Identités numériques

Les cahiers de veille **de la Fondation Télécom**

FONDATION TELECOM

Édito

Avril 2010

Après un premier cahier de veille consacré à la géolocalisation des biens et des personnes, nous poursuivons nos travaux de prospective en abordant les questions de l'identité à l'ère du numérique.

Nicolas Auray, Claire Levallois-Barth, Frédéric et Nora Cuppens, enseignants-chercheurs de l'Institut Télécom, ont réuni leurs compétences en sociologie, en droit et en informatique pour analyser ces différentes identités numériques que nous construisons, que nous dévoilons, dont nous jouons ou sommes joués, que nous vivons ou que nous appelons de nos vœux.

L'identité numérique couvre un large spectre de pratiques, allant de l'authentification et l'identité administrative à une « aura sociale » que nous maîtrisons mal et qui laisse des traces durables mais qui fonde un nombre croissant de services. Plurielle, contextuelle, évolutive, elle s'inscrit pourtant dans les réseaux. Il nous faut apprendre à la construire, la gérer, la protéger et surtout l'utiliser.

Ce cahier de veille permettra, nous l'espérons, aux enseignants-chercheurs et aux partenaires de la Fondation Télécom d'approfondir cette réflexion pour imaginer les services et les usages qui demain s'appuieront sur nos persona numériques.

Henri Verdier
Directeur du Think Tank
de la Fondation Télécom

Sommaire

P02 La construction des identités à l'ère numérique
- P02 Qu'e-suis-je ?
- P05 Les menaces d'interconnexion : une inquiétude qui se répand
- P06 Les défis de l'exposition de soi
- P07 La gestion de la notoriété
- P07 Le contrôle réalisé par chacun, de manière autorégulée
- P08 Un marché stratégique : les services de gestion de la réputation en ligne
- P09 Le calcul des scores de réputation : un algorithme délicat
- P11 Les avatars et les pseudos : l'emballement fictionnel des identités
- P12 Les différences sociales dans la mise en scène de son avatar
- P13 L'usurpation et le forgeage d'identité

P14 Technologies de l'identité numérique
- P14 Enjeux de la gestion des identités numériques
- P14 La crise de la gestion des identités numériques et des accès
- P15 Une réponse : la fédération d'identités
- P16 Vie privée, identité numérique et fédération d'identités
- P18 Fédération d'identités : mise en œuvre / implémentation
- P19 SAML 2.0 (Security Assertion Markup Language)
- P20 Contrôle d'accès et négociation fondée sur l'échange de certificats
- P21 XACML 2.0 (eXtensible Access Control Markup Language)

P22 Perspectives stratégiques
- P22 L'implication des industriels et des institutions gouvernementales
- P23 Les actions à lancer

P27 Contributeurs & Glossaire

La construction des identités à l'ère numérique

Qu'e-suis-je ?

Dans la nouvelle de science-fiction récente d'Eric Holstein, *Tertiaire*, est dépeint un monde où tout s'achète, tout se vend, y compris son propre nom. Le narrateur, qui avait choisi de louer un patronyme flatteur (*Emerson Mighty*), se retrouve affligé du sien (*Abel Marguerite*), avant d'être finalement obligé de le louer à son tour pour gagner un peu d'argent, quitte à devoir se contenter d'un numéro (*Abel 8328*), ou à opter pour un nom publicitaire (*Abel MSOffice Vision*).
D'abord description d'un monde aux pratiques financières extrêmes, cette nouvelle est également un avertissement sur la gestion de son identité. Aujourd'hui, devant la multiplication des sites où l'on peut choisir et paramétrer non seulement son identité, mais ses identités, on doit reconnaître que les technologies de la communication nous ont offert des instruments de sculpture du soi, permettant de travailler des expressions identitaires de manière plus souple. Leur usage quotidien nous fait prendre le chemin d'un développement des identités personnelles.

Du profil à la *persona* numérique

L'imaginaire d'Internet a souvent été associé à l'idée du travestissement identitaire. Mais la plasticité du Web permet de jouer plus fortement avec les décalages, les modulations ou les transformations dans l'image de soi que l'on projette. Souvent, les usagers cherchent moins la métamorphose que « l'augmentation » de soi.
« Les *profils* sont la représentation numérique publique de l'identité », comme l'a noté l'anthropologue américaine Danah Boyd. Les réseaux sociaux ne doivent leur existence qu'aux informations que les internautes veulent bien laisser d'eux-mêmes. Leur succès correspond à l'importance nouvelle que prend, dans nos sociétés individualistes, le souci que chacun a de présenter une identité originale et attractive. De nombreux lieux de l'Internet sont ainsi ni plus ni moins que les outils de représentation sociale que les internautes veulent alimenter. Les informations ainsi déposées sur Internet sont de multiple nature.

Les profils sont la représentation numérique publique de l'identité

L'identité numérique se compose de trois facettes : *qui on est, qui on connaît et ce que l'on fait*.

Les sites au contenu produit par les utilisateurs – lieux d'indexation et de partage de photos de type Flicker, plateformes de mise à disposition de vidéos de type DailyMotion ou Youtube, blogs – exposent des contenus amateurs aux yeux de tous. L'encyclopédie collaborative Wikipedia révèle les connaissances de ses contributeurs. eBay en dit long sur les besoins d'équipement de ses 248 millions d'utilisateurs. Les sites de réseaux sociaux, par l'intermédiaire de la consultation des profils publics de leurs membres dans les moteurs de recherche, dévoilent par ailleurs de nombreuses informations sur les gens que l'on connaît.

Une collecte des données personnelles encadrée

Récemment, la question éthique des limites à donner à l'extension de la collecte des données personnelles – sur qui l'on est, ce que l'on fait et qui l'on connaît – s'est posée dans le contexte de plusieurs affaires. D'une part, une sensibilité a émergé concernant la diffusion des informations de *localisation* : le service Google Latitude géolocalise ainsi ses amis sur Google Maps en s'appuyant sur la fonction GPS du terminal ou des données provenant des antennes de transmission. On peut imaginer ce que pourrait en faire un employeur ou un conjoint mal intentionnés. D'autre part, les affaires se multiplient sur la collecte d'informations sensibles touchant aux pratiques sexuelles, à l'état de santé ou aux opinions politiques des personnes. La Commission Nationale de l'Informatique et des Libertés (CNIL) cite par exemple le cas d'une société américaine qui a lancé le passeport Safe Sex pour certifier qu'un internaute flirtant en ligne n'avait pas de maladies sexuellement transmissibles en cas de rencontres passionnées de visu. Enfin, autour du marché de la réputation en ligne, se développent des polémiques mettant en évidence les risques de *diffamation* suite à la divulgation de témoignages venus de tiers et imputant à la personne des faits ou comportements non vérifiés. Citons ainsi un phénomène qui a pris de l'ampleur : les services en ligne proposant de noter les médecins ou les professeurs. En mars 2008, le Tribunal de Grande Instance de Paris et la CNIL les ont jugé illégitimes, notamment parce que les évaluations sont attribuées *de façon subjective par des tiers dont on ne peut vérifier la qualité*.

L'avis du juriste

Donnée personnelle (Donnée à caractère personnel) : *« toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres »* (Article 2 de la loi Informatique et libertés). Pour déterminer si une personne est identifiable, il convient de considérer *« l'ensemble des moyens en vue de permettre son identification, dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne »*.

La loi Informatique et Libertés transpose ainsi la directive européenne 95/46/CE *« Protection des données »* applicable à l'ensemble des 27 États membres de l'Union européenne. Ce texte précise : *« est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale »*.

Notamment, le nom, le prénom, le pseudonyme (au sens juridique du terme), un numéro de téléphone, une liste de contact, le numéro de carte bancaire, une photo et selon la CNIL un identifiant ou une série de chiffres telle que l'adresse IP ou l'adresse Bluetooth sont des données personnelles dans la mesure où ces informations sont « rattachables » à une personne. Dans ce sens, la proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique considère que *« toute adresse ou tout numéro identifiant l'équipement terminal de connexion à un réseau de communication »* constitue une donnée personnelle.

Comment collecter et utiliser légalement des données personnelles ?

Selon la directive 95/46/CE *« Protection des données »*, le responsable de traitement de données personnelles doit :

- en règle générale, déclarer son traitement auprès de l'autorité de contrôle, en France la CNIL : **principe de déclaration**
- recueillir et traiter des données uniquement pour une finalité déterminée, explicite et légitime : **principe de finalité**
- ne traiter que des données adéquates, pertinentes et non excessives par rapport à cette finalité : **principe de proportionnalité**
- sauf exceptions, recueillir le consentement préalable de la personne concernée : **principe de légitimation**
- informer la personne concernée que ses données personnelles sont collectées, ce qui permet ensuite à la personne d'exercer son droit d'accès aux données, et au besoin de les faire rectifier, voire supprimer : **principe de transparence**
- permettre à toute personne de s'opposer *pour des raisons prépondérantes et légitimes* à ce que ses données fassent l'objet d'un traitement. Lorsque ces données sont utilisées à des fins de prospection, en particulier commerciale, la personne n'a à justifier d'aucun motif.

Noter qu'une durée limitée de conservation des données, en fonction des finalités, et la consultation et la communication protégées des données, découlent de ces principes.

En cas de non-respect de ces principes, le responsable de traitement encoure des sanctions pénales (par exemple 5 ans de prison et 300 000 euros d'amende pour une collecte de données personnelles par un moyen frauduleux, déloyal ou illicite) et des sanctions administratives et financières de la part de la CNIL.

Les menaces d'interconnexion : une inquiétude qui se répand

Se montrer pour être visible, sans en pâtir

Un des enjeux de l'identité numérique, outre sa très grande visibilité, est que de nombreuses données personnelles sont collectées, puis traitées sans même que l'individu concerné n'en soit informé. Ignorant l'existence même d'un traitement de données, ce dernier ne peut pas exercer ses droits d'opposition ou de suppression. Certes, les 27 CNILs européennes, réunies au sein du *groupe de travail Article 29* sur la protection des données, ont estimé à l'unanimité qu'une durée de conservation de 6 mois des données personnelles enregistrées par les moteurs de recherche constituait une durée raisonnable. Cette durée, considérée par certains comme trop longue a, de plus, du mal à être appliquée : elle est contestée par Google, seul parmi les trois moteurs de recherche majoritaires à conserver les données 9 mois (au lieu de 18 mois initialement).

L'une des caractéristiques de l'univers numérique est de laisser des traces, ce qui ne convient pas à chacun. De très nombreux internautes se retrouvent ainsi piégés par les ragots, les textes ou les photos qui traînent sur Internet : un vieux blog d'étudiant, une photo de soirée arrosée. Grâce à des outils en ligne sophistiqués, comme des moteurs de recherche spécialisés dans la recherche de personnes, ou des métamoteurs de recherche ou d'agrégation de conversations sur ce qui se dit sur les réseaux sociaux, les blogs, les actualités, les vidéos et les tags (www.samepoint.com ou www.whostalkin.com par exemple), il est devenu très facile de compiler en quelques minutes la vie numérique d'une personne. Début 2010, le site de réseau social Facebook ne prévoyait toujours pas de bornage pour la rétention des données de connexion de ses utilisateurs, alors que des campagnes étaient en cours pour la limiter à 18 mois.

Quelle est la nature de nos identités plurielles ?

Pendant combien de temps une donnée personnelle peut-elle être stockée ?

Aucun texte juridique ne définit de durée de conservation standard ou se réfère à un « droit à l'oubli ».

La loi Informatique et libertés prévoit simplement que « *les données personnelles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées* ».

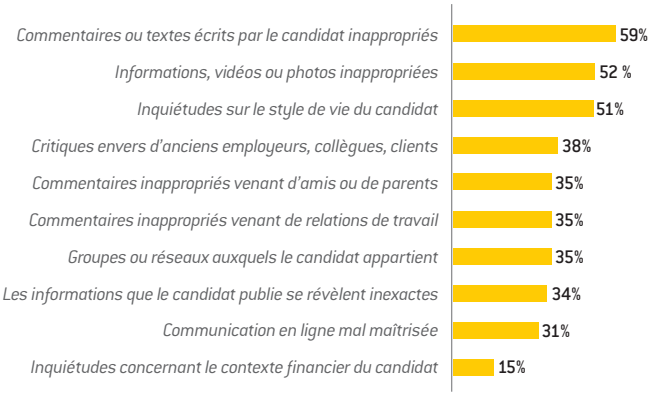
Il appartient au responsable de traitement de fixer lui-même cette durée en fonction des caractéristiques de son traitement. Par exemple, la CNIL préconise que les données prospects ne soient conservées que pour la durée nécessaire à la réalisation des opérations de prospection, soit 1 an maximum après le dernier contact ou sans réponse après deux sollicitations successives.

Les défis de l'exposition de soi

L'exposition de soi est un risque qu'on recherche devant les amis, les collègues, la famille, les amants, les voisins... Sur un réseau saturé d'informations, l'exhibition curieuse et personnelle est une condition de la visibilité. Se montrer en se démarquant est devenu une condition de l'attractivité. Dès lors, et justement parce qu'il est souvent minimisé, le risque existe : risque de rencontrer un prédateur sexuel, risque de la liberté d'expression, comme pour ces étudiants dont les propos ont conduit à leur exclusion de l'université, ou risque des crises de réputation, quand des recruteurs ont refusé des candidats après consultation de leurs pages dans des réseaux sociaux en ligne. Le monde du travail met ainsi en exergue deux situations dans lesquelles une mauvaise gestion de l'exposition de soi s'avère préjudiciable.

Le cas du recrutement

De nombreuses personnes disent avoir des difficultés à trouver ou retrouver un emploi parce qu'elles se retrouvent stigmatisées par un passé conservé sur Internet et qui devrait légitimement faire l'objet d'un oubli ou d'une amnistie : que penser par exemple de tel entrepreneur qui a fait un jour faillite, est depuis lors passé à autre chose avec succès, mais qui voit toujours son nom accolé sur le Web à cet épisode de sa vie? Ou de ce jeune issu d'une école de commerce, inséré sur le marché du travail, mais confronté à des images accusatrices parce qu'il était amateur de soirées arrosées ?



Raisons pour lesquelles les entreprises américaines rejettent des candidatures.
Source : http://dataprivacyday2010.org/

Certains cabinets de chasseurs de tête (comme Altaïde, cabinet de conseil en recrutement actif dans le secteur des technologies de l'information) pratiquent désormais ce que l'on appelle le recrutement 2.0, directement sur les réseaux sociaux et les blogs.

Il n'est plus un recruteur qui n'aille désormais étudier le « profil 2.0 » d'un candidat. Dans un pays comme les USA, 70 % des gens à la recherche d'un emploi postulent par Internet. Une étude récente a révélé que la moitié d'entre eux n'étaient pas retenus à cause d'une mauvaise réputation virtuelle. Cela a entraîné le développement de « services de gestion de l'identité numérique ».

Le cas du licenciement

L'utilisation des données provenant de l'identité numérique d'un salarié peuvent également conduire à son licenciement. Une salariée a ainsi été licenciée par son employeur suisse pour avoir utilisé Facebook durant son congé maladie. Selon ce dernier, étant en arrêt maladie pour cause de migraine, avec obligation de rester dans le noir, elle ne pouvait se retrouver devant son écran. L'employeur n'ayant pas apprécié de la voir se connecter sur son compte Facebook, l'a licenciée.

Que ce soit sur ces cas extrêmes qui ont fait parler d'eux en 2009, ou pour bien d'autres situations, il est devenu essentiel de se donner les moyens de maîtriser son identité numérique pour éviter toute mauvaise surprise. Ce contrôle passe avant tout aujourd'hui par une prise de conscience, par l'information et l'éducation des personnes, et par la mise en place de politiques de confidentialité des données à caractère personnel par les principaux acteurs concernés.

La gestion de la notoriété

Le contrôle réalisé par chacun, de manière autorégulée

L'exposition de soi sous un mode personnel et singulier est devenue une opportunité de connexion, une manière de faire du lien en produisant un commentaire admiratif ou amusé. Dès lors, il est difficile de s'autoréguler et de savoir à quel seuil le dévoilement devient une impudeur. Beaucoup d'utilisateurs doivent gérer eux-mêmes cette tension. Ils le font souvent de manière rusée, en utilisant l'*allusion*, le message plein de sous-entendus incompréhensibles pour ceux qui ne sont pas proches. L'information est indexicale, enveloppée dans le contexte relationnel. D'autres n'ont pas cette prudence, et des Skyblogs ont défrayé la chronique parce qu'ils ont par exemple exhibé des comportements « à risque » de jeunes filles « aventureuses en ligne ». Devant la demande d'exhibitionnisme, il y a une éducation à la prudence à trouver, à construire. À cet égard, la proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique prévoit une initiation aux dangers de l'exposition de soi et d'autrui dans les programmes scolaires.

Un exemple de cette autorégulation est la manière dont chaque utilisateur d'un réseau social doit trouver ses propres repères dans l'exercice de son droit à l'image. La fonction qui permet de marquer une personne sur une photo peut par exemple s'avérer réellement gênante. Contre ses effets potentiellement délétères sur l'image, on peut empêcher les autres d'accéder à l'image, en modifiant les « paramètres de confidentialité ». Mais la photo reste tout de même en place, et si quelqu'un regarde les photos de l'ami qui a tagué, il pourra se reconnaître, ce qui peut être un petit drame.
Dès lors, il peut s'avérer utile de vouloir faire supprimer la photo. Pour cela il faut copier l'adresse de la photo telle qu'elle apparaît dans le navigateur, cliquer sur *Signaler cette photo* en bas de la photo, et exiger au nom du droit à l'image le retrait de la photo du site, en remplissant un formulaire automatique. Après soumission de la notification, en quelques jours la photo est effacée, et la personne en reçoit la confirmation.

Il est parfois nécessaire d'agir pour un tiers non présent dans le réseau social pour signaler un contenu (ici un profil abusif).

Le Web 2.0 et sa pratique poussent à dévoiler plus de soi qu'on ne le ferait d'ordinaire, et les internautes doivent s'autoréguler.

Le comportement le plus central (« show-off », crâneur), révèle une caractéristique originale : on se montre avec ses amis, on fait le clown et la fête, on est cool et décontracté, mais c'est en réalité une image très travaillée et contrôlée pour paraître le plus naturel possible. Et cela s'accompagne d'une vie active et sociale plutôt intense facilitant la narration permanente de son identité.

L'utilisation de l'image d'une personne

Droit à l'image : toute personne physique, quelle que soit sa notoriété, dispose sur son image et sur l'utilisation qui en est faite d'un droit exclusif et peut s'opposer à sa reproduction et diffusion sans son autorisation.

Droit à la protection des données personnelles : une image représentant une personne physique est une donnée personnelle qui peut de surcroit être associée à d'autres données personnelles contenues dans le marquage. Le *Groupe Article 29* recommande que les réseaux sociaux conseillent à leurs utilisateurs de ne pas mettre en ligne des photos ou des informations concernant d'autres personnes sans le consentement de celles-ci.

Un marché stratégique : les services de gestion de la réputation en ligne

Face à la prolifération de traces non désirées, de nombreuses petites sociétés, comme la société suisse WnG Solutions ou la société britannique Garlik, en Europe, se sont positionnées pour proposer des services de gestion de réputation. Elles couplent un service, sur abonnement, de veille, et des prestations essentiellement de déréférencement. Leurs clients reçoivent un rapport hebdomadaire établi à partir de pages Internet, de documents publics et de bases de données commerciales ou autres. Certaines proposent un service d'évaluation de la réputation numérique, comme Qdos, qui mesure la présence d'un individu sur la Toile, à partir de critères tels que son niveau d'activité en ligne.

Aux États-Unis, pays où ces questionnements sont les plus avancés, des sociétés comme ClaimID se sont constituées pour « nettoyer » les traces. Le leader mondial en la matière, la société californienne Reputation Defender, a été fondée en 2006. Surnommée la « Google insurance », elle emploie déjà 70 personnes et son modèle d'affaire est l'abonnement. Par une habile politique de discrimination tarifaire, cette société, qui utilise un moteur de recherche maison, a constitué deux créneaux de clientèle. Une clientèle « professionnelle », émanant d'entreprises ou d'organisations soucieuses d'améliorer leur image sur le réseau, ou de professionnels libéraux voulant contrôler en temps réel leur notoriété numérique, est prête à payer des prestations en dizaine de milliers de dollars. Une clientèle de particuliers bénéficie par ailleurs de prestations à moindre coût pour quelques dizaines de dollars par mois : elle est constituée de parents souhaitant contrôler la réputation de leurs enfants dans la perspective de favoriser leur insertion sur le marché du travail, ou de consommateurs soucieux de protéger leur vie privée.

Comme il est souvent difficile de faire retirer le contenu qui pose problème, car les sites de contenu sont souvent peu coopératifs, la gestion de réputation repose sur la méthode consistant à cacher les contenus posant problème derrière des éléments positifs sur la personne. Les internautes ne s'arrêteraient en effet, dans la grande majorité des cas, qu'aux dix premiers résultats qui apparaissent dans Google. Il s'agit donc de créer de nouveaux contenus positifs cette fois, par exemple sur des plateformes sociales ou des réseaux professionnels comme Linkedin, et d'utiliser des outils élaborés qui améliorent le référencement de ces nouvelles informations et les font passer en tête.

Des acteurs dominants utilisent leur situation d'intermédiaire incontournable pour se lancer sur le marché de la gestion de réputation. Google, par exemple, a lancé en 2009 un nouveau service, baptisé *Google Profiles*. Il s'agit d'une page de type carte de visite, avec coordonnées, biographie, liens vers blogs ou profils de réseaux sociaux (LinkedIn, Viadeo, Facebook, etc.), comptes photos, partage de vidéos... voire vers un CV formalisé (Doyoubuzz par exemple). Ils sont parfois doublés par des francs-tireurs, qui mettent en place des indicateurs quantitatifs permettant

Vie privée et données à caractère personnel : 2 droits, 2 façons de protéger l'utilisateur

Le droit à la vie privée correspond à la protection d'une zone privilégiée propre à chaque personne. Cette zone se compose à la fois du **secret de la vie privée** entendu comme une retraite avec le conjoint et les enfants au domicile, siège privilégié de la vie privée et de l**a liberté de la vie privée** conçu comme la sortie de cette retraite pour développer sa personnalité physique, intellectuelle, morale ou spirituelle.

La protection des données personnelles entend protéger l'individu de façon préventive par rapport à un risque précis, celui lié à l'usage des technologies de l'information. Si elle protège la vie privée, elle consacre d'autres libertés (libertés d'expression, de crédit, de logement, etc.) et la non-discrimination. Cet objectif est atteint en limitant les activités de traitement des données personnelles et en permettant à la personne de maîtriser la circulation de son image informationnelle, notamment son identité numérique.

Cet objectif explique que dans l'approche européenne les données personnelles ne constituent pas de simples valeurs marchandes. Elles sont régies par des règles de droit public dont le but est la protection des libertés et de manière plus essentielle la dignité humaine.

La directive « Protection des données » reconnaît le droit pour toute personne de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, tels que son rendement professionnel, son crédit, sa fiabilité, son comportement, etc.

le calcul de réputation. L'entreprise Venyo, par exemple, souhaite mettre en place un indice multi-plateforme pour évaluer une réputation, indice exposé ensuite par l'internaute sur son propre site web. Mais, avec des projets comme celui de Venyo, le score de réputation serait généralisé sur l'ensemble des activités sur Internet, et franchirait les limites d'une plateforme sociale donnée.

Ces projets reposent sur l'objectif de demander aux connaissances de chaque individu de lui attribuer des notes de réputation qui chiffrent la confiance qu'on peut lui accorder. Le principe repose sur l'évaluation par la communauté du Web c'est-à-dire sur « la sagesse de la foule ». Ces indices sont évolutifs, et généralement conçus pour éviter les biais introduits par la connaissance réflexive.

Le calcul des scores de réputation : un algorithme délicat

Certes, des scores de réputation sont déjà calculés sur des sites spécialisés, comme celui du facilitateur de transactions entre particuliers eBay, qui demande aux vendeurs et aux acheteurs de s'attribuer mutuellement des notes qui chiffrent la confiance qu'on accorde au partenaire une fois la transaction conclue. Depuis septembre 2007, Wikipedia allemand affecte à ses contributeurs des « indices de confiance ». Seuls les contributeurs de « confiance » voient leurs corrections immédiatement visibles. Ces indices de confiance sont fondés sur l'historique des interventions : les contributeurs enregistrés et anciens sont privilégiés, et notamment ceux dont les contributions sont robustes aux rectifications ultérieures.

Le calcul d'un score est complexe car l'indicateur doit parer les principaux détournements liés à l'anticipation que font les acteurs des conséquences de leur activité sur l'évolution de leur propre score de réputation. Ainsi, les études de gouvernance des communautés en ligne ont mis en évidence que des dispositifs appropriés de contrôle des évaluateurs doivent être mis en place pour éviter la crainte de représailles. Sur eBay, par exemple, *les acheteurs craignaient les représailles de vendeurs, qui notent en second ; de ce fait, il s'était introduit un « biais gentil » par lequel de nombreux acheteurs préféraient ne pas laisser d'évaluation négative ou neutre lorsqu'ils ont eu une mauvaise expérience, par crainte de recevoir en retour une évaluation négative du vendeur.* La connaissance réflexive du calcul de l'évaluation aboutit à un biais. Dès lors, pour corriger cet effet de réflexivité, depuis mai 2008, ont été interdites les évaluations négatives ou neutres aux acheteurs. De même, le site de nouvelles Slashdot repose sur un contrôle des évaluations apportées par les membres les uns sur les autres : il introduit des « métamodérateurs ». Si un membre a ses modérations notées comme inéquitables, il voit aussitôt décroître le nombre de points qu'il peut utiliser pour son pouvoir de modération. Le système est autorégulé, au sens où les métamodérateurs sont recrutés parmi les modérateurs ayant le score le plus élevé.

Chacun est devenu entrepreneur de sa notoriété

Ce sont désormais les internautes eux-mêmes qui se font les entrepreneurs de leur notoriété. Chacun doit s'autopromouvoir ou veiller à faire lui-même sa communication en étant visible aux endroits stratégiques de ses réseaux de relations. Dans une sphère d'information marquée par la difficulté par chacun de capter l'attention, cette obligation de « soigner son image » peut être vécue sur le mode du malaise par les personnes. Jean-Samuel Beuscart a particulièrement travaillé ce malaise de la notoriété auprès des jeunes artistes amateurs qui déposent leurs créations sur les plateformes comme Youtube ou Myspace. Cette dernière, en obligeant chaque membre à gérer stratégiquement ses listes d'amis et de « meilleurs amis », en fonction de leur facteur d'impact ou des retombées attendues sur leur propre visibilité, transforme chaque individu en gestionnaire de sa notoriété, créant une tension entre inspiration et plan. Cette tension peut être racontée sur le mode du *dégoût* de soi-même (le créateur a le sentiment de vendre son âme ou de se « prostituer ») ou du *scrupule* (le créateur a le sentiment d'être un hypocrite, parce que, pour garder ses amis, il s'autolimite dans les commentaires négatifs). Ce *malaise identitaire* est caractéristique de notre culture occidentale de la reconnaissance et de la valorisation de l'expressivité individuelle.

Des outils aident les internautes à fabriquer des CV originaux ou clairs. Ainsi, la plateforme DoYoubuzz permet d'agréger des vidéos, des transparents, aux formats traditionnels (format imprimable PDF), et de le diffuser en ligne, en l'intégrant par exemple dans le profil Facebook ou en le transformant en un véritable site web avec un nom de domaine personnalisé. Mais surtout, beaucoup de jeunes désormais sur le marché du travail utilisent les fonctionnalités de recommandation. Ainsi, le service numéro 1 de réseau social professionnel LinkedIn, utilisé par plus de 38 millions de professionnels dans 120 pays, a noué un partenariat avec l'Apec. Les cadres peuvent connecter leur compte Linkedin avec leur compte Apec sans quitter le site Apec. Cela leur permet d'identifier directement sur une offre d'emploi Apec les personnes de leur réseau Linkedin qui travaillent dans l'entreprise proposant le poste. Le système de recommandation permet de formaliser une référence professionnelle, une expérience réussie, un service rendu ou une compétence. Pour avoir du poids, une recommandation doit faire état du cadre de la relation (collègue, subordonné, employé, client, fournisseur...) et montrer en quoi ses compétences sont mises en valeur. Une recommandation crée de la valeur car elle implique la personne qui donne son avis. Les recommandations donnent ainsi une crédibilité au profil.

Compléments de lecture et références

Dana Boyd, « Friendster and Publicly Articulated Social Networks. » *Conference on Human Factors and Computing Systems* (CHI 2004). Vienna: ACM, April 24-29, 2004.

Pour une synthèse sur le design et la gouvernance des systèmes de réputation, cf. Auray, N., 2009, « Information communities and open governance: boundaries, statuses and conflicts », in E. Brousseau, M. Marzouki, C. Méadel (Ed.), *Governance, Regulations and Powers on the Internet*, – Cambridge University Press

Article 2 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée notamment en 2004.

Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Les avatars et les pseudos : l'emballement fictionnel des identités

Le réseau est certes devenu un lieu de sculpture de soi, mais les internautes ont parfois pris l'habitude d'exercer leur activité sous « *pseudonyme* » (rattachable à leur identité principale) ou dans l'*anonymat* (sous un « *alias* » non rattachable à leur identité principale). La personne en elle-même a ainsi souvent, dans ses pratiques de communication, trois identités numériques :

- une identité principale, adresse e-mail professionnelle ou familiale par exemple,
- une identité pseudonymique, nom de contributeur sur Wikipedia ou sur eBay par exemple,
- des « alias » pour se livrer à des activités sous masque et condition d'anonymat.

Sur Second Life, 30 % des gens en moyenne changent de sexe.

Certains avatars ressemblent à leur incarnation réelle : William Gibson (*Neuromancien*) et son double

Dans l'hindouisme, un avatar est l'incarnation d'une divinité sur Terre. Certains sont des avatars complets, d'autres des incarnations partielles, ou encore des manifestations de certains aspects du divin.

Ces *avatars* sont pourtant aussi des identités numériques car ils constituent autant d'expressions des pensées, angoisses, mythes et rêves d'un individu. Il s'agit de personnages virtuels, définis, programmés, et néanmoins structurés par une personne réelle en arrière-plan. Ils constituent des sortes de « lanternes magiques » où se peaufine l'image du moi, de manière oblique et parfois en empruntant des chemins opaques. C'est en s'inventant une « seconde vie » par la socialisation virtuelle de ses identités fictives que l'individu pourra trouver son chemin ou « libérer son enfant intérieur », enfoui sous les contraintes de la vie sociale réelle.

Comment créer et utiliser légalement un pseudo et un alias ?

Choisi librement, le pseudo ou l'alias doit respecter l'ordre public (ne pas refléter des propos antisémites, racistes, négationnistes, diffamants, etc.) et les droits de propriété intellectuelle des tiers. Il n'est pas possible d'opter pour une marque si ce choix porte atteinte à un droit antérieur, notamment au nom patronymique d'une personne, à son pseudo ou à son image. Une fois choisi, le pseudo s'inscrit dans le commerce juridique : il peut être loué, vendu et faire l'objet de toute opération, payante ou non.

Avatar et propriété intellectuelle

L'avatar est une représentation graphique, le plus souvent en 3D, d'un personnage, dont le maître est propriétaire au titre du droit d'auteur (si l'avatar est original), du droit des marques ou du droit des dessins et modèles. Dans ce dernier cas, l'avatar peut être déposé à l'INPI (Institut National de Propriété Intellectuelle), comme les personnages de jeux vidéo.

Le choix de l'avatar obéit aux mêmes règles que celles qui s'appliquent aux pseudo et alias.

Responsabilité des avatars

À l'instar du propriétaire d'un animal, le propriétaire d'un avatar est responsable des « actes » de ce dernier si son imprudence ou sa négligence, par exemple la divulgation de ses identifiant et mot de passe, permettent à un tiers de s'accaparer l'avatar. Dans tous les autres cas, la responsabilité est celle de la personne qui utilise l'avatar au moment des faits.

Les différences sociales dans la mise en scène de son avatar

Que montre-t-on de soi sur Internet ? Que cache-t-on ? Avec qui et comment faisons-nous connaissance sur Internet ?

Sociogeek est un jeu-enquête qui permet de se révéler son propre profil en choisissant des photos et des amis plausibles parmi un vaste corpus de situations :
http://www.sociogeek.com/

La façon d'animer les avatars est variée selon les origines sociales. Les internautes de milieu modeste mettent plus facilement leur corps en scène, jusqu'à la provocation, que les cadres ou les chefs d'entreprise. Les mêmes clivages se retrouvent lorsqu'il s'agit d'accepter ou refuser les demandes d'intégration du cercle intime. Là où les « modestes », les « traditionnels » et les classes sociales aisées restent prudents, les « provos », les « exhibitionnistes » et les classes sociales moins favorisées ouvrent largement leur cercle. Ce recours à la provocation et à la mobilisation plus immédiate de l'image du corps physique chez les catégories populaires va de pair avec une réduction de la palette des soi « virtuels » endossés : ceux-ci sont moins nombreux, correspondent à des comportements plus stéréotypiques, et sont formulés avec moins de mots. Le « soi virtuel » emblématique, pour les milieux modestes, est ainsi la figure du « fan », fan de musique populaire à la gestuelle répétitive et ritualisée, ou supporteur de club de football. Le « soi virtuel » des catégories dominantes, cadres supérieurs ou professions libérales, est plus narratif, plus singulier, et se détourne de manière plus forte des représentations du corps propre.

Les mineurs requièrent des impératifs de protection supplémentaires

En janvier 2009, sous l'impulsion de la Commission européenne (et notamment la *Social Networking Task Force*, un groupe de travail qui réunit des sites de socialisation, des ONG et des chercheurs sous l'égide du commissariat chargé de la Société de l'information et des médias), 17 sites de réseaux sociaux, dont Facebook et MySpace, mais aussi le monde persistant ciblant des enfants comme Habbo Hotel, ont signé un accord. Un absent est notable : la plateforme de blogs Skyblog. L'objectif de cette autorégulation est d'assurer la poursuite de la croissance des sites signataires en garantissant un certain niveau de protection aux jeunes internautes lorsqu'ils élargissent leurs réseaux et lorsqu'ils mettent en ligne leurs données personnelles.
Ainsi, les sites se sont engagés notamment à :

- placer sur leur site un bouton « Signaler un abus » ; accessible et simple d'emploi, il permet aux utilisateurs de signaler en un seul clic toute conduite et tout contact jugés inappropriés d'un tiers,
- veiller à ce que les profils et les listes de contacts des utilisateurs qui se sont déclarés comme mineurs soient privés par défaut, pour qu'il soit plus difficile pour des personnes mal intentionnées d'hameçonner ces jeunes internautes,
- s'assurer que les profils privés des utilisateurs mineurs ne soient pas accessibles, ni directement à partir du site, ni via les moteurs de recherche,
- garantir que les options de vie privée soient bien visibles et accessibles à tout moment, afin que les utilisateurs puissent facilement déterminer si ce qu'ils diffusent en ligne peut être vu par le monde entier ou par leurs amis seulement,
- empêcher les enfants trop jeunes d'utiliser leurs services : si un site de socialisation a pour cible les adolescents de 14 ans et plus, il doit être difficile pour un enfant plus jeune de s'y enregistrer.

L'usurpation et le forgeage d'identité

Les réseaux sociaux sont devenus des cibles privilégiées des voleurs d'identité. Construire un profil factice est aussi monnaie courante sur le réseau.

Fin 2008, le tribunal correctionnel de Dinan jugeait le cas d'un jeune homme s'étant fait passer pour un faux policier louant des voitures anciennes sur la Toile. Il a été condamné à deux mois de prison avec sursis assorti d'une obligation de soins. Une autre histoire a fait grand bruit début 2007 aux États-Unis.
Une blogueuse renommée dans la communauté des programmeurs a reçu des menaces de mort par blogs interposés, émanant d'un autre blogueur célèbre, habitué des forums de discussion en ligne, patron d'une société de création de sites web et animateur d'un blog collaboratif réputé chez les informaticiens. Or, il s'est avéré par la suite que ce blogueur avait lui-même été la victime d'une usurpation d'identité. Après avoir piraté son ordinateur et détourné ses comptes e-mail, un détraqué utilisait ses identifiants pour poster des menaces de mort et harceler sur son blog. Ayant du mal à démasquer l'agresseur, et à prouver qu'il n'était pas l'auteur, voyant sa réputation ternie dans toute la blogosphère, l'homme à l'identité usurpée a été contraint de fermer son blog, et finalement cesser de participer aux débats de la blogosphère. Il n'existe donc plus sur Internet. Un spammeur américain en 2008 a été condamné par un juge fédéral de Los Angeles à 230 millions de dollars de dommages et intérêts. Il avait créé plus de 11 000 fausses identités de membres du réseau social Myspace. Il avait aussi dérobé des mots de passe pour accéder aux pages personnelles de membres. Il a ensuite adressé en leurs noms des centaines de milliers de faux messages dans le but de promouvoir des sites pornographiques et casinos en ligne…
L'**usurpation d'identité** est une pratique ancienne qui atteint une autre échelle sur Internet. « Dans le monde réel, l'identité est un système composé d'identifiants, d'un registre qui recense ces identifiants (le registre d'état-civil) et de titres d'identité délivrés sur la base de ce registre (carte nationale d'identité…). La gestion de l'identité est assumée par l'État. Ce système est totalement absent d'Internet : l'identité y est éparpillée, inscrite dans des mégabases de données qui s'échangent dans l'illégalité la plus complète », souligne l'avocat Olivier Itéanu. Internet a, par ailleurs, engendré ses propres techniques d'usurpation d'identité, comme le phishing ou hameçonnage, consistant à obtenir les identifiants d'une personne, en se faisant passer pour un individu, une entreprise ou une autorité publique : il est en effet plus simple de créer un faux site bancaire qu'une fausse agence bancaire dans la rue d'une ville.
Le **forgeage d'identité** est une pratique dont les modalités sont variables. Il peut consister à emprunter ou « voler » des identités déjà existantes, puis les vivre, et ainsi causer un préjudice à leur détenteur qui se retrouve trahi. Il peut reposer sur l'invention d'une identité fictive, par l'endossement d'un rôle comme celui de policier ou d'avocat. Le forgeage peut aussi être animé plus ou moins directement par le motif d'escroquer, et dans certains cas uniquement causer un abus de confiance. Ainsi, un des domaines les plus courants du forgeage d'identité sur Internet est celui de la construction de *fakes*, qui consistent à créer des profils attractifs (par exemple des clones de gens célèbres) sur les sites de réseaux sociaux pour instrumentaliser leur notoriété.

Manipuler sa réputation en ligne : le cas Essjay

L'usurpation d'identité peut aussi reposer sur une simulation complète de celle-ci, ou plus modestement sur une déformation limitée à quelques segments biographiques, comme le diplôme. Cela est bien montré à travers l'exemple de Essjay.

Essjay était un contributeur très actif sur Wikipedia. Il se présentait comme « un professeur d'études religieuses doté de doctorats en droit et en philosophie », alors qu'en fait il était un jeune homme de 24 ans dépourvu du moindre diplôme. Mais arrivait-il vraiment à tricher : ses actes ne trahissaient-ils pas déjà son être supposé ? Au cours d'une discussion sur l'usage du terme « imprimatur » dans la religion catholique, par exemple, il défendit son utilisation du livre *Catholicism for Dummies* en déclarant : « J'exige souvent que mes étudiants lisent ce livre, et je gagerais volontiers mon doctorat sur sa crédibilité ».

L'inlassable activité d'Essjay lui avait permis d'accéder à presque tous les niveaux de responsabilité existant dans Wikipédia. Il était si bien considéré qu'il fut mis en avant pour être interviewé en vue d'un article sur l'encyclopédie dans le prestigieux magazine The New Yorker. On lui proposa également un poste de directeur communautaire (*community manager*), ou modérateur, au sein de Wikia, l'organisation à but lucratif lancée par Jimmy Wales en 2004.

La découverte de l'imposture fut à l'origine de diverses propositions pour mieux gérer la vérification des références permettant de juger de la qualité des auteurs dans Wikipédia.

Comment le droit français réglemente-t-il l'usurpation d'identité ?

Selon une enquête de novembre 2009 du Credoc, le Centre de recherche pour l'étude et l'observation des conditions de vie, plus de 210 000 français sont victimes chaque année d'une usurpation d'identité dont le coût moyen s'élève à 2 229 euros.

Or, comme dans la plupart des pays européens, l'usurpation d'identité n'est pas sanctionnée en tant que telle en France ; seules le sont les conséquences de l'usurpation, si et uniquement si elles entraînent des poursuites pénales : diffamation, escroquerie, faux, spam, contrefaçon de marque, délit d'accès frauduleux à un système d'information, etc. C'est pourquoi le projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI 2) qui devrait être adoptée en 2010 propose de sanctionner « *le fait d'utiliser, de manière réitérée, sur un réseau de communication électronique l'identité d'un tiers ou des données qui lui sont personnelles, en vue de troubler la tranquillité de cette personne ou d'autrui* » d'un an de prison et de 15 000 euros d'amende.

Aux États-Unis, le vol d'identité est puni de deux ans de prison et, au Royaume-Uni, de dix ans de prison.

Technologies de l'identité numérique

Les utilisateurs de services en ligne ou d'applications informatiques recherchent de la valeur dans leurs activités : ils doivent pouvoir faire confiance dans les technologies et techniques qui leur sont offertes et dans les acteurs qui les fournissent ou les maintiennent.

Qu'est-ce que l'identité dans un système informatique ?

❶ De manière très générique, on décrit l'*identité* comme l'*existence* d'une *entité* pour une autre, cette existence pouvant être traduite sous une forme quelconque.

Dans le monde numérique, une entité sujet, respectivement, objet, d'un processus informatique, revêt, respectivement, se voit associée, une identité au sein de ce processus.

Enjeux de la gestion des identités numériques

La numérisation de l'information a conduit à une société de l'information où la masse de données disponibles n'importe où et en tous temps est de plus en plus importante. Cette société a atteint de nos jours une étape de développement caractérisée par la génération, la collecte, l'analyse, le traitement et l'échange d'une quantité importante de données personnelles, stockée potentiellement pour une durée indéterminée. Et très rapidement la création ainsi que la gestion des identités sont apparues comme de grands défis à relever.

Plus particulièrement, une gestion en toute confiance et toute sécurité des identités est essentielle. En effet, la création de services novateurs et compétitifs pour réaliser les objectifs de l'économie numérique, pour encourager les investissements, la croissance et l'emploi ne peut se faire avec succès que si elle se fonde sur la protection de la vie privée. Et donc sur l'utilisation de mécanismes d'authentification sûrs pour éviter les abus et la malveillance, et permettre l'imputabilité, la désignation et la qualification des responsabilités.

Les caractéristiques numérisées relatives à la personne sont en train de changer progressivement la façon d'identifier les personnes et gérer les relations entre elles, notamment les interactions virtuelles, à travers l'Internet par exemple. Comme le réseau public a ouvert de nouveaux espaces de vie, des identités numériques nouvelles, appelées identités virtuelles, ont émergé. Elles l'ont fait entre autres pour des raisons de transactions à but lucratif, d'entraide ou de sécurité. L'apparence physique d'un individu est devenue aujourd'hui aussi virtuelle qu'un compte d'un utilisateur sur un serveur web, une adresse e-mail ou le numéro d'un téléphone mobile. Ces identités virtuelles et multiples et les nouveaux processus développés pour les gérer défient la notion d'identité classique telle que nous la connaissions.

La crise de la gestion des identités numériques et des accès

❷ On distingue un premier *aspect fonctionnel* de l'identité, celui du référencement et de la description. L'identité numérique est ainsi un ensemble de données que l'on peut désigner par un *identifiant*, une valeur unique dans l'espace des valeurs servant à l'identification des identités pour un système. Lorsque l'identité représente un individu, une partie de la description peut être faite par des *attributs* le décrivant. Ce sont les attributs d'identité qui constituent le *profil* de l'individu. Autrement dit c'est une *représentation informatique* d'une entité.

Des bribes de l'identité de l'utilisateur, de l'abonné, du client, peu importe le qualifiant, sont éparpillées dans les réseaux et les systèmes d'informations des banques, des entreprises d'assurance ou de télécommunications, des agences gouvernementales, des fournisseurs internet, des réseaux sociaux, et la liste ne cesse de s'agrandir avec le temps. L'utilisateur est parfois amené à gérer une liste importante de mots de passe nécessitant énormément de coordination. C'est à lui de se souvenir de ces multiples logins / mots de passe et de tenir à jour les diverses informations sur son profil dans les différents sites web. Souvent, il manque voire perd le contrôle sur ses identités et se sent perdu devant l'hétérogénéité des systèmes d'authentification et d'autorisation ; ce qui l'amène à préférer utiliser toujours le même couple de login / mot de passe sur chaque site. Il va sans dire que cela conduit bien évidemment à une diminution de sa sécurité.

Comment le droit encadre-t-il l'utilisation d'un mot de passe ?

L'accès à son identité numérique passe par un identifiant et un mot de passe, qui protège cette identité.

Confidentiel, le mot de passe doit respecter les règles de sécurité définies en octobre 2009 par la CNIL. Il doit comporter au minimum huit caractères incluant chiffres, lettres et caractères spéciaux, être modifié dès la première connexion par l'utilisateur et être renouvelé fréquemment, par exemple tous les 3 mois. En cas de non-respect à ces obligations, et notamment de négligence en laissant le mot de passe en évidence à côté de l'ordinateur, la personne engage sa responsabilité si son manquement cause un préjudice à un tiers, comme une escroquerie.

❸ L'identité possède un deuxième aspect fonctionnel inhérent à l'entité interagissant avec un système. Celle-ci peut obtenir un ensemble de droits auprès du système, qui se traduisent en pratique par des autorisations d'accès à des données et des processus contrôlés par le système. L'entité se voit alors associée une identité numérique dès lors que l'accès est autorisé.

Il est courant que cet accès soit soumis au fait qu'une entité ait à emprunter une identité numérique déjà existante sur le système. L'entité doit donc établir une identité existante généralement à l'aide d'une preuve. L'identité existante permet donc à une entité de l'*emprunter* afin d'exercer un ensemble de droits qui lui sont associés. Il est notamment possible qu'une entité puisse revêtir une identité distincte sur différents systèmes, ou plusieurs identités sur un même système.

De leur côté, les organisations possèdent, pour la plupart, plusieurs fichiers d'identités et de droits d'accès, souvent un fichier pour chaque système / application. Ceci crée des difficultés de gestion notamment lorsque les utilisateurs ont des combinaisons différentes de login et mot de passe pour chaque système / application. Cette complexité augmente d'autant plus que, maintenant plus que jamais, les technologies de l'information doivent répondre aux exigences économiques grandissantes et implanter rapidement et efficacement de nouveaux processus métier, souvent au-dessus d'applications existantes, qui doivent systématiquement être sécurisés. Il est alors difficile de garder une cohérence et d'avoir une vue d'ensemble sur les droits d'accès aux différents services offerts. La gestion de l'ensemble du système devient complexe pour l'administrateur et est source d'erreur souvent grave de conséquences.

La collaboration entre organisations est une autre source de complexité. Il s'agit d'appliquer des politiques de sécurité à travers des organismes multiples tout en...

- maintenant confidentielles les données personnelles,
- réduisant les coûts,
- rendant l'authentification et l'autorisation portables et réutilisables à travers les grands réseaux de fournisseurs dans lesquels des identités peuvent être possédées par des partenaires externes,
- rationalisant la navigation entre les applications internes et celles hébergées par les partenaires,
- et respectant la politique de sécurité de chaque organisation, et les contraintes de confidentialité liées à l'expression de ces politiques.

Une réponse : la fédération d'identités

❹ L'établissement d'une identité n'est pas toujours un pré-requis à des accès autorisés auprès d'un système. En effet, l'un des enjeux de la gestion des autorisations est de permettre un accès à une entité préalablement inconnue. Ainsi, une identité peut être créée dynamiquement lors d'un accès ou préalablement à celui-ci, par exemple via la création d'un *pseudonyme*.

La création d'une infrastructure de fédération d'identité (FIM : *Federated Identity Management*) est une solution viable pour les systèmes centralisés. Elle comprend les technologies, les normes et les cas d'utilisation qui permettent la portabilité des informations relatives à l'identité dans des domaines de sécurité autonomes. L'objectif ultime est de permettre à des utilisateurs d'un domaine d'accéder de façon sécurisée à des données ou à des systèmes d'un autre domaine sans problème, et sans besoin d'administration complètement redondante et superflue d'utilisateurs.

Contrairement à une approche fédérée, une gestion centralisée des identités telle que pratiquée dans les systèmes actuels reste confinée aux utilisateurs internes de l'entreprise. Il n'est pas souhaitable, par exemple, de créer un compte dans le système d'information pour un collaborateur extérieur à l'entreprise, car cela pourrait lui donner accès à d'autres ressources de ce système d'information. Ce type de gestion devient rapidement empirique et complexe lorsque l'authentification sort du cadre intra-organisationnel.

Le système de gestion centralisé des utilisateurs n'est pas non plus adapté à la nature des services web largement déployés de nos jours, qui sont par définition distribués et qui nécessitent des identités qui soient :

- *fédérées*, car pour de nombreux utilisateurs, la vue d'une simple page de création de compte, nécessitant l'introduction d'un certain nombre d'informations souvent personnelles, reste un frein. La plupart des utilisateurs, lassés, rechignent à renseigner ces formulaires,
- *interopérables*, de manière à pouvoir s'échanger des informations sur les utilisateurs,
- *mobiles*, les utilisateurs pouvant aller de site en site sans devoir remplir un nouveau formulaire.

De plus, en absence de fédération, le système de gestion d'identité stocke les informations d'authentification dans un seul serveur. Celui-ci devient de ce fait le point faible du système d'authentification. Il suffit qu'un agent malveillant prenne le contrôle de ce dernier pour compromettre tout le système d'information. Même si le risque de prise de contrôle de la FIM ne doit pas être négligé, les mécanismes de protection de la FIM fournissent un niveau d'assurance supérieur comparée à la gestion distribuée.

Collaborateurs : **membres du cercle de confiance qui peuvent fournir ou consommer des services.**

Le principe de la FIM est que l'accès soit accordé à un utilisateur dès lors qu'un collaborateur s'en porte garant, tout en sachant que la majorité des fuites passent par une complicité interne, un collaborateur garant n'apporte pas beaucoup de confiance. Chaque collaborateur a, par ailleurs, spécifié la politique d'accès aux différents services et applications. La FIM rend ces informations disponibles aux fournisseurs de service sur demande, en ligne et dans des délais raisonnables. Ainsi, l'actualisation et la qualité des données s'en trouvent améliorées en comparaison de celles obtenues lorsque les données d'identité sont maintenues par chaque utilisateur et dans plusieurs endroits.
La FIM augmente la sécurité pour plusieurs raisons. Tout d'abord, la mise à jour des politiques d'accès et d'usage est répertoriée sur l'ensemble des offres de services des différents collaborateurs de confiance. Ensuite, les comptes externes des utilisateurs sont automatiquement supprimés dès lors que ces utilisateurs ne sont plus garantis par l'un des collaborateurs. Elle réduit par ailleurs les coûts et la redondance, les organismes n'ayant plus besoin d'acquérir, stocker et maintenir des politiques d'autorisation sur tous les utilisateurs liés à leurs collaborateurs. Enfin la FIM améliore la protection des données personnelles, en ayant recours à des solutions qui, tout en étant compatibles avec la réglementation américaine (Sarbanes Oxley, HIPAA, GLBA), assurent que seules les données nécessaires à l'utilisation du service offert sont communiquées aux différents collaborateurs.

Données personnelles aux États-Unis

La loi **Sarbanes-Oxley** impose aux entreprises d'organiser une procédure d'alerte permettant aux salariés de dénoncer les pratiques illicites en matière comptable ou financières au sein de l'entreprise. L'organisation de ce système de *whistleblowing* (ou de « coup de sifflet ») par les filiales françaises de sociétés américaines durant l'année 2005 a conduit la CNIL à en préciser les modalités de mise en œuvre.

L'Health Insurance Portability and Accountability Act (HIPAA) réglemente la transmission électronique des données médicales. Il précise les obligations de sécurité, d'archivage, de standardisation et de confidentialité.

Le Gramm-Leach-Bliley Act (GLBA) supprime toutes les barrières entre les banques commerciales, les sociétés de placement et les compagnies d'assurances. Un titre entier porte sur la protection des données personnelles des clients des banques.

Vie privée, identité numérique et fédération d'identités

Avant de voir comment la FIM est mise en œuvre techniquement, plaçons-nous du point de vue de l'utilisateur.
Lorsqu'un individu communique, il s'expose au reste du monde. Pour autant, l'humain s'évertue généralement à ne présenter qu'un ensemble restreint des informations le concernant au monde extérieur selon le contexte ou l'interlocuteur. Chacun de ces ensembles restreints constitue l'identité visible de l'individu conformément à ses exigences. Comme les communications numériques ont permis la virtualisation de ces identités, l'identité numérique au sein d'un système n'est rien d'autre que la partie visible d'une identité. À l'instar du monde physique, une observation peut permettre de créer une identité sans que l'entité observée puisse en être consciente. À l'inverse, un utilisateur, pour se préserver, devrait pouvoir développer un ensemble d'identités distinctes qui ne seraient pas assimilables à une même entité.

Dans un environnement distribué, l'enjeu de la protection des données personnelles consiste en deux points essentiels :

- gérer la diffusion des informations d'identité,
- ne pas associer les multiples identités empruntées par une même entité avec ses activités entre différents systèmes.

L'interopérabilité recherchée et les avantages apportés par une gestion fédérée des identités nécessitent la convergence de ces identités pour véhiculer des informations de l'une vers l'autre. Des organisations, possédant des identités visibles distinctes d'une même entité, peuvent souhaiter échanger des informations sur ces identités. Cela revient à faire correspondre les identités, ce qui va à l'encontre des précautions liées au respect des données personnelles qui préconisent l'impossibilité d'associer ces identités. Il s'agit donc de mettre en œuvre des mécanismes permettant d'assurer les conditions de l'anonymat décrites précédemment. Autrement dit, l'*association des identités d'une même entité ne doit être possible que par l'entité elle-même*. Il s'agira également de permettre des interactions faisant intervenir de multiples organisations et identités visibles d'une entité, en offrant à celle-ci des moyens de diffusion de ses informations simples et contrôlables.

Cette protection des données personnelles dans le cadre fédéré est assurée par deux stratégies.

La confiance attribuée aux acteurs impliqués

Elle doit être expliquée, entretenue et garantie par des contrats établis entre les différents collaborateurs entre eux et avec les utilisateurs finaux. Concrètement, ce sont les échanges de *certificats* qui permettront l'établissement d'une relation de confiance. Cependant, il est difficile de déterminer le besoin de contrôle ou de confiance que chaque certificat permet de satisfaire. Il est alors plus correct de dire que les éléments présentés dans ces certificats visent à satisfaire des besoins de contrôle afin de pouvoir établir une relation de confiance.

L'anonymisation

C'est la possibilité donnée à l'utilisateur qui ne fait pas entièrement confiance au système de s'identifier via un pseudonyme qui, tout en le distinguant des autres, lui permet de masquer sa vraie identité. Ce pseudonyme devrait par ailleurs avoir une durée de validité, celle d'une session par exemple, qui assurerait une anonymisation efficace et qui évite ainsi le traçage des services qu'il a pu consommer. Concrètement, cela suppose des échanges de certificats et l'utilisation de schémas de *signatures* de ces *certificats* qui satisfont les propriétés précitées de non-associativité des transactions entre tiers ainsi que des identités.

Que signifie l'obligation (légale) de sécurité ?

« Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès » (Article 35 de la loi Informatique et Libertés). Le non-respect de cette obligation est sanctionné de 5 ans d'emprisonnement et de 300 000 euros d'amende.

En février 2008, la CNIL a condamné la Société VPC KHADR à 5 000 euros d'amende : son site internet permettait l'accès, via la rubrique « suivi de votre commande », à la liste nominative des commandes accompagnée de commentaires sur leur état de fabrication et leur règlement par le client concerné.

La proposition de loi modifiée visant à mieux garantir le droit à la vie privée à l'heure du numérique prévoit qu'en cas d'atteinte au traitement de données personnelles, le responsable du traitement avertit sans délai le Correspondant Informatique et Libertés (CIL), ou, en l'absence de celui-ci, la CNIL. Le CIL devra alors prendre immédiatement les mesures nécessaires pour permettre le rétablissement de l'intégrité et de la confidentialité des données et en informer la CNIL. Le responsable du traitement devra pour sa part en informer les personnes concernées.

Existe-il un droit à l'anonymat ?

Si aucun texte ne reconnaît expressément un « droit à l'anonymat », il est possible d'agir de façon anonyme à condition que cet anonymat ne serve pas de support à des activités illicites. On remarque d'ailleurs que l'anonymat est l'un des garants de la protection des libertés individuelles.

Pour autant, l'anonymat est relatif, toute action d'un individu créant en permanence des traces, aussi bien dans sa vie réelle (traces de téléphone mobile ou de déplacement) que dans sa vie virtuelle (adresse IP), susceptibles d'être identifiantes. Le droit encadre la conservation de ces traces : ainsi, les opérateurs de communications électroniques et les personnes dont l'activité est d'offrir un accès à des services de communications au public en ligne (par exemple une entreprise mettant un accès Wi-Fi à disposition de ses clients) ont l'obligation de conserver les données de trafic pendant un an pour les mettre, en cas de besoin, à la disposition des autorités judiciaires et policières.

Fédération d'identités : mise en œuvre / implémentation

La Fédération d'identités sous-entend la création de cercles de confiance (ou CoT pour *Circle of Trust*). Un CoT contient un ensemble d'entités fournissant des services et / ou des identités et / ou des attributs entre lesquels une relation de confiance a été établie et auxquels, après une authentification unique, l'utilisateur peut accéder librement de façon sûre, sécurisée, conviviale et la plus transparente possible.

La FIM nécessite également des moyens d'authentification. L'authentification est définie comme un ensemble de mécanismes et de protocoles permettant d'établir l'identité d'une entité, et inversement, permettant à une entité d'établir une identité auprès d'un système. Elle peut être *faible*, et ne reposer dans ce cas que sur un seul facteur (un mot de passe), ou *forte*, et plusieurs paramètres être alors nécessaires : ce que détient un utilisateur (un badge), ou ce qu'il est (une empreinte digitale). Les mécanismes d'authentification se fondent sur la notion de preuve qui peut être de *connaissance* ou de *possession*. De plus, et pour éviter à l'utilisateur de s'authentifier trop souvent, la FIM offre la possibilité de l'*authentification unique*.

La FIM nécessite enfin une architecture logicielle à couplage lâche pour l'échange d'informations sur les identités entre des systèmes hétérogènes.

Pour satisfaire les deux exigences précitées, plusieurs standards (Liberty, Shibboleth , *SAML* (*OASIS*), OpenId, Info Card, SXIP, voir pp. 20-21) et des implémentations (voir tableau ci-dessous) plus ou moins complètes existent qui permettent une authentification unique sécurisée intra et inter cercles de confiance, avec préservation de la vie privée.

Ces standards ont été précédés par la publication d'un livre blanc contenant une feuille de route pour le développement de la sécurité des web services, appelée WS-*. Établie conjointement par Microsoft et IBM, cette feuille de route décrit plusieurs modules qui ensemble devaient apporter une solution globale :

- WS-Security, un mécanisme pour attacher des tags de sécurité aux messages, y compris des tags liés à l'identité,
- WS-Policy, un langage de description de la politique de sécurité d'un web service,
- WS-Trust, un langage qui permet d'émettre et de valider des jetons de sécurité,
- WS-Federation pour orchestrer les interactions et permettre la fédération de différents domaines de sécurité.

Les différents consortiums de normalisation des protocoles de fédération d'identités ont travaillé à enrichir une des briques de base pour la mise en place de l'authentification unique : SAML. Ils semblent tous avoir adopté SAML 2.0.

Diverses implémentations de la fédération d'identités

Désignation	Description	Site
Enterprise Sign On Engine (ESOE) par *Intient*	Implémentation Java de SAML V2.0 Inclut le module de dérivation de politique XACMLv2-based	www.esoeproject.org
simpleSAMLphp, SAML V2.0 SP, SAML V2.0 IdP par *FEIDE research and development*	Implémentation PHP compatible avec Shibboleth 1.3 et 2.0 existence de passerelles inter-protocolaires (connecteur du fournisseur de service Shibboleth 1.3 à la Fédération SAML 2.0)	rnd.feide.no/simplesamlphp
Lasso - Liberty Alliance Single Sign-On par *Entr'ouvert*	Connecteurs disponibles pour Java, Perl, Python et PHP Implémenta d'abord Liberty ID-FF 1.2 et ajouta plus tard des supports pour ID-WSF et SAMLv2 Tests d'interopérabilité de Liberty réussis pour ID-FF 1.2 et SAMLv2	lasso.entrouvert.org
OpenSSO Implémentation Java de *Sun Microsystems*	Base pour la future version du produit de gestion des accès web de Sun - Sun Java System Federated Access Manager 8.0 Utilisé dans SSOCircle	www.opensso.org
OpenSAML par *Internet2*	toolkits pour C++ et Java SAML V1.1 et V2.0 Implémentation des assertions, protocoles et connecteurs SAML (pas de profils)	www.opensaml.org
Shibboleth par *Internet2*	inclut Identity Provider (Java) et Service Provider (module Apache C++) Shib 1.3 implémente SAML V1.1 SP et IdP Shib 2.0 implémente SAML V2.0 SP et IdP en plus de SAML V1.1 implémentation fondée sur OpenSAML	shibboleth.internet2.edu
SourceID par *Ping Identity*	FIM Open Source Implémente SAML V1.1 (avec des modules support supplémentaires pour ID-FF et WS-Fed)	www.sourceid.org/download
ZXID par *Sampo Kellomäki*	Open Source de gestion d'identités pour Masses - SAML SSO Implémenté en C mais supporte (via SWIG) Perl, PHP et Java Implémente SAML V2.0 SP (à 98%) et SAML V1.1 SP (à 60%) Supporte d'autres protocoles (ID-FF, ID-WSF et WS-Fed)	www.zxid.org

SAML 2.0 (Security Assertion Markup Language)

Normalisé en mai 2005 par l'*OASIS*, il permet l'échange sécurisé d'informations d'identité (authentification et autorisation). Les échanges d'informations de sécurité se font au travers de messages au format XML, appelés *assertions*. Un ensemble de profils a également été défini correspondant à des cas d'utilisation qui présentent la cinématique d'échange des messages, les paramètres attendus et renvoyés. Le protocole fait appel essentiellement à deux entités :

- le fournisseur de service (SP pour *Service Provider*) qui protège l'accès aux applications, bloque tout accès sans authentification préalable et redirige l'utilisateur non authentifié vers son fournisseur d'identité,
- le fournisseur d'identité (IdP pour *Identity Provider*) qui se charge d'authentifier l'utilisateur ainsi que de récupérer des informations additionnelles sur son identité.

Dans le cas multiCoTs, une troisième entité appelée service de découverte (DS pour *Discovery Service*) permet à l'utilisateur de sélectionner son domaine.

Les Profils SAML

Le profil le plus courant est le *Web Browser SSO*. Il décrit en particulier les étapes d'authentification d'un utilisateur et les échanges entre le SP et l'IdP. L'utilisateur tente d'accéder à une ressource protégée par le SP. Le SP vérifie que l'utilisateur est authentifié, et s'il ne l'est pas, le redirige vers son IdP (comme par exemple, MyOpendId ou Authentic). L'IdP demande à l'utilisateur de s'authentifier (identifiant puis mot de passe par exemple) puis renvoie une *assertion SAML* au SP contenant l'identité de l'utilisateur et la garantie qu'il est authentifié. Le SP autorise alors l'utilisateur à accéder à la ressource initialement demandée. Ce profil permet aussi de récupérer un ensemble d'attributs supplémentaires relatifs à l'identité de l'utilisateur lorsque la ressource l'exige. Avec la fédération d'identités et le SSO (*Single Sign On*), l'étape d'authentification ne se fait qu'une fois, dès lors que le SP appartient à un CoT.

Un second profil fondé sur des références à un message SAML (appelés aussi artefacts) offre la possibilité de décorréler l'authentification de la collecte des informations d'identité. Le SP reçoit de l'IdP une assertion SAML contentant un artefact. Le SP doit alors interroger directement l'IdP pour obtenir les informations liées à l'identité de l'utilisateur.

Il existe d'autres profils, le plus novateur étant très certainement le SLO (*Single logout*). Au lieu d'avoir à se déconnecter lui-même de chaque service, l'utilisateur se déconnecte en une seule fois auprès du fournisseur d'identité de tous les fournisseurs de services.

La sécurité apportée par SAML : chiffrement et signature

Les assertions SAML sont le moyen sécurisé pour échanger des informations d'authentification et d'autorisation. Elles sont fondées sur l'utilisation de couches SOAP, de XML Encryption et de XML Signature.

SOAP est le protocole d'encapsulation standard des messages XML, son utilisation facilite la communication et évite les problèmes de proxys et pare-feu par rapport à d'autres technologies plus anciennes. Il s'adapte à différents protocoles de transport, est indépendant de la plateforme et du langage. *XML Encryption* est le protocole standard de chiffrement des messages XML. Il a la particularité de permettre le choix de la granularité du chiffrement. Ainsi, il est possible de chiffrer la globalité du message ou simplement un sous-ensemble précis (par exemple, cela permet d'avoir un document XML en clair avec des valeurs d'attributs chiffrées). *XML Signature* est le protocole standard de signature des messages XML qui permet, comme XML Encryption, de cibler l'élément à signer. Cela permet à plusieurs intervenants de signer chacun une partie différente du document XML.

Le SP et l'IdP sont deux entités qui ont connaissance chacune l'une de l'autre en termes d'identifiant et de certificat. Ils utilisent une infrastructure *PKI* pour les échanges. Les messages XML qui transitent sur le réseau sont donc chiffrés par la clé publique du destinataire, seul capable de déchiffrer le message avec sa clé privée. L'émetteur signe ses assertions avec sa clé privée permettant au destinataire de vérifier sa provenance.

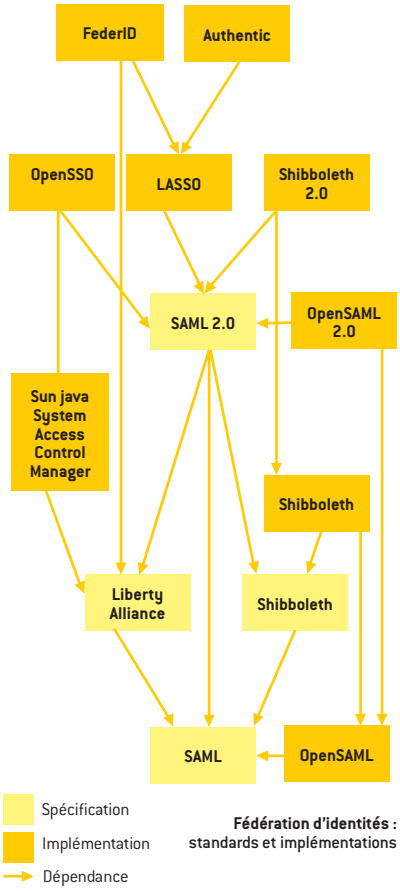
SAML et OpenID

OpenID date de 2005. C'est un protocole issu du Web 2, puisque lancé d'abord par le site LiveJournal (où les utilisateurs pouvaient concevoir un blog ou un journal et le maintenir) puis repris et co-développé par Janrain, Sxip et Verisign.

Comme SAML, OpenID permet la délégation de l'authentification ainsi que le SSO. Cependant, la notion de CoT est absente et est remplacée par une administration complètement décentralisée, ce qui signifie que n'importe qui peut devenir fournisseur d'identité ou fournisseur de service sans avoir à s'enregistrer auprès d'une autorité. Sa spécificité est d'être, comme il se veut, proche de l'utilisateur : celui-ci va pouvoir gérer comme il le souhaite son identité. En effet, une identité OpenID est tout simplement une adresse URL. Ce qui signifie que l'utilisateur peut utiliser l'URL de son blog ou de son site comme identité.

OpenID est donc un protocole beaucoup moins complexe que ceux qui se fondent sur SAML (comme Liberty et Shibboleth). Essentiellement orienté Web SSO, aucune spécification des moyens de protéger les données personnelles et de se prémunir de l'usurpation d'identité n'est fournie dans le Standard. Il n'en demeure pas moins qu'OpendID, bien que ne bénéficiant pas de travaux de normalisation par un organisme reconnu, est aujourd'hui un standard de fait, stable, largement utilisé dans un nombre important de logiciels. Il fera probablement partie des systèmes décentralisés de gestion d'identités, permettant aux utilisateurs de garder le contrôle sur leurs identités.

Contrôle d'accès et négociation fondée sur l'échange de certificats



Fédération d'identités : standards et implémentations

En l'absence d'une infrastructure appropriée pour la gestion d'identités, les utilisateurs sont souvent amenés à fournir plus de données personnelles que nécessaire pour accéder aux services souhaités.

Les utilisateurs sont de plus en plus exigeants vis-à-vis de leurs systèmes d'information ; ils souhaitent des applications plus sophistiquées, plus personnalisées mais pas au dépend de la sécurité. La diversité de leurs besoins nécessite souvent des interactions entre différents services, eux-mêmes fournis par différents organismes afin d'offrir un service global. Ainsi, une transaction est souvent distribuée sur plusieurs organisations. La gestion de l'accès est dorénavant fondée sur des mécanismes d'authentification à travers des domaines autonomes. Ceci amène à considérer d'autres aspects connexes au contrôle d'accès : **la gestion de la confiance et l'introduction de la négociation.**

Face à une divulgation non maîtrisée de données à caractère personnel à différents services, il est légitime que des utilisateurs exigent des garanties quant à la protection de la vie privée. Ils doivent pouvoir contrôler la distribution et la révélation de leurs données personnelles. Plusieurs projets tels que « Privacy and Identity Management for Europe » (PRIME) et « Platform for Privacy Preferences Project » (P3P) étudient cette problématique.

La gestion de la confiance

Le partage inter-organisationnel des données nécessite des mécanismes spécifiques pour l'authentification des utilisateurs d'une organisation donnée, accédant à des ressources fournies par une autre organisation. Dans les modèles traditionnels de contrôle d'accès, les utilisateurs sont connus à l'avance par le système. L'autorisation est alors fondée sur leur identité qui est vérifiée d'une manière centralisée (donc localement), et obtenue après authentification. Comme les architectures actuelles sont de plus en plus distribuées, les organisations ont recours à des mécanismes d'authentification différents, déployés au sein de chaque service. La fédération d'identités, comme vu précédemment, apporte une solution à ce problème. Cependant, la fédération d'identités dépend essentiellement d'une confiance établie entre des organisations et leurs services qui collaborent. C'est uniquement lorsqu'un service fait confiance à un autre service, que les assertions porteuses d'informations d'identité et d'autorisation sont traitées. En outre, ces informations contenues dans les assertions sont généralement associées à un rôle local, ou toute autre structuration des entités conformément au modèle de politique de sécurité utilisé, qui active les règles correspondantes de contrôle d'accès. Pour faciliter de telles associations de structuration des entités, des contraintes doivent être spécifiées et des accords doivent être établis entre les organisations concernées. Ceci conduit à la révélation de tout ou partie des politiques de sécurité de ces organisations afin de définir une politique globale pour gérer les échanges. Cependant, lorsqu'une organisation souhaite cacher une partie de sa politique de sécurité, des techniques fondées sur l'obfuscation de la politique doivent être utilisées.

C'est ainsi que le groupe de normalisation OASIS a proposé un langage d'expression de politiques de contrôle d'accès appelé XACML. XACML peut être utilisé dans les assertions SAML porteuse des informations d'autorisation, qu'il étend avec un procédé permettant de spécifier des contrats entre ces organisations qui interopèrent.

Cependant, pour arriver à un accord global sur les politiques d'authentification et d'accès et les informations échangées ou échangeables, un processus de négociation est nécessaire.

La négociation

Il existe deux approches possibles pour cette négociation.

La première approche est fondée sur des accords préétablis entre les organisations qui interopèrent : quelles sont les données partagées, quels utilisateurs ont le droit d'accéder à ces données et pour quoi faire. L'état négocié doit au moins satisfaire les contraintes de contrôle d'accès de tous les domaines impliqués. Cependant, l'inconvénient majeur d'une telle approche est l'existence de certaines politiques sensibles que les organisations peuvent ne pas vouloir révéler pour des raisons de sécurité. Dans ce cas, l'agent de négociation traite des données partielles obtenues après obfuscation. L'établissement d'un accord dans de telles situations est un problème difficile.

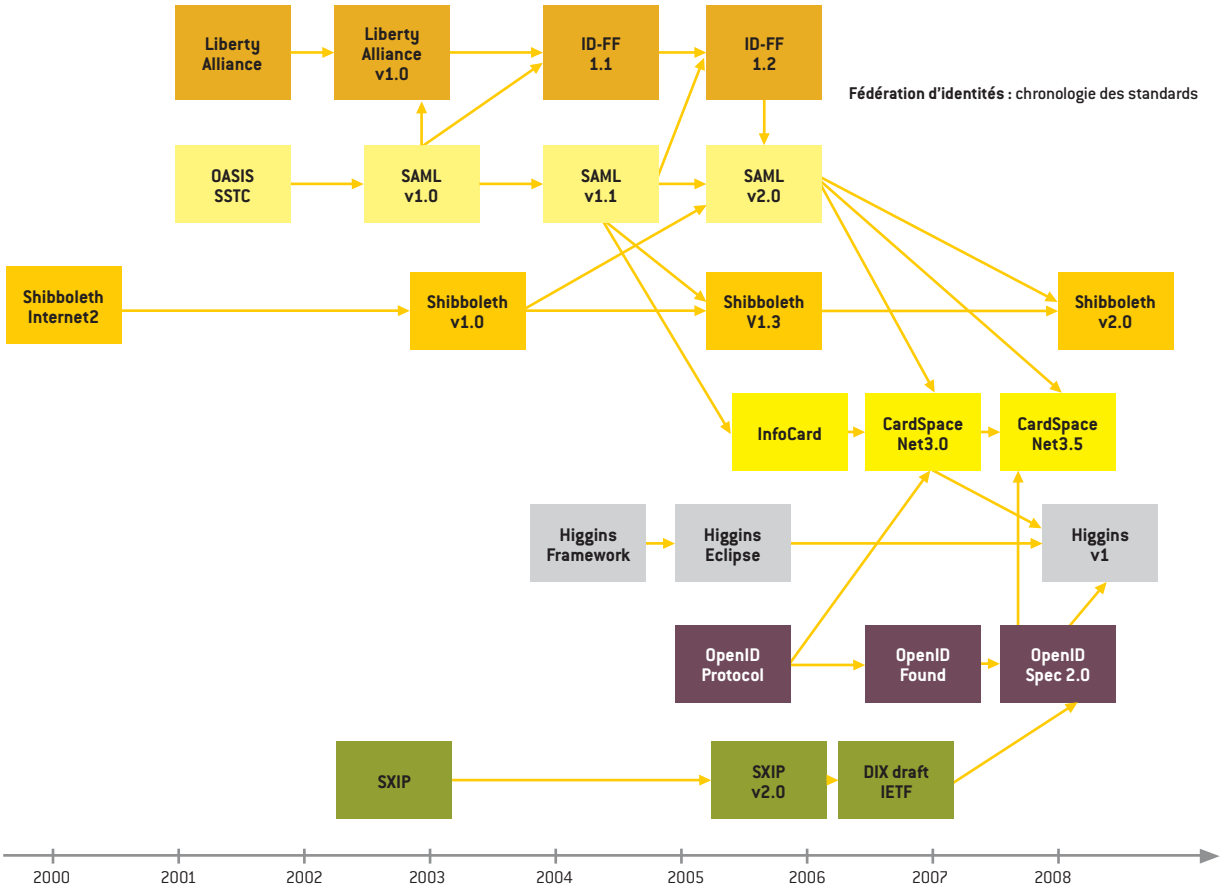
Dans la seconde approche, aucun accord préétabli n'existe. Une négociation est menée pour chaque demande d'accès qui permettra de réunir les attributs sur le profil de celui qui souhaite utiliser le service. Ces attributs permettent d'évaluer la requête. Cette approche est essentiellement utilisée dans les systèmes de négociation de la confiance, des échanges de certificats et de politique d'accès. Elle suppose l'existence de tiers de confiance pour certifier les données fournies par les utilisateurs.

XACML 2.0 (eXtensible Access Control Markup Language)

Normalisé par l'OASIS en février 2005, XACML est un langage, implémenté en XML, utilisé pour l'expression de politiques d'autorisations ainsi que des requêtes d'accès et des décisions de sécurité.

Les principaux composants définis dans l'architecture XACML sont le *Policy Enforcement Point* (PEP), le *Policy Decision Point* (PDP), le *Policy Administration Point* (PAP) et le *Policy Information Point* (PIP). Le PEP est l'entité qu'interroge le demandeur d'accès à qui est confiée la mise en œuvre des décisions d'accès. Le PEP transmet la requête au PDP, l'entité qui a le pouvoir décisionnel. En fonction des informations (attributs, profil, contexte...) transmises par le PIP et des politiques transmises par le PAP, le PDP donnera une suite positive ou négative à la requête. Il peut par ailleurs souhaiter avoir des informations supplémentaires avant la prise de décision, et dans ce cas le PEP se chargera de collecter ces informations auprès de l'émetteur de la requête.

Il est prévu que le protocole SAML soit utilisé pour exprimer les assertions afin de sécuriser les messages SOAP et gérer les identités (signatures et certificats). XACML, porté par des assertions SAML, serait utilisé pour l'expression des règles d'accès. On peut aussi préférer que SAML soit utilisé pour la formulation de la requête au PEP par le client et pour la réponse du PEP au client, alors que XACML permettrait de définir les échanges de décisions entre le PEP et le PDP.



Fédération d'identités : chronologie des standards

Perspectives stratégiques

Cette partie est la synthèse d'une consultation effectuée auprès des chercheurs de l'Institut Télécom

Nous avons présenté dans ce cahier différentes dimensions de la gestion des identités, selon des angles technique, social et juridique. Le point de vue étudié est celui où ces identités gérées sont l'enveloppe de données personnelles exprimant une **personnalité**, totale ou partielle. Cette persona numérique n'est qu'une des manières d'aborder les enjeux de l'identité numérique. Des internautes aux collectifs de citoyens, des think tanks aux expérimentations locales, de la puissance publique aux entreprises offrant des solutions, chacun en propose une vision différente : craintes des données produites à l'insu des utilisateurs, peur d'une société prédite par Orwell dans *1984*, nouvelles approches psychologiques, perspectives d'une citoyenneté au-delà des États, promesses d'un lien social amélioré et d'une utilisation des réseaux fondée sur la confiance…

Réfléchir sur l'identité numérique est en effet plus délicat qu'il n'y paraît. Si elle nous engage clairement sur les trois chemins de l'**identité-possédée** (elle me définit, je la protège) de l'**identité-authentifiante** (elle me définit, tu me reconnais) et de l'**identité-administrative**, cette réflexion ne peut laisser de côté une interrogation continuelle qui est celle de la construction, à tout âge, de sa propre identité, par rapport à soi, aux autres, et au corps social. Et certainement, alors que l'humanité semble débuter un nouveau processus d'évolution vers l'Homme augmenté, et que les Sociétés ne cessent de réinventer le contrat social, personne ne souhaite que la définition de notre future identité à l'ère du numérique masque nos aspirations et nos désirs individuels de construction et les noie dans un plus petit dénominateur commun qui serait définitif.

C'est avec cette interrogation toute personnelle que nous envisagerons chacun les perspectives **sociologiques** et **économiques** proposées à présent, ainsi que la construction des **normes** et les approches **marketing** qui s'y rapportent.

Pour devenir fournisseur d'identités, il faut satisfaire certaines conditions :

- posséder les procédures et processus nécessaires au traitement et à la sécurisation des données confidentielles et à l'identification des personnes auxquelles des identités numériques ont été attribuées,
- détenir un fichier d'identités assez fourni

L'implication des industriels et des institutions gouvernementales

Un engagement de l'action publique encore assez lent

Une entité qui pourrait jouer le rôle de fournisseur de services d'identité peut être une institution gouvernementale telle qu'un centre de recensement de la population. Il s'agira alors de l'émission de cartes d'identité numériques pour les citoyens et la définition d'un ensemble de directives pour l'implémentation de services utilisant ces cartes par des fournisseurs de services. De plus, de nos jours, la plupart des internautes possède également un téléphone portable, ce qui permettrait une authentification fondée sur ces mobiles.
Mais, les institutions gouvernementales n'ont montré jusqu'ici qu'un faible intérêt dans le fait de devenir des fournisseurs d'identités. Ceci combiné au fait qu'il existe un besoin client réel pour ce type de service, donne l'avantage au secteur privé qui voit en cette nouvelle technologie une opportunité commerciale tentante et lucrative.

Il convient cependant d'observer en France le lancement de IDéNum par le Secrétariat d'État au développement de l'économie numérique début février 2010. IDéNum fournira aux internautes un système d'authentification forte qui soit indépendant du couple login / mot de passe, et qui fonctionne avec un code alpha numérique associé à un support physique (clef USB avec module cryptographique, téléphone portable ou carte à puce). Les usages cités sont d'abord d'ordre administratif : compte bancaire, demandes de prêts, signature numérique de documents, inscription sur des listes électorales, demandes d'allocations… IDéNum n'est a priori pas associée à une carte d'identité numérique et n'est pas interopérable pour l'instant avec des systèmes mis en place par d'autres pays. Elle repose sur une démarche volontaire de l'internaute soucieux d'être identifié. Ce pourrait donc être une solution intermédiaire, participant à l'éducation des publics, avant le déploiement de solutions plus complètes.

Banques et opérateurs de télécommunications satisfont aux conditions pour devenir fournisseurs d'identités

Un modèle économique viable pour les opérateurs

La France n'est en revanche pas en retard concernant les initiatives privées. Le leader mondial de la carte d'identité numérique est Gemalto. La Poste et MyID.is (qui a certifié l'identité d'utilisateurs dans 37 pays) préparent une solution complète (IDenTIC) fondée sur une procédure en ligne cryptée suivie de la remise en main propre de la carte numérique par le facteur.

Actuellement il existe deux secteurs d'activité dont pourraient sortir des fournisseurs d'identités : le **secteur bancaire** et les **opérateurs de télécommunications**.
Les banques sont des candidats potentiels pour devenir des fournisseurs d'identité, mais cet aspect n'est pas étroitement lié à leur cœur de métier. D'où le manque d'intérêt, à tort ou à raison, qu'elles ont montré vis-à-vis de la problématique de fédération d'identités jusqu'à maintenant.
De leur coté, les opérateurs de téléphonie mobile sont souvent à la recherche de nouvelles opportunités commerciales et de nouveaux modèles économiques. Comme leurs recettes sont en période de décroissance dans leurs traditionnelles offres d'opérateur, ils doivent trouver de nouveaux champs d'investigation pour au moins maintenir les recettes courantes. Pour les opérateurs télécom, la plupart des processus requis sont déjà en place et ils ont par ailleurs des fichiers d'identités assez conséquents du fait des services qu'ils offrent (la plupart d'entre nous est client d'au moins un opérateur).
Les recettes d'un potentiel fournisseur d'identités proviendront des droits prélevés aux fournisseurs de service et des clients utilisant ces services. Pour le fournisseur de service, les avantages sont clairs : il bénéficie d'une authentification externe (déléguée), d'une base importante de clients potentiels qui ne peut que croître en raison de leur appartenance aux mêmes CoTs que d'autres fournisseurs de services. Le SSO permet à ces clients d'utiliser les services des autres fournisseurs de services de mêmes CoTs. Ceci permet différents types de stratégies de marketing collaboratif pour le partage des clients.
Les consommateurs sont également bénéficiaires puisqu'il leur sera possible d'utiliser une seule identité numérique rattachée à leur mobile (comme la carte SIM) sans avoir besoin de différentes identités et mots de passe pour chaque service. Ils sont probablement prêts à payer pour ce type de service.

Les actions à lancer

Nouveaux modèles économiques liés à l'identité

Parmi les nouvelles activités liées à l'émergence de l'identité numérique, trois nous semblent toujours une source de travaux de recherche et d'expérimentation.

La première concerne l'**économie de la notoriété**. On a vu dans ce cahier comment la protection de son identité numérique, et donc de sa notoriété (numérique ou non), était au cœur de la gestion des identités. Mais comment fonctionne-elle réellement ? Quels sont les impacts sur la gestion de la notoriété telle qu'on la faisait auparavant ? Qui sont les nouveaux médiateurs ? Quels sont les biais possibles, qui créeraient par exemple artificiellement des notoriétés du monde réel à partir de notoriétés acquises numériquement ? Quelles sont les différences d'enjeu de notoriété d'un individu en tant que tel, puis en tant que salarié, citoyen de son pays, mais également croyant ou non, adepte d'une thèse écologique ou d'une autre... chacun de ces échelons voyant ses propres valeurs et sa propre notoriété évoluer, en fonction de dynamiques elles-mêmes sommes de mouvements individuels ? Quelles seront les libertés de manœuvre de l'individu dans la gestion de son identité et de sa notoriéré associée ? Jusqu'à quel point la notoriété dépend de la communauté dans laquelle elle s'établit ?
Cette approche économique pourrait être couplée à une approche juridique relative à la gestion des conflits de notoriété.

La deuxième traite de l'**économie des attributs de l'identité** : posséder un avatar dans un monde persistant est une chose, le distinguer des autres avatars croisés nécessite de l'habiller (selon les circonstances), de l'équiper, et de lui donner la possibilité d'offrir des biens à un autre avatar. Il ne s'agit pas là d'un comportement futile, mais de la nécessité de dis-

poser de métaphores, qui formalisent des intentions, dans les interactions d'avatar à avatar. À ce titre, l'échange de tels biens relève plutôt d'une économie de services.
Ceci peut être généralisé à n'importe quelle manifestation de l'identité, qu'elle soit graphique (quasi-réelle) ou non. Une économie de biens virtuels associés à l'identité numérique se met en place. De nouvelles monnaies se créent, parfois connectées avec un taux de change aux monnaies réelles, parfois destinées à remplacer l'argent comme moyen et non comme une fin, et plus récemment dans des réseaux sociaux tel twitter comme preuve de remerciement et gage de confiance.

Enfin, dans le contexte de l'internet des objets, **l'identité numérique des objets**, construite éventuellement à partir de leur adresse sur le réseau, est un axe d'étude à envisager, dès lors que cette identité peut participer de l'identité numérique de leurs propriétaires.

Implémentation des normes & standards

Nous avons montré que des standards tels que SAML et OpenID s'imposent peu à peu. Certaines solutions techniques reposant sur ces standards commencent à être déployées. Notamment, Shibboleth est une solution open source de fédération d'identités compatible avec SAML 2.0, développée par le consortium « Internet2 Middleware Initiative » pour le monde de l'enseignement et de la recherche. Shibboleth a déjà été adopté ou est en cours d'adoption dans de nombreux pays, notamment USA, Suisse, Australie, Angleterre, Finlande, Norvège, Espagne, Pays-Bas. La France commence seulement à s'intéresser à ce type de solution et les premiers déploiements de Shibboleth par le CRU (Comité Réseaux des Universités) au niveau académique, conformément aux recommandations pour les annuaires de l'enseignement supérieur (SUPANN 2009), sont encore expérimentaux.
Parmi les besoins encore mal pris en compte, on peut citer les **problèmes d'interopérabilité entre organisations ayant des politiques de sécurité différentes.** Ainsi, le langage XACML est maintenant un standard que les organisations peuvent utiliser pour définir leur politique d'autorisation interne. Mais ce langage reste encore peu utilisé et peu de solutions de gestion des identités et des accès (*IAM – Identity and Access Management*) sont actuellement compatibles avec XACML. De plus, XACML reste limité à l'expression des politiques de sécurité internes à une organisation. Il n'est pas suffisant pour exprimer la politique de sécurité servant à contrôler l'interopérabilité entre organisations différentes. De nouveaux standards doivent donc être définis pour répondre à ces besoins. Ils devront prendre en compte les travaux de normalisation sur la *Privacy* en cours de discussion notamment au Comité Européen de Normalisation.

Mieux gérer la confiance

Il ne faut naturellement pas oublier que les différentes solutions de gestion d'identités se doivent d'être respectueuses de la vie privée des utilisateurs et plus largement de l'ensemble de leurs libertés. Pour pouvoir accorder un accès, de nombreux services réclament à l'utilisateur des données souvent personnelles. D'une part, les interfaces doivent être définies de telles sorte qu'elles soient conformes aux principes Informatique et Libertés. Il s'agit ici notamment de déterminer les cas dans lesquels le consentement de l'utilisateur est nécessaire à la collecte et à la transmission des données. D'autre part, les serveurs hébergeant ces services devraient pouvoir fournir des preuves de non conservation et de non transmission à des services tiers de ces données personnelles. Dans les solutions déployées de nos jours, l'utilisateur doit faire confiance au serveur. **De nouvelles solutions sur l'accord de la confiance doivent être explorées**, par exemple celles reposant sur l'usage des TPM (*Trusted Platform Module*), un composant cryptographique matériel déjà intégré dans certains ordinateurs et qui pourrait être utilisé pour prouver la suppression d'une donnée.

La superposition de trois régimes d'identité numérique : vers des propositions d'enquêtes

Il ressort de nos analyses et enquêtes effectuées sur les pratiques de communication numérique des français que les utilisateurs chevronnés d'Internet s'engagent simultanément sous trois régimes d'identité numérique :

- un **régime d'identification nominale**, par lequel ceux-ci cherchent à capitaliser une notoriété sur leur nom propre, que ce soit leur état civil ou l'identité professionnelle sous laquelle ils sont reconnus,
- un **régime de pseudonymat**, par lequel ceux-ci cherchent à développer, par le regard positif venu d'autrui, une reconnaissance qui va s'exprimer par le sentiment de recueillir de l'estime dans des espaces confinés et caractéristiques d'une « passion » ou d'un engagement dans le cadre des loisirs. Ainsi, sur de nombreux sites allant des jeux massivement persistants aux plateformes de contenus générés par les utilisateurs, c'est à travers des pseudonymes que les individus se rendent célèbres et visibles. Ces espaces, que l'on pourrait qualifier de « chambres d'appel », sont des lieux de tâtonnements identitaires dans lesquels les participants s'engagent en louvoyant,
- un **régime d'anonymat**, par lequel ils cherchent à se soulager, à respirer ou à se défouler en pratiquant des activités de libération de ses pulsions, sous la forme de l'exutoire. Ces lieux ont vu un développement fréquent avec l'essor des réseaux, depuis les espaces où les individus peuvent soulager leurs penchants pour la violence (qu'on pense aux jeux de tir ou à la série *Grand Theft Auto*), ou leurs pulsions sexuelles (qu'on pense à l'essor de la pornographie et aux sites de dialogue en ligne qui ne débouchent que rarement sur la rencontre physique).

Il semble important de réfléchir à trois directions de recherche. Il s'agit tout d'abord de **laisser à chacun la possibilité de vivre dans les trois régimes.** En particulier, cette préconisation débouche sur le maintien d'un « droit à l'anonymat ». Face aux contraintes de normalisation de l'identité subjective, qui sont présentes à travers l'injonction au sourire ou à l'égalité d'humeur se manifestant dans la vie professionnelle ou à travers les disciplines du travail en projet, les individus ont parfois besoin de se défouler, de respirer en se constituant des « poches d'air » qui leur permettent de compenser le travail de contrôle de leur image. Il y a un lien entre le développement d'un « entrepreneuriat de la notoriété » et la nécessité que se multiplient les « poches d'air » où pouvoir défouler ses pulsions et soulager son âme. Il convient d'observer également comment vont évoluer ici les segmentations entre réseaux sociaux privés et publics.
D'autre part, il faut également **mieux comprendre les régulations par lesquelles les deux régimes d'identité « seconde » doivent s'autolimiter.** Il y a notamment un travail tout particulier à faire sur les limites du régime de pseudonymat. Plusieurs affaires d'ores et déjà permettent de comprendre, dans leurs grandes lignes, les autolimitations. Sous un régime de pseudonymat, par exemple, comme le montre l'affaire de l'amant électronique, on ne peut pas dépasser certaines frontières.

Enfin, il semble capital de réfléchir aux **évolutions de design** par lesquelles pourraient être rendus appropriables par une large population d'utilisateurs les systèmes de « fédération d'identité ». Il pourrait exister une tension entre l'alignement des profils réalisé par les systèmes de fédération d'identité et l'objectif de maintenir une diversité de régimes d'existence sur Internet. Cela découle sur un travail de design participatif à mener avec un panel d'utilisateurs sur la mise en place des modalités de contrôle par l'utilisateur des paramètres de la fédération d'identité. Comment sécuriser les accès ? Comment paramétrer la transitivité, dans certains contextes, des informations identifiantes ?

Par ailleurs, une étude des **différences sociales** dans l'avatarisation mériterait d'être poursuivie pour comprendre les façons de jouer avec la multiplicité de l'identité dans les pratiques de communication.
Jouer : la dimension ludique ne doit pas être ignorée dans nos travaux. C'est en partie grâce aux jeux vidéo que les avatars se sont démocratisés, c'est également grâce au jeu que l'on pourrait dédramatiser les enjeux de l'identité numérique. La société Mimesis-Republic a ainsi montré la voie récemment, avec Black Mamba Nation, un jeu massivement multi-joueurs dans un univers persistant non absorbant (personne n'est obligé d'investir tout son temps pour y progresser) qui offre aux joueurs la possibilité de gérer simultanément plusieurs avatars, reflet de ses personnalités partielles.

De l'individu au réseau : une meilleure appréhension de la société

En quelques années, une partie de l'humanité a élargi considérablement ses horizons, d'abord par l'arrivée, pas toujours décryptée et utilisable, d'informations en provenance du monde entier, puis par l'élargissement de son réseau de connaissances et d'amis. Dans le même temps, les approches marketing fondées sur une offre de masse ont laissé peu à peu la place à des approches plus ciblées, sans doute sous les deux impulsions que sont un certain retour à l'individualisme d'une part, et l'aide au choix éclairé par les pairs d'autre part. Quand les objectifs du **marketing ciblé** rencontrent les possibilités techniques inhérentes à l'identité numérique, le juriste peut travailler sur les **marges de manœuvre** qui sont possibles des deux côtés.

Élargissant à présent l'angle de vue, et observant les **motifs** qui émergent des réseaux sociaux, tout un nouveau champ de recherche sur les **structures sociales** devient possible. Plusieurs auteurs ont ainsi observé à travers les graphes des réseaux sociaux des motifs, statiques ou dynamiques, permettant de prendre des décisions sous un jour nouveau : il en est ainsi de la propagation des grippes par la simple analyse des messages – géolocalisés – des internautes, de l'état de santé corrélé au nombre de relations dans les réseaux, voire même de la prédiction du comportement des politiques en fonction du graphe de leurs sponsors (aux États-Unis). Des savoirs tacites, des structures implicites sont tout à coup visibles et analysables. Ceci pourrait ouvrir la voie vers de nouveaux **outils de prédiction, de prévention et de notation.**
Sur le plan juridique, la mise en place de nouveaux titres d'identités numériques, la création d'outils de notoriété ou de prédiction, le recours à un avatar et l'utilisation de nouvelles manifestations d'identité impliquent une interprétation et une mise en cohérence des textes français et européens. Au-delà de cette mise en cohérence, se pose la question de la modification de la législation en vigueur. On peut notamment s'interroger sur l'opportunité de créer un droit à l'oubli ou un droit au pseudonymat.
Pour appréhender ce **droit en action**, une étude pourrait porter sur la mise à l'épreuve des textes juridiques relatifs à l'identité numérique par les différents acteurs (instances politico-juridiques comme la CNIL, autorités policières, entreprises, publicitaires, consommateurs, groupes de pression, etc.) aux compétences techniques, juridiques et marketing. Anticipant les usages « naturels » et « déviants », ce processus dynamique compose avec des intérêts et arguments divergents (imbrication nouvelle des logiques commerciales et sécuritaires, confrontées à d'autres formes de bien public, comme le respect de la vie privée). On pourrait ainsi saisir dans une perspective pluridisciplinaire sociologique et juridique les débats et controverses qui irriguent ce travail de construction sociale de nos identités numériques. Ces travaux devraient prendre également en compte les différences d'appréciation de l'identité entre les cultures occidentales et orientales, encore peu étudiées à ce jour.

Contributeurs

Ce cahier de veille a été rédigé par quatre auteurs principaux.

Nicolas Auray, **maître de conférences en sociologie,** au département Sciences Économiques et Sociales de Télécom ParisTech (dirigé par Christian Licoppe), est également chercheur associé à l'Institut Marcel Mauss et notamment au GSPM (EHESS). Il est co-responsable scientifique du projet ANR PANIC (Prosumérisation des audiences et numérisation des industries culturelles).

Nicolas Auray s'intéresse à la transformation de l'intégration sociale correspondant à l'essor des technologies de l'information. Un de ses axes de recherche est la constuction identitaire des adolescents et des jeunes, usant des jeux et recherchant la reconnaissance sur des réseaux sociaux virtuels.

Claire Levallois-Barth, **docteur en droit,** est chercheur dans ce même département, spécialiste du Droit des nouvelles technologies et plus particulièrement de la protection des données personnelles (Privacy).

Claire Levallois-Barth est membre du comité de pilotage du mastère spécialisé « Management et Protection des données à caractère Personnel » de l'Institut Supérieur d'Électronique de Paris (ISEP) et Secrétaire générale de l'Association Française des Correspondants à la protection des Données à caractère Personnel (AFCDP).

Frédéric Cuppens, **professeur,** et Nora Cuppens-Boulahia, **chercheur,** travaillent tous deux au département Logique des Usages, Sciences Sociales et de l'Information de Télécom Bretagne (dirigé par Yvon Kermarrec), membre de l'UMR CNRS Lab-STICC.

Frédéric Cuppens est responsable du projet structurant SERES. Il travaille sur différents sujets en sécurité informatique, notamment sur la modélisation de politiques de sécurité, du contrôle d'accès aux réseaux et aux systèmes d'information, la détection d'intrusion et les techniques formelles pour raffiner les politiques de sécurité et apporter la preuve de propriétés de sécurité. Il est l'auteur de plus de 150 articles dans des conférences et des revues internationales à comité de lecture. Frédéric Cuppens a été président ou membre du comité de programme des principales conférences internationales de son domaine. En 2009, il a co-organisé les conférences internationales ESORICS et RAID. Il est le co-fondateur de la conférence internationale SETOP.

Les travaux de recherche de Nora Cuppens-Boulahia comprennent entre autres la formalisation de propriétés et de politiques de sécurité système et réseau, l'analyse de protocoles cryptographiques, la validation formelle de la sécurité et l'analyse et la gestion des vulnérabilités et des risques. Ses thèmes de recherche actuels s'orientent vers la sécurité dans les réseaux de capteurs, le confinement d'applications et de services (adressage IPv6), la fédération d'identités et la sécurité des web services. Elle a publié plus de 80 articles dans des conférences et revues internationales. Elle a présidé ou fait partie de plusieurs comités de programme dans le domaine de la sécurité. Elle est membre du comité éditorial de « Computer & Security journal », représentante française de IFIP TC11 « Information Security » et co-responsable de l'axe sécurité de la SEE.

D'autres équipes de l'Institut Télécom mènent des recherches sur des sujets liés aux identités numériques. Citons par exemple Maryline Laurent à Télécom SudParis, Christine Balagué, Claudine Guerrier et Xavier Strubel à Télécom École de Management, ou encore Annie Blandin à Télécom Bretagne. Les écoles associées ne sont pas en reste avec notamment Jacques Fayolle et Bruno Sauviac à Télécom Saint-Etienne.

Des documents complémentaires sont accessibles sur l'espace partenaire du site de la Fondation (www.fondation-telecom.org).

Auteurs des illustrations page 5 : Stephan Nielsen (stilfoto) / Fotopedia ; Brian Snelson (exfordy) / Flickr.

Glossaire

Alias : *désigne un identifiant utilisé par une entité en remplacement de son identité réelle. L'alias est un pseudonyme pour le juriste.*

Anonymat : *état d'une entité dont on ignore l'identité. L'utilisation de pseudonyme est un moyen pour assurer l'anonymat.*

Assertion : *dans SAML 2.0, les échanges d'informations de sécurité se font au travers de messages au format XML, appelés assertions.*

Avatar : *apparence que prend un internaute dans un univers virtuel, voire dans des forums de discussion.*

Certificat numérique : *lien entre une personne physique ou morale et l'entité numérique. L'autorité de certification (qui gère les certificats et établit le lien entre la personne physique ou morale et l'entité numérique) fait foi de tiers de confiance et atteste du lien entre l'identité physique et l'entité numérique. Le standard le plus utilisé pour la création des certificats numériques est le X.509.*

Groupe Article 29 : *ce groupe de travail a été établi en vertu de l'article 29 de la directive 95/46/CE. Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la directive 95/46/CE et à l'article 15 de la directive 2002/58/CE.*

OASIS : *Organization for the Advancement of Structured Information Standards, consortium qui développe et fait adopter des standards ouverts pour la Société de l'Information.*

Obfuscation : *stratégie de protection qui consiste à publier des informations fausses ou imprécises sur un sujet de manière à dissimuler les informations pertinentes le concernant.*

PKI : *Public Key Infrastructure, Infrastructure à clés publiques, ensemble de composants physiques, de procédures humaines et de logiciels gérants le cycle de vie des certificats numériques.*

Profil utilisateur : *ensemble de données qui concernent l'utilisateur d'un service informatique.*

Pseudonyme : *identifiant que l'entité souhaite volontairement non-associable ni à son identité réelle, ni à aucune action en dehors de celles que cette entité mène en déclinant ce pseudonyme. À la différence d'un pseudonyme, un alias est un identifiant qu'une entité souhaite volontairement associable à son identité réelle.*

SAML : *Security Assertion Markup Language.*

Signature numérique : *mécanisme permettant d'authentifier l'auteur d'un document électronique et de garantir son intégrité. La signature électronique est devenue possible grâce à la cryptographie asymétrique.*

Les cahiers de veille **de la Fondation Télécom**

Les cahiers de veille de la Fondation Télécom sont le résultat d'études menées conjointement par des enseignants-chercheurs de l'Institut Télécom et des experts industriels. Chaque cahier, qui traite d'un sujet spécifique, est confié à des chercheurs de l'Institut qui réunissent autour d'eux des experts reconnus. Tout à la fois, complet et concis, le cahier de veille propose un état de l'art technologique et une analyse tant du marché que des aspects économiques et juridiques, en mettant l'accent sur les points les plus cruciaux. Il se conclut sur des perspectives qui sont autant de pistes possibles de travail commun entre les partenaires de la Fondation Télécom et les équipes de l'Institut Télécom.

Avec le soutien de :
Alcatel-Lucent, BNP Paribas, Orange, SFR, partenaires fondateurs de la Fondation

Et de Accenture

Fondation Télécom
46, rue Barrault - 75634 Paris Cedex 13 - France
Tél. : + 33 (0) 1 45 81 77 77
Fax : + 33 (0) 1 45 81 74 42
info@fondation-telecom.org
www.fondation-telecom.org

FONDATION TELECOM

Nereis - Le Studio T 02 98 33 74 04 - RCS 926950912 B