Chaire Valeurs et Politiques
DES INFORMATIONS PERSONNELLES

INSTITUT
Mines-Télécom

DOCUMENTS DE TRAVAIL
WORKING PAPER SERIES

Document de travail CVPIP-13-02

Les enjeux de l'identité numérique

Claire Levallois-Barth

Novembre 2013

A paraitre dans la Revue de la Gendarmerie Nationale, janvier 2014

Internet : www.informations-personnelles.org

Email : contact@informations-personnelles.org

Les enjeux de l'identité numérique

Par Claire Levallois-Barth, maître de conférences en droit ; Institut Mines-Télécom : Télécom ParisTech ; CNRS LTCI ; coordinatrice de la chaire Valeurs et politiques des informations personnelles

La vie connectée impose de définir clairement l'identité numérique, ses composantes et ses utilisations. L'usurpation d'identité, dans sa version numérique, entraîne des préjudices tels qu'il devient indispensable de mener des actions préventives fortes. La mise en place d'identités numériques sécurisées et normalisées constitue un enjeu capital pour les pays membres de l'Union Européenne.

Le terme identité vient du latin *identitas* qui signifie « le même ». Sur le plan juridique, il peut être défini comme « ce qui fait qu'une personne est elle-même et non une autre »[1]. L'identité d'un individu permet donc de distinguer une personne d'une autre, de l'individualiser à partir d'un ensemble d'éléments appelés attributs. Une identité est donc composée d'attributs renvoyant à des caractéristiques spécifiques : âge, sexe, adresse, employeur, login, mot de passe, donnée biométrique, etc.. Une combinaison d'attributs constitue UN profil qui est propre à UN individu.

LA MULTIPLICATION DES IDENTITES NUMERIQUES

Dans le monde réel, l'identité est limitée à l'état civil (nom, prénom, date et lieu de naissance, etc.) d'une personne. Elle est attribuée soit par le lien de filiation pour le nom patronymique, soit sous le contrôle des autorités publiques.

Dans le monde virtuel, il en va tout autrement. L'identité numérique peut être définie par une entité externe (administration, banque en ligne, opérateur de téléphonie, etc.) ou être composée librement par la personne elle-même. L'utilisateur d'un réseau social (Twitter, Facebook) crée sa propre identité en recourant à des éléments constants comme dans le monde réel (nom, prénom) ou variables (login, mot de passe, adresse électronique, adresse IP).

Apparaît alors la notion d'identités numériques fragmentées, chaque identité pouvant avoir sa vie propre selon qu'elle évolue dans un cadre marchand ou non, une sphère privée, publique ou professionnelle. Il est ainsi possible de parler d'identité citoyen pour le titulaire d'un passeport biométrique, d'identité client pour l'utilisateur d'un site de commerce en ligne, d'identité professionnelle attribuée à un gendarme ou un médecin. S'ajoute l'identité d'une personne morale (numéro SIRET par exemple) et l'identité d'un objet (comme le numéro de la carte SIM), ce type d'identité étant amené à se multiplier avec l'Internet des objets.

Les formes de l'identité numérique sont tout aussi variées : elles peuvent aller de l'anonymat, en passant par le pseudonymat, un profil sur un réseau social, un avatar, à l'identité qualifiée, vérifiée. L'enjeu ici est de pouvoir gérer le lien entre une identité numérique et une identité réelle, en fonction des besoins du citoyen, de l'entreprise et de l'État, notamment des forces de l'ordre.

[1] Vocabulaire juridique, sous la direction du Doyen Gérard Cornu, 9e éd., PUF, Quadrige, août 2011, p. 431.

LA SECURISATION DES IDENTITES NUMERIQUES

Cependant, la fragilité des attributs composant l'identité numérique donne lieu à des fraudes de plus en plus fréquentes, à des détournements de droits et des vols de biens alors même que se développent de nouveaux services et usages numériques.

Les usurpations d'identités semblent augmenter : en 2009, on comptabilisait plus de 210 000 victimes par an pour un préjudice global de 3,874 milliards d'euros. Fin 2012, 400 000 personnes se déclaraient victimes d'une usurpation d'identité au cours des dix dernières années, soit 8 % des français. Cette forme de délinquance est en passe de devenir la deuxième infraction en France, derrière le vol de véhicules.

Afin de lutter contre ce fléau, le code pénal sanctionne depuis mars 2011 le délit d'usurpation d'identité en tant que tel : « 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 »[2]. Le député Marc Le Fur a par ailleurs proposé en juillet 2013 de sanctionner plus sévèrement l'usurpation d'identité commise par le biais de réseaux de communication électronique en doublant la peine encourue[3]. Cette réponse pénale doit notamment être complétée par une véritable politique de sensibilisation et d'éducation du citoyen, ce dernier ayant assurément un rôle actif à jouer pour assurer la confidentialité de ses propres identités et attributs.

LES ENTREPRISES ET ADMINISTRATIONS DIRECTEMENT CONCERNEES

La question de la garantie de l'identité concerne aussi l'ensemble des administrations et des entreprises. Ces dernières doivent veiller à la sécurité de leurs propres identités mais aussi des identités de leurs administrés, clients et agents lors des communications, transactions et paiements électroniques, y compris lors de l'utilisation de smartphones. Or, selon le rapport du cabinet américain *Ponemon Institute*, la perte des clés et des certificats électroniques pourrait se traduire par une perte d'environ 400 millions de dollars pour les 2 000 plus importantes entreprises internationales. En outre, 59% des responsables français ne connaîtraient pas le nombre de clés et de certificats utilisés dans leur organisation[4]. Il convient donc de mettre en place les conditions d'une gestion efficace du cycle de vie (validité, perte, vol) des clés de chiffrement et/ou des certificats électroniques associés à l'identité enrôlée. Au-delà de cette nécessité, il est important de sécuriser l'ensemble du processus, y compris l'enrôlement et l'attribution de l'identité en passant par la qualification des prestataires de services[5] afin que le destinataire puisse avoir pleinement confiance dans les données qu'il reçoit.

L'enjeu porte également sur la sécurisation des supports de l'identité numérique**.** En 2012, une proposition de loi sur la carte nationale d'identité électronique prévoyait la création d'une base centrale des titres d'identité devant à terme réunir les données biométriques de 45 à 50 millions de personnes. Après un long débat sur l'objectif que devait poursuivre le fichier, le texte est en

[2] Art. 2 de la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, JORF du 15 mars 2011.

[3] Proposition de loi visant à aggraver la sanction pénale applicable à l'usurpation d'identité commise par le biais de réseaux de communication électronique, présentée par M. Marc LE FUR, député, N° 1316, 24 juillet 2013.

[4] Ponemon Institute, *2013 Annual Cost of Failed Trust Report: threats & Attacks*.

[5] A cet égard, voir le site de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) : http://www.ssi.gouv.fr/.

partie censuré par le Conseil Constitutionnel[6]. Ce faisant, le Conseil ne se prononce pas contre un fichier central réunissant des données biométriques. Il estime seulement que les garanties entourant la mise en œuvre d'un tel fichier ne sont pas suffisantes, compte tenu notamment de son ampleur, de la nature des données enregistrées et des conditions de consultation des données enregistrées[7]. Pour l'instant, aucun autre projet de loi n'a été présenté, le gouvernement français ayant prévu d'adopter d'ici 2014 un plan d'action pour le développement des services d'identité numérique sécurisés et respectueux de la vie privée. Parallèlement, le projet Idenum a été relancé.

Ces initiatives posent la question du rôle de l'État dans la mise en place d'un système fiable d'authentification publique. Doit-il y avoir une certaine forme de délégation au secteur privé ? Une réponse positive implique alors de définir les modalités de la délégation, celles-ci devant garantir l'indépendance et la pérennité du système qui sera mis en place. Il s'agit également de préciser les conditions de consultation et de transmission des données, de sorte que seules les personnes strictement habilitées accèdent aux attributs d'identité.

En la matière, la France pourrait s'inspirer des modèles européens déjà mis en place. En effet, la liste des pays ayant d'ores et déjà développé un programme d'identité numérique est longue[8]. Ces programmes se basent sur différentes technologies. Ils revêtent également des formes diverses tant en ce qui concerne les fournisseurs de l'identité (l'État mais aussi des banques, des postes, des chambres de commerce, etc.) que les usages et services associés : déclarer les impôts en ligne, envoyer des documents électroniques et des courriers électroniques recommandés, sécuriser les sessions Internet des enfants ou s'identifier sur le réseau informatique de son entreprise.

L'étape suivante consiste à s'assurer que ces services puissent être fournis au-delà des frontières nationales. Typiquement, un citoyen estonien doit pouvoir s'authentifier et signer électroniquement sur le site d'une banque en ligne française.

L'INTEROPERABILITE DES IDENTITES NUMERIQUES A L'ECHELLE EUROPEENNE

La question de l'interopérabilité des identités numériques à l'échelle transnationale concerne tout d'abord le monde professionnel. Une carte de qualification de conducteur mutuellement reconnue par les États membres de l'Union européenne existe d'ores et déjà tandis que des discussions visent à créer une carte d'identité professionnelle européenne. Cette carte permettrait aux médecins, architectes et autres professionnels de s'établir plus facilement dans un autre pays de l'Union européenne[9].

L'interopérabilité des identités implique également d'encadrer la création, l'utilisation et le partage des attributs de l'identité, autrement dit des données personnelles des citoyens. A cet égard, une proposition de règlement destinée à remplacer une directive européenne adoptée en 1995 est

[6] Conseil constitutionnel, décision n° 2012-652 du 22 mars 2012, Loi relative à la protection de l'identité.

[7] Conseil Constitutionnel, commentaire de la décision n° 2012-652 du 22 mars 2012, Loi relative à la protection de l'identité.

[8] Ainsi, la Belgique, l'Allemagne, l'Espagne, la Portugal, l'Estonie et la Lituanie ont déployé ou sont en train de déployer leur projet tandis que la Pologne, la République Tchèque, la Slovaquie, la Hongrie, la Roumanie, la Slovénie et la Turquie définissent actuellement leur programme.

[9] Proposition de directive du Parlement européen et du Conseil modifiant la directive 2005/36/CE relative à la reconnaissance des qualifications professionnelles et le règlement concernant la coopération administrative par l'intermédiaire du système d'information du marché intérieur, COM(2011)883 final.

actuellement en cours de discussion[10]. L'enjeu de cette refonte est double : tenir compte des évolutions des technologies et renforcer l'effectivité des principes réglementant l'utilisation des données personnelles.

L'action des institutions européennes porte aussi sur l'identification électronique et les services de confiance. Ainsi, la Commission européenne a publié en juin 2012, un projet de règlement destiné à remplacer une directive européenne sur les signatures électroniques de 1999[11]. Ce projet, tout comme la proposition de règlement sur la protection des données personnelles, fait partie des textes prioritaires devant être adoptés en 2014[12]. L'objectif ici est, non pas d'obliger les États membres à mettre en place des systèmes d'identification électronique, mais de fixer des règles d'interopérabilité afin que les systèmes nationaux acquièrent une dimension européenne. Dans cette optique, la proposition couvre deux types de services : les services d'identification et les services de confiance, à savoir les services de signatures électroniques, de cachets électroniques, d'horodatages électroniques, de documents électroniques, de services de fournitures électroniques, d'authentification de site web et de certificats électroniques. Ces services posséderont pour la plupart d'entre eux deux niveaux : un niveau simple où le service bénéficiera d'une simple garantie de non-répudiation et un niveau qualifié où il bénéficiera d'effets juridiques identiques au même service ou instrument ramené au papier, lorsqu'il existe. Par ailleurs, chaque État membre devra reconnaître et accepter les identités numériques émises par un autre État, dès lors que cet État aura notifié à la Commission européenne des systèmes remplissant certains critères[13].

Ces systèmes devront donc faciliter la preuve de l'identité numérique, à la fois pour les citoyens et les forces de l'ordre dans un contexte d'enquête et d'apport de la preuve. Leur succès implique de sécuriser chacun des maillons de la chaîne d'identité : l'enrôlement, l'émission de titres, les processus d'identification, la répudiation, les applications fournies par des prestataires de confiance, les serveurs d'intermédiation de chaque État membre, etc.

Surtout, ces systèmes devront faire l'objet d'une véritable appropriation par le grand public. Malgré leur complexité technique, ils doivent être faciles d'utilisation et permettre à chaque titulaire du support d'identité, en fonction des différents contextes d'utilisation, d'adapter et de cloisonner ses différentes identités, de contrôler en toute transparence les attributs qu'il souhaite diffuser et les droits associés. Dans le monde numérique comme dans le monde réel, le citoyen doit conserver la possibilité d'agir en véritable acteur responsable.

[10] Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données du 25 janvier 2012, COM (2012)11 final.

[11] Proposition de règlement du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, COM(2012)238 final.

[12] Commission européenne, communiqué de presse du 22 octobre 2013, La Commission adopte son programme de travail pour 2014 : une année de mise en œuvre et de résultats.

[13] Les identités numériques devront notamment être délivrées par cet État, en son nom ou sous sa responsabilité ; l'État garantira l'attribution univoque des données d'identification personnelle ainsi que la disponibilité en ligne, 24 heures sur 24 et gratuitement des éléments de vérification de l'identité du titulaire.