La Lettre

Chaire Valeurs et Politiques des Informations Personnelles

www.informations-personnelles.org

N° 2 - Mars 2016

Identités numériques

Editorial Les enjeux soulevés par les systèmes de gestion d'identités numériques au regard de la circulation des données personnelles

Quand nous accédons à des services sur Internet, nous avons besoin de nous identifier et de nous authentifier, à l'aide de notre identité réelle ou d'un pseudonyme. Nous pouvons ainsi accéder à notre espace personnalisé et donc à notre profil, à nos dernières commandes, à nos ouvrages préférés... Cette procédure d'authentification et d'identification est effectuée via un système de gestion d'identités numériques. Dans ce cadre, les fournisseurs d'identités gèrent les identités numériques de leurs clients pendant tout leur cycle de vie (enrôlement, révocation, maintenance), assurent un service d'identification et d'authentification qui correspond à un certain niveau de sécurité et aident, si besoin, les autorités policières et judiciaires à retrouver l'identité d'un internaute.

Autrefois réalisée de façon autonome par les fournisseurs de services, le rôle de fournisseurs d'identités privés a été assuré par les opérateurs de télécommunications, puis par des multinationales comme Facebook et Google. Ces dernières ont en cela saisi l'occasion d'assoir leur position dominante dans le secteur du numérique par la maitrise des identités numériques et des données personnelles associées. Quand on sait que le marché des données personnelles est estimé, pour l'Europe seulement, à 1000 milliards d'euros d'ici 2020 (Boston Consulting Group, 2014), on en comprend mieux les enjeux.

Cependant, certains fournisseurs collectent les données personnelles des utilisateurs dans des contextes autres que celui de la stricte fourniture du service de gestion des identités, comme les sites Internet visités, les mots clés tapés dans un moteur de recherche, la géolocalisation à la minute près... Bien souvent, les modalités de cette activité sont définies via une charte que les clients sont tenus de signer s'ils souhaitent bénéficier d'un bouquet de services. Les données collectées servent à enrichir les profils des utilisateurs du service. A partir de ces

...

Sommaire

TELECOM ParisTech
TELECOM Ecole de Management
TELECOM SudParis
INSTITUT Mines-Télécom

profils, les fournisseurs d'identités sont mieux à même de cibler les annonces publicitaires susceptibles de déclencher un acte d'achat ou la visite d'un site tiers. De plus, les profils peuvent faire l'objet de transactions lucratives comprenant leur revente directe ou la vente de listes d'abonnés présentant certaines caractéristiques.

Par ailleurs, un internaute laisse au cours de sa navigation un si grand nombre de traces dans le système d'informations que l'administrateur d'un site est en mesure de détecter qu'il s'agit de la même personne qui revient visiter son site. Sans pour autant connaitre son identité au sens strict du terme, il est donc en mesure de le profiler pour lui proposer des produits, des publicités ciblées… En croisant ce profil incomplet avec d'autres bases de données suffisamment riches et à jour, il lui est même possible de déduire l'identité réelle de la personne. Il importe donc de soutenir des démarches qui pallient au déséquilibre actuel entre, d'une part, des fournisseurs d'identités privés qui « surconsomment » de la donnée et, d'autre part, des Internautes bien souvent résignés devant la « fuite » de leurs données personnelles.

A cet égard, cette Lettre présente dans une perspective pluridisciplinaire plusieurs pistes de réflexion : tout d'abord, le point de vue philosophique qui souligne combien il est essentiel que chaque personne puisse disposer de plusieurs identités pour se présenter aux autres comme elle l'entend ; puis, l'approche technique par les « schémas de preuves » qui garantissent la véracité des attributs sans dévoiler l'identité de la personne ; enfin, l'approche réglementaire en ce qui concerne le renforcement et l'effectivité des droits des personnes, notamment à travers le futur règlement général sur la protection des données personnelles.

Maryline Laurent
Professeur en sciences de l'informatique à Télécom SudParis et Membre fondateur de la Chaire

Parution du Cahier de la Chaire n°1 : Identités numériques

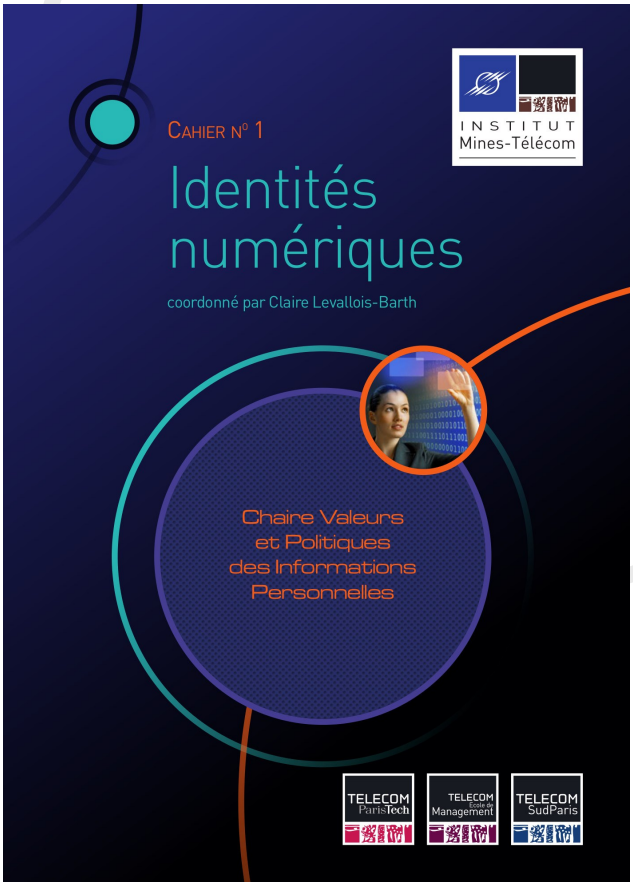
Le premier Cahier de la Chaire qui porte sur la problématique des identités numériques paraitra début mars. Il sera présenté et discuté lors de la conférence-débat organisée le jeudi 10 mars 2016 à 17h à Télécom ParisTech.

Ce cahier est conçu pour être un outil de compréhension et de vulgarisation pour tout citoyen, professionnel, chef d'entreprise, enseignant, pour qui la question des identités numériques représente un véritable enjeu. Le lecteur pourra poursuivre sa réflexion via les nombreuses références bibliographiques et les conseils de lecture.

Fruit d'une démarche interdisciplinaire, cet ouvrage souligne d'abord les enjeux liés aux identités numériques, en mobilisant la philosophie, le droit, les sciences informatiques et l'économie. Les grands principes de fonctionnement et une analyse comparative des systèmes de gestion des identités numériques régaliens dans certains Etats européens sont ensuite présentés. Le Cahier se concentre enfin sur les aspects réglementaires et leur mise en application en France et dans l'Union européenne. La problématique des preuves d'attributs préservant le pseudonymat de l'utilisateur y est aussi abordée.

Cahier à télécharger : www.informations-personnelles.org.

Armen Khatchatourov
Ingénieur de recherche à Télécom Ecole de Management et membre de la Chaire



Identités numériques / identités multiples

La question des identités numériques est aujourd'hui au centre du débat public sur l'utilisation de l'Internet. Elle interroge les effets de la métamorphose numérique sur notre manière de nous présenter à autrui et d'être au monde en cristallisant, dans son versant « sécurité », les craintes liées à l'utilisation frauduleuse de différents services en ligne. Si, de ce point de vue, les problématiques soulevées concernent des thématiques et des disciplines assez éloignées, l'ambition du travail mené au sein de la Chaire est de considérer dans une approche pluridisciplinaire les aspects techniques, réglementaires, économiques et sociétaux relevant des identités numériques.

Dès ses débuts, l'Internet a été perçu à la fois comme un risque potentiel quant à la difficulté d'identifier ses utilisateurs et comme une formidable ouverture sur un nouvel espace public, en permettant de nouvelles formes d'expression politique et en générant de nouvelles opportunités en termes d'accès à l'information. Ainsi, le fait qu'un utilisateur puisse – ou non – se présenter sous de multiples « identités » (« mère », « fan de musique », « demandeur d'allocation familiale », « contribuable ») dans cet espace, a souvent constitué un enjeu central des démarches techniques et législatives dans ce domaine.

Cependant, il convient de prendre la juste mesure de ce qui se joue dans la question des identités multiples, et de souligner qu'il ne s'agit pas simplement de « privacy » si l'on entend par celle-ci uniquement la préservation de l'intimité individuelle.

Pour bien saisir ces enjeux, il faut rappeler, en suivant en cela une longue tradition philosophique, que l'individu peut être abordé de deux manières. D'une part, il peut être perçu comme le résultat d'une identification ; on considère alors que la personne est définie une fois pour toutes, comme la somme de ses différentes caractéristiques telles que l'état civil, la profession, le statut social, etc. (en sciences informatiques, ces caractéristiques formelles sont appelées « attributs »). On définit alors l'individu de l'extérieur et comme identique à lui-même, sous le terme d'identité-idem. D'autre part, on peut considérer que l'individu est d'abord un rapport à soi-même, que ce rapport est essentiellement un processus, une dynamique tournée vers l'avenir ; et que l'individu ne peut être saisi de manière pertinente en dehors de toute considération sur l'horizon de sens qui s'ouvre à lui. Cette identité-ipse est en cela irréductible à la définition « de l'extérieur » telle qu'évoquée ci-dessus. L'enjeu fondamental de cette distinction entre idem et ipse est alors la possibilité pour l'individu de conserver une certaine initiative sur sa propre construction.

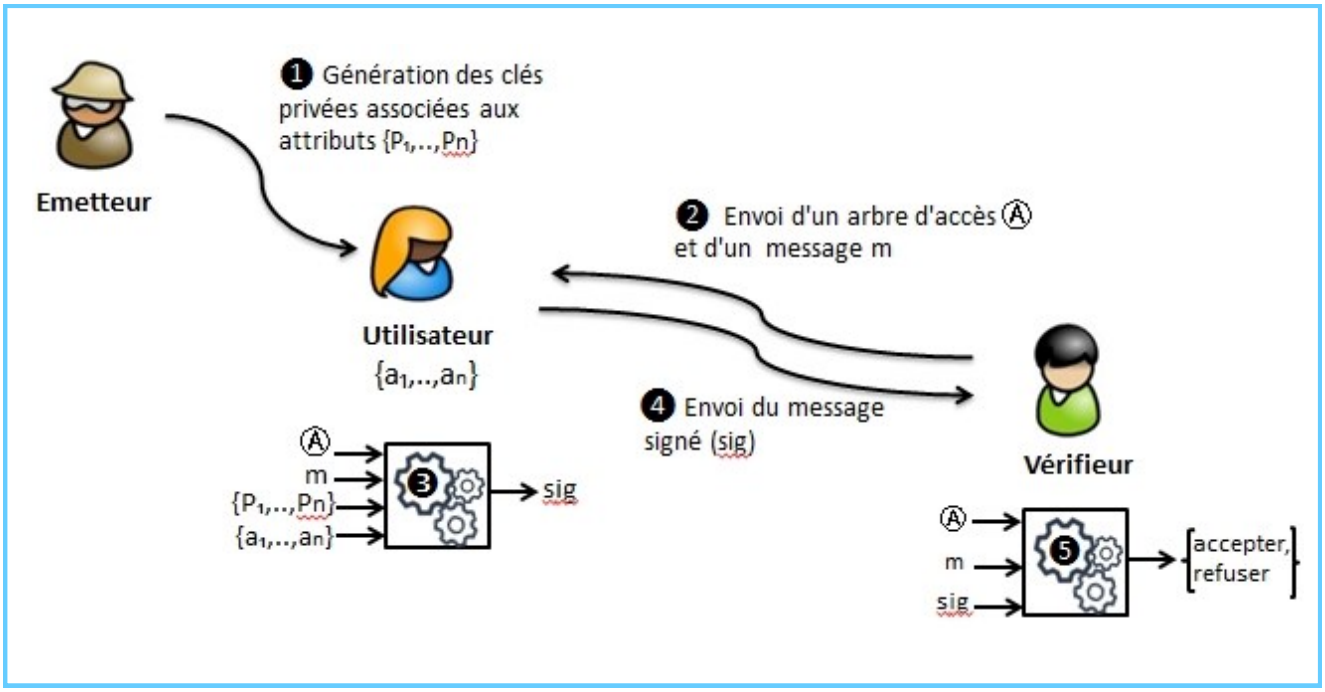
Sans cette initiative, sans la possibilité d'opérer des choix y compris dans la manière de se présenter à autrui et ainsi ne pas être soumis à la visibilité totale, c'est l'autonomie même de l'individu qui risque d'être remise en question. Par exemple, le croisement des données personnelles entre les différents contextes (relations amicales, contacts professionnels, données médicales) sans tenir compte de la spécificité de chacun d'entre eux, conduit à réduire l'espace dans lequel l'individu peut se construire. Or aujourd'hui, en raison de développements technologiques récents comme l'Internet des objets les occasions de tels croisements, qui sont susceptibles de conduire à une mise en surveillance des actions des individus, se font de plus en plus nombreuses.

La préservation de cette initiative de l'individu est également cruciale pour qu'il puisse agir en tant que citoyen. On peut en effet se demander si ce croisement des données personnelles ne risque pas de constituer un frein à l'exercice de certaines formes de libertés publiques et en premier lieu la liberté d'expression. Plus fondamentalement encore, le croisement des données et le profilage qui l'accompagne comportent un risque réel d'enfermer la personne dans des bulles informationnelles certes de plus en plus personnalisées, mais susceptibles de remettre en cause le « référentiel commun » nécessaire à la constitution du lien social.

En ce sens, préserver la possibilité pour un même individu de disposer de plusieurs identités numériques est un enjeu qui va bien au-delà de la simple protection de la « vie privée ». Cet enjeu touche à notre sens à la possibilité de cultiver des espaces de différences existentielles, et par-là même, des sociétés démocratiques.

Armen Khatchatourov
Ingénieur de recherche à Télécom Ecole de Management et membre de la Chaire et
Pierre-Antoine Chardel
Professeur de philosophie sociale et d'éthique à Télécom Ecole de Management et membre fondateur de la Chaire

Un schéma de preuves d'attributs qui préserve le pseudonymat



La problématique des preuves d'attributs préservant le pseudonymat de l'utilisateur est exposée dans le cahier n°1 « Identités Numériques » de la Chaire, à paraître en mars. Il s'agit ici d'apporter à un fournisseur de service la preuve de l'identité d'une personne ou la garantie que cette personne répond à certains critères, par exemples d'âge (plus de 18 ans), de statut. On distingue à cet égard deux types de preuves. La preuve complète est générée par une entité (l'émetteur) et porte sur un ensemble d'attributs associés à une personne ; elle est techniquement garantie comme valide grâce à la signature apposée par l'émetteur. La preuve dégradée est, quant à elle, générée à partir de la preuve complète sur un sous-ensemble d'attributs. Ces attributs sont choisis sélectivement par la personne concernée afin de répondre à la politique d'accès du fournisseur de service.

L'équipe de la Chaire travaille actuellement sur un schéma de preuves qui soit plus performant que les solutions actuelles « Idemix » de IBM et « U-Prove » de Microsoft. Pour ce faire, nous nous intéressons aux signatures de type Attribute-Based qui permettent à la fois à la personne de générer une preuve sur un ensemble d'attributs à l'aide de clés privées envoyées par un émetteur, tout en préservant son pseudonymat et au fournisseur de service de vérifier que la preuve dégradée satisfait sa politique d'accès, cette politique étant définie de façon « expressive » (grâce à des opérateurs logiques) sous forme d'arbre d'accès.

Par exemple, l'autorisation d'accès au service est octroyée lorsque la preuve satisfait une « expression logique » : il faut que l'utilisateur fournisse la preuve qu'il a plus de 18 ans OU qu'il possède un permis de conduire.

Le schéma de preuve que nous proposons, basé sur les signatures Attribute-Based, présente plusieurs avantages en termes d'efficacité et de flexibilité. Tout d'abord, la génération de la preuve complète ne repose pas sur un protocole interactif entre la personne et l'émetteur, contrairement aux solutions existantes, ce qui nous permet un gain de bande passante et de temps. Ensuite, la taille de la preuve complète est constante quel que soit le nombre d'attributs utilisés, et ce grâce à l'emploi d'algorithmes d'accumulation qui privilégient l'agrégation d'un ensemble de résultats plutôt que leur concaténation. Enfin, ce schéma gagne en expressivité pour définir la politique d'accès des fournisseurs de services grâce à l'utilisation des arbres d'accès.

Nesrine Kaâniche
Post-doctorante en sciences de l'informatique
à Télécom SudParis et membre de la Chaire

Vers l'adoption prochaine du règlement (UE) Données personnelles

Le député Jan Philipp Albrecht, rapporteur du Parlement Européen sur le projet de règlement « Données personnelles »

Après près de quatre ans de discussions, le Parlement européen, le Conseil des ministres de l'Union européenne et la Commission européenne sont enfin parvenus à un accord global le 15 décembre 2015. Les négociations portaient sur deux textes : un règlement général sur la protection des données personnelles et une directive spécifique concernant les données utilisées par la police et les autorités judiciaires.

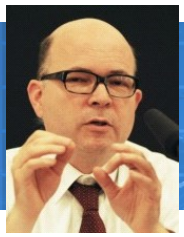
Le règlement, applicable directement, entrera en vigueur deux ans après son adoption, qui devrait intervenir d'ici juin 2016. Son objectif est de renforcer la protection des citoyens de l'Union européenne tout en facilitant l'application des règles pour les entreprises.

Parmi les nouveautés, on retiendra le droit à la portabilité des données, le droit à l'oubli (sous la forme d'un droit au déréférencement), la promotion de l'intégration de la composante « données personnelles » dès la conception des produits et services fournis par les entreprises (« data protection by design »), le principe de responsabilité (« accountability ») et le renforcement des sanctions puisque les amendes pourront atteindre jusqu'à 4 % du chiffre d'affaires annuel de l'entreprise contrevenante.

Les conséquences de cette réforme en matière d'identité numérique ont été exposées par Claire Levallois-Barth lors de la Conférence organisée par l'ASCIEL le 14 décembre 2015 sur le thème « Impact on eIDAS of the future regulation on General Data Protection ». Son intervention a notamment porté sur les notions de « donnée personnelle », « donnée pseudonymisée » et « donnée anonymisée ».

Claire Levallois-Barth
Maître de conférences en droit à Télécom ParisTech
et coordinatrice de la Chaire

Les données personnelles dans les traités et accords internationaux



Paul Nemitz

Claude Moraes

Isabelle Falque-Pierrotin

Cette rencontre qui s'est tenue le 8 janvier 2016 était animée par Jean-Sébastien Lefebvre, journaliste à Contexte. Elle a accueilli Claude Moraes, député européen, Président de la Commission LIBE (Libertés civiles, justice et affaires intérieures), Responsable adjoint du Labour Party européen (EPLP), Isabelle Falque-Pierrotin, Présidente de la CNIL et du G29, et Paul Nemitz, Directeur Droits fondamentaux et citoyenneté de l'Union européenne, Direction Générale Justice de la Commission européenne.

G29 : Groupe de travail rassemblant les autorités nationales de protection des données personnelles de l'Union européenne, auxquelles s'ajoutent un représentant de la Commission européenne et le Contrôleur européen de la protection des données.

Devant plus d'une centaine de personnes, la rencontre a permis de discuter des conséquences de l'arrêt Schrems de la Cour de Justice de l'Union européenne du 6 octobre 2015 qui invalide le Safe Harbor (mécanisme qui permettait à une entreprise américaine de transférer des données personnelles de l'Union européenne vers les Etats-Unis). Le débat a également porté sur la différence de protection des données personnelles offerte par les Etats-Unis, d'une part, et l'Union européenne, d'autre part, notamment au regard du futur règlement sur la protection des données personnelles qui devrait être adopté d'ici juin 2016. Enfin, la question de la transformation du cadre législatif international a été discutée, en particulier la nécessité de conclure (ou non) un nouveau traité commercial et de parvenir à un accord sur la question de l'accès aux données personnelles par les services d'espionnage.

Pour plus d'information : www.latribune.fr/economie/international/ue-et-etats-unis-peinent-a-concilier-leurs-approches-de-protection-des-donnees-542397.html

Claire Levallois-Barth
Maître de conférences en droit à Télécom ParisTech
et coordinatrice de la Chaire

Rendez-vous 2016, 1er trimestre

Colloque Défense & Sécurité, quelles continuités ?

2 & 3 mars 2016, Paris, Ecole Militaire.
Le 3 mars à 9h15, table ronde "Liberté versus sécurité" avec la participation de Gabriel Périès, membre de la Chaire.
www.defense.gouv.fr/actualites/operations/colloque-defense-et-securite.-quelles-continuites-le-2-3-mars-2016-a-l-ecole-militaire

Trust & Privacy Day

18 mars 2016, Paris, Palais Brongniart
Avec la participation de Claire Levallois-Barth, coordinatrice de la Chaire.
www.trustandprivacy.org

37th IEEE Symposium on Security and Privacy

23-25 mai 2016, The Fairmont, San Jose, Californie, USA
www.ieee-security.org/TC/SP2016

A savoir et à lire

Le Projet de règlement européen sur les données personnelles, version du 28 janvier 2016
http://data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/en/pdf

Sélection d'articles sur le *Privacy Shield*

EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield
http://europa.eu/rapid/press-release_IP-16-216_en.htm

The EU-U.S. Privacy Shield
www.itic.org/safeharbor

EU-US Privacy Shield : encore Top Secret !
www.linformaticien.com/actualites/id/39449/eu-us-privacy-shield-encore-top-secret.aspx

Après le Safe Harbor, le Privacy Shield. Un bouclier de papier ?
www.nextinpact.com/news/98366-apres-safe-harbor-privacy-shield-un-bouclier-papier.htm

Agenda

LES PROCHAINS RENDEZ-VOUS DE LA CHAIRE

Jeudi 10 mars, 17h-19h, Rencontre « Identités numériques » avec :
- 17h-18h – Présentation du Cahier Identités numériques
- 18h-19h – Table ronde : quel avenir pour les identités numériques en France ?

Jeudi 19 mai, 14h-15h30, Séminaire « La loyauté des plateformes » : Valérie Peugeot, Orange Labs, Sociology and Economics of Networks and Services, pour ses travaux au CNNum (Conseil national du numérique).

Jeudi 16 juin 2016, 13h30 – 15h, Séminaire « Les algorithmes » avec Célia Zolynski, Professeur de droit privé à l'Université de Versailles – Saint-Quentin-en-Yvelines.

Ces rendez-vous ont lieu à Télécom ParisTech, 46 rue Barrault (Paris 13e). Certaines dates sont susceptibles de changer. Pour avoir plus de détails sur les événements et vous inscrire, consultez le site :

www.informations-personnelles.org

Contact

https://twitter.com/CVPIP

www.informations-personnelles.org

www.youtube.com

Chaire Valeurs et Politiques des Informations Personnelles
Portée par l'Institut Mines-Télécom et soutenue par les Mécènes.
46, rue Barrault, 75634 Paris Cedex 13
Tél. : 01 53 73 22 22
www.informations-personnelles.org
Édition trimestrielle
Dépôt légal : à publication
Rédacteur en chef : Claire Levallois-Barth