura été volée à ce dernier.

## II. - LES DIFFÉRENTS MODES D'USURPATION D'IDENTITÉ SUR INTERNET

Se faire voler son identité, sur la Toile ou dans la vraie vie, une seule fois ou sur le long terme, est un danger dont les Français sont de plus en plus conscients : 9 Français sur 10 pensent qu'il est compliqué de faire valoir ses droits lorsque l'on est victime de ce type d'infraction. Et ce malgré les récentes avancées de la loi « Loppsi » (loi d'orientation et de programmation pour la performance de la sécurité intérieure) de mars 2011, qui reconnaît l'usurpation d'identité comme infraction principale et prévoit de la punir d'une peine de un an de prison et 15 000 € d'amende. Dans la vie courante, la transmission de données personnelles est un passage obligé pour ouvrir un compte, louer un appartement, souscrire un abonnement, etc. 78 % des Français déclarent d'ailleurs avoir fourni au moins une copie papier de leurs données personnelles au cours des 12 derniers mois. 55 % ont transmis ce type d'information en ligne, une pratique moins courante. La protection des données sur la Toile est d'ailleurs considérée comme moins sûre pour 77 % des sondés.

En outre, une majorité de Français (62 %) aurait désormais le réflexe de détruire les documents mentionnant des informations personnelles et confidentielles dont ils n'ont plus besoin. Un chiffre en progression. À titre de comparaison, seulement 36 % des sondés déclaraient détruire leurs factures avant de les jeter.

Aujourd'hui, ceux qui veulent effacer leurs traces choisissent en majorité de brûler leurs papiers (51 %). Viennent ensuite les « déchiqueteurs » qui découpent les documents en très petits morceaux avant de les répandre dans une poubelle (33 %) puis les « méthodiques », adeptes du destructeur de documents (15 %). Les relevés bancaires sont les pièces jugées les plus « sensibles » par 85 % des Français qui les surveillent avec attention, avant les papiers d'identité

(79 %), les bulletins de salaire (42 %), les actes de naissance (33 %) ou les factures d'électricité et de gaz (25 %).

Le vol d'identité est une activité illicite dont l'histoire remonte bien avant l'internet. Typiquement, le vol d'identité classique était - et est encore - perpétré au moyen de techniques comme la fouille de poubelles, le vol de cartes de paiement, le faux-semblant, l'espionnage « par-dessus l'épaule », l'écrémage, ou le vol d'ordinateur. Ces dernières années, ces agissements ont été modernisés du fait du développement rapide de l'internet, qui permet aux voleurs d'identité d'installer des logiciels malveillants sur les ordinateurs et d'utiliser la méthode de l'« hameçonnage », laquelle peut être elle-même perpétrée au moyen de logiciels malveillants et du spam.

### A. - Les logiciels malveillants

Le terme général de « logiciel malveillant » désigne un code ou logiciel introduit dans un système d'information afin de causer des dommages à ce système ou à d'autres systèmes, ou destiné à une utilisation autre que celle voulue par leurs utilisateurs légitimes. Avec l'essor de programmes malveillants furtifs comme ceux qui enregistrent les frappes des touches de clavier, ou comme les virus ou « chevaux de Troie » qui se cachent dans un système informatique et capturent secrètement des informations, le logiciel malveillant est devenu un outil technique permettant à lui seul de voler les informations personnelles des victimes.

### B. - Le phishing

Le terme anglais « *phishing* » a été inventé en 1996 par des pirates informatiques américains qui détournaient les comptes d'America Online (AOL) en soutirant les mots de passe des utilisateurs. L'utilisation du « ph » dans cette terminologie remonte aux années 1970, avec les premiers pirates qui se livraient au « *phreaking* », piratage des systèmes téléphoniques.

L'hameçonnage, ou le « *phishing* », est aujourd'hui décrit, en général, comme une méthode de tromperie que les voleurs utilisent pour « pêcher » les informations d'identité personnelles d'utilisateurs de l'internet peu méfiants, au moyen de messages électroniques et de sites internet miroirs revêtant l'apparence de messages émanant d'entreprises légitimes telles que des établissements financiers ou des administrations publiques.

Un autre type de message électronique d'hameçonnage bien connu est celui de « l'escroquerie 419 » (également appelée « escroquerie nigériane ») par laquelle les criminels tentent de perpétrer une escroquerie sur avance de frais en demandant à leurs cibles un paiement initial ou un transfert d'argent. Ces escrocs offrent habituellement à leurs victimes potentielles de partager avec elles une grosse somme d'argent qu'ils veulent transférer hors de leur pays. Ils demandent alors aux victimes de payer les frais, redevances ou taxes pour aider à débloquer ou transférer les fonds. Victime de son propre succès, cette escroquerie est aujourd'hui bien connue des utilisateurs de l'internet et se raréfie.

L'*Anti-Phishing Working Group*, « APWG », association de l'industrie ayant pour but d'éliminer le vol d'identité résultant de l'hameçonnage, collecte et enregistre les exemples de messages électroniques ou de faux sites internet d'hameçonnage. Ce consortium, qui sert de forum où l'industrie, les entreprises et les organismes chargés de faire respecter la loi discutent de l'impact de l'hameçonnage, entretient un site internet public permettant à ses membres d'échanger des informations et des bonnes pratiques pour éliminer ce problème.

### C. - Le *vishing*

La téléphonie sur Protocole Internet (*Voice over Internet Protocol* ou VoIP) offre également un nouveau moyen pour dérober les informations personnelles des individus par le biais des téléphones. Dans ce cas, le criminel envoie un message électronique maquillé classique, présenté

comme provenant d'une entreprise ou institution légitime et invitant le destinataire à former un numéro de téléphone. Les victimes se sentent habituellement plus en sécurité dans ce cas de figure, étant donné qu'il ne leur est pas demandé de se connecter à un site internet où elles fourniraient leurs informations personnelles. Quand elles appellent, un répondeur automatique leur demande de saisir des informations personnelles telles qu'un numéro de compte, un mot de passe ou toute autre information à des fins prétendues de « vérification de sécurité ». Dans certains cas, le criminel ne recourt même pas à un message électronique et appelle à froid les consommateurs pour leur soutirer des informations financières.

Les techniques décrites ci-dessus reposant sur les logiciels malveillants évoluent et se transforment rapidement en de nouveaux genres de menaces. Elles peuvent même être combinées, comme le remarquait en 2005 l'*Identity Theft Technology Council* (« ITTC ») des États-Unis dans son rapport intitulé *Online Identity Theft*(ITTC, 2005, p. 7). L'ITTC déclare que « *les distinctions entre les types d'attaques* [d'hameçonnage] *sont floues, étant donné que beaucoup d'attaques sont de nature hybride, employant plusieurs technologies* ». Ce rapport illustre cette assertion en prenant l'exemple d'un message électronique d'hameçonnage fallacieux qui peut diriger un utilisateur vers un site qui a été corrompu par injection de contenu et qui installe alors un logiciel malveillant infectant le fichier d'hôtes de l'utilisateur. Il en résulte que les tentatives ultérieures de connexion à des sites internet légitimes sont redirigées vers des sites d'hameçonnage où les informations confidentielles sont détournées par la technique de « l'homme du milieu ». Cette attaque hybride combine le *pharming* et l'attaque de « l'homme du milieu ».

D. - Le détournement des cartes de paiement

En France, depuis 2001, la fraude sur les cartes de paiement est devenue un sujet d'« intérêt public ». Contrairement à d'autre pays, où c'est d'abord le secteur privé bancaire et financier qui publie les statistiques de fraude sur les moyens de paiement, la France s'est dotée d'une structure créée par la loi et rattachée à la Banque de France. Il s'agit de l'Observatoire de la sécurité des cartes de paiement (OSCP) qui, comme son nom l'indique et du moins jusqu'à ce jour, traite presque exclusivement des cartes de paiement. Cet observatoire publie un rapport annuel, remis au ministre de l'Économie et des Finances et transmis au Parlement. Véritable « baromètre » officiel du niveau de fraude sur les cartes de paiement, il permet de suivre les tendances progressives et dégressives de la fraude d'une année sur l'autre, selon une analyse assez détaillée.

Pour comprendre cette mutation, il faut revenir un instant sur la matrice de classification des fraudes sur la carte. La première catégorie, au sein de cette classification, regroupe les fraudes utilisant des supports physiques authentiques. Il peut s'agir soit de cartes perdues ou volées (c'est la fraude la plus traditionnelle), soit de cartes dites « *non parvenues* », car elles sont dérobées avant que le titulaire n'entre en leur possession. La deuxième catégorie rassemble des motifs ou origines liés à l'exploitation frauduleuse des données. Cela peut se traduire par l'utilisation de supports contrefaits avec des numéros de cartes usurpés, par l'usurpation du numéro de carte sans utilisation d'un support, ou encore par l'ouverture de compte sous une fausse identité.

Contrairement à d'autre pays, où c'est d'abord le secteur privé bancaire et financier qui publie les statistiques de fraude sur les moyens de paiement, la France s'est dotée d'une structure créée par la loi et rattachée à la Banque de France.

La logique des cartes contrefaites combine la fraude sur les données avec la contrefaçon d'un support physique. C'est donc un système mixte. Mais, pour le reste, la fraude sur les numéros de cartes est exclusivement une fraude sur les seules données.

La France n'est évidemment pas la seule à connaître cette mutation importante de la fraude, également constatée, par exemple, au Royaume-Uni où les cartes perdues et volées, qui représentaient, il y a dix ans, la majorité des utilisations frauduleuses, n'en représentent plus

aujourd'hui que moins de un dixième. De l'autre côté de la Manche, la fraude sur les cartes a donc aussi totalement changé de visage. Et les paiements par carte des autres pays suivent cette tendance générale.

Malheureusement pour les systèmes bancaires de paiement, les cartes ne constituent pas le seul problème. Les fraudes sur les données menacent aussi un autre pilier au cœur de l'organisation des paiements courants : le système des virements et des prélèvements bancaires.

### E. - Le détournement des coordonnées bancaires

Une fois les coordonnées du compte bancaire obtenues par le *phishing*, les fraudeurs peuvent accéder à un certain nombre de biens et de services. Ils peuvent donc espérer un profit illicite dans les conditions suivantes.

Première possibilité : ils réussissent à prélever un montant indolore pour chaque victime mais qui, multiplié par un grand nombre de comptes, peut rapporter gros. Ce type de fraude de « microprélèvements » est fondé sur les montants faibles comme des arrondis ou des surfacturations de quelques euros. C'est selon un scénario similaire que le compte bancaire du président de la République s'était vu détourné en 2008. Une infortune pour les fraudeurs : s'ils n'avaient pas eu ce client célèbre dans leur liste de victimes, ils n'auraient sans doute jamais été inquiétés ! En France où, il y a encore quelques années, le nombre d'émetteurs autorisés était limité, et où la dématérialisation de l'autorisation de prélèvement était encore un processus relativement long et difficile pour les entreprises, ce schéma de fraude était le plus utilisé, car il permettait de s'affranchir de validations éventuellement plus poussées quant à l'émetteur du prélèvement. Concrètement, cela signifie qu'il était plus facile pour un fraudeur de trouver un complice dans une grande entreprise connue, dont la légitimité pour faire des prélèvements ne serait pas questionnée, que dans une petite entreprise où les demandes de prélèvement devaient souvent s'accompagner de justificatifs des autorisations client.

De grands opérateurs de courrier, de télécommunications ou d'énergie, ainsi que leurs sous-traitants, ont ainsi connu les affres de la lutte contre l'infiltration de mafias de fraudeurs plus ou moins organisées, avec leurs réseaux parallèles de complices passifs, complaisants ou volontaires.

Deuxième possibilité : pour des montants beaucoup plus importants, réussir à faire sortir l'argent du compte de la victime et le faire circuler, avant que celui-ci ne puisse être réclamé par la victime. Cette fraude est donc essentiellement fondée sur une gestion astucieuse des détails d'encaissement, et des délais de réaction comme le délai du rejet du prélèvement, le délai de la contestation émise par la victime, ou le délai de preuve de la fraude. Une des astuces souvent utilisées est de prétendre être le titulaire du compte (fausse identité, faux RIB) et de demander un virement urgent. Cela fonctionne souvent par fax et dans des situations (jours fériés, etc.) où le responsable du compte ou l'agent normal du client ne sont pas disponibles. Les fraudeurs profitent aussi du fait qu'il n'existe jusqu'à présent pas de correspondance ou de clé de contrôle entre le numéro du RIB et le titulaire du compte. Pour les fraudeurs, le challenge principal consiste en fait à faire sortir l'argent du système bancaire national avant que celui-ci ne puisse être bloqué. La solution peut être une personne (intermédiaire) ou une frontière (pays). Avec la dématérialisation et la globalisation des échanges bancaires, ce type de fraude constitue un danger de plus en plus redoutable.

## III. - LUTTE CONTRE L'USURPATION D'IDENTITÉ

Aujourd'hui, de nombreux acteurs parmi lesquels les Gouvernements, les entreprises, l'industrie et la société civile, tant aux niveaux national qu'international, combattent la propagation des attaques électroniques. Divers outils d'éducation ont été déployés pour alerter les internautes au sujet du vol d'identité. Dans certains pays, différents organismes ont lancé des actions nationales

coordonnées pour enquêter et engager des poursuites contre cette infraction. Toutes ces actions illustrent la lutte active des Gouvernements et du secteur privé contre le vol d'identité et pour l'élaboration de pratiques modèles dans l'industrie, l'éducation des consommateurs ainsi que des initiatives répressives ciblées. Il convient ainsi d'étudier dans cette partie les ripostes juridiques nationales et internationales en matière de lutte contre l'usurpation d'identité (A) ainsi que la spécialisation des filières de police et de gendarmerie (B).

### A. - Les ripostes juridiques nationales et internationales en matière de lutte contre l'usurpation d'identité

Du fait du nombre croissant des délits reconnus et des outils techniques destinés à automatiser les infractions en ligne (*systèmes anonymes de partage de fichiers, logiciels de création de virus informatiques, etc.*), la lutte contre la cybercriminalité est devenue une activité essentielle des services de répression dans le monde entier. Dans les pays développés comme dans les pays en développement, cette lutte est un véritable défià relever. Le développement des TIC est tellement rapide, tout particulièrement dans les pays en développement, qu'il est aujourd'hui essentiel d'élaborer et de mettre en œuvre, dans le cadre des programmes de cybersecurité nationaux, une stratégie anticybercriminalité efficace. Ainsi, notre étude dans cette partie s'attache aux ripostes juridiques nationales (1º/), puis aux ripostes juridiques internationales (2º/).

#### Les ripostes juridiques nationales

##### a) France

En France, la création du délit d'usurpation d'identité numérique marque une avancée importante dans la prise en compte par le droit pénal de la spécificité des nouvelles technologies. Prévue par l'article 2 de la loi d'orientation et de programmation pour la performance de la sécurité intérieure, cette nouvelle incrimination comble un vide juridique au moment où le web participatif est en constante progression.

Il ne s'agit pourtant pas d'une idée totalement nouvelle puisqu'elle avait déjà été proposée en 2006 par le sénateur Michel Dreyfus-Schmidt qui regrettait le vide juridique en la matière. À l'époque, le Gouvernement n'avait pas retenu cette proposition, estimant que le droit pénal était complet. Plusieurs parlementaires estimaient en effet que le délit d'escroquerie, en raison de sa formulation neutre (voir C. pén., art. 313-1), permettait de répondre efficacement à l'usurpation d'identité sur internet. Il faut aussi noter que le Code pénal contient un article 434-23 selon lequel : « *Le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales, est puni de cinq ans d'emprisonnement et de 75 000 € d'amende.* » Par une interprétation extensive de cette disposition, la chambre criminelle de la Cour de cassation a considéré, le 20 janvier 2009, que le fait d'utiliser l'adresse électronique d'un tiers, lorsqu'il s'est ensuivi un risque de poursuites pénales pour cette personne, constitue un délit d'usurpation d'identité. Néanmoins, toutes les situations n'étaient pas prises en compte par la loi, notamment celles qui n'avaient pas de conséquences juridiques ou économiques. De même, certains comportements comme le « *phishing* » ou « hameçonnage » ne pouvaient pas être appréhendés par le droit pénal dans la mesure où l'usurpation d'identité en elle-même n'était pas sanctionnée.

L'idée d'un nouvel article incriminant spécifiquement l'usurpation d'identité sur internet a donc fait son chemin jusqu'au dépôt d'un projet de loi le 29 mai 2009. La loi d'orientation et de programmation pour la performance de la sécurité intérieure a réintroduit le concept d'usurpation d'identité numérique. Dans cette optique, l'article 226-4-1 du Code pénal dispose que : « *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.* »

L'élément matériel constitutif du délit est réalisé à partir d'un réseau de communication électronique, ce qui vise notamment l'envoi de courriers électroniques mais aussi la publication d'un message sur un blog ou un réseau social. Il semble que le web 2.0 soit particulièrement visé par ce texte dans la mesure où la mise en ligne d'une photo ou d'un texte *via* un outil participatif peut facilement nuire à la tranquillité ou à la réputation d'un tiers. Le député Éric Ciotti a fait le constat suivant : « *L'usurpation d'identité sur internet doit également être plus sévèrement sanctionnée. Jusqu'à présent, elle ne pouvait être poursuivie que s'il en avait résulté un préjudice financier. Or, cette usurpation peut avoir de très graves conséquences non financières, par exemple en matière de diffamation. La multiplication des forums de discussion et des réseaux sociaux de type Facebook en a accru les risques. Le projet rend désormais condamnable l'usurpation de l'identité d'autrui sur internet, même sans préjudice financier*. » La notion d'identité n'est pas définie dans le texte. On peut en déduire que ce terme, créé spécialement pour l'univers numérique, recouvre à la fois les identifiants électroniques d'une personne, mais aussi son véritable nom, son surnom ou son pseudonyme. L'identité numérique d'une personne peut apparaître sous des formes dont la diversité n'aurait pas pu être prise en compte par une définition précise. Outre les noms d'utilisateurs, citons aussi les mots de passe, adresses URL, adresse IP, avatar, etc. Il faut aussi noter que l'article 434-23 du Code pénal réprimant le délit d'usurpation d'identité ne définit pas non plus la notion d'identité. L'élément intentionnel de l'infraction est susceptible de poser davantage de difficultés au juge. Le texte prévoit que le délit est caractérisé dès lors qu'il est réalisé en vue de troubler la tranquillité d'autrui ou de porter atteinte à son honneur ou à sa réputation.

La condition de réitération ayant été retirée du texte, des doutes subsistent quant à l'interprétation de cet élément intentionnel. Par exemple, la publication d'une photo sur un réseau social peut constituer, pour certaines personnes, une atteinte à la tranquillité dans la mesure où elles ne veulent pas être identifiées sur internet. Pour la personne qui a mis en ligne la photo litigieuse, il n'est pas certain que son intention ait été de nuire à la tranquillité d'autrui. Dans ce contexte, il appartiendra au juge, par son interprétation, de définir les conditions d'application de l'élément intentionnel de cette nouvelle incrimination et d'en préciser les contours.

### b) États-Unis

Aux États-Unis, il faut attendre le début des années 2000 pour qu'apparaissent au niveau fédéral les premières lois destinées à lutter directement contre l'usurpation d'identité. Ainsi, l'*Identity Theft and Assumption Deterence Act* détaille explicitement les informations d'identification personnelle comme le nom, le numéro de sécurité sociale, la date de naissance, un document ou un numéro officiel public, le permis de conduire ou le numéro fiscal, ou tout autre numéro de contrat ou d'identification d'une partie tierce. Pour la première fois, l'usurpation d'identité est ainsi devenue une infraction fédérale, ce qui devait permettre de mener plus aisément des poursuites. Cette loi établissait également la *Federal Trade Commission* (FTC) comme l'entité du Gouvernement chargée d'établir les procédures et de recevoir les plaintes des personnes victimes de ce nouveau délit. Incriminer l'usurpation d'identité indépendamment des fraudes et délits qui y sont rattachés permettait aussi de sanctionner des faits plus facilement détectables, avec un effet plus dissuasif

vis-à-vis des fraudeurs.

L'*Identity Theft and Assumption Deterence Act* détaille explicitement les informations d'identification personnelle comme le nom, le numéro de sécurité sociale, la date de naissance, un document ou un numéro officiel public, le permis de conduire ou le numéro fiscal, ou tout autre numéro de contrat ou d'identification d'une partie tierce.

L'arsenal législatif américain ne s'est pas arrêté là. En 2003, les victimes d'usurpation d'identité obtiennent le droit de faire corriger les informations les concernant dans les bureaux de crédit, avec le *Fair and Accurate Credit Transaction Act*.

Cette loi prévoit aussi que les bureaux de crédit ne pourront considérer des informations personnelles comme suffisantes pour une identification totale et absolue des clients. Elle institue également pour les clients le droit de placer des « alertes » sur leur nom de manière ponctuelle ou durable.

Le concept d'« *usurpation d'identité aggravée* » est également créé au niveau fédéral, pour lutter contre des fraudes organisées de type mafieux ou relatives au crime organisé (réseaux d'immigration, armes à feu, etc.). Créée en 2004, puis amendée en 2007, la sanction peut aller maintenant jusqu'à cinq ans de prison et 250 000 dollars d'amende, en plus des condamnations pour autres infractions. Parallèlement, la plupart des États se sont dotés d'une législation incriminant à titre spécifique l'usurpation d'identité. En revanche, le périmètre des fraudes concernées par l'usurpation d'identité, ainsi que les seuils d'amendes et de poursuites judiciaires varient souvent d'un État américain à l'autre.

c) Royaume-Uni

Avant les années 2003/2005, le Royaume-Uni ne disposait que d'une législation assez générale contre la fraude. Celle-ci était constituée essentiellement de mesures contre la tromperie et l'escroquerie, condamnables dans le cadre du *Theft Act* de 1968. Les données personnelles étaient protégées par le *Data Protection Act* de 1998, qui couvre l'ensemble des données personnelles détenues par des organisations et ressemble quelque peu à la loi « Informatique et libertés ». Concernant les données détenues par le secteur public, l'accès aux informations y était défini par le *Freedom of Information Act* de 2000.

Tout d'abord, en 2003, le Gouvernement fait passer le *Criminal Justice Act* qui permet de mieux répondre aux utilisations frauduleuses des passeports et permis de conduire. Puis, en 2005 et 2006, sont introduites les bases d'une nouvelle législation pour les données et l'identité, à travers deux lois majeures : le *Fraud Act* et l'*Identity Card Act*.

Le *Fraud Act*, élément essentiel de ce nouvel arsenal juridique, permet de qualifier de nouveaux types de fraudes (possession, transfert ou intention frauduleuse dans certains cas). Il rend passibles de poursuites pénales plusieurs formes d'usurpation d'identité à l'aide de son article 2 (fraude par fausse représentation), de son article 6 (possession d'un article ou d'un objet pour utilisation à des fins frauduleuses) ou de son article 7 (transmission d'articles ou de données personnelles susceptible de générer des fraudes). L'*Identity Card Act* cible la possession, le contrôle ou l'utilisation de documents d'identité falsifiés. Il prévoit la création d'un registre national d'identité (le *National Identity Register*) répertoriant une cinquantaine de données personnelles administratives, biométriques et diverses, et le déploiement progressif d'une carte nationale d'identité qui est adossée au registre national d'identité.

2º/ Les ripostes juridiques internationales

La Convention du Conseil de l'Europe sur la cybercriminalité est le premier et seul traité international ayant force obligatoire qui aborde les problèmes liés à l'expansion de la

cybercriminalité. Signée à Budapest en 2001, la convention est entrée en vigueur le 1er juillet 2004. Eu égard à la numérisation, à la convergence et à la mondialisation permanente des réseaux informatiques, la convention demande aux parties d'établir des lois érigeant en infractions pénales les atteintes à la sécurité résultant d'intrusions informatiques, d'interceptions illégales de données ou d'atteintes à l'intégrité d'un système informatique, mettant en danger l'intégrité et la disponibilité des réseaux.

Cet instrument vise à promouvoir « *une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale* ». À cette fin, les parties s'engagent à introduire dans leur droit pénal des délits relatifs à la criminalité informatique. Si le vol d'identité en ligne n'est pas en soi mentionné dans la convention parmi les agissements illégaux que les signataires doivent ériger en infractions pénales, il est néanmoins couvert indirectement au titre des délits qui lui sont étroitement liés comme l'accès illégal à des ordinateurs, l'accès illégal à des données informatiques ou la fraude informatique qui figurent dans le traité.

Les parties à la convention conviennent également d'adopter des législations procédurales nationales conférant à leurs organismes chargés de l'application de la loi les pouvoirs nécessaires pour la prévention, la conduite des enquêtes et les poursuites contre la cybercriminalité et pour une participation active aux efforts de coopération internationale. Cette participation devrait revêtir la forme d'une entraide aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou pour la collecte en temps réel de données relatives au trafic pouvant apporter la preuve d'une infraction pénale. Des mesures pour la conservation des données sont également mentionnées. En outre, la convention invite les parties à échanger spontanément des informations obtenues dans le cadre de leurs propres enquêtes lorsqu'elles estiment que cela pourrait aider la partie destinataire à engager ou à mener à bien des enquêtes ou des procédures.

Ainsi, la convention encourage une approche plus cohérente dans la lutte contre les attaques électroniques. Par exemple, elle est reconnue comme un modèle international important pour l'élaboration d'une législation contre la cybercriminalité dans les pays membres de la coopération économique pour l'Asie-Pacifique. Certaines entreprises du secteur privé ont pris des initiatives pour contribuer à accroître l'influence des principes de la convention.

### 3º/ La spécialisation des filières de police et de gendarmerie

Au-delà de la collaboration des opérateurs du secteur privé, le travail d'enquête nécessite de la part de la police et de la gendarmerie des compétences spécialisées, ainsi que du matériel adéquat qui suppose un investissement important. En France, les principaux services spécialisés dans les enquêtes sur la cybercriminalité se sont développés et restent placés sous la houlette du ministère de l'Intérieur. Il en est ainsi pour l'Office central de lutte contre la criminalité liée aux technologies (OCLCTIC), qui assure la gestion des échanges internationaux avec Interpol, et Europol. Il dispose d'un réseau d'enquêteurs spécialisés.

Pour détecter les éléments de preuve de fraudes ou d'infractions, les enquêteurs disposent d'outils spécialisés comme des connexions internet dédiées et anonymes. Ils utilisent aussi des matériels et des logiciels spécifiques, permettant notamment de relever les éléments de preuves sur un disque dur ou un réseau de communication intercepté.

Il existe également une structure similaire, la Brigade d'enquêtes sur les fraudes aux technologies de l'information (Befti), service opérationnel dépendant de la direction régionale de la police judiciaire de Paris. Spécialisée dans les enquêtes en milieu informatique, elle intervient principalement pour des affaires de piratage informatique, de contrefaçon de logiciels ou de bases de données. Elle mène beaucoup d'actions en connexion avec des fraudes aux cartes bancaires. Une cellule spécialisée en technologie numérique (baptisée « NTECH ») analyse les supports de

preuves, mène les investigations, et effectue aussi des tâches de « surveillance de l'internet ».

Face au défides atteintes à la sécurité *via* les données et la nouvelle technologie, la France s'est également dotée de moyens supplémentaires, comme la nouvelle Agence nationale de la sécurité des systèmes d'information (Anssi) dont les larges missions regroupent la formation des agents de l'État, la contribution à l'élaboration réglementaire, et la certification et la labellisation de sécurité vis-à-vis de technologies ou de solutions d'entreprises.

L'expertise de cette agence permet des analyses sur des systèmes technologiquement complexes et le déploiement de systèmes sécurisés au sein de l'État. Enfin, d'autres services peuvent aussi être impliqués de manière ponctuelle dans cette lutte pour la protection des données sensibles : le Pôle de lutte contre la délinquance financière au sein de la Direction centrale de la police judiciaire, la DCRI (Direction centrale du renseignement intérieur) en cas de menace d'intelligence économique ou de terrorisme, ou encore les douanes. Plus largement, à l'échelle européenne, les autorités policières et judiciaires de nombreux pays ont mis en place des structures et des outils similaires, pour rendre possibles les investigations.

## PERSPECTIVES

Dans quelques années, on pourra être amené à constater que, alors que le paysage de l'information aura été bouleversé par internet, réduisant la prééminence et la sacralisation des communications officielles, le nouvel écosystème de l'identité numérique s'insérera dans un environnement numérique global, et participera probablement à la diminution de l'importance relative de l'identité régalienne des États, au profit de nouveaux systèmes identitaires de natures distinctes. L'identité numérique deviendrait ainsi non seulement un important symbole du futur, mais aussi un catalyseur de formes de relations nouvelles, en tant que moyen devenu privilégié de notre reconnaissance par les auteurs et par nous-mêmes.

## CONCLUSION

Sous le double impact de la mondialisation et de la numérisation, nos données personnelles sont en train de prendre une importance fondamentale dans notre vie. Aussi incroyable que cela puisse paraître, elles sont devenues en l'espace de quelques décennies à la fois le socle principal et la représentation prioritaire de notre identité.

Nous sommes en train d'oublier les pratiques des générations précédentes, avec leur état civil flamboyant et leurs registres documentaires. Dans une cinquantaine d'années, il y a fort à parier que les papiers d'identité ne seront plus que des souvenirs, encadrés et mis sur des étagères comme vestiges pittoresques et charmants de l'histoire de l'humanité.

Les données incarnent bien une identité de « l'être » et de « l'avoir ». Dans le premier cas, elles nous représentent pour révéler qui nous sommes, faire reconnaître notre lien social et nous permettre d'exister dans la société. Dans le deuxième, elles sont nos clés de la relation économique et utilitaire, pour agir, transformer, générer, et échanger à titre privé comme à titre professionnel.

Les fraudeurs, attirés par le potentiel économique de ces données, détectent et exploitent un nombre important de vulnérabilités systémiques ou humaines, pour commettre les infractions sur des supports documentaires ou numériques. Ils ciblent particulièrement les données sensibles leur permettant d'abuser des identités des personnes physiques et morales.

Ainsi, pour que le monde numérique se hisse au même plan que le monde physique, il doit développer, en son sein, des cercles progressifs de sécurité, de reconnaissance et de confiance.

Dans le cadre du monde numérique et mondialisé annoncé pour le XXIe siècle, porter cette dimension humaine de la confiance, alors que nous sommes identifiés par ces données, personnelles, reste sans conteste un défipour tous. « Être ou ne pas être » : la question lancinante se pose plus que jamais à chacun d'entre nous.

**Indications bibliographiques**Leclair A., Usurpation d'identité : les Français inquiets, 2011, Disponible sur internet.

Tsoutsanis A., *Tackling Twitter and Facebook Fakes : ID Theft in Social Media, World Communications Regulations Report*, 2012, p. 1-3.

Hoofnagle C., *Internalizing Identity Theft, UCLA Journal of Law & Technology*, 2010 ; *Identity theft : Making the known unknowns known, Harvard Journal of Law and Technology*, vol. 21, 2007.

Solove D., *Identity theft, privacy an d the architecture of vulnerability, Hastings Law Journal*, vol. 54, 2003, p. 1127.

Sorrells D., *Social Security Numbers and ID Theft*, NY, Nova Science, 2010.

Desgens-Pasanau G. et Freyssinet E., L'identité à l'ère numérique, Paris, Dalloz.

Felcourt G., L'usurpation d'identité, Paris, 2011, CNRS éditions.

Nehf J., *Limiting Identity Theft in an E-commerce World, New Zeland Business Law Quarterly*, vol. 8, 2002, p. 37.

Stickley J., *Identity Theft*, New Jersey, Pearson Education, 2009.

Winn J. et Govern H., *Identity Theft : Risks & Challenges to Business of Data Compromise, Temple Journal of Science, Technology & Environmental Law*, vol. 28, nº 49, 2009.

James L., *Phishing exposed*, NY, Syngress, 2005.

Lopucki L., *Did privacy cause identity theft ?, Hastings Law Journal*, vol. 54, nº 4, 2003.

Neuer L., La spirale ubuesque de l'usurpation d'identité, 2012, disponible sur internet.

Soullier L., La loi sur l'usurpation d'identité adoptée, 2012, disponible sur internet.

Berguig M., L'usurpation d'identité sur Internet, mémoire de DESS, 2001, université Paris-II.

Faget M., L'usurpation d'identité sur Internet, mémoire de recherche, 2009, université Paris-II.

OCDE, Document exploratoire sur le vol d'identité en ligne, 2008, disponible sur internet.

Iteanu O., L'identité numérique en question, Paris, 2008, Eyrolles ; Usurpation d'identité, 2004, disponible sur internet.

Boileau P., Usurpation d'identité, Paris, 1983, Éditions J'ai lu. Wong R. et Savirimuthu J., *Identity Principles in the Digital Age : A Closer View, International Journal of Intellectual Property Management*, vol. 2, nº 4, 2008, p. 396-410.