INSTITUT Mines-Télécom

CAHIER N° 1

Identités numériques

coordonné par Claire Levallois-Barth

Chaire Valeurs et Politiques des Informations Personnelles

TELECOM ParisTech

TELECOM Ecole de Management

TELECOM SudParis

Cahier n° 1

Identités numériques

Chaire Valeurs et Politiques
des Informations Personnelles

ISBN en cours - Imprimerie nationale - mars 2016

Sommaire

Introduction 1

Fiche 1. La construction
de l'identité dans la société contemporaine : enjeux théoriques 11

Fiche 2. Le rôle du droit dans la recherche d'un équilibre
entre l'identification et l'épanouissement personnel 17

Fiche 3. Réflexions sur l'évolution de l'usage de l'identité numérique
en sciences informatiques 29

Fiche 4. Les enjeux économiques des identités numériques 37

Fiche 5. Fonctionnement d'un système de gestion
des identités numériques 45

Fiche 6. Identité numérique et gestion des données personnelles 51

Fiche 7. Intégration des principes de protection des données
personnelles dans les systèmes de gestion des identités numériques 63

Fiche 8. Analyse comparative des choix de conception
des systèmes de gestion des identités numériques 71

Fiche 9. L'identité numérique en France 85

Fiche 10. La réglementation mise en place par l'Union européenne
en matière d'identification électronique et des services de confiance
(règlement eIDAS) 95

Fiche 11. Les preuves d'identités ou d'attributs préservant
le pseudonymat 109

Conclusion 115

Introduction

Armen Khatchatourov,
Pierre-Antoine Chardel
et Claire Levallois-Barth

Du point de vue de l'utilisateur, l'identité numérique est un moyen d'accéder à des ressources (voir une photo, consulter son compte utilisateur) et d'accomplir certaines actions (inviter un ami ou payer ses impôts) dans l'environnement numérique en s'identifiant en tant qu'utilisateur enregistré et autorisé à accomplir ces actions.

Ce type d'identité concerne déjà de nombreux usages, notamment :

- **l'identité régalienne** pour le titulaire d'une carte d'identité électronique afin d'accéder à des services d'administration électroniques (impôts, état civil) ;
- **l'identité citoyenne** locale pour accéder aux services proposés par la commune ou la mairie, comme l'inscription des enfants en crèche ;
- **l'identité privée** comme un compte sur un réseau social ;
- **l'identité client** pour l'utilisateur d'un site de commerce en ligne ou d'une banque ;
- **l'identité professionnelle** attribuée à un avocat, gendarme ou médecin ;
- **l'identité d'une personne morale** dans ses relations avec les entreprises, ses clients ou l'État.

Ce spectre s'élargit de jour en jour et devrait dans un futur proche couvrir tous les usages courants. Il nous permet en particulier de démultiplier nos manières de nous dévoiler aux autres et nos manières d'être, en nous offrant, par exemple, la possibilité de nous présenter sous diverses identités, notamment sur les réseaux sociaux.

Ce faisant, l'utilisation des technologies numériques questionne la manière dont l'individu se rapporte à lui-même et aux autres, car nous élaborons notre subjectivité (qui désigne le caractère de ce qui est personnel, ce qui est propre à une personne), en fonction non seulement de critères stables (nom, prénom par exemple), mais aussi de diverses possibilités offertes par la numérisation. Ceci est rendu possible par l'architecture des réseaux numériques. En effet, du fait même de cette architecture, dont les caractéristiques ont été définies dès la création de l'internet, il n'est pas toujours possible de connaître aisément l'identité d'une personne au sens civil du terme, lorsque celle-ci envoie un message ou consulte un site web.

Cette absence d'identification immédiate peut dans certains cas être perçue comme une difficulté, par exemple lorsque l'identification s'avère nécessaire pour assurer une transaction bancaire ou pour lutter contre des contenus illicites, comme la pédopornographie ou la vente de drogue en ligne. Dans le même temps, elle constitue un formidable gage de liberté, à la fois en termes de liberté d'information, d'action et d'expression dans le cadre des débats favorisés techniquement par ce nouvel espace public qu'est le web.

Il est ainsi possible d'appréhender l'« identité numérique » sous deux angles :

- d'un côté, les effets de la numérisation sur la construction de l'identité comprise comme un rapport à soi, aux autres et à l'espace public ;
- de l'autre, l'identification de l'utilisateur et de ses actions.

Ces deux aspects complémentaires constituent précisément le point essentiel de notre sujet.

À cet égard, on remarque que le premier aspect, celui de l'influence du numérique sur la construction par l'individu de ses multiples identités comme manière de se présenter aux autres, est un phénomène déjà étudié par les sciences humaines et sociales[1].

À l'ère de la « multitude »[2] au sein de laquelle l'activité de milliards de personnes connectées est captée, les effets d'un mouvement inverse sont en revanche bien moins connus. Ce mouvement consiste à ramener les multiples pratiques d'une personne qui se présente sous différentes identités en fonction des contextes dans lesquels elle évolue (par exemple, un même individu se présente comme « joueur de football », « père », « fan de musique », « demandeur d'emploi », « atteint d'une maladie incurable ») à un individu « unique » identifiable. Dans cette opération, la personne est « réduite » à sa seule identité civile ou à un profil composé de l'ensemble quasi complet de ses données personnelles. Cette assimilation n'est pourtant pas sans conséquence : elle renforce la transparence des différentes facettes de l'individu, augmente les risques de discrimination et diminue la richesse des possibles interactions.

Le présent Cahier propose donc de s'interroger sur ce mouvement, que nous appelons « unification des identités numériques ». Cette unification est-elle souhaitable ? Dans quels cas ? Quels pourraient être ses inconvénients, ses points faibles ? Comment peut-on éventuellement les éviter ? Selon quelles modalités de régulation ?

1 En se limitant au corpus francophone et de manière non exhaustive, on peut penser ici aux travaux sociologiques comme ceux de Nicolas Auray, Dominique Cardon, Julie Denouël, Antonio Casilli, Fanny Georges ou Fabien Granjon, notamment.

2 Nous renvoyons ici à Guattari, F. (2006). Entretien avec Jacques Robin : Révolution informatique, écologie et recomposition subjective, *Multitudes,* n° 24, ainsi qu'à Colin, N., Verdier, H. (2014) *L'âge de la multitude. Entreprendre et gouverner après la révolution numérique,* Paris, Armand Colin.

MÉTHODE

Afin de mettre en lumière les différents enjeux soulevés par les identités numériques dans nos sociétés contemporaines, ce Cahier adopte une approche pluridisciplinaire originale. Nous pensons en effet que si cette mise en perspective passe nécessairement par l'informatique et le droit, elle soulève également de nombreuses questions relatives aux incitations économiques ainsi qu'à leurs implications éthiques, philosophiques et sociétales.

Nous proposons ici une approche fondée à la fois sur des enjeux théoriques fondamentaux et sur la pratique des acteurs (au travers d'entretiens, de la participation à des réunions avec les acteurs-clés et d'analyses comparatives).

La mise en place d'une identification univoque, qui pourrait prendre la forme d'un identifiant unique conduisant à une identification permanente, se trouve aujourd'hui au centre du débat public. Elle concerne à la fois certains États et acteurs économiques.

Au niveau des acteurs économiques, les GAFA (Google, Apple, Facebook, Amazon) ont mis en place des identités numériques dites « privées ». L'identité Facebook par exemple est utilisée sur le réseau social lui-même, mais aussi, et de plus en plus, dans d'autres contextes. Ainsi, le bouton Facebook Connect permet d'utiliser cette identité sur les forums de discussion ou lors d'un achat en ligne. À cet égard, on note que les GAFA ont à plusieurs reprises tenté de mettre en place la politique dite de « *real ID* » (« identité réelle ») qui consiste à obliger leurs utilisateurs à leur fournir la preuve régalienne de leur identité civile. Cette évolution est-elle souhaitable ? Dans quelles conditions ?

Au niveau des États, ainsi que l'a démontré l'affaire Snowden, le croisement et le regroupement des différentes données personnelles d'une même personne renforcent le risque de surveillance, et ce, à l'échelle de la population entière. On note à cet égard que les États ne recourent pas nécessairement à un identifiant unique (au sens d'un numéro d'identification, tel le numéro de sécurité sociale).

Vis-à-vis de cela, nous nous interrogeons plus particulièrement sur le mouvement d'institutionnalisation des identités numériques des individus. Par là, nous entendons le processus même de la formation des institutions qui encadrent les relations sociales, participent à l'organisation de la société ou de l'État, et finalement imposent des valeurs et des normes de comportement (comme l'institution du mariage). Dans le cas des identités numériques, ce processus de pérennisation s'appuie sur l'introduction de dispositifs techniques particuliers et l'adoption de dispositions légales, dont la mise en œuvre influence à son tour les relations sociales dans leur ensemble.

En France, ce processus est en plein essor. Si l'on note le développement d'identités « sectorielles » au premier rang desquelles figure l'identité de l'assuré *via* sa carte vitale, on relève l'absence d'identité numérique régalienne mise en place et reconnue, comparable à l'identité civile garantie par l'État dans le monde « réel ». Toutefois, d'autres pays ont mis en place — ou sont en train de le faire — des identités numériques, qui peuvent s'appuyer sur différents supports (carte nationale d'identité électronique, téléphone mobile, carte de sécurité sociale, carte bancaire, clé USB, etc.).

À cet égard, la dynamique actuellement en marche au niveau étatique pose notamment les questions suivantes :

- Si l'identité numérique couvre l'ensemble de la population, quels sont les effets de cette mise à l'échelle, par exemple en ce qui concerne les politiques publiques ?
- Si l'utilisation de l'identité numérique est rendue obligatoire, comment les comportements des citoyens pourront-ils être modifiés ? Quelles pourraient être les conséquences coercitives et disciplinaires éventuelles sur chaque citoyen alors qu'une grande partie de ses actions en ligne devient plus facilement traçable ?
- De manière plus large, quel doit être le niveau de responsabilité attribué à l'utilisateur ?
- Comment réguler l'usage des identités régaliennes au sein du secteur privé ?

Par ailleurs, on note que les pouvoirs publics perçoivent le plus souvent l'utilisation des systèmes régaliens de gestion des identités numériques par les acteurs privés comme un moteur à l'adoption des systèmes qu'ils proposent. On suppose en effet que les utilisateurs sont plus enclins à utiliser quotidiennement ces systèmes et que les coûts peuvent être partagés entre les secteurs public et privé.

Ce Cahier examine donc la manière dont certains États — la France et les pays de l'Union européenne — entendent mettre en place des systèmes de gestion des identités à l'échelle de la société et comment l'Union européenne intervient sur ce terrain. Il apporte ainsi une contribution à l'étude des conséquences potentielles de cette mise en « système » sur les équilibres sociaux et démocratiques. En la matière, on constate depuis quelques années que les États poursuivent plusieurs objectifs :

- améliorer les niveaux de sécurité des moyens d'identification utilisés par les citoyens ;
- simplifier les démarches des citoyens ;
- généraliser l'usage de ces moyens de sorte qu'ils puissent être employés dans des contextes de plus en plus variés, pour développer les usages et faire des économies d'échelle.

Cette tendance forte à la « généralisation » comporte néanmoins des risques qu'il convient de souligner, notamment si l'une de ses conséquences est de rassembler toutes

les « identités » du citoyen (notamment les identités régalienne, citoyenne, privée, client et professionnelle) à une seule et même identité « unique ». En particulier, si cette mise en visibilité peut constituer une garantie forte dans les contextes de transactions électroniques, elle peut aussi être perçue comme une démultiplication des possibilités de surveillance, à la fois par l'État et par le secteur privé. Dès lors, la création d'une identité « unique » pose des questions en termes de préservation des libertés publiques. Cette préservation semble se poser de manière plus aigüe de nos jours qu'au début de l'informatique et de l'adoption de la loi Informatique et libertés en 1978.

Ainsi, l'équilibre à trouver entre les objectifs poursuivis est loin d'être aisé. Les décisions techniques et politiques peuvent avoir de nombreuses implications qui vont au-delà de la simple maîtrise des flux informatiques. Il en va par exemple de la possibilité d'assumer un rôle de lanceur d'alerte. Nous entendons ici la possibilité de porter au grand jour et de bonne foi un danger ou un risque menaçant pour l'homme, par exemple porter à la connaissance des médias un dysfonctionnement majeur au sein d'une entreprise pouvant entraîner des conséquences néfastes pour l'environnement.

De façon plus générale, on peut se demander si une certaine forme d'opacité de l'individu n'est pas requise pour que ce dernier soit en capacité de formuler une parole d'opposition. Comment garantir cette opacité afin de préserver la liberté d'expression, et plus largement le fonctionnement même de nos sociétés démocratiques ? Comment s'assurer que le citoyen n'est pas immédiatement pris dans les réseaux techniques de l'identification qui sont par essence indifférents et insensibles à la singularité des contextes dans lesquels il s'exprime ?

Il s'agit également de faire en sorte que le citoyen en tant que sujet de droit puisse continuer à agir sur la manière dont il entend se présenter à autrui, en préservant autant que possible son autonomie. Quels seront les effets des logiques d'identification et de croisement entre les contextes sur son autonomie ? À cet égard, on peut s'interroger sur les conséquences d'un rapprochement systématique de ses actions, par exemple les livres consultés dans une bibliothèque avec des demandes d'allocations. Ne convient-il pas de renforcer l'encadrement de telles pratiques et de promouvoir de nouveaux droits ?

COMMENT FONCTIONNE UNE IDENTITÉ NUMÉRIQUE ?

Pour accomplir certaines actions dans l'environnement numérique, il est nécessaire que l'utilisateur y soit autorisé. Le système de gestion des identités permet de gérer ces autorisations à l'aide de moyens d'authentification, comme le couple *login*/mot de passe, ou bien d'équipements dédiés comme les cartes à puce ou le lecteur d'empreintes. Ces derniers seront amenés à se développer pour des raisons de sécurité technique et juridique. Une fois authentifié, l'utilisateur est défini par un jeu d'attributs (nom, âge, employeur) et des droits (accès à certains documents, modification de ces documents). Il faut souligner deux aspects : tout d'abord, une seule personne physique peut détenir plusieurs identités numériques, et même dans certains cas au sein d'un même système de gestion ; ensuite, le jeu d'attributs et de droits peut être défini par l'utilisateur lui-même ou une autorité qui gère l'identité, et ce jeu peut être figé ou évolutif. Tout dépend des choix d'architecture opérés lors de la conception du système de gestion des identités.

Le rôle des instances qui délivrent initialement l'identité numérique est ici crucial, tant au niveau de la gestion de son cycle de vie qu'au niveau du crédit que l'on apporte à cette identité : on n'accorde pas la même valeur à une carte nationale d'identité émise par un État qu'à une carte professionnelle. Les choix d'architecture ne sont donc pas simplement des choix techniques. Ils constituent des choix stratégiques, y compris sociétaux, qui doivent être effectués en fonction du contexte d'usage dans lequel l'identité numérique s'inscrit.

Partant de ce questionnement, ce Cahier propose un parcours interdisciplinaire à travers un ensemble de fiches pouvant être lues à la fois de façon linéaire et non linéaire, indépendamment les unes des autres.

La fiche 1 s'attache à montrer comment la question de l'identité est liée à celle de l'autonomie de la personne, et comment l'autonomie détermine la construction de l'individu et sa capacité d'action dans la société. L'enjeu majeur porte ici sur la possibilité même de la démocratie, dans le sens où la préservation de la capacité d'action autonome est une condition nécessaire du vivre ensemble. Il s'agit par-là d'insister sur le fait que la construction de l'identité passe par la possibilité d'avoir recours à des identités multiples, et sur les risques relatifs à l'identification univoque de l'individu.

La fiche 2 évoque la manière dont s'articule une telle autonomie de la personne, en se focalisant sur le contexte européen et français. Classiquement, le droit conçoit l'identité sous deux prismes : celui de l'État, qui a organisé un système de constatation de l'état civil afin d'individualiser une personne parmi d'autres ; celui de la personne qui bénéficie d'un droit à l'épanouissement personnel lui permettant d'établir elle-même les composantes de son

identité d'être humain. La numérisation massive de nos existences nécessite de trouver un nouvel équilibre entre l'identification massive des personnes par les instances administratives et la possibilité pour un individu d'agir de façon libre et autonome.

La fiche 3 se focalise sur les moyens techniques. Après avoir distingué les notions d'identification et d'authentification, elle fait état de l'évolution de l'utilisation des identités numériques dans les systèmes d'informations et des possibilités permettant de tracer les activités d'un utilisateur. Elle fournit un argumentaire quant aux limites des solutions d'anonymat et de pseudonymat actuellement déployées.

La fiche 4 aborde quelques enjeux économiques. Dans la mesure où la majorité des modèles d'affaires utilisent aujourd'hui le ciblage publicitaire et la discrimination par les prix basés sur la connaissance des préférences de l'utilisateur, il est important de comprendre de quelle manière l'éventuel pseudonymat de ce dernier influence sa disponibilité à payer. On peut aussi se demander s'il est possible de concevoir des modèles d'affaires qui ne sont pas basés sur la monétisation directe des données personnelles.

La grande question est alors de savoir comment mettre en place des systèmes de gestion des identités numériques de telle sorte que l'équilibre entre l'autonomie de la personne, le respect de ses droits fondamentaux, notamment son droit à la protection de ses données personnelles, et les intérêts des acteurs économiques soit optimal. Dans cette perspective, ce Cahier se focalise sur le paysage des identités numériques susceptibles d'être utilisées par un individu dans le contexte européen. À cette fin, il examine les questions suivantes du point de vue de la protection des données personnelles :

- Quels sont les enjeux fondamentaux soulevés par les systèmes de gestion des identités numériques ?
- Comment ces systèmes de gestion ont-ils été ou sont-ils en train d'être déployés en France et en Europe ?
- Quelles sont les limites des systèmes actuels ?

Tandis que la fiche 5 fournit les bases pour comprendre le fonctionnement des systèmes existants, la fiche 6 explique comment mettre en œuvre les principes clés de protection des données personnelles afin que ces systèmes collectent et utilisent légalement les attributs des individus. Cette approche juridique doit nécessairement être complétée par une approche technique. À cet égard, la fiche 7 évoque les solutions qui peuvent être mises en œuvre dès la conception d'un système de gestion des identités numériques, puis tout au long de son cycle de vie en se référant à l'approche « *Data protection by design* ».

La fiche 8 propose alors une analyse comparative des systèmes déployés dans quatre pays européens. L'accent est mis sur les identités numériques régaliennes dont le déploie-

ment représente aujourd'hui un enjeu politique majeur dans la mesure où il touche aux modalités concrètes, aussi bien administratives que techniques, de la reconnaissance des citoyens par leur propre État et les autres États européens.

Les fiches 9 et 10 s'intéressent au futur proche ; elles décrivent respectivement le cadre réglementaire actuellement mis en place au sein de l'Union européenne *via* le règlement (UE) n° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (*electronic IDentification And trust Services* – eIDAS*)* et les différentes manières dont cette dynamique se traduit dans le contexte français.

Enfin, la fiche 11 part du constat que les systèmes de gestion des identités numériques classiques sont insuffisants pour garantir la multi-identité et protéger les données personnelles. Elle présente une alternative qui repose sur l'échange de preuves d'identités ou d'attributs. Ces preuves présentent l'avantage d'attester de certaines caractéristiques de l'individu sans pour autant dévoiler ses données personnelles.

Ce Cahier est conçu pour être un véritable outil pour toute personne, citoyen, chef d'entreprise, professionnel, enseignant, pour qui la question des identités numériques représente un véritable enjeu.
Le lecteur pourra poursuivre sa réflexion *via* les nombreuses références bibliographiques, les conseils de lecture et les conférences organisées par la Chaire Valeurs et Politiques des Informations Personnelles (CVPIP).

Fiche 1. La construction de l'identité dans la société contemporaine : enjeux théoriques

Armen Khatchatourov
et Pierre-Antoine Chardel

1.1. **De l'identité à l'identité numérique**

Une manière d'aborder la problématique de l'identité du point de vue de la philosophie contemporaine consiste à proposer une distinction entre l'identité *idem* et l'identité *ipse*, en suivant en cela Paul Ricœur[3].

> L'identité *idem* correspond à un regard porté sur l'individu de l'extérieur, qui le considère comme une somme de caractéristiques stables.
> L'identité *ipse* correspond à l'individu tel qu'il se rapporte à lui-même.

Pour bien comprendre cette distinction, il faut remonter à Edmund Husserl[4], philosophe allemand du début du XX^e^ siècle, qui introduit une distinction entre le corps-chose et le corps vécu. Le corps-chose est une chose du monde, un objet de la science ou de la médecine, qui peut être décrit par un regard extérieur comme un ensemble de caractéristiques objectives. Le corps vécu est le corps tel qu'il est essentiellement mien, tel que je le vis de l'intérieur. À la différence du corps-chose, le corps vécu est ce qui ouvre un horizon de sens à l'existence individuelle. À la suite d'Edmund Husserl, Martin Heidegger[5] définit cette existence comme étant essentiellement de l'ordre du projet, ouvert sur un avenir, et en cela non réductible à une entité stable.

Dans l'horizon de la question de l'identité, la distinction entre *idem* et *ipse* est donc à comprendre comme deux points de vue sur l'individu : l'un le réduisant à un ensemble d'attributs et l'insérant dans la société au même titre que les autres, c'est-à-dire de manière égale, en tant que sujet de l'État par exemple. L'autre point de vue accorde à l'individu une dimension irréductible inscrite dans un horizon de sens qui est le sien. Cet horizon de sens, tel qu'il est thématisé par ces deux auteurs, ne s'ouvre qu'à partir de l'interaction avec les autres, et conduit à une compréhension toujours renouvelée du monde extérieur et du sujet par lui-même.

Cette manière de décrire les enjeux liés à l'identité semble fructueuse lorsqu'on s'intéresse à la problématique des identités numériques. En la matière, deux attitudes peuvent être adoptées. D'une part, sur le mode de *l'idem*, une identité comme un ensemble d'attributs stables, tels le nom, le sexe, l'adresse, etc., utilisés dans le cadre des échanges ou transactions électroniques. L'exemple type est ici celui de l'identité dite régalienne, qui se concrétise dans la carte nationale d'identité électronique (*cf.* fiche 2). D'autre part, sur le

3 Ricœur, P. (1990.) *Soi-même comme un autre*, Le Seuil.

4 Salanskis, J.-M. (1996). *Husserl*, Paris, Les Belles Lettres.

5 Salanskis, J.-M. (1998). *Heidegger*, Paris, Les Belles Lettres.

mode de *l'ipse*, une identité comme projection active de l'individu vers les autres et la société, à l'initiative de l'individu. Il faut alors souligner que l'aspect « projection » et l'aspect « rapport à soi » sont intimement liés : c'est parce que l'individu est capable de se projeter dans son rapport avec les autres et la société qu'il est aussi capable d'avoir un rapport à soi. L'exemple type est l'utilisation d'un réseau social où la personne donne à voir, de sa propre initiative, des éléments de son identité, notamment ses publications, photos, ou relations sociales.

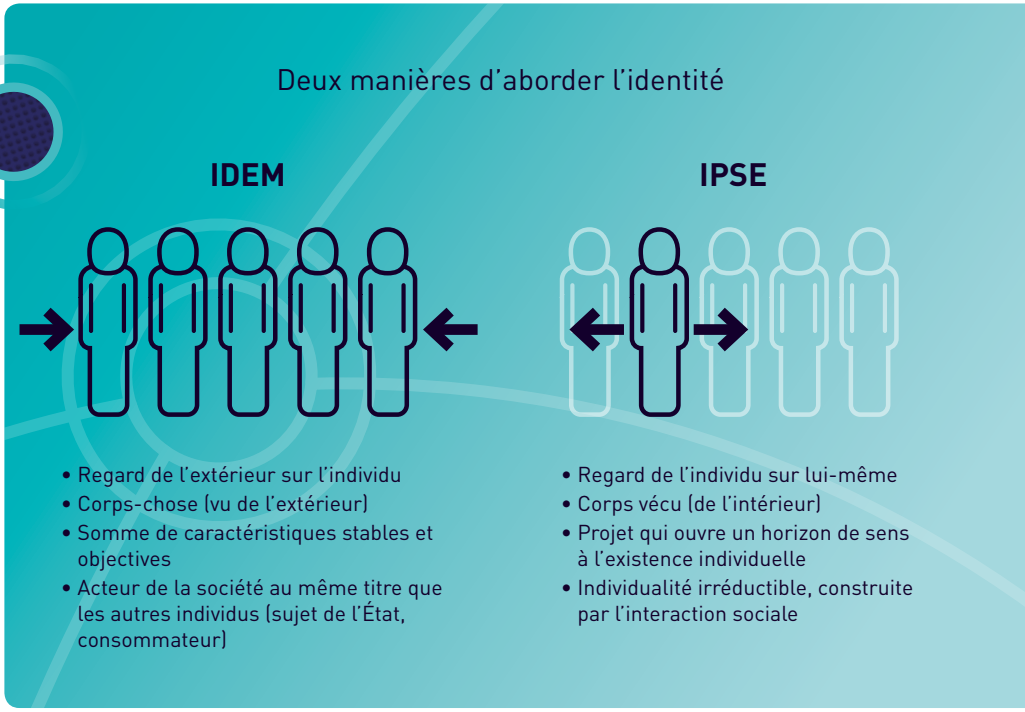


FIGURE 1. *Idem* et *Ipse*

Si cette utilisation a été souvent décrite comme la production d'un masque, une « représentation » dans le sens péjoratif du terme, la sociologie qui s'inspire des travaux d'Erving Goffman[6] nous apprend qu'il s'agit bien plutôt d'une construction de l'identité, construction où l'identité personnelle est le produit de la socialisation, et où l'identité n'est pas une

6 Goffman, E. (1973). *La mise en scène de la vie quotidienne*, t. 1 La présentation de soi, Paris, Éditions de Minuit, coll. « Le Sens Commun ».

entité préexistante à ses relations. De ce point de vue, l'identité *ipse* peut être comprise comme le produit « dynamique », jamais complètement stabilisé, d'un processus de négociation de ses propres frontières.

1.2. La construction de l'identité dans les environnements numériques

À partir de ce schéma fondamental, il convient de s'interroger sur la manière dont la numérisation de nos existences modifie le processus de la construction de l'identité.

L'enjeu essentiel, en cette période de mutation technologique majeure, est la préservation de l'équilibre complexe et fragile entre la construction de soi et le pouvoir formatif de la technologie, par lequel cette dernière façonne nos existences. En effet, dans le but de proposer à l'individu des produits et services personnalisés, des algorithmes complexes analysent les traces que celui-ci laisse, de manière volontaire ou non, dans les environnements numériques. Ces algorithmes construisent, à chaque action ultérieure de l'utilisateur, les profils de comportement de plus en plus affinés. Cet affinage continu peut alors être vu comme une boucle de rétroaction qui se renforce de plus en plus, en conduisant à la réduction de l'espace pour la construction de l'identité et à l'adoption des comportements stéréotypés qui se contentent de reproduire des suggestions « personnalisées ».

Or, pour que le processus de la construction de l'identité puisse prendre place de manière à permettre l'autonomie de la personne, il est nécessaire de préserver un « espace de jeu », comme le montre par exemple Julie Cohen[7], espace dans lequel l'initiative de négociation des frontières entre le soi et la société est laissée à l'individu, et dans lequel il peut se retrouver dans l'intimité d'un chez-soi.

Cet espace de jeu passe aujourd'hui entre autres par la construction active de son identité numérique, comprise sur le mode de l'*ipse*. Cependant, la particularité de la situation actuelle est qu'aucune modalité de l'identité ne semble pouvoir s'extraire des logiques techniques et marchandes. En témoigne l'exemple des réseaux sociaux tels que Facebook ou Google Plus, qui sont aujourd'hui fournisseurs de l'identité numérique « molle », ou « Soft eID »[8] : là où on aurait pu espérer un espace pour la construction de l'identité numérique sur le mode *ipse*, les logiques d'exploitation des données personnelles à des fins de profilage font que cette construction ne peut se faire qu'à la marge pour le grand public, ou alors

7 Cohen, J. (2012). *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*, Yale University Press.

8 Zarsky, T., Gomes de Andrade, N. N. (2013). Regulating Electronic Identity Intermediaries: The 'Soft eID' Conundrum, *Ohio State Law Journal*, Vol. 74, No. 6. http://ssrn.com/abstract=2368986

en faisant appel à des pratiques de contournement de la part des utilisateurs avertis. Ici, l'*ipse* ne se construit pas comme une projection de soi dont l'individu serait à l'origine, car la construction de « l'identité Facebook » est difficilement dissociable des logiques marchandes de son fournisseur, sur lesquelles l'individu n'a pas assez de prise.

Voilà donc ce qui semble en jeu dans le domaine des identités numériques : non seulement la protection des données personnelles et de la sphère privée, mais à un niveau beaucoup plus fondamental, la sauvegarde de l'espace de jeu dans lequel l'identité peut se construire.

1.3. **Les différents contextes d'usages et l'unification des identités**

Une manière de construire l'identité consiste à séparer les contextes sociaux dans lesquels l'individu évolue. Par exemple, nous ne partageons pas les mêmes informations — c'est-à-dire nous ne construisons pas notre relation de la même manière — dans le contexte familial, professionnel ou médical. Ces frontières ne sont pas fixées une fois pour toutes : elles peuvent être renégociées en fonction des situations et des acteurs. Dans le champ du numérique, Helen Nissenbaum[9] a thématisé cette approche à travers la notion de vie privée en contexte (« *Privacy in context* »). Selon elle, les flux d'informations doivent respecter les contextes d'usages, car chaque contexte relationnel possède ses normes, explicites ou non, qui correspondent aux attentes des usagers quant à la manière dont les informations vont circuler. Lorsque ces normes sont enfreintes, par exemple en communiquant mes données de géolocalisation du week-end à mon employeur, l'intégrité contextuelle est rompue.

Ce qui est ainsi perçu comme une exigence de séparation des contextes se traduit en pratique par le recours, pour une même personne, à des « identités multiples », dont le choix et la gestion sont à l'initiative de cette dernière. Cependant, la tendance actuelle semble aller à l'encontre de cette exigence indispensable à la construction de soi. En effet, on assiste à ce que l'on pourrait appeler l'unification des identités. Tout d'abord, la même identité numérique, par exemple celle dont l'individu dispose auprès d'un réseau social, est utilisée dans des contextes différents allant de l'identification auprès d'un site de commerce électronique en passant par l'identification sur un forum à connotation politique.

---

9 Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press. Voir également : *La vie privée en contexte, regards croisés Asie-Amérique du Nord*, 3e Rencontre de la Chaire Valeurs et Politiques des Informations Personnelles, 15 oct. 2013, avec Nissenbaum, H., New York University et Dalgliesh, B., University of Tokyo : https://cvpip.wp.mines-telecom.fr/2013/09/19/troisieme-rencontre-de-la-chaire-le-mardi-15-octobre-2013-de-17h-a-19h-a-linstitut-mines-telecom/

Ensuite, à un niveau plus fondamental, on observe une unification entre l'identité numérique « forte » ou régalienne et l'identité numérique « souple » (« soft eID »). D'un côté, l'identité régalienne, comme le montre le cas de certains pays (*cf.* fiche 8), peut servir à accéder à des services privés, y compris ceux qui ne nécessitent pas nécessairement une identité forte. De l'autre côté, les fournisseurs de « *soft* eID », comme Facebook et Google, entendent mettre en place une politique dite des « noms réels » en demandant à l'utilisateur de fournir la preuve de son identité régalienne. Ces acteurs se positionnent potentiellement comme des opérateurs privés délivrant une identité forte, et ouvrent la porte à l'utilisation ultérieure de ce type d'identité dans des contextes qui sont *a priori* étrangers aux buts initiaux, par exemple pour l'administration électronique[10].

Cette « confusion des genres », au service des logiques marchandes et de surveillance, se trouve facilitée par l'utilisation de l'identifiant unique. Elle ne contribue nullement à ce que l'on pourrait appeler les « conditions de possibilité » de la construction de l'identité sur le mode *ipse*. Une des manières de pallier cette situation est de soutenir la démarche qui consiste à cloisonner les contextes d'usage, et à développer les identités numériques multiples. Cette démarche peut prendre plusieurs formes, en allant du développement des dispositifs techniques de pseudonymisation en fonction des contextes à des démarches pédagogiques qui visent à sensibiliser les utilisateurs à ne pas utiliser la même identité numérique dans des situations différentes.

L'enjeu majeur des identités numériques du point de vue de la philosophie contemporaine et de la sociologie consiste à identifier les conditions de possibilité de la construction de l'identité dans l'environnement numérique, de manière à permettre à l'individu d'être acteur de son propre devenir.

10 Le G29 estime à cet égard que les réseaux sociaux «devraient donc pouvoir justifier le fait de contraindre leurs utilisateurs à agir sous leur véritable identité plutôt que sous un pseudonyme». G29, avis 5/2009 sur les réseaux sociaux en ligne, WP 163, p. 12.

Fiche 2. Le rôle du droit dans la recherche d'un équilibre entre l'identification et l'épanouissement personnel

Claire Levallois-Barth
et Delphine Chauvet

En droit français, l'identité est envisagée comme « *un agrégat de composants définissant la personne au-delà de son appartenance à l'humanité* »[11]. Si cet agrégat a pour objectif de différencier la personne de ses semblables, il est toutefois difficile de dresser la liste des caractéristiques biologiques et sociales permettant d'identifier facilement un individu au sein de la société dans laquelle il vit. En effet, ces attributs varient en fonction du contexte géographique, du milieu culturel et des périodes de l'histoire.

Ainsi, assiste-t-on à l'ère hypermoderne à la multiplication des composantes participant à la définition de la personne. Cet accroissement conduit à s'interroger davantage sur les modalités de régulation de l'identité qui peut être appréhendée selon deux modes : comme fonction d'individualisation par l'État et comme l'autodétermination de la personne.

2.1. La conception de l'identité

Classiquement, l'identité permet à l'État d'individualiser une personne. Cette conception quelque peu réductrice a ensuite évolué vers un droit plus complexe reconnaissant la possibilité pour un individu de se « projeter » en choisissant lui-même les éléments de son identité qu'il souhaite voir représentés et reconnus.

L'identité comme fonction d'individualisation par l'État

Afin que l'individualisation d'une personne puisse être opérée à chaque instant, les États ont mis en place, avec le développement de l'administration centrale, un système d'identification permettant de tracer chaque individu et de conserver les éléments le caractérisant. La solution retenue a été de sélectionner un certain nombre de critères considérés comme fondamentaux dans la description de la personne.

Le droit français a ainsi organisé un système de constatation de l'état civil. Cet état est d'ordre public (toute personne dispose d'un état dont elle ne peut se dispenser), opposable de plein droit au tiers, sans publicité. Ainsi, les éléments d'identité d'une personne comme le nom, le sexe, etc. se prouvent par tout moyen, à l'aide de différents documents officiels : extrait d'acte de naissance, livret de famille, carte d'identité ou passeport en cours de validité.

Ces attributs se caractérisent par leur immuabilité et leur indisponibilité, sous certaines réserves autorisées par la loi. Ils contribuent à ce que la personne soit « elle », et pas une autre, et marquent l'existence de l'individu en tant que sujet de droit. En ce sens, ces éléments participent de l'identité idem telle qu'évoquée en philosophie (*cf.* fiche 1).

11 Chauvet, D. (2014). *La vie privée. Étude de droit privé*, th. Paris-Sud.

Immuabilité : la personne ne peut pas faire modifier ou faire disparaître les éléments de son identité par sa seule volonté.
Indisponibilité : la personne ne peut pas réaliser une transaction sur les éléments qui composent son « état ».
Imprescriptibilité : l'écoulement du temps n'a pas d'influence sur le non-usage des éléments de l'état civil.

Au premier rang, le **nom de famille**, la **filiation**, la **nationalité** et le sexe participent directement à cette individualisation. À côté de ces éléments qui forment le « noyau dur » de l'identité, d'autres attributs concourent à une identification plus indirecte. La personne peut être **rattachée à un lieu déterminé**, son domicile, où elle est susceptible de se trouver et donc d'être localisée géographiquement. L'individualisation peut aussi s'effectuer *via* un **numéro**, notamment le numéro d'inscription au répertoire national d'identification des personnes physiques (NIR) dit « numéro de sécurité sociale » qui peut identifier jusqu'à 10 000 milliards de personnes. Il est utilisé par la sécurité sociale mais aussi par d'autres administrations et des entités privées. Le numéro de téléphone permet d'atteindre directement la personne et de troubler sa tranquillité s'il est utilisé de manière intempestive. Enfin, la **date de naissance** détermine l'âge de la personne ; elle peut constituer une limite justifiée à la conclusion d'actes juridiques ou injustifiée si elle est utilisée pour discriminer la personne.

Parmi ces composantes, le nom de famille est sans nul doute la marque fondamentale de la personne vis-à-vis de l'état civil, celle qui la caractérise de façon permanente et continue. Immuable et imprescriptible, le nom doit être connu et utilisé publiquement, sous peine de sanctions pénales prévues par l'article 433-19 du Code pénal[12].

12 *« Est puni de six mois d›emprisonnement et de 7 500 euros d'amende le fait, dans un acte public ou authentique ou dans un document administratif destiné à l'autorité publique et hors les cas où la réglementation en vigueur autorise à souscrire ces actes ou documents sous un état civil d'emprunt :*

1° De prendre un nom ou un accessoire du nom autre que celui assigné par l'état civil ;

2° De changer, altérer ou modifier le nom ou l'accessoire du nom assigné par l'état civil ».

Art. 1er de la loi du 6 fructidor, an II : «*Aucun citoyen ne pourra porter de nom, ni de prénom autres que ceux exprimés dans son acte de naissance. Ceux qui les auraient quittés sont tenus de les reprendre.*»

Le nom se conçoit ainsi comme une institution de police civile dans la mesure où il intéresse l'État dans l'identification des citoyens. Cela n'entrave pas la possibilité pour une personne notoire de recourir à un pseudonyme dans le cadre de ses activités publiques afin de préserver son droit à la tranquillité. Par ailleurs, le nom permet à la personne d'être rattachée à une famille, de nouer des relations avec autrui et de se distinguer. Son titulaire dispose d'ailleurs d'un « droit au respect de son nom » qui lui permet de se défendre contre d'éventuelles utilisations irrégulières. L'usurpation du nom d'autrui est pénalement réprimée par l'article 434-23 alinéa 1er du Code pénal.

Art. 434-23 alinéa 1er du Code pénal : «*Le fait de prendre le nom d'un tiers, dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales, est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.*»

Le nom de famille, comme la nationalité, étant un effet de la filiation, le droit considère ces attributs comme permanents et les impose sans que la personne puisse les choisir, sauf exception.

Cette approche initiale de l'identité correspond à une certaine conception du lien entre l'individu et l'État. Il s'agit d'asseoir l'emprise de l'État-nation sur la personne, laquelle est envisagée abstraitement. Cependant, les composantes de l'identité juridique ne sont pas uniquement imposées par l'État à travers une somme de caractéristiques stables sur le mode *idem*. Elles peuvent, dans une certaine mesure, être choisies par l'individu. On se trouve alors en présence d'une identité construite.

L'identité construite par la personne

La reconnaissance du droit pour chacun d'établir les détails de son identité d'être humain se fonde sur une interprétation extensive du droit au respect de la vie privée. Ce droit doit s'entendre à l'échelle européenne comme le droit « à l'épanouissement personnel et celui de nouer et de développer des relations avec ses semblables et le monde extérieur »[13].

13 CEDH, 6 févr. 2001, *Bensaid c. R.-U, §47.* : *JCP* G 2001, I, 342, nº 17, obs. F. Sudre.

Ainsi, la Cour européenne des droits de l'homme (CEDH) consacre un « **droit à l'identité** » protégé par l'article 8 de la Convention européenne des droits de l'Homme[14]. Cette tendance à la construction de l'identité par la personne qui en détermine elle-même les composantes s'explique par la revendication de mettre en adéquation ces composantes avec l'identité véritablement vécue, ressentie. La fonction assignée à l'état des personnes s'en trouve modifiée puisque cette fonction participe à rendre effectif un droit à l'épanouissement personnel sur le mode *ipse* (*cf.* fiche 1).

Art. 8 § 1 de la Convention européenne des droits de l'Homme (telle que ratifiée par les 47 États membres du Conseil de l'Europe) : « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.* »

Il en résulte un droit à connaître ses origines, origines à partir desquelles la personne se construit et entrevoit son avenir. On observe que les circonstances et les effets de la naissance de l'enfant, par exemple l'accouchement sous X, ne sont pas sans effet sur sa vie privée. S'il est impératif pour la personne de savoir d'où elle vient, elle doit aussi avoir la possibilité d'écrire sa propre histoire. Cette possibilité est illustrée par le droit du transsexuel — et depuis peu du transgenre — de demander la modification de la mention de son sexe sur les registres de l'état civil[15]. Cette rectification évite à l'individu de révéler sa transsexualité à des tiers et d'être en conséquence marginalisé.

Ce rôle accordé à la volonté individuelle dans la sélection des signes distinctifs de l'identité est cependant relativisé par l'essor des nouvelles technologies, qui s'inscrivent pour une large part dans l'instauration d'une société de la transparence.

2.2. La régulation de l'identité à l'ère numérique

À l'ère numérique, la dématérialisation métamorphose la façon dont l'identité est capturée et représentée. Si le droit est récemment intervenu afin que l'identité soit reconnue de façon sécurisée, il ne faut pas perdre de vue la nécessité d'établir les conditions permettant à la personne d'agir de façon autonome pour choisir les composantes de son identité.

14 V. par ex. CEDH, 7 févr. 2002, *Mikulic c. Croatie* : *JCP* G 2002, I, 157, n° 13, chron. F. Sudre.

15 Cass. ass. plén., 11 déc. 1992 : *JCP* G 1993, II, 21 991, concl. M. Jéol et note G. Mémeteau ; *RTD Civ.* 1993, p. 99, obs. J. Hauser.

La décomposition et la recomposition de l'identité

Selon certains auteurs, « l'identité numérique est à rapprocher de la notion de donnée personnelle »[16], c'est-à-dire de toute information, numérisée ou non, susceptible d'identifier directement ou indirectement une personne physique. Cette notion, qui s'entend largement (*cf.* fiche 6), couvre non seulement les éléments de l'état civil mais aussi l'image d'une personne, ses coordonnées bancaires, ses données de santé et de géolocalisation, ses loisirs, etc. Ces traces sont appelées à se multiplier avec l'internet des objets. Laissées volontairement – en témoigne le fait que la personne bénéficie d'une « e-notoriété »[17] sur le net par le biais des moteurs de recherche ou d'une « e-réputation » se traduisant par sa présence sur les réseaux sociaux (Facebook, Twitter, LinkedIn, etc.) – ou involontairement, elles contribuent à distinguer une personne des autres, à la profiler, à la discriminer.

Les informations physiologiques, qualifiées de données personnelles, participent elles aussi à la singularité de la personne. Le corps offre une identification supposée infaillible : l'ADN, l'iris, la main, la voix, etc. constituent des sources illimitées pour extraire d'importantes données sur la personne. Amplifiée par le numérique, la biométrie indexe l'individu dans ses moindres « recoins » tandis que la génétique sert l'identification de l'individu jusqu'à lui déceler certaines « anomalies ». Ces caractéristiques visent à redonner de la stabilité à l'état des personnes, compte tenu des changements possibles de certains éléments traditionnels composant l'état civil (sexe, nom de famille) et de leur complexité. On les retrouve sous forme numérique dans des traitements de données.

La numérisation concerne ainsi les documents officiels avec la généralisation du passeport biométrique pour les quelque cinq cents millions de citoyens européens et de la carte d'identité électronique déployée dans de nombreux pays (*cf.* fiche 8). Elle porte également sur la création de nouvelles bases de données. À titre d'illustration, en France, le Fichier national des empreintes génétiques (FNAEG) et le Fichier national automatisé des empreintes digitales (FNAED) répertorient les données biométriques des personnes condamnées ou suspectées.

Les nouvelles technologies tendent ainsi à transformer l'être humain en un objet statique qui est décomposé, puis recomposé. Cette décomposition prend la forme d'une démultiplication des attributs de la personne tandis que la recomposition des éléments identitaires (des profils) d'une même personne est favorisée par la prolifération des traitements infor-

16 Caprioli, E. A., Mattatia, F., Vuillet-Tavernier, S. (2011). L'identité numérique, *Cahier de droit de l'entreprise* 2011, n° 3, entretien 3.

17 Reprenant les termes mentionnés *in Le Lamy droit du numérique* (2015), Wolters Kluwer, pp. 608-609, n° 4007.

matisés de ses données personnelles et l'interconnexion de ceux-ci à l'ère du *big data*. Il s'agit ici d'un mouvement général de réification de la personne qui conduit à détacher des composantes du corps humain (à l'image du prélèvement et de l'implantation d'un organe) ou des éléments qui contribuent à sa personnalité (comme l'illustre la cession de l'utilisation de son nom ou de son image à une entreprise pour la publicité d'un produit). Se pose alors la question de la commercialisation de ces éléments, traditionnellement considérés par le droit comme hors commerce. En particulier, convient-il d'instaurer un droit de propriété sur les données personnelles[18] ?

Pour autant, nous pensons que les données personnelles ne sont pas des « objets » ordinaires, que l'être humain n'est pas réductible aux données le concernant et donc à sa seule identité numérique. Percevant le danger, le législateur donne dès 1978 la primauté à l'être humain.

> « *L'informatique doit être au service de chaque citoyen. [...] Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques* » (art. 1er de la loi Informatique et libertés).

Dans le même temps, la régulation vise à redonner à l'identité une nouvelle stabilité, stabilité qui apparait comme une condition de la sécurité des échanges numériques.

La sécurisation des échanges

La sécurisation des échanges électroniques entend répondre à la demande des autorités administratives et des individus eux-mêmes, désireux d'établir des liens de confiance et de bénéficier de garanties, notamment lors de transactions électroniques formelles. Afin de redonner de la stabilité à l'identité dans un monde dématérialisé, des mesures juridiques visent à lutter contre le vol d'identité et à faciliter l'établissement de la preuve de l'identité.

Le « vol » d'identité est simplifié par le numérique ainsi qu'en témoigne la jurisprudence sur la création de faux profils Facebook[19]. Prenant acte de cette cyberdélinquance, de nombreux pays ont adopté des lois visant à lutter contre ce fléau. Depuis 2006, le *Fraud Act* adopté par le Royaume-Uni prévoit qu'un individu usurpant l'identité d'une personne à

18 Purtova, N. (2015). The illusion of personal data as no one's property, *Law, Innovation and Technology*, 7:1, pp. 83-111.

19 T. corr. Paris, 24 nov. 2010 : *CCE* 2011, n° 3, comm. 28, note A. Lepage. – *Adde* CA Paris, 10 oct. 2014 : *CCE* 2015, n° 1, comm. 9, obs. E. A. Caprioli. – T. corr. Paris, 24 mars 2015 : disponible sur www.legalis.net. – Rappr. à propos de la création d'un faux site officiel de Rachida Dati, v. T. corr. Paris, 18 déc. 2014 : disponible sur www.legalis.net

des fins de *phishing* peut encourir une peine maximale d'emprisonnement de dix ans. Au Canada, la « fraude à l'identité » est un « acte criminel » puni depuis 2010 d'une peine similaire tandis que le « vol d'identité », qui renvoie au processus préparatoire consistant à acquérir les données personnelles d'une personne à des fins criminelles, est passible de cinq ans de prison[20].

En France, la loi du 14 mars 2011[21] a créé le délit d'usurpation d'identité ou d'usage de données permettant d'identifier un tiers.

> Art. 226-4-1 du Code pénal : « *Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende. Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne.* »

Une circulaire précise l'expression « *données de toute nature permettant d'identifier un tiers* ». Elle indique qu'« *au-delà des noms et prénoms d'une personne, il peut […] s'agir d'une adresse électronique, du numéro de sécurité sociale, d'un numéro de téléphone, d'un numéro de compte bancaire, d'un pseudonyme…* »[22]. La liste n'est donc pas exhaustive. On peut ajouter l'image, l'adresse IP, le *login* et le mot de passe, etc.

Au niveau européen, le règlement sur l'identification électronique et les services de confiance (règlement eIDAS) adopté le 23 juillet 2014 vise à instaurer les conditions de reconnaissance, au-delà des frontières nationales, d'une identification connue avec un fort degré d'assurance (*cf.* fiche 8). L'établissement de la preuve de l'identité reste, quant à elle, une compétence nationale. Par exemple, l'Estonie a adopté en février 1999 une loi sur les documents d'identité prévoyant l'instauration d'une carte d'identité électronique[23]. Cet État précurseur a été suivi en mars 2004 par l'Autriche qui a défini les conditions de mise en place de la « carte citoyenne »[24]. On peut également citer la loi allemande de juin 2009

---

20 Code criminel du Canada, art. 402 sur le vol d'identité et art. 403 sur la fraude à l'identité.

21 Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (dite « LOPPSI 2 ») : JO, 15 mars 2011, p. 4582.

22 Circulaire du 28 juill. 2011 relative à la présentation des dispositions de droit pénal général et de procédure pénale générale de la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure : BO min. Just. 31 août 2011.

23 Identity Documents Act passed 15.02.1999, RT I 1999, 25, 365.

24 The Austrian E-Government Act: Federal Act on Provisions Facilitating Electronic Communications with Public Bodiest published in the Austrian Federal Law Gazette, part I, Nr. 10/2004, https://www.digitales.oesterreich.gv.at/DocView.axd?CobId=19380

sur les cartes d'identité[25]. En France, la loi du 27 mars 2012[26] a introduit la carte d'identité électronique qui comprend, à l'instar du passeport électronique[27], une puce électronique sécurisée. Cette loi a été partiellement censurée par le Conseil constitutionnel (*cf.* fiche 9).

Pour autant, l'identification sur les réseaux ne doit pas être systématique.

La nécessité de rechercher un nouvel équilibre entre l'identification de la personne et la protection de son autonomie informationnelle

Tout comme dans le monde réel, il convient d'assurer un équilibre entre les besoins d'identification et la nécessité de préserver un espace dans lequel tout être humain a la possibilité de se comporter librement en garantissant, en particulier, les libertés d'expression, de communication et de déplacement. Afin que la personne puisse agir sur les modalités de sa propre protection au sein de la société et non subir les effets d'une « simple » identification univoque, il convient de construire une nouvelle forme de contrôle sur ses identités. À cette fin, de nouveaux droits doivent, à notre sens, être instaurés. Ces droits contribueraient à la mise en œuvre d'un droit à l'autodétermination informationnelle, droit proclamé par la Cour constitutionnelle fédérale allemande en 1983[28].

Droit à l'autodétermination informationnelle : droit déduit des articles 1er (dignité de l'Homme) et 2d (droit au libre développement de sa personnalité) de la Constitution allemande qui vise à garantir la capacité de l'individu à décider lui-même quand et dans quelle mesure une information relevant de sa vie privée peut être communiquée à autrui.

La possibilité de choisir librement, selon les situations, l'identité sous laquelle la personne souhaite se présenter doit se traduire par un **véritable droit à la multi-identité**[29]. Ce droit répondrait au besoin de chacun de créer et d'utiliser, selon le contexte dans lequel il évolue, des identités partielles à la fois physiques et numériques afin de protéger certaines facettes de sa personnalité. Il comprendrait la possibilité de ne pas dévoiler sa véritable identité, notamment son état civil. Or, cette nécessité n'est que partiellement prise

25 Act on Identity Cards of 18 June 2009 (Federal Law Gazette I, p. 1346), amended by Article 4 of the Act of 22 December 2011 (Federal Law Gazette I, p. 2959), http://www.personalausweisportal.de/SharedDocs/Downloads/EN/Legal-bases/Act_Identity_Cards_and_Electronic_Identification.pdf?__blob=publicationFile

26 Loi nº 2012-410 du 27 mars 2012 relative à la protection de l'identité : *JO*, 28 mars 2012, p. 5604.

27 Décret no 2005-1726 du 30 déc. 2005 relatif aux passeports électroniques : *JO*, 31 déc. 2005, p. 20742.

28 Cour constitutionnelle fédérale allemande, 15 déc. 1983, BVerfGE 65, p. 1.

29 En ce sens, Gomes de Antrade, N. N. (2011). Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization, *in Computers, Privacy and Data Protection: An Element of Choice*, Gutwirth, S., Poullet, Y., De Hert, P., Leenes, R., (Eds.), Springer, pp. 65-97.

en compte par le règlement eIDAS qui — loin de reconnaître un véritable droit au pseudonymat — se contente de préciser que « *l'utilisation de pseudonymes dans les transactions électroniques n'est pas interdite* »[30].

Il s'agit non seulement de permettre à la personne d'agir sur la construction de son identité future, mais aussi de supprimer des parties de son identité narrative, de faire disparaître certains aspects du passé. Cette possibilité passe par la reconnaissance d'un **droit à l'oubli numérique** qui a été consacré en mai 2014 par la Cour de justice de l'Union européenne (CJUE) dans l'arrêt historique Google Spain et Google Inc. contre AEPD[31] sous la forme d'un droit au déréférencement. Précisément, les juges ont reconnu le droit pour une personne physique de demander la suppression des résultats obtenus *via* des moteurs de recherche à partir de son nom vers des pages comportant ses données personnelles, notamment si les informations sont périmées ou inexactes. La mise en œuvre du droit à l'oubli est cependant délicate, car il faut tout à la fois tenir compte :

- de l'intérêt de la personne concernée (en protégeant sa vie privée et ses données personnelles en fonction notamment de la nature de l'information et sa sensibilité) ;
- de l'intérêt du public à accéder à l'information (en garantissant la liberté d'expression et le droit à l'information) ;
- du devoir de mémoire.

À cet égard, la Cour de justice juge que les droits au respect de la vie privée et à la protection des données personnelles « *prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt de ce public à accéder à ladite information lors d'une recherche portant sur le nom de cette personne. Cependant, tel ne serait pas le cas s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question* » (§99).

Pour autant, la CNIL a été saisie de plusieurs centaines de demandes de particuliers s'étant vus refuser le déréférencement de liens internet (ou adresses URL) par Google.

30 Art. 5 (2) du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juill. 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE : *JOUE* L 257/73 du 28 août 2014.

31 CJUE, 13 mai 2014, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos, Mario Costeja González* : *Légipresse* 2014, n° 319, chron. N. Mallet-Poujol ; *JCP* G 2014, p. 1300, note L. Marino ; *D.* 2014, p. 1476, note V.-L. Benabou et J. Rochfeld ; *ibid.*, p. 1481, note N. Martial-Braz et J. Rochfeld.

Le débat sur le droit au déréférencement est donc loin d'être clos. Selon toute vraisemblance, il devrait être consacré législativement lors de l'adoption prochaine de la proposition de règlement de l'Union européenne relatif à la protection des données personnelles (*cf.* fiche 6). Reste à savoir comment il sera mis en œuvre. Contribuera-t-il réellement à un droit à l'autodétermination dans un monde de mise en données où la multiplication des capteurs en tout genre s'accentue avec le développement concomitant de l'internet des objets ?

Fiche 3. Réflexions sur l'évolution de l'usage de l'identité numérique en sciences informatiques

Maryline Laurent

3.1. Une « représentation informatique » dynamique pour identifier et authentifier

L'identité numérique peut être considérée comme une « représentation informatique » d'une entité[32]. Ce sont les moyens informatiques et technologiques qui permettent à cette entité de se projeter dans le monde du numérique, cette projection pouvant prendre plusieurs formes selon son contexte (administratif, professionnel, réseaux sociaux, etc.). Dans la suite des explications, dans un souci de clarté, la notion d'entité, bien qu'elle puisse concerner une personne morale ou un groupe d'individus, sera réduite à celle de « personne physique », encore dénommée « individu ».

D'un point de vue technique, cette représentation informatique consiste à associer à un individu un ensemble de données numériques, également appelées « attributs ». Ces attributs peuvent être relativement statiques dans le temps comme nom, prénom, adresse, empreinte vocale, ou fortement dynamiques comme ses centres d'intérêt, le nom de l'application utilisée avec son heure de démarrage et la durée de l'utilisation, voire la géolocalisation de la personne s'il s'agit d'une application sur mobile.

La distinction entre identification et authentification d'un individu réside dans le degré de confiance établi entre l'identité déclarée par l'individu et l'identité numérique dont il est détenteur. Une **identification** repose en général sur la simple déclaration par l'individu de son identité sous la forme d'un identifiant numérique de type numéro de sécurité sociale, nom, alias, pseudonyme, etc.

A contrario, une **authentification** suppose que l'individu déclare son identité et apporte la preuve de cette identité, que cette preuve provienne de lui-même ou bien d'un tiers. Cette preuve s'appelle en informatique un « credential ». Elle peut prendre la forme d'un mot de passe, d'une signature électronique faisant en général référence à un certificat électronique, d'une empreinte biométrique… avec des niveaux de robustesse et de fiabilité très hétérogènes. Les techniques modernes renforcent même le niveau d'authentification par le biais d'analyses comportementales.

3.2. Une identité numérique à double tranchant

L'identité numérique, quel que soit son champ d'application, a pour fonction essentielle en sciences informatiques de tracer les activités des utilisateurs. Deux grands secteurs font un usage différent de ces traces : la sécurité des systèmes d'information (SSI) et les sociétés commerciales.

32 Laurent, M., Bouzefrane, S. (Eds.) (2015). *La gestion des identités numériques*, Londres, ISTE.

D'un côté, la SSI a pour mission d'assurer la protection des systèmes d'information (SI). À ce titre, elle prévoit des mesures préventives et réactives. Les mesures préventives concernent, par exemple, l'authentification des utilisateurs préalablement à l'accès aux ressources d'une entreprise. Les mesures réactives sont mises en place, dans le cas de dysfonctionnements — qu'ils soient accidentels ou malveillants — pour comprendre après coup les différents évènements qui ont affecté le SI, corriger et réparer le SI, et en cas d'actes malveillants avérés, pouvoir retrouver le fautif. Ainsi, les traces conservées dans le SI servent principalement à soutenir l'administrateur dans sa tâche de supervision de son SI.

Selon la configuration réalisée par son administrateur, le système conserve un volume plus ou moins grand de traces, appelées dans le jargon technique des « logs ». Ces traces peuvent contenir les heures de connexion des utilisateurs enregistrés sous l'identité déclinée, les principales erreurs générées dans le système, etc. Pour une dizaine de machines, le volume peut facilement atteindre plusieurs centaines de mégaoctets par jour. Plus le volume de traces est important, plus difficile et longue sera la tâche d'analyse des logs, mais meilleure sera la précision de l'analyse. La difficulté pour l'administrateur est donc de sélectionner les traces à conserver. En SSI, la démarche adoptée, en cas de dysfonctionnement, consiste à remonter jusqu'à son origine. Une mauvaise configuration d'un équipement, une erreur de programmation d'un serveur, voire un acte malveillant peut en être la cause.

En cybercriminalité, la démarche peut être amorcée suite à la détection d'un évènement répréhensible ou sur la base d'une suspicion forte pesant sur un individu. Dans ce dernier cas, ce n'est plus l'évènement qui guide l'investigation, mais l'individu. Les enquêteurs vont alors se concentrer sur les traces laissées par un individu pour évaluer son implication. Sont à leur disposition plusieurs systèmes de surveillance dont la puissance a été révélée par l'affaire Snowden. Leurs usages sont strictement encadrés par des lois dont l'adoption a été fortement critiquée du fait qu'elles étendent à la fois les finalités de surveillance et les services habilités à surveiller[33].

D'un autre côté, les sociétés commerciales sont devenues beaucoup plus agressives dans leur façon de collecter les données des consommateurs. L'objectif de cette collecte est de profiler les personnes de manière à connaître leurs habitudes et centres d'intérêt, et d'utiliser dans un second temps cette classification massive des individus pour leur proposer des

33 Loi de programmation militaire de 2013 et Loi du 24 juin 2015 relative au renseignement, qui autorise l'aspiration de données, notamment à des fins de promotion des intérêts économiques, industriels et scientifiques français.

services et produits personnalisés. Notons qu'il n'est pas nécessaire d'indiquer sur un site web ses nom et prénom pour être profilé. Les outils utilisés de façon récurrente, comme le navigateur internet à son domicile, ou mieux son *smartphone* personnel, sont suffisants pour relier une navigation supposée anonyme à l'identité de la personne. En effet, tous les logiciels ou équipements utilisés par un individu sont des éléments certes périphériques à son identité, mais révélateurs de son identité. Prenons le cas de Google qui est au centre d'un très vaste champ de données. En plus de contrôler une grosse part des boites email Gmail des internautes et donc d'avoir accès à leur contenu, Google contrôle aussi le système d'exploitation (OS) des *smartphones* sous Android, ce qui met à sa disposition un très large panel de données personnelles comme la géolocalisation (transmise à Google 10 fois par minute selon l'étude réalisée dans le cadre du projet Mobilitics de la CNIL). De plus, grâce à son outil d'analyse d'audience Google Analytics très prisé des entreprises, la multinationale américaine connaît la plupart des applications auxquelles accède un utilisateur, y compris les plages temporelles d'accès. Vu le gros volume de données collectées, les outils de traitement sont très sophistiqués, de type *datamining*, voire *big data* et nécessitent un niveau d'expertise élevé.

3.3. Le pseudonymat et l'anonymat sont-ils un leurre ?

Une solution technique pour protéger l'identité de l'individu consiste à couper le lien entre l'identité numérique et l'identité réelle de la personne. Deux propriétés entendent répondre à cet objectif : le pseudonymat et l'anonymat.

Le **pseudonymat** implique nécessairement l'utilisation d'un pseudonyme, c'est-à-dire un identifiant pouvant aisément être relié à une identité réelle par une autorité légitime.

L'**anonymat** se distingue du pseudonymat par la difficulté à établir ce lien. C'est sur ce niveau de difficulté à remonter à l'identité réelle de la personne que les scientifiques et les juristes divergent. Les juristes, par l'intermédiaire notamment du G29, définissent l'anonymat comme l'impossibilité de remonter à la personne, et ce, de façon irréversible.

L'AVIS DU G29 SUR LES TECHNIQUES D'ANONYMISATION

Cet avis, émis par les autorités de protection des données de l'UE, reprend le vocabulaire juridique d'anonymat et décrit plusieurs techniques d'anonymisation. Cependant, il limite volontairement la portée de la démarche au cas des bases de données déjà constituées et ne traite que des données détachées du contexte informatique de leur collecte.

Les scientifiques, qui savent que les approches techniques ne sont pas fiables à 100 %, préfèrent définir un seuil de résistance d'un mécanisme d'anonymat face à des tentatives

de levée d'anonymat initiées par un adversaire potentiel. Ainsi, suivant la force de frappe de cet adversaire (typiquement, sa capacité à casser un protocole cryptographique), le mécanisme d'anonymat résistera ou ne résistera pas.

La propriété d'inassociabilité (*unlinkability* en anglais) désigne quant à elle l'incapacité à relier au moins deux informations distinctes (enregistrements, messages, URL, actions, identifiants) relatives à un individu ou à un groupe d'individus.

Quand bien même une brique du système d'informations garantirait assurément l'anonymat, l'utilisateur en pratique n'a aucune certitude de rester anonyme. En effet, même en utilisant ce mécanisme d'anonymat, la personne laisse quantité d'autres traces, comme l'explicite la Figure 2. Ces traces sont propres aux ressources matérielles ou logicielles utilisées par l'utilisateur. Il peut s'agir d'un *smartphone*, d'un ordinateur ou plus insidieusement d'un objet communicant situé dans son entourage. Ces ressources matérielles transmettent bien souvent à l'insu de la personne des adresses de connexion, des *cookies*, des données de géolocalisation… qui sont autant d'éléments identificateurs. Si la personne utilise son propre terminal, l'identification sera encore plus aisée, car chaque terminal émet de multiples empreintes numériques (*fingerprinting* en anglais) qui le rendent unique vis-à-vis d'autres terminaux. Parmi ces empreintes, on peut citer la liste des réseaux Wi-Fi sur lesquels le terminal s'est connecté, les habitudes de navigation sur le web, la liste des applications hébergées sur le terminal, la version des différents éléments systèmes, services ou protocoles. Quand on sait que quatre points de géolocalisation associés à une heure de la journée suffisent à identifier avec 95 % de succès un individu parmi un panel de 1,5 million de personnes[34], on se rend mieux compte de la capacité offerte par les technologies actuelles pour tracer les personnes.

D'autres traces peuvent être laissées sciemment par l'utilisateur, notamment lors de ses interactions sur un réseau social, lors de l'utilisation d'une messagerie instantanée ou lors du dépôt de certains contenus sur des services de partage (Youtube, AWS d'Amazon). Pire, les informations peuvent aussi provenir d'un ami qui dépose une photo taguée du nom de l'utilisateur sur Instagram. Toutes ces traces sont très riches en renseignements, car elles relèvent les cercles de personnes fréquentées, les centres d'intérêt, activités et comportements de l'utilisateur et les évènements auxquels il a participé ou envisage d'assister.

Comme le montre la figure 2, on peut distinguer au centre un utilisateur clairement identifié par ses données d'identité, et à la périphérie, des données qui rayonnent autour de lui et qui peuvent révéler un certain nombre d'informations sur son comportement, ses

34 De Montjoye, Y.-A., Hidalgo, C.A., Verleysen, M., Blondel, V.D. (2013). Unique in the Crowd: The Privacy Bounds of Human Mobility, *Nature,* srep. 3, 1376 ; DOI:10.1038/srep01376, http://www.nature.com/articles/srep01376

activités… Ces deux catégories ont des caractéristiques extrêmement différentes. Les **données d'identité** (le numéro de sécurité sociale ou tout autre identifiant direct) sont peu nombreuses, bien qualifiées, à diffusion bien maîtrisée par l'utilisateur ; ces données bénéficient généralement d'une bonne protection. *A contrario*, les **données périphériques** sont très nombreuses, mal connues des utilisateurs, et peu protégées, avec une diffusion difficilement maîtrisée, car ces données sont nécessaires au bon fonctionnement d'un service réseau ou informatique. Si les données périphériques en tant que telles apparaissent plus ou moins discriminantes, prises de façon corrélée, elles permettent d'identifier leur propriétaire.

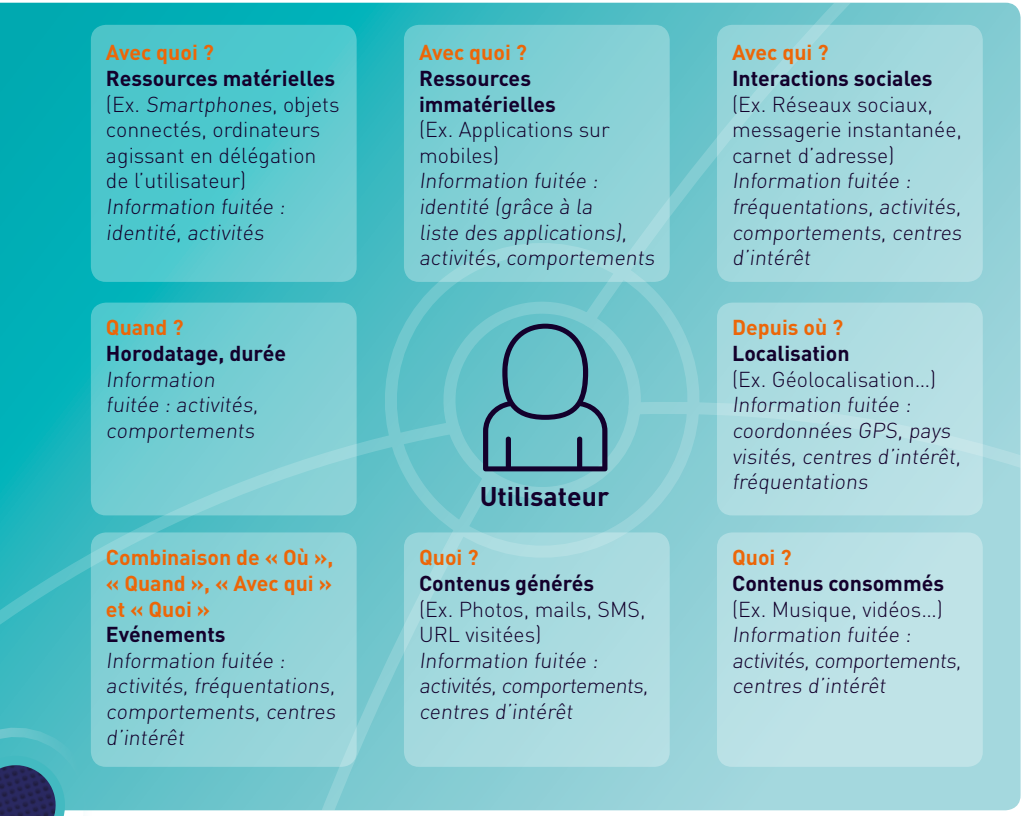


FIGURE 2. Illustration des multiples manières dont les données périphériques sont diffusées

En conclusion, il est extrêmement difficile pour un utilisateur, même averti, d'utiliser les technologies actuelles tout en préservant sa vie privée et ses données personnelles. Cependant, une chose semble certaine : rester intraçable implique nécessairement de ne posséder ni téléphone mobile ni objets communicants ; il s'agit là d'une condition nécessaire, mais loin d'être suffisante du fait de tous les autres moyens technologiques à disposition par ailleurs. Aujourd'hui, de nombreux efforts sont réalisés par les chercheurs et ingénieurs pour améliorer le niveau de protection de la vie privée. Les approches « *Privacy by design* » qui consistent à intégrer dès la conception des produits des techniques de protection en font partie, tout comme les solutions de preuves d'identité ou d'attributs préservant le pseudonymat.

Fiche 4. Les enjeux économiques des identités numériques

Patrick Waelbroeck

La première question à laquelle cette fiche tente de répondre porte sur l'importance économique de la notion d'identité numérique. Ce point soulève deux autres questions :

- Est-ce juste un phénomène important économiquement ?
- Est-ce que ce qui se passe en ligne a une influence sur l'économie réelle ?

La réponse à ces deux questions est affirmative, et ce, pour quatre raisons. Premièrement, la façon dont les gens gèrent ou non leurs identités en ligne influence de manière fondamentale le développement des communautés en ligne et la quantité ainsi que la fiabilité des informations qui y circulent. D'une part, les communautés telles que celles présentes sur Amazon.com ou ebay.com sont très actives pour générer des informations sur les produits et les vendeurs de ces plateformes d'échanges. Ces informations conduisent souvent à des recommandations personnalisées qui ont une grande valeur économique dans la mesure où les internautes peuvent prendre des décisions informées à la fois en ligne ou dans le monde physique.

Deuxièmement, les évènements qui se produisent en ligne peuvent avoir un impact important dans la vie réelle. Pour ne prendre qu'un exemple, les sites de rencontres en ligne permettent aux gens de prendre contact en ligne pour éventuellement se rencontrer réellement. Les effets entre le monde réel et le monde virtuel peuvent se faire ressentir dans les deux sens, puisqu'une différence de point de vue lors d'une rencontre physique peut se répercuter en ligne ; inversement, des photos ou des messages échangés sur Facebook peuvent avoir des répercussions énormes sur la vie privée des gens ; de nombreux tabloïds illustrent quotidiennement ce point. Enfin, de plus en plus souvent, une rencontre physique est précédée par une « prise de contact virtuelle » (par exemple dans le cadre d'un recrutement ou d'un contact commercial). La connaissance de l'identité de l'internaute et sa « e-réputation » sont donc de plus en plus essentielles pour le recrutement professionnel. Le développement de sites de réseaux professionnels tels que Linkedin témoigne de cette évolution.

Troisièmement, la manière dont les gens gèrent leurs identités peut avoir un impact sur des entreprises telles que Google ou Facebook qui exploitent les données personnelles. En effet, dans un environnement de confiance, les internautes seraient prêts à céder leurs informations privées en échange de services personnalisés et d'offres adaptées à leurs besoins et à leurs envies. Ces données personnelles représentent un enjeu financier considérable.

Enfin, les économistes devraient s'intéresser à la notion d'identités numériques, car la manière dont les gens se présentent aux autres ou sont identifiés par les autres a un impact sur leurs choix économiques et donc sur leurs demandes et donc sur le marché auquel ils participent.

Cependant, les recherches économiques sur les identités numériques, leur gestion et leurs effets économiques ont rarement fait l'objet de travaux académiques pour deux raisons. Premièrement, les économistes postulent l'existence d'une fonction d'utilité qui mesure le niveau de bien-être ou de satisfaction d'un individu, mais n'expliquent pas comment cette utilité se construit (construction de l'identité sociale, construction des goûts et des références culturelles). Deuxièmement, les identités numériques se construisent par les interactions avec les autres, et là encore, la théorie économique n'est pas adaptée pour analyser les interactions directes entre les agents économiques. Ce double constat est partagé par Kirman[35] (2004) qui plaide pour que les sciences économiques s'intéressent plus à la question des interactions et, de manière implicite, à celle de l'identité. En effet, pendant plus de trente ans, les sciences économiques ont évolué autour du paradigme de l'équilibre général. Dans ce cadre, les consommateurs et les entreprises sont des atomes isolés et sans identité qui n'interagissent qu'à travers un système de prix. La notion d'identité n'est donc pas essentielle pour comprendre ces interactions. Cependant, même si tous les agents sont anonymes, le marché fonctionne bien. Un point sur lequel nous reviendrons dans la dernière section.

4.1. **Enjeux des business modèles du numérique**

Les identités numériques des internautes jouent un rôle primordial dans l'économie numérique où les entreprises développent des business modèles en collectant les informations personnelles de leurs clients pour pratiquer de la discrimination par les prix, du ciblage publicitaire et des recommandations personnalisées. Ces identités ont donc un impact sur les actions économiques des individus. Pour les entreprises commerciales, les identités numériques d'un individu sont analysées à travers le prisme de sa disponibilité à payer. Même sans connaître avec certitude l'identité d'un client, ses informations personnelles sont de bons indicateurs de ses identités numériques et de sa disponibilité à payer pour les produits offerts.

Une partie de la littérature économique aborde la notion de l'identité sous l'angle de la discrimination par les prix : les entreprises cherchent à collecter les informations personnelles liées à l'identité d'une personne pour trouver le meilleur prix auquel elles peuvent vendre leurs produits et services en fonction de la disponibilité à payer des clients potentiels. Ceux-ci bénéficient alors de services personnalisés ou customisés. Ces réseaux sociaux sont financés par la publicité et dépendent donc fondamentalement du comportement des

35 Kirman, A. (2004). The Structure of Economic Interaction: Individual and Collective Rationality, *in Cognitive Economics: An Interdisciplinary Approach*, Bourgine, P., Nadal J.-P. (Eds.), Springer, Ch. 18.

internautes et des traces qu'ils laissent ou non lors de leur parcours de navigation. Dans le cas extrême où les internautes utilisent des pseudonymes ou naviguent de manière anonyme, de tels sites deviennent moins attractifs auprès des annonceurs qui cherchent à cibler leurs offres. Étant donné le manque d'informations, les annonceurs ne peuvent plus aussi facilement pratiquer des prix en fonction de leur cible : la discrimination par les prix en est donc rendue difficile. Ainsi, la gestion active des identités remet en question la métaphore de l'oignon qui postule que l'identité d'une personne est constituée de couches successives laissées par les influences socio-cultures passées. Il suffirait alors pour mieux cibler les internautes de peler les différentes couches pour arriver au noyau. Hui et Png (2004)[36] et Rochelandet (2010)[37] proposent une revue de cette littérature sur l'économie de la protection de la vie privée.

Un deuxième aspect des identités numériques porte sur l'utilisation des informations personnelles pour :

- mieux cibler les publicités (par exemple la technologie de *retargeting* de Criteo) ;
- améliorer l'adéquation produit/consommateur (par exemple, Compass Coffee optimise chaque étape de la préparation d'un café en fonction de paramètres déterminés par des préférences personnelles, grâce à des capteurs de température).

Enfin, les identités numériques sont utilisées pour fournir des recommandations personnalisées (ces algorithmes sont bien développés chez Spotify, Deezer ou Netflix) à partir de traces de navigation ou de contributions sur des sites web.

Les membres des communautés d'expériences proposent de découvrir de nouveaux produits au reste de la communauté. On voit ainsi sur les sites communautaires de plus en plus de fonctions permettant soit de faire des liens entre les produits (par exemple, sur www.amazon.com, sur la page de présentation du produit, on trouve une rubrique intitulée « *Les internautes ayant acheté cet article ont également acheté* »), soit de faire des liens entre les différents membres de la communauté (par exemple en fonction du rapprochement des notes données aux produits évalués). Bounie et al. (2008)[38] relèvent l'importance des commentaires laissés par les autres consommateurs et du bouche-à-oreille, principalement *via* des forums, pour l'achat de jeux vidéo.

---

36 Hui K.L., Png I.P.L. (2006). The Economics of Privacy, *in Handbooks in Information Systems*, Hendershott, T. (Ed.), Elsevier.

37 Rochelandet, F. (2010). Économie des données personnelles et de la vie privée, Paris, La Découverte, coll. « Repères ».

38 Bounie, D., Bourreau, M., Gensollen, M., Waelbroeck, P. (2008). *Do Online Customer Reviews Matter ? Evidence from the Video Game Industry*, Telecom ParisTech Working Paper N° ESS-08-02. http://ssrn.com/abstract=1091449.

4.2. **Gestion des identités numériques**

On ne partage pas les mêmes informations personnelles avec l'administration, les acteurs de commerce électronique et les réseaux sociaux (Nissenbaum, 2010)[39]. Autrement dit, l'offre d'informations personnelles dépend de la sphère, et du rôle que l'on joue dans cette sphère. Il est donc important de donner aux utilisateurs de services numériques plus de contrôle sur leurs données personnelles. Ainsi, Balgobin et al. (2015)[40] montrent à partir des quatre vagues du baromètre de la confiance de l'ACESL-CDC (environ 1000 personnes par enquête) que le nombre de personnes qui ne veulent pas partager des informations avec aucun acteur économique est passé de 5 % en 2009 à plus de 20 % en 2015. Par ailleurs, ces personnes ne souhaitent pas communiquer certaines informations sensibles, comme les informations de santé et les informations personnelles avec les réseaux sociaux et les acteurs du web, alors qu'elles sont prêtes à partager des données bancaires avec les administrations publiques et les banques. Les internautes et utilisateurs d'outils numériques souhaitent donc avoir le contrôle sur la manière dont ils sont identifiés par les principaux acteurs économiques et ne souhaitent pas partager les mêmes informations avec tout le monde.

Nous analysons par ailleurs les facteurs économiques (coût/bénéfice) qui influencent le niveau de partage d'un individu du sondage : les risques liés à l'utilisation des réseaux sociaux et d'internet, l'activité en ligne, la sociabilité et la visibilité en ligne, l'âge.

Les facteurs socio-économiques expliquent l'offre d'informations personnelles et la manière dont les individus sont identifiés en ligne.

4.3. **Identités numériques et réputation en ligne**

La littérature sur les asymétries d'information analyse la notion d'identité en ligne à travers la notion de réputation. Le développement d'une bonne réputation explique pourquoi il est important pour l'individu de gérer ses informations personnelles sur les plateformes de ventes telles qu'eBay ou Amazon Marketplace : il existe une prime à la réputation qui permet de facturer un produit ou service plus cher que celui de son concurrent.

La théorie économique de la réputation apporte également un éclairage sur les motivations des gens dans leur manière de gérer de manière active leurs identités. La réputation

39 Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press.

40 Balgobin, Y., Bounie, D., Waelbroeck, P. (2015). *Quelle acceptation par les Français du partage de leurs données personnelles ?*, document de travail.

est définie comme un « *goodwill* », qui est un stock qui augmente avec les expériences positives. Cette « prime à la réputation » a une valeur économique, qui est cependant difficile à mesurer à partir de données collectées sur internet en partie parce que la réputation peut être manipulée. Il existe même des marchés de la réputation où des vendeurs paient pour recevoir de bonnes évaluations. Il s'agit alors pour l'acheteur d'évaluer la réputation comme un signal imparfait de la véritable fiabilité d'un vendeur. Les études montrent qu'il existe une faible prime à la réputation. La réputation a cependant un effet sur la probabilité d'effectuer une transaction (pour un vendeur). Par exemple, Cabral et Hortacsu (2010)[41] montrent qu'une augmentation d'un pour cent du nombre d'évaluations négatives conduit à une baisse de 7,5 % du prix de vente. Ils montrent également que lorsqu'un vendeur reçoit sa première évaluation négative, son volume de vente baisse de 13 %. Un vendeur qui reçoit plusieurs évaluations négatives a plus de chance de quitter la plateforme de vente. De manière similaire, Bounie et al. (2012) montrent qu'il existe une prime à la réputation sur Amazon Marketplace qui peut atteindre 10 % du prix de vente[42].

La gestion active de son profil de vendeur a une valeur économique et explique pourquoi les gens cherchent à se présenter sous leur meilleur jour.

4.4. *Financial Privacy*

Nous étudions dans Balgobin et al. (2015)[43] d'un point de vue théorique et empirique l'impact du degré d'anonymat du moyen de paiement sur la fréquence et le montant des achats en ligne. Nous développons tout d'abord un modèle théorique qui montre que l'introduction d'un moyen de paiement anonyme en plus de la carte bancaire qui identifie toutes les transactions d'un individu permet à certains internautes soucieux de la protection de leurs transactions financières de participer au marché. Les frais de transaction collectés par l'entreprise qui propose le moyen de paiement anonyme lui permettent de générer des bénéfices lui assurant de collecter un minimum d'informations sur ses clients. Nous utilisons ensuite la quatrième vague du baromètre de la confiance pour tester l'hypothèse que les internautes qui utilisent des moyens de paiement anonyme achètent plus souvent

41 Cabral L., Hortascu A., (2010). The Dynamics of Seller Reputation : Theory and Evidence from eBay, *Journal of Industrial Economics*, Vol. 58.

42 Bounie, D., Eang, B., Sirbu, M. A., Waelbroeck, P. (2012). *Online Price Dispersion : An International Comparison*. http://ssrn.com/abstract=1625847

43 Balgobin, Y., Bounie, D., Quinn, M., Waelbroeck, P. (2015). *Payment Instruments, Financial Privacy and Online Purchases*, document de travail.

en ligne que les autres, toute chose étant égale par ailleurs. Nous utilisons des méthodes économétriques qui indiquent que cette hypothèse est satisfaite.

L'utilisation de moyens de paiement anonyme augmente le volume d'achats en ligne.

4.5. **Perspectives**

Anonymat et discrimination par les prix

La question que les économistes doivent se poser est la suivante : quelle situation, entre la discrimination par les prix du premier degré où tout le monde est parfaitement identifié et l'anonymat où personne n'est identifié augmente le plus la participation sur le marché, génère le plus d'opportunités commerciales et maximise le bien-être pour la société ? Cherchant à augmenter leur revenu de ciblage, les sociétés de l'internet utilisent des outils de plus en plus intrusifs pour collecter des données personnelles. Face au ciblage, les internautes adoptent des outils numériques pour protéger leurs informations, ce qui pourrait entraîner une course aux armements. La littérature économique a peu discuté des stratégies de protection des consommateurs et de la proposition de valeur liée à la protection de l'anonymat. Quel serait l'équilibre d'un marché où une entreprise pratique la discrimination de prix et une autre garantirait l'anonymat de ses clients ?

Big data et véracité : vers une modélisation des identités numériques

De plus en plus de compagnies développent des services basés sur l'exploitation massive de données personnelles collectées en ligne. Dans quelle mesure ces données sont-elles représentatives de la réalité des individus concernés ? Cette fiche soulève d'importantes limites à l'utilisation des données issues de collectes d'identités numériques et au *big data* de manière générale. Premièrement, la métaphore de l'oignon est incomplète : les internautes ne protègent pas une identité principale, mais gèrent des identités multiples en fonction d'un contexte socionumérique. Deuxièmement, les individus peuvent se présenter sous de fausses identités ou des identités partielles ou espérées ou s'identifier au minimum pour rester le plus anonyme possible. Troisièmement, ils peuvent contribuer beaucoup ou peu à des projets collectifs (open source, Wikipedia, forums et autres communautés de savoir). Dès lors, certaines caractéristiques et opinions seront surreprésentées. Les solutions à ces problèmes de données se trouveront dans la modélisation explicite du choix des identités et de l'étendue de la contribution des individus. De rares travaux économiques, principalement théoriques et hétérodoxes, abordent cependant des questions liées

à l'identité et aux informations personnelles. Akerlof et Kranton (2000)[44] ou Sen (2002)[45] ont directement abordé la modélisation de la notion d'identité dans la fonction d'utilité en vue d'expliquer par exemple les dons d'argent à l'université. Ces recherches analysent les identités numériques dans un contexte socio-économique qui précise des normes et des liens d'interactions. Elles devront être poussées pour mieux comprendre le choix d'une identité numérique parmi plusieurs disponibles.

44 Akerlof, G.A., Kranton, R.E. (2000). Economics and Identity, *Quarterly Journal of Economics*, 115(3).

45 Sen, A. (2002). *Rationality and Freedom*, Harvard, Harvard Belknap Press.

Fiche 5. Fonctionnement d'un système de gestion des identités numériques

Armen Khatchatourov
et Claire Levallois-Barth

Cette fiche fournit les bases quant au fonctionnement des systèmes de gestion des identités numériques déployés. Elle décrit schématiquement les acteurs susceptibles d'être impliqués, le cycle de vie d'une identité numérique, puis fournit deux exemples représentatifs, celui de l'identité numérique régalienne s'appuyant sur une carte nationale d'identité électronique et celui d'une identité numérique « privée » s'appuyant sur un réseau social.

5.1. **Quels sont les acteurs d'un système de gestion des identités numériques ?**

Un système de gestion des identités numériques implique schématiquement trois types d'acteurs.

L'**utilisateur** est la personne physique ou le représentant d'une personne morale détenteur de l'identité. Il est représenté par un jeu d'**attributs** (nom, sexe, adresse, revenu fiscal, photos, etc.).

Le fournisseur de services est un service électronique public ou privé qui permet à l'utilisateur d'accéder à des ressources en ligne ou d'accomplir des actions en ligne. Pour cela, il doit authentifier l'utilisateur, c'est-à-dire s'assurer qu'il s'agit bien de la bonne personne en recourant, en règle générale, à un tiers de confiance.

Le **tiers de confiance** englobe trois fonctions qui peuvent être assurées par un seul organisme ou des organismes différents :

- **l'autorité de délivrance** délivre l'identité numérique, en faisant le lien initial entre la personne physique ou morale et l'identité numérique ;
- **le fournisseur d'identités** gère l'identité numérique au quotidien et la confirme auprès du fournisseur de services. Dans sa fonction minimale, le fournisseur d'identités gère et confirme uniquement les attributs nécessaires pour l'authentification (par exemple nom, numéro de carte à puce et validité de l'identité numérique) ;
- **les fournisseurs d'attributs** sont des acteurs facultatifs qui fournissent les attributs « supplémentaires » décrivant l'utilisateur. Ainsi, le fournisseur d'identités confirme au fournisseur de services l'identité numérique elle-même et les attributs de base ; le fournisseur d'attributs confirme les attributs supplémentaires comme le revenu fiscal ou l'exercice d'une profession.

5.2. **Comment naît, vit et meurt une identité numérique ?**

La procédure de délivrance de l'identité numérique comporte une phase dite d'**enrôlement**, pendant laquelle une autorité de délivrance octroie à l'utilisateur, *via* le fournisseur d'identités, une identité numérique comportant des attributs.

Lorsque l'utilisateur se connecte à un service, il s'authentifie en utilisant des moyens d'**authentification** qui servent à prouver au fournisseur d'identités que le porteur de l'identité numérique est bien celui qu'il prétend être. Ces moyens sont variés, pouvant se présenter sous la forme d'un couple *login*/mot de passe, d'une authentification à deux facteurs (*login*/mot de passe + envoi d'un SMS vers un deuxième terminal pour communiquer le mot de passe supplémentaire à usage unique, tel 3DSecure) ou de solutions hautement sécurisées telles une carte à puce dédiée ou une carte SIM dans un *smartphone*. Ces moyens d'authentification présentent des niveaux de sécurité différents. Cette question est traitée à la fois dans le projet européen à grande échelle STORK[46], *via* les normes adoptées par l'Organisation internationale de normalisation, l'ISO (*International Organization for Standardization*), et par le règlement sur l'identification et les services de confiance eIDAS (*cf.* fiche 10 sur ces deux derniers points).

Une fois authentifiée, la personne est en mesure d'**utiliser le service**. En fonction des actions qu'elle accomplit, le jeu des attributs qui la représente peut évoluer, soit en fonction d'une action qu'elle effectue explicitement (déclaration du revenu annuel), soit à son insu (collecte de données de géolocalisation).

Le fournisseur d'identités, éventuellement en conjonction avec l'autorité de délivrance, gère également la **révocation** de l'identité numérique. Typiquement, lorsque le support de l'identité numérique (par exemple une carte à puce) a été perdu, celle-ci est révoquée et ne pourra plus être utilisée.

5.3. L'exemple d'une identité numérique s'appuyant sur une carte nationale d'identité électronique

Sans préjuger de la diversité des solutions nationales mises en place (*cf.* fiche 8), le schéma type est le suivant en ce qui concerne la carte nationale d'identité électronique.

L'autorité de délivrance et le fournisseur d'identités sont représentés par deux organismes qui travaillent conjointement. **L'enrôlement** passe par un guichet d'enrôlement qui est une instance de l'autorité publique en charge de l'identité (par exemple, le ministère de l'Intérieur ou l'administration fiscale), laquelle vérifie l'identité en la présence physique de l'utilisateur. La gestion quotidienne est déléguée à une entité dédiée qui peut être un consortium public-privé assurant les fonctions du fournisseur d'identités. Le fournisseur d'identités sert également de tiers de confiance pour l'ensemble des fournisseurs de ser-

46 Pour plus d'informations sur cette plateforme d'interopérabilité des identités numériques à l'échelle européenne : https://www.eid-stork.eu/

vices qui composent l'écosystème (école, banque, caisse d'allocations familiales) confirmant les attributs de l'identité numérique.

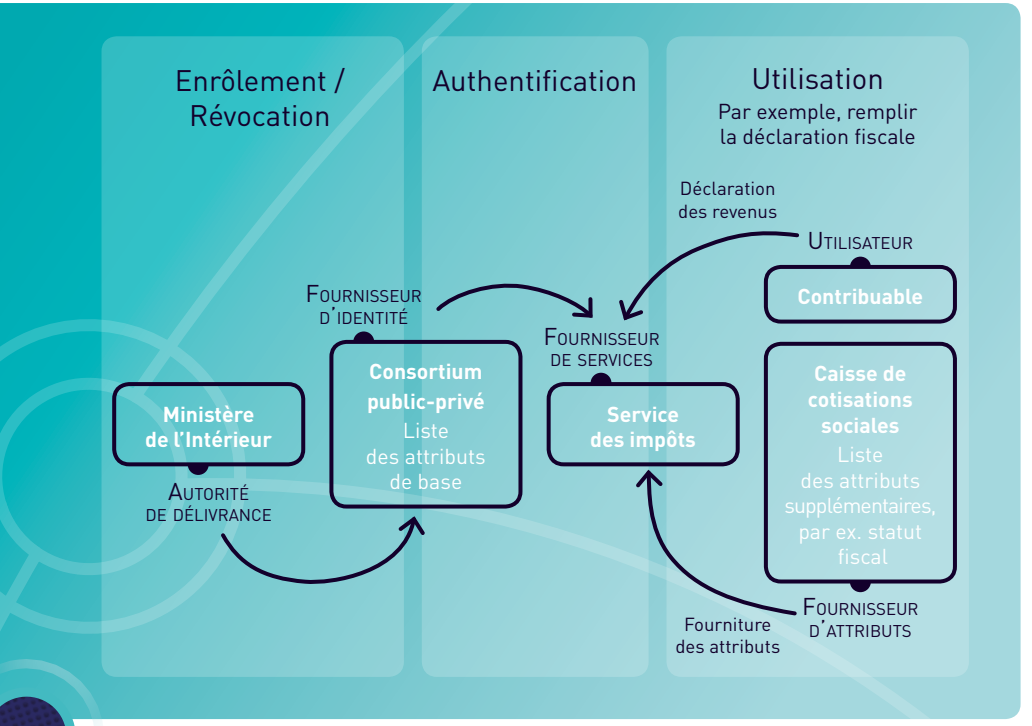


Figure 3. **Gestion de l'identité numérique : exemple d'implémentation de la carte nationale d'identité électronique**

Lorsque l'utilisateur se connecte à un service de déclaration de revenus en ligne, le service fait appel au fournisseur d'identités pour confirmer :

- que le porteur de l'identité numérique est bien celui qu'il prétend être (**authentification** à l'aide d'une carte à puce par exemple) ;
- que ce porteur habite bien dans le département concerné, et qu'il exerce une profession libérale l'autorisant à bénéficier d'un régime d'imposition particulier.

Cet attribut « supplémentaire » (dans le sens où le fait d'exercer une profession libérale n'est pas nécessairement connu par le fournisseur d'identités lors de l'enrôlement) peut être fourni par un fournisseur externe d'attributs, comme un ordre professionnel ou une

caisse de cotisations sociales. À l'issue d'une session, les attributs de l'utilisateur ont évolué en intégrant son nouveau revenu fiscal.

Si la carte à puce est perdue ou volée, l'utilisateur contacte le fournisseur d'identités et/ou l'autorité de délivrance qui procèdent à sa **révocation** en inscrivant la carte sur la liste des cartes non valides (dite « liste de révocation »).

5.4. L'exemple d'une identité numérique s'appuyant sur un réseau social

Dans le cas de l'identité numérique s'appuyant sur un service de réseautage social (réseau social), tels FacebookConnect ou Google+ Sign-In, la même société délivre et gère l'identité numérique. Facebook est à la fois l'autorité de délivrance et le fournisseur d'identités. **L'enrôlement** se résume à la création d'un compte en ligne et à la fourniture de certaines données personnelles par l'utilisateur. Les attributs sont variés et évoluent dans le temps : les photos, les commentaires publiés, le nombre d'amis, etc.

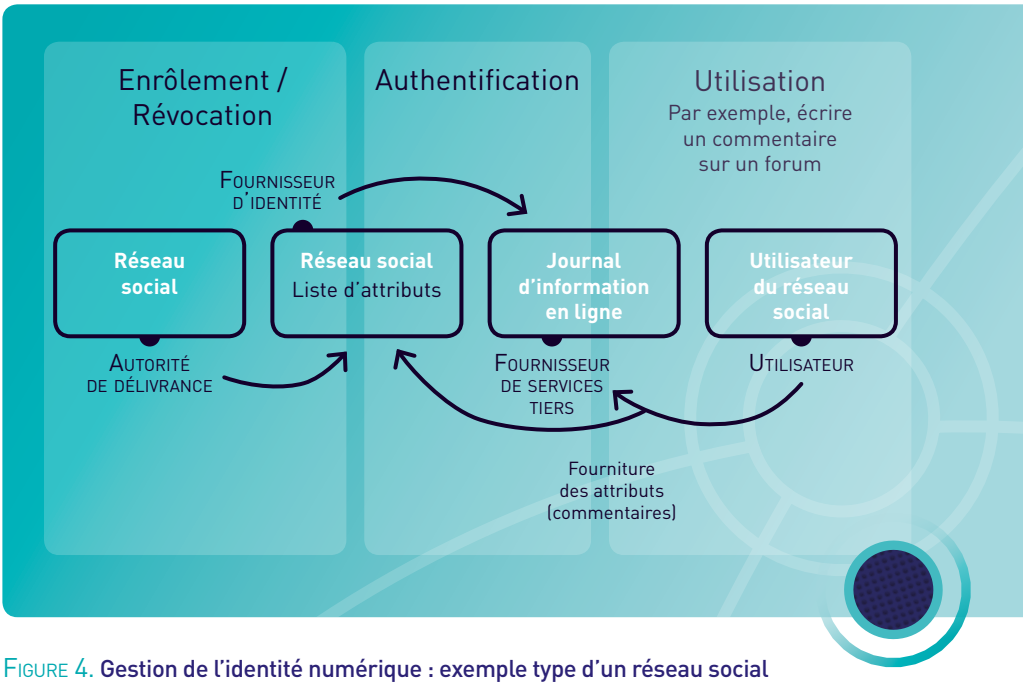


Figure 4. Gestion de l'identité numérique : exemple type d'un réseau social

Lorsque l'utilisateur du réseau social visite un site fourni par un tiers, comme le site d'un journal d'information en ligne, le site du journal lui demande de **s'authentifier** à l'aide de son identité numérique attachée à son réseau social. Le journal délègue donc au réseau social l'authentification de l'utilisateur par la saisie de l'identifiant et du mot de passe. Le site tiers récupère alors les données identifiantes de l'utilisateur ainsi que certaines données personnelles qui lui permettent de mieux cibler l'utilisateur.

Une fois authentifié, l'utilisateur peut accomplir les actions sur le site du journal, par exemple en publiant des commentaires. Ces commentaires sont alors visibles sur le forum du journal comme étant produits par l'utilisateur en question. De plus, ces commentaires apparaissent sur le compte du réseau social de l'utilisateur (son « mur » Facebook). Ce faisant, le lien entre les activités de l'utilisateur sur les différents sites tiers est effectué et rendu public sur le site du réseau social.

À l'issue d'une session, les attributs de l'utilisateur détenus par le réseau social et le site du journal ont évolué en intégrant sa nouvelle publication.

La **révocation** est gérée par le fournisseur d'identités qui peut suspendre, puis supprimer le compte et les attributs soit à la demande de l'utilisateur, soit de sa propre initiative.

Fiche 6. Identité numérique et gestion des données personnelles

Claire Levallois-Barth

Cette fiche décrit les principes clés de protection des données personnelles afin que les systèmes de gestion des identités numériques collectent et utilisent les attributs des individus conformément au cadre légal. Si, au niveau international, il existe un certain consensus sur les principes de base destinés à encadrer la collecte et le traitement des données personnelles, on note cependant des divergences significatives quant à l'objectif visé et à la perception même des concepts juridiques de « donnée personnelle » et de « vie privée »[47]. Cette fiche se concentre sur la législation de l'Union européenne, et se réfère plus particulièrement à l'exemple français.

> « *Toute personne a droit à la protection des données à caractère personnel la concernant* » (art. 8 § 1 de la Charte des droits fondamentaux de l'Union européenne).

Lors de la phase d'enrôlement, une autorité de délivrance octroie à l'utilisateur une identité numérique comportant des attributs. Cette identité et les attributs sont par la suite enregistrés par le fournisseur de services et le tiers de confiance (*cf.* fiche 5).

Sur le plan juridique, les attributs dans la mesure où ils sont qualifiables de données personnelles relèvent de la **directive européenne 95/46/CE** Protection des données[48]. Ce texte a été transposé dans chaque État membre de l'UE, notamment en France par la loi du 6 août 2004 modifiant ainsi la **loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés** (dite « loi Informatique et libertés »)[49].

La directive prévoit que chaque État doit charger une ou plusieurs autorités de surveiller son application. En France, il s'agit de la Commission nationale de l'informatique et des libertés (CNIL). Cette dernière participe avec les autorités de protection des données personnelles des 27 autres États membres de l'UE à un groupe de travail dit « groupe de l'article 29 » (ou « G29 » en référence à l'article 29 de la directive). Le G29 remplit une mission consultative.

Notons que la directive Protection des données devrait être remplacée par un règlement, *a priori* mi-2016.

---

47 Levallois-Barth, C. (2014). Global Privacy Governance and Legal Issues, *in Cahier de prospective The futures of privacy,* Dartiguepeyrou, C. (Ed.), Fondation Télécom, Institut Mines-Télécom, pp. 55-61.

48 Directive n° 95/46/CE du Parlement européen et du Conseil du 24 oct. 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 : *JOCE,* L. 281 du 23 nov. 1995, p. 31.

49 Loi n° 78-17 du 6 janv. 1978 relative à l'informatique, aux fichiers et aux libertés : *JO*, 7 janv. 1978, p. 227 ; modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (*JO*, 7 août 2004, p. 14063).

6.1. Quand un système de gestion des identités numériques effectue-t-il un traitement de données personnelles ?

Un attribut est qualifié de « donnée personnelle » lorsqu'il concerne « *toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; 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* » (art. 2a) de la **directive européenne 95/46/CE** (Protection des données (*cf.* fiche 2).

Ainsi, dès qu'une information a un lien même ténu avec un individu, elle constitue une donnée personnelle. Il peut s'agir des nom et prénom, d'une adresse de courrier électronique, d'un pseudonyme, d'un numéro de téléphone ou de carte bancaire, de données de géolocalisation, du lieu et de la date de naissance, des goûts et préférences. Les adresses IP — lorsqu'elles permettent l'identification de l'internaute — et les données biométriques, notamment la voix, l'iris, le réseau veineux, la forme du visage, constituent également des données personnelles[50].

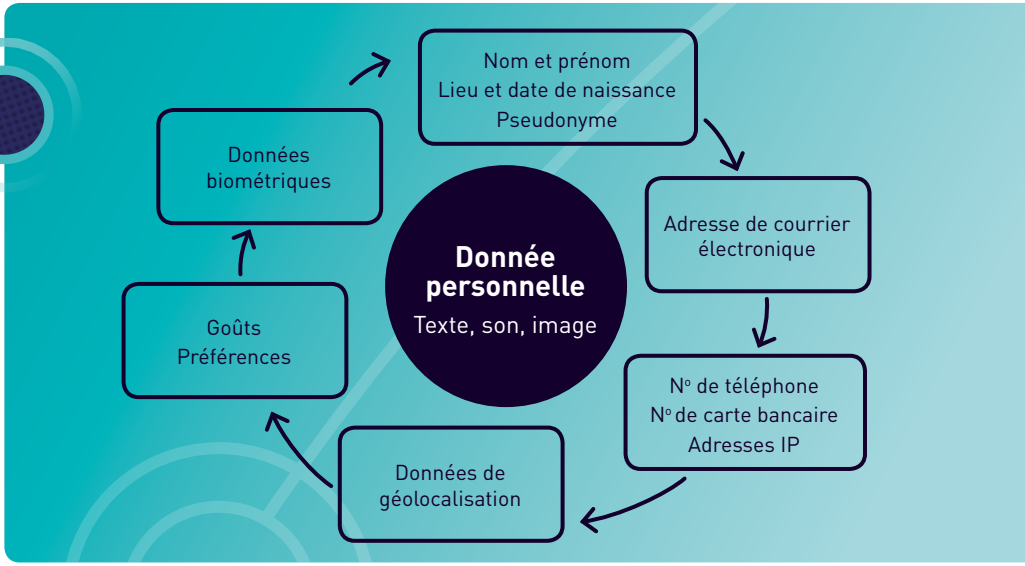


FIGURE 5. **Exemples types de données personnelles**

50 V. Groupe Article 29, Avis 4/2007 sur le concept de donnée à caractère personnel, adopté le 20 juin 2007, WP 136.

Une information anonyme ne constitue pas une donnée personnelle.

L'anonymisation suppose de détruire le lien de façon irréversible entre l'information et la personne ce qui implique non pas de considérer une donnée isolée, mais de prendre en compte les croisements possibles entre les informations (*cf.* fiche 3 sur l'anonymat et le pseudonymat).

La **directive européenne 95/46/CE** Protection des données s'applique lorsqu'un système de gestion des identités numériques effectue un traitement de données personnelles. Cette notion, entendue largement, désigne « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction » (art. 2b) de la directive 95/46/CE Protection des données). Cette définition s'applique, quels que soient la technologie utilisée, l'organisation particulière des données et le service.

6.2. Sur qui pèse la responsabilité ?

Le **responsable du traitement** de données personnelles doit veiller au respect de la directive. Il s'agit de l'autorité publique, du service ou de l'organisme qui détermine les finalités et les moyens du traitement[51].

La responsabilité pèse sur la personne qui a le pouvoir de définir ou de contrôler le contenu du traitement, qui exerce une influence de fait.

En principe, le fournisseur d'identités, le fournisseur de services ou le tiers de confiance peuvent chacun être qualifié de responsable du traitement. Ils doivent collecter, utiliser et transmettre légalement les attributs qualifiés de données personnelles, notamment en s'acquittant des formalités administratives à effectuer auprès de l'autorité de protection des données personnelles. Dans le cas contraire, ils encourent des sanctions qui sont définies au niveau national. En France, la CNIL peut prononcer des sanctions pénales, civiles et administratives. Cette autorité peut ainsi prononcer un avertissement, une mise en de-

51 Sauf désignation expresse par les dispositions législatives ou réglementaires de la personne, *cf.* art. 2 de la directive précitée.

meure, une injonction de cesser le traitement ou une amende. Elle dispose également d'un pouvoir de perquisition.

Le responsable du traitement doit être distingué du **sous-traitant**, lequel traite les données pour le compte du premier. En pratique, le sous-traitant est un prestataire externe contractuellement lié au responsable du traitement agissant sur instruction de ce dernier.

Précisons que chaque État membre applique les dispositions nationales transposant la directive au responsable du traitement établi sur son territoire. Dans le cas où le responsable du traitement est établi hors UE, il est soumis à la loi de l'État de l'UE où sont situés les moyens de traitement. Dans ce dernier cas, à titre d'illustration, la loi française s'applique lorsqu'un fournisseur d'identités établi aux États-Unis participe à des actions de lecture ou d'écriture de données personnelles figurant dans un ordinateur ou un *smartphone* localisé en France.

6.3. **Comment collecter et utiliser légalement les attributs qualifiés de données personnelles ?**

La législation de l'UE vise à définir un équilibre entre la protection des personnes et l'utilisation des données par des entités privées ou publiques.

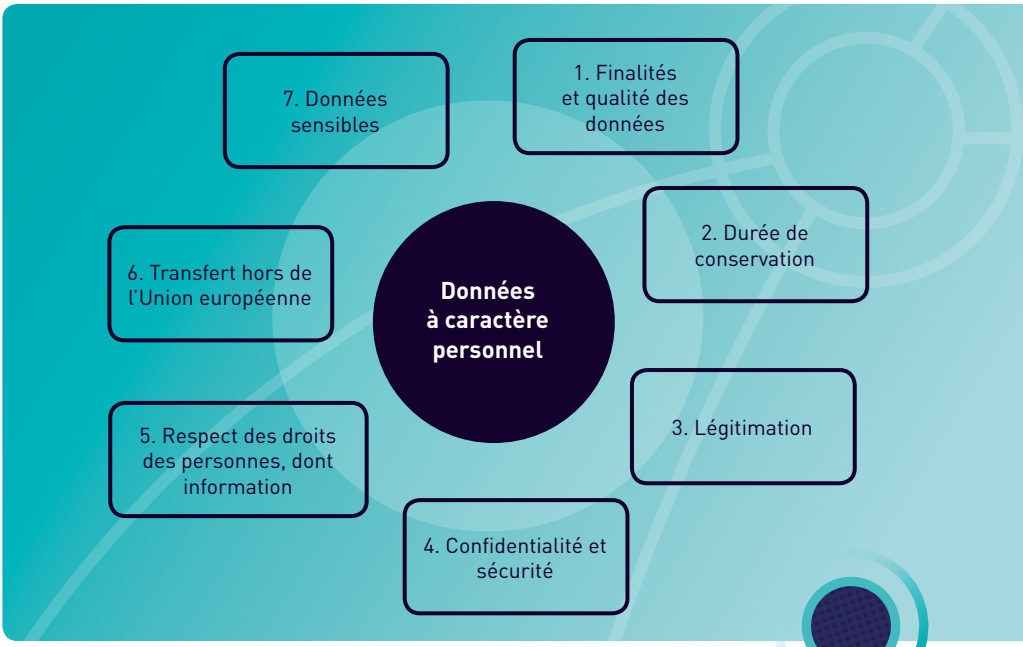


FIGURE 6. **Principes clés de protection des données personnelles**

Dans ce cadre, le responsable du traitement, avant de collecter une donnée personnelle, doit :

1. Déterminer les finalités du traitement (c'est-à-dire les usages ou les objectifs qui doivent être explicites et légitimes) et **s'assurer de la qualité des données :** conformément au principe de proportionnalité, seules des données « adéquates, pertinentes et non excessives au regard des finalités » et « exactes, complètes et, si nécessaire, mises à jour » doivent être collectées (art. 6 de la directive 95/46/CE Protection des données).

2. Fixer une durée de conservation des données en veillant à ne pas excéder la durée nécessaire aux finalités. Passé ce délai, les informations doivent être supprimées ou anonymisées :

- **la directive 95/46/CE** Protection des données (comme la loi Informatique et libertés) ne définit pas de durée de conservation standard. Le responsable du traitement doit lui-même définir cette durée en fonction des caractéristiques de son traitement ;
- La durée de conservation des données peut être déterminée par un texte légal. Par exemple, en France, l'article L. 561-12 du Code monétaire et financier fixe la durée de conservation des éléments d'identité des clients habituels et occasionnels à 5 ans à compter de la clôture du compte ou de la cessation de la relation commerciale.

3. S'assurer qu'il se conforme au principe de légitimation : le responsable de traitement doit recueillir le consentement de la personne, ou bien s'assurer que le traitement remplit l'une des conditions suivantes, à savoir que le traitement est nécessaire :

- au respect d'une obligation légale incombant au responsable du traitement, ou
- à la sauvegarde de l'intérêt vital de la personne concernée, ou
- à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, ou
- à l'exécution d'un contrat auquel la personne concernée est partie ou de mesures précontractuelles prises à la demande de celle-ci, ou
- à la réalisation de l'intérêt légitime que poursuit le responsable du traitement ou le destinataire des données, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

Le consentement vise ici « *toute manifestation de volonté libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement* » (art. 2h) de la directive 95/46/CE Protection des données.

Cette manifestation doit être « indubitable », c'est-à-dire exprimée par une action comme celle de souscrire à un service ou de remplir un questionnaire.

4. Assurer la confidentialité et la sécurité des données personnelles

Pour aller plus loin : se reporter aux documents publiés par la CNIL : Guide « *La sécurité des données personnelles* » (2010)/Guide : « *Gérer les risques sur les libertés et la vie privée, la méthode* » (juin 2012)/Guide : « *Mesures pour traiter les risques sur les libertés et la vie privée* » (juin 2012).

5. Respecter les droits de la personne concernée :

- en informant la personne que ses données sont collectées, ce qui lui permet ensuite d'exercer son droit d'accès aux données et au besoin de faire rectifier les données, voire de demander à les supprimer. L'information doit porter sur l'identité du responsable du traitement, la finalité de son traitement, le caractère obligatoire ou facultatif des réponses, les destinataires des données, les droits dont la personne dispose, les transmissions de données envisagées hors de l'UE ;
- en offrant à la personne la possibilité de s'opposer pour des raisons prépondérantes et légitimes à ce que ses données fassent l'objet d'un traitement. Lorsque les données sont utilisées à des fins de prospection, en particulier commerciale, la personne n'a pas à justifier d'un motif.

6. En cas de transfert de données personnelles hors de l'UE, s'assurer que le transfert a lieu vers un pays offrant un niveau de protection « adéquat ».
Les pays se conformant au critère d'adéquation sont peu nombreux.

Les décisions d'adéquation prises par la Commission européenne concernent les trois États membres de l'Espace économique européen (Norvège, Liechtenstein et Islande), Andorre, Argentine, Canada, Suisse, Israël, Uruguay, Nouvelle-Zélande, Îles Féroé, Guernesey, l'Île de Man et l'Australie.

Si le transfert des données personnelles a lieu vers un pays ne disposant pas d'un niveau de protection adéquat, plusieurs solutions sont à envisager, notamment :

- l'entreprise transférant les données et celle les recevant insèrent dans un contrat les clauses contractuelles types définies par la Commission européenne ;
- un groupe d'entreprises adopte des règles internes (*Binding Corporate Rules* : BCR).

Le cas des données transférées vers les États-Unis est un peu particulier. Conformément à une décision de la Commission européenne rendue le 26 juillet 2000[52], une entreprise américaine pouvait effectuer un tel transfert si elle avait adhéré aux principes de la « sphère de sécurité » (« *Safe harbor* ») publiés par le département du commerce américain. Tel était notamment le cas de Facebook ou de Linkedin. Cette possibilité a été remise en cause par la Cour de justice de l'Union européenne dans un arrêt du 6 octobre 2015[53]. En effet, cette juridiction a invalidé la décision de la Commission en retenant « qu'une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée ». Est ici notamment visée la surveillance exercée par la NSA sur les données personnelles des citoyens européens hébergées aux États-Unis illustrée par l'affaire Snowden.

Les entreprises américaines doivent désormais s'appuyer sur les modes de transferts précédemment cités (clauses contractuelles et BCR) pour remplir le critère d'adéquation.

7. Identifier les données dites « sensibles »

Pour les informations révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la santé ou la vie sexuelle, la directive 95/46/CE Protection des données pose un principe d'interdiction de collecte.

Il existe néanmoins une dizaine d'exceptions à ce principe d'interdiction. Ainsi, les données personnelles sensibles peuvent notamment faire l'objet d'un traitement si elles ont été manifestement rendues publiques par la personne concernée, si le traitement est justifié

52 Décision 2000/520/CE de la Commission du 26 juill. 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du Commerce des États-Unis d'Amérique [notifiée sous le numéro C (2000) 2441] (Texte présentant de l'intérêt pour l'EEE) : *JOCE*, L. 215 du 25 août 2000, p. 7.

53 CJUE, 6 oct. 2015, *aff. C 362/14, Maximillian Schrems c. Data Protection Commissioner* : disponible sur www.curia.europa.eu

par un « motif d'intérêt public important » ou si la personne concernée a donné un consentement « explicite ».

➔ Si un réseau social fait figurer sur un formulaire d'inscription des questions portant sur des données sensibles, il doit indiquer très clairement que les réponses sont facultatives.

En outre, la directive laisse le soin aux États membres de déterminer les conditions dans lesquelles un numéro national d'identification ou tout autre identifiant de portée générale peut faire l'objet d'un traitement. En France, ce type d'identifiant, comme le numéro de sécurité sociale (NIR), est considéré comme étant une donnée sensible. Son utilisation est strictement encadrée et nécessite l'autorisation préalable de la CNIL. Cette dernière exige systématiquement que le responsable du traitement justifie de l'existence d'un texte législatif ou réglementaire spécifique légitimant sur le plan juridique l'utilisation de cette donnée. Ainsi, l'usage du NIR est limité aux sphères sociales et de la santé.

Le cadre légal ainsi présenté est en cours de révision.

6.4. Le futur règlement (UE) Données personnelles

Le 25 janvier 2012, la Commission européenne a publié une proposition de règlement ayant vocation à se substituer à l'actuelle directive 95/46/CE[54]. Ce règlement devrait *a priori* être adopté d'ici juin 2016 ; il entrera en vigueur deux ans après sa publication au Journal officiel de l'Union européenne. Directement applicable, il ne nécessitera pas de transposition en droit national. En France, la loi Informatique et libertés sera en grande partie abrogée tandis que la CNIL interprétera directement le nouveau texte.

En l'état actuel des négociations, le projet se caractérise par une grande complexité[55].

Il reprend la définition de la notion de « *donnée personnelle* » fournie par la directive 95/46/CE Protection des données tout en précisant qu'une personne « *peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identité, une donnée de géolocalisation ou un identifiant en ligne ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique,*

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

55 Nous nous référons ici à la version publiée le 28 janvier 2016. Brussels, 28 January 2016 (OR, en), 5455/16, disponible sur data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/en/pdf

génétique, psychique, économique, culturelle ou sociale »[56]. Il ajoute que « *les données qui ont subi une pseudonymisation, qui peuvent être attribuées à une personne physique par le biais d'informations additionnelles, doivent être considérées comme des informations relatives à une personne physique identifiable.* »[57]

Le règlement **reprend également les principes de protection exposés ci-dessus** (finalité, qualité des données, légitimation, niveau de protection adéquat, protection renforcée des données sensibles, etc.) **tout en ajoutant de nouveaux principes**, par exemple le principe de portabilité des données ou le droit à l'oubli numérique.

> ***Le droit à l'oubli numérique prend la forme d'un droit à l'effacement*** *des* ***données personnelles et à la cessation de leur diffusion,*** *en particulier en ce qui concerne des données que la personne a rendues disponibles lorsqu'elle était mineure* (art. 17 de la proposition de règlement en lien avec l'art. 8 [1] – traduction libre).

> ***Le droit à la portabilité des données*** *correspond au droit d'obtenir une copie des données dans un format informatisé et standardisé et le droit de transmettre les données d'un système de traitement automatisé à un autre système si le traitement est fondé sur le consentement ou sur un contrat* (art. 18 de la proposition de règlement – traduction libre).

Dans le même temps, on assiste à un **renforcement du consentement**, en particulier en ce qui concerne les enfants. Les **mesures fondées sur le profilage** sont également encadrées tandis que l'obligation de notifier les **failles de sécurité** auprès de l'autorité de contrôle (en France, la CNIL) est généralisée.

Sous l'influence anglo-saxonne, de nouveaux concepts apparaissent. Le principe de « *Privacy by design* » laisse une large part à la dimension technologique. Il consiste à intégrer par défaut la protection des données et de la vie privée, dès le stade de la conception d'un service ou d'un produit.

---

56 Traduction libre de l'article 4-1 de la proposition de règlement Protection des données dans sa version du 28 janvier 2016 selon lequel « 'personal data' *means any information relating to an identified or identifiable natural person* "data subject » *; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person* ».

57 Traduction libre du considérant 23 de la proposition de règlement Protection des données dans sa version du 28 janvier 2016 selon lequel « *Data which has undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered as information on an identifiable natural person* ».

Le principe d'« *accountability* » (ou principe de responsabilité) fait référence à l'ensemble des mesures internes prises par le responsable du traitement afin de démontrer le niveau de conformité des traitements effectués[58]. Cette démonstration peut se faire de différentes manières : rédaction de règles internes transparentes et facilement accessibles pour les personnes concernées, mise en place de mesures appropriées telles que la pseudonymisation des données pour lutter contre le vol d'identité, conservation des traces documentaires donnant des instructions au sous-traitant, désignation d'un délégué à la protection des données, réalisation d'audits (internes et externes), mise en œuvre des obligations en matière de sécurité des données ou d'une procédure de gestion des plaintes, analyses d'impact.

Pseudonymisation : *Traitement appliqué sur des données à caractère personnel de manière telle que ces données ne puissent pas être associées à une personne concernée spécifique sans l'utilisation d'informations supplémentaires, et ce tant que ces informations supplémentaires sont conservées séparément et soumises à des mesures techniques et organisationnelles garantissant la non-attribution des données à une personne identifiée ou identifiable* (art. 4 [3b] de la proposition de règlement – traduction libre[59]).

Pour aller plus loin sur l'analyse d'impact : voir les deux guides de la CNIL *Étude d'impact sur la vie privée* (EIVP ou PIA pour *Privacy Impact Assessment*) révisés en juin 2015 en prévision de l'adoption de la proposition de règlement :
➔ PIA, la méthode : **Comment mener une étude d'impact sur la vie privée** et
➔ PIA, l'outillage : **Modèles et bases de connaissances**

L'*accountability* s'inscrit dans une démarche de corégulation qui invite l'entreprise à se responsabiliser et à définir elle-même les mesures de mise en conformité qu'elle estime les plus appropriées. Sur cette base, le responsable du traitement est tenu de rendre des comptes à la fois aux autorités de protection et aux personnes concernées. À cette fin, la mise en place de mécanismes de certification, de marques et de labels, qui permettent aux

58 V. Groupe Article 29, Avis 3/2010 sur le principe de responsabilité, adopté le 13 juillet 2010, WP 173.

59 Traduction libre de l'article 4 (3b) de la proposition de règlement Protection des données dans sa version du 28 janvier 2016 selon lequel « 'pseudonymisation' *means the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional info rmation, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non -attribution to an identified or identifiable person* ».

personnes concernées d'évaluer rapidement le niveau de protection des données offert, doit être encouragée par les États membres et la Commission européenne. Parallèlement, les formalités préalables sont considérablement allégées tandis que la CNIL conserve un fort pouvoir de contrôle. Les sanctions sont largement renforcées (amendes pouvant aller jusqu'à 20 millions d'euros et 4 % du chiffre d'affaires mondial annuel).

Fiche 7. Intégration des principes de protection des données personnelles dans les systèmes de gestion des identités numériques

Claire Levallois-Barth
et Armen Khatchatourov

Le cadre légal ne saurait à lui seul assurer l'entière protection des données personnelles des utilisateurs. Le respect des principes clés posés par la directive 95/46/CE Protection des données (*cf.* fiche 6) nécessite, en effet, que ces principes soient mis en œuvre dès la phase de création, puis tout au long du cycle de vie des systèmes, terminaux, applications, procédés et architectures. Cette approche est connue sous le nom de *Privacy by design* ou protection de la vie privée dès la conception. Cette fiche propose de l'intégrer sous le vocable de *Data protection by design* au sein des systèmes de gestion des identités numériques.

7.1. L'approche *Privacy by design*

Un concept global

L'approche dite « *Privacy by design* » est apparue à la fin des années 1990 sous l'impulsion de la Commissaire à l'information et à la protection de la vie privée de l'Ontario (Canada), Ann Cavoukian[60]. Partant du constat que le cadre légal ne peut intervenir qu'*a posteriori* pour corriger les abus, la Commissaire propose d'intégrer le respect de la vie privée directement dans la conception et le fonctionnement des systèmes et réseaux informatiques, et ce, pendant toute la période de conservation des données personnelles. Cette forme de régulation *ex ante* consiste donc à agir en amont de l'utilisation abusive des données, en mettant en œuvre des systèmes qui, dans leur conception même, sont capables soit de prévenir les abus potentiels, soit de rendre explicites leurs modalités de fonctionnement et d'orienter les choix des utilisateurs dans le sens d'une meilleure protection.

Cette démarche a été reprise, en octobre 2010, lors de la 32e Conférence internationale des Commissaires à la protection des données et de la vie privée[61]. Selon la résolution adoptée sur proposition de Mme Cavoukian, « *la protection intégrée de la vie privée [constitue] un concept global pouvant s'appliquer à l'ensemble des activités d'une organisation de bout en bout, y compris à la technologie de l'information, aux pratiques administratives, aux procédés, à la conception matérielle et aux réseaux* ». Ce concept s'articule autour de sept principes fondamentaux qui « *décrivent les mesures proactives à prendre pour faire de la protection [des données personnelles] le mode implicite de fonctionnement de toutes les organisations, tout en assurant une fonctionnalité intégrale* ».

60 Cavoukian, A. (2009). Privacy by Design: The 7 Foundational Principles. Information and Privacy Commissioner of Ontario, Canada, https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

61 32e Conférence internationale des Commissaires à la protection des données et de la vie privée, Résolution sur la protection intégrée de la vie privée, du 27 au 29 oct. 2010, Jérusalem, Israël, https://www.ipc.on.ca/site_documents/pbd-resolution-f.pdf

LA PROTECTION INTÉGRÉE DE LA VIE PRIVÉE : LES SEPT PRINCIPES FONDAMENTAUX

1. Prendre des mesures proactives et non réactives ; des mesures préventives et non correctives
2. Assurer la protection implicite de la vie privée
3. Intégrer la protection de la vie privée dans la conception
4. Assurer une fonctionnalité intégrale selon un paradigme à somme positive et non à somme nulle
5. Assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements
6. Assurer la visibilité et la transparence
7. Respecter la vie privée des utilisateurs

À titre d'illustration, focalisons-nous sur le quatrième principe qui concerne à bien des égards le domaine de l'identité numérique. Pendant très longtemps, la position dominante a été de considérer qu'améliorer la sécurité conduirait nécessairement à diminuer le niveau de protection des données personnelles. On désigne cette position de principe par l'expression de « jeu à somme nulle ». L'approche *Privacy by design* entend démontrer qu'il est réellement possible de réaliser les deux objectifs à la fois. Dans le domaine des identités numériques, elle conduit essentiellement à mettre en place des schémas d'authentification pseudonymisée. Tout en assurant le pseudonymat de l'utilisateur, ces schémas permettent de prouver une identité ou de garantir qu'une personne répond à certains critères (être majeur, détenir un permis de conduire avec un nombre de points suffisant, etc.).

La résolution sur la protection intégrée de la vie privée invite également les Commissaires à « favoriser l'intégration des principes fondamentaux… dans le libellé des politiques et textes de loi sur la protection de la vie privée dans leur territoire de compétence ». Cette invitation a été entendue des deux côtés de l'atlantique, notamment par la *Federal Trade Commission* (FTC)[62] et le législateur européen.

Bientôt reconnu par le législateur européen

Ainsi, l'article 23 de la proposition de règlement Données personnelles est intitulé « Protection des données dès la conception et protection des données par défaut » ; il se réfère notamment à la pseudonymisation.

62 Aux États-Unis, la *Federal Trade Commission* (FTC) a notamment recommandé dans son rapport « Protecting consumer privacy in an Era of rapid Change » de mars 2012 que les entreprises adoptent une approche Privacy by design, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

« *Compte tenu de l'état de l'art et des coûts de mise en œuvre et en prenant en compte la nature, la portée, le contexte et les finalités du traitement ainsi que la probabilité et la gravité des risques pour les droits et libertés des individus engendrés par le traitement, le responsable de traitement met en œuvre, à la fois lorsqu'il détermine les moyens du traitement et lors du traitement lui-même, les mesures techniques et organisationnelles appropriées, tels que la pseudonymisation, qui est conçue pour mettre en œuvre les principes de protection des données, tels que la minimisation des données, de façon effective et de manière à intégrer les garanties nécessaires dans le traitement afin de répondre aux exigences du règlement et protéger les droits des personnes concernées* » (art. 23 [1] « *Protection des données dès la conception et protection des données par défaut* » – traduction libre[63]).

On note qu'il est ici question de « données personnelles » et non de « vie privée ». Cette différenciation met en lumière le fait qu'il existe deux droits de l'homme, certes différents mais complémentaires :

- **le droit au respect de la vie privée** est notamment consacré par l'article 12 de la Déclaration universelle des droits de l'Homme adoptée en 1948 et l'article 8 de la Convention européenne des droits de l'Homme de 1950 ;
- **le droit à la protection des données personnelles** a été consacré en 2000 par l'article 8 de la Charte des droits fondamentaux de l'Union européenne : il est promu au même rang que le droit au respect de la vie privée et la liberté d'expression.

De plus en plus de pays modifient leur constitution afin de reconnaître le droit à la protection des données personnelles à côté du droit au respect de la vie privée.

De façon générale, le droit au respect de la vie privée correspond au droit de ne pas voir révéler des informations liées à son intimité (sphère physique mais aussi expression d'une relation avec autrui) et à son identité pour permettre à la personne de s'épanouir

63 Traduction libre de l'article 23-1 de la proposition de règlement Protection des données personnelles dans sa version du 28 janvier 2016 selon laquelle : « *Having regard to the state of the art and the cost of implementation and taking of the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective way and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects* ».

(*cf.* fiche 1). Il entend protéger l'opacité de la personne[64]. Il s'agit d'un droit défensif : l'atteinte doit avoir eu lieu pour que la personne puisse bénéficier de la protection.

Le droit à la protection des données personnelles correspond, pour sa part, à un droit essentiellement préventif : il entend protéger l'individu par rapport à un risque précis, celui lié à l'usage des technologies de l'information. Ce faisant, il préserve par ailleurs la vie privée mais aussi d'autres libertés (libertés d'expression, de communication, etc.) et participe à la lutte contre la discrimination. Cet objectif est atteint, d'une part, en limitant par défaut le traitement des données personnelles effectué par le responsable de traitement et, d'autre part, en permettant à la personne de maîtriser la circulation de son image informationnelle.

L'article 23 distingue dans son paragraphe 2 la notion de « protection des données dès la conception » (*Data protection by design*) de la notion de « protection des données par défaut » (*Data protection by default*).

> « *Le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées visant à garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires à chaque finalité spécifique du traitement seront traitées ; ceci s'applique à la quantité de données, l'étendue de leur traitement, leur durée de conservation et leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles sans intervention humaine à un nombre indéterminé de personnes physiques* » (art. 23 [2] Protection des données dès la conception et protection des données par défaut[65])

L'approche « protection des données par défaut » a été présentée par la Commissaire européenne à la justice Viviane Reding à l'occasion de la révision de la directive 95/46/CE Données personnelles[66]. Elle consiste à instaurer un paramètre par défaut basé sur le plus haut niveau de protection des données personnelles. L'objectif est d'éviter une exploitation abusive des données, ainsi qu'une réutilisation à d'autres fins que celles pour lesquelles la

64 De Hert, P., Gutwirth, S. (2009). Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionlisation in Action, in Reinventing Data Protection ?, Gutwirth, S., Poullet, Y., Hert, P., Terwangne, C., Nouwt, S. (Eds.), Springer.

65 Traduction libre de l'article 23-2 de la proposition de règlement Protection des données personnelles dans sa version du 28 janvier 2016 selon laquelle : « *The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed; this applies to the amount of data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without human intervention to an indefinite number of individuals* ».

66 Viviane Reding, Vice-President of the European Commission, EU Justice Commissioner, « *Your data, your rights : Safeguarding your privacy in a connected world* », discours prononcé à Bruxelles le 16 mars 2011, SPEECH/11/183, http://europa.eu/rapid/press-release_SPEECH-11-183_fr.htm

personne a initialement consenti. À cet égard, la Commissaire a précisé que l'utilisation des données à d'autres fins que celles mentionnées ne devrait être autorisée qu'avec le consentement explicite de l'utilisateur ou s'il existe une autre raison pour un traitement licite (*cf.* fiche 6, principe de légitimation).

De la sorte, l'approche *Privacy by design*, qui figure déjà implicitement dans les principes clés existants de protection, devrait prochainement obtenir une reconnaissance législative explicite. Il existe néanmoins un risque non négligeable de récupération par des logiques marchandes et de détournement de l'esprit de l'approche afin de promouvoir certaines solutions technologiques. Il convient donc de veiller à ce que l'esprit même de l'approche soit respecté, afin que celle-ci ne devienne pas un nouveau « *buzzword* ».

7.2. Application de l'approche *Data protection by design* au système de gestion des identités numériques

Appliquée aux systèmes de gestion des identités numériques, l'approche *Data protection by design* doit, selon nous, envisager les risques potentiels d'atteintes aux données personnelles à la fois par le fournisseur de services et le fournisseur d'identités. Elle doit empêcher la divulgation disproportionnée des données et l'associabilité des actions de l'utilisateur.

La divulgation sélective des attributs auprès du fournisseur de services

Le premier risque est celui de la divulgation disproportionnée de données personnelles, à savoir une situation dans laquelle le jeu d'attributs divulgué lors d'une transaction contient plus d'informations que celles qui sont strictement nécessaires pour l'utilisation du service. Par exemple, si un utilisateur doit prouver qu'il est âgé de plus de 18 ans pour accéder à un service, le système divulgue sa date de naissance et/ou son identité civile.

Pour remédier à ce problème, certains systèmes mettent en œuvre le principe de la divulgation sélective des attributs. À l'aide d'une interface utilisateur comportant des cases à cocher, l'utilisateur sélectionne les attributs qu'il souhaite communiquer aux fournisseurs de services. Le fournisseur d'identités peut ainsi confirmer que l'utilisateur a plus de 18 ans sans divulguer la date de naissance, indiquer le département de résidence sans mentionner l'adresse exacte, ou divulguer l'âge sans révéler l'adresse.

De son côté, le fournisseur de services doit se conformer à cette politique et accepter l'authentification avec ce jeu partiel d'attributs. Il s'agit donc ici de mettre en place la cohérence technique et organisationnelle de l'ensemble de l'écosystème.

La non-associabilité des actions de l'utilisateur par le fournisseur de services

Le second risque est celui de **l'associabilité** qui consiste pour un fournisseur de services à pouvoir relier les actions effectuées par l'utilisateur dans des contextes différents auprès d'autres fournisseurs de services. Typiquement, le service des impôts peut être en mesure de savoir que l'utilisateur a visité un site de jeux en ligne, un service bancaire que son client a consulté quotidiennement le service d'assurance maladie. L'association des actions de l'utilisateur entre différents fournisseurs de services permet d'affiner la connaissance de son comportement et donc son profilage.

Une manière de limiter ces risques consiste à mettre en œuvre l'**authentification pseudonymisée**, à savoir créer un identifiant arbitraire, différent de l'identité civile, pour l'identification et l'authentification à un service en ligne. Elle implique de compartimenter les différents identifiants pseudonymisés, en créant un pseudonyme par contexte d'usage, et en veillant à préserver cette séparation. Dans ce cas, seuls l'autorité de délivrance et éventuellement le fournisseur d'identités ont connaissance de l'identité civile et du pseudonyme, ce qui permet de lever le pseudonymat dans les situations prévues par la loi, typiquement en cas de fraude ou d'usurpation d'identité. De leur côté, les différents acteurs sont dans l'incapacité de reconstruire une identité complète de l'utilisateur et de la relier de manière univoque à toutes les actions de ce dernier.

L'authentification pseudonymisée peut être mise en œuvre de différentes manières :

- certains systèmes de gestion des identités numériques offrent l'authentification pseudonymisée par défaut, d'autres de manière optionnelle ;
- des systèmes utilisent des **pseudonymes statiques** (le pseudonyme est alors le même, quel que soit le contexte d'utilisation), d'autres optent pour des **pseudonymes sectoriels** (par exemple un pseudonyme pour une banque, un autre pour la sécurité sociale) et autorisent ainsi des **identités multiples**.

En fonction de la combinaison des choix effectués, la protection des données personnelles et la perception de cette protection par l'utilisateur peuvent être très différentes. De même, l'efficacité de la **divulgation sélective** dépend de la façon dont l'authentification et le flux des données entre les différentes entités sont conçus. Ces deux aspects sont à considérer simultanément. Par exemple, un système qui implémente l'authentification pseudonymisée, mais qui permet aux fournisseurs de services la collecte des attributs de l'utilisateur qui ne sont pas nécessaires à l'authentification elle-même (comme l'adresse postale), pourrait conduire à l'identification de l'utilisateur.

La non-associabilité des actions de l'utilisateur par le fournisseur d'identités

Lors des transactions initiées par un utilisateur pour accéder aux services d'un fournisseur de services, le rôle occupé par le fournisseur d'identités prend différentes formes suivant l'approche techno-organisationnelle adoptée.

À l'un des extrêmes, le fournisseur d'identités intervient de façon minimaliste en gérant uniquement les listes de révocation et en renseignant le fournisseur de services quant à l'état de révocation d'une identité numérique donnée.

➔ Cette approche est implémentée dans les infrastructures classiques à clés publiques dites « PKI », comme la carte nationale d'identité en Estonie (*cf.* fiche 8).

À l'autre extrême, le fournisseur d'identités est une instance centrale qui à la demande du fournisseur de services authentifie l'utilisateur lors de chaque transaction, voire fournit au fournisseur de services les attributs de l'utilisateur.

➔ Cette approche est implémentée dans Google+ Sign-In basé sur le protocole OpenID Connect et dans le système de gestion de l'identité numérique officielle en Autriche (*cf.* fiche 8).

Compte tenu du rôle central joué par le fournisseur d'identités, il n'est pas toujours suffisant de se prémunir uniquement contre l'associabilité entre les fournisseurs de services. En effet, dans le cas où toutes les authentifications passent par le fournisseur d'identités, ce dernier est capable de savoir à quels services l'utilisateur a accédé et à quel moment. C'est pourquoi certains systèmes de gestion des identités numériques mettent en place des mécanismes spécifiques pour se prémunir contre cette situation, comme la connexion directe entre l'utilisateur et le fournisseur de services sans passer à chaque fois par le fournisseur d'identités ; tel est le cas en Allemagne (*cf.* fiche 8).

Fiche 8. Analyse comparative des choix de conception des systèmes de gestion des identités numériques

Armen Khatchatourov,
Claire Levallois-Barth
et Maryline Laurent

Cette fiche propose une analyse comparative des systèmes de gestion des identités numériques dans quatre pays européens : l'Estonie, l'Autriche, l'Allemagne et la Suisse. À cette fin, nous avons retenu trois critères de comparaison (*cf.* fiche 7) :

- la divulgation sélective des attributs auprès des fournisseurs de services ;
- l'authentification pseudonymisée auprès des fournisseurs de services ;
- la protection vis-à-vis du fournisseur d'identités.

Presque tous les pays européens ont déployé ou sont en train de déployer des systèmes de gestion des identités numériques, sous forme de systèmes dédiés ou basés sur les identités existantes comme les identités bancaires. Si la France et la Grande-Bretagne faisaient figure d'exceptions, les initiatives GOV.UK Verify et France Connect (*cf.* fiche 9) lancées en 2014 rapprochent ces deux pays de la tendance générale.

En pratique, le périmètre d'utilisation de ces systèmes est sensiblement le même : d'une part, les services publics comme la sécurité sociale ; d'autre part, les services privés comme les banques, les assurances et le commerce en ligne. Les choix de conception sont, quant à eux, très divers. Quatre pays nous semblent cependant représenter la diversité des solutions adoptées allant d'une protection limitée des données personnelles à des systèmes complexes offrant un haut niveau de protection[67].

Légende pour la colonne « Présence/absence » :
* signifie qu'une solution est présente, mais qu'elle n'a pas le caractère du schéma national officiel

Légende pour la colonne « infrastructure » :
Publique : financée et entretenue essentiellement par les pouvoirs publics
Privée : financée et entretenue essentiellement par les entreprises privées
Publique-privée : consortium mixte
Publique et privée : coexistence des différentes solutions

67 Cette fiche reprend les éléments développés dans Khatchatourov, A., Laurent, M., Levallois-Barth, C. (2015). Privacy in Digital Identity Systems: Models, Assessment, and User Adoption, *in Electronic Government, Lecture Notes in Computer Science*, Springer.

Pays	Présence/ absence	Infrastructure	Usage dans les secteurs
ALLEMAGNE	Oui	Publique	Public et privé
Pour en savoir plus : http://www.personalausweisportal.de/EN/Citizens/Electronic-Identification/Electronic-Identification_node.html			
AUTRICHE	Oui	Publique	Public et privé
Pour en savoir plus : https://www.buergerkarte.at/en/			
BELGIQUE	Oui	Publique	Public et privé
Pour en savoir plus : http://eid.belgium.be/fr/			
BULGARIE	Pilote en cours	Inconnue	Inconnu
Pour en savoir plus : http://eid.egov.bg/			
CHYPRE	Inconnu	Inconnue	Inconnu
CROATIE	Oui	Publique	Public
Pour en savoir plus : https://vlada.gov.hr/the-e-citizens-system/15215			
DANEMARK	Oui	Privée	Public et privé
Pour en savoir plus : https://www.nemid.nu/dk-en/			
ESPAGNE	Oui, plusieurs systèmes	Publique (en cours) et publique-privé	Public et privé
Pour en savoir plus : http://www.dnielectronico.es/PortalDNIe/			
ESTONIE	Oui	Publique-privée	Public et privé
Pour en savoir plus : http://www.id.ee/?lang=en			
FINLANDE	Oui	Publique-privée	Public et privé
Pour en savoir plus : https://www.suomi.fi/suomifi/english/index.html			
FRANCE	Non	Néant (cf. fiche 9)	Néant (cf. fiche 9)
GRÈCE	Inconnu	Inconnue	Inconnu
HONGRIE	En cours	publique	Public et privé
IRLANDE	Inconnu	Inconnue	Inconnu
ITALIE	Oui	Publique	Public et privé
Pour en savoir plus : http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/spid			
LETTONIE	Oui	Publique et privée	Public et privé
Pour en savoir plus : https://www.eparaksts.lv/en/eid-card/eid-users/			
LITUANIE	Oui	Publique	Public
Pour en savoir plus : https://www.epaslaugos.lt/portal/en			

Pays	Présence/ absence	Infrastructure	Usage dans les secteurs
LUXEMBOURG	Oui	Publique et privée	Public et privé (public pour services publics, privé pour services publics et privés)
Pour en savoir plus : http://www.guichet.public.lu/citoyens/fr/support/faq/carteidentite-certificats/index.html • https://www.luxtrust.lu/fr			
MALTE	En cours	Inconnue	Inconnu
Pour en savoir plus : https://identitymalta.com/id-cards/			
PAYS-BAS	Oui, 2 systèmes (fusion en cours)	1) Publique/privée 2) Privée	1) Public 2) Privé
Pour en savoir plus : https://www.digid.nl/en/ • https://www.eherkenning.nl/erecognition/			
POLOGNE	En cours	Inconnue	Inconnu
Pour en savoir plus : http://plid.obywatel.gov.pl/about			
PORTUGAL	Oui	Publique	Public et privé
Pour en savoir plus : https://www.cartaodocidadao.pt/			
RÉP. TCHÈQUE	Oui *	Privée	Public et privé
Pour en savoir plus : https://www.mojeid.cz/			
ROUMANIE	Inconnu	Inconnue	Inconnu
ROYAUME-UNI	En cours	Privée	Public et privé
Pour en savoir plus : https://www.gov.uk/service-manual/identity-assurance			
SLOVAQUIE	Oui	Inconnue	Public et privé
Pour en savoir plus : http://www.sdisk.eu/projekty/2014/study-of-the-eid-model-in-slovakia/			
SLOVÉNIE	Inconnue	Inconnue	Inconnue
SUÈDE	Oui	Privée	Public et privé
Pour en savoir plus : https://www.bankid.com/en/			
SUISSE	Oui*	Privée	Public et privé
Pour en savoir plus : www.SuisseID.ch/fr			

Figure 7. **Tableau comparatif des systèmes de gestions des identités numériques déployés en Europe**

8.1. **Quatre exemples de systèmes de gestion des identités numériques**

L'un des premiers pays qui s'est lancé dans le déploiement de l'identité numérique est **l'Estonie**. Le système mis en œuvre dès 2002 est souvent décrit comme une grande réussite. La carte d'identité électronique sert à la fois de carte nationale d'identité et de moyen d'identification et d'authentification en ligne auprès des services publics et privés. L'utilisateur est identifié par un numéro d'identification personnel basé sur le registre de la population.

Dans le système **autrichien**, massivement déployé à partir de 2006, l'identité numérique peut être intégrée à divers supports comme le téléphone mobile ou les cartes à puce (carte de sécurité sociale ou carte bancaire). Il n'y a pas ici de support « principal », et aucun des supports n'est un document officiel d'identité. Comme en Estonie, il existe une base de données centrale appelée « Registre central des résidents ». Cependant, la législation nationale interdit l'utilisation de ces identifiants par les fournisseurs de services.

Lancée en 2010, l'identité numérique **allemande,** au format carte de crédit, remplit deux fonctions : la fonction nPA (acronyme de *neue PersonalAusweis* pour « nouveau passeport ») qui est à la fois une carte nationale d'identité et un document de voyage, et la fonction d'identification et d'authentification électronique. Ce système offre un haut niveau de protection dans la mesure où la législation nationale interdit la création d'une base de données centrale des identifiants.

Lancé également en 2010 sous différentes formes (carte à puce, clé USB et mobile), **SuisseID** sert uniquement à l'authentification en ligne. Ce système principalement financé par le secteur privé ne fournit pas de documents officiels d'identité. L'une de ses caractéristiques est qu'il permet d'intégrer de nouveaux fournisseurs d'attributs afin d'étendre son utilisation notamment au contexte professionnel.

8.2. **Utilisation des pseudonymes**

Seule l'Estonie ne recourt pas aux pseudonymes. Dans ce système, l'utilisateur est toujours identifié par un identifiant unique lié de façon univoque à son identité civile. Cet identifiant est stocké directement dans le certificat électronique figurant dans la carte et est divulgué à chaque authentification. En conséquence, chaque fournisseur de services est en mesure d'« associer » les actions de l'utilisateur entre différents services.

Pour remédier à ce problème d'associabilité, entendu ici dans son sens restreint d'associabilité entre l'identifiant numérique et l'identité civile, les autres pays se sont intéressés à

deux techniques : le pseudonyme unique quel que soit le contexte de l'usage, ou les pseudonymes multiples.

Pseudonyme unique et pseudonymes sectoriels

Le moyen le plus simple est de représenter l'utilisateur par *un et même* pseudonyme en s'assurant que le lien entre ce pseudonyme et l'identité civile est connu seulement par le fournisseur d'identités. Le fournisseur de services identifie alors l'utilisateur uniquement *via* le pseudonyme. Cette approche est mise en œuvre par SuisseID.

L'Allemagne et l'Autriche utilisent un mécanisme plus sophistiqué. Les pseudonymes spécifiques pour chaque secteur d'activité sont générés de manière logicielle. L'Autriche distingue ainsi vingt-six secteurs, allant de la sécurité sociale à la banque, ce qui empêche un secteur de connaître les opérations effectuées dans un autre secteur. Du point de vue du fournisseur de services, le pseudonyme sert à identifier l'utilisateur, et l'identité civile est un éventuel attribut lié à ce pseudonyme. Cette approche n'utilise pas de pseudonyme ou d'identifiant « racine ». En effet, la législation allemande interdit tout registre central des citoyens, et de manière générale, tout numéro d'identification unique. L'identité numérique autrichienne est, quant à elle, basée sur le Registre Central des Résidents (CRR). Cependant, un mécanisme de hachage unidirectionnel à deux phases assure qu'il n'est pas possible de remonter du pseudonyme sectoriel au CRR.

Il faut préciser que, quel que soit le choix de pseudonymisation, certains fournisseurs de services (administration fiscale, sécurité sociale) exigent de toute façon l'identité civile pour assurer leur fonctionnement.

Le lien entre les pseudonymes et le support de l'identité numérique

Afin de préciser la relation entre les supports physiques et les pseudonymes, nous nous appuyons ici sur le concept de générateur d'identité numérique[68]. Le générateur est une fonctionnalité logicielle abstraite qui joue le rôle d'une « couche » intermédiaire entre le support et l'identité numérique (*cf.* fig. 7). Ainsi, le même générateur peut être lié à différents supports qui produisent alors la même identité numérique.

- En Estonie, le générateur ne produit aucun pseudonyme et divulgue le même identifiant à partir de trois supports (carte nationale d'identité électronique, carte optionnelle élec-

68 Concept introduit dans Khatchatourov, A., Laurent, M., Levallois-Barth, C. (2015). Privacy in Digital Identity Systems: Models, Assessment, and User Adoption, *in Electronic Government, Lecture Notes in Computer Science*, Springer.

tronique appelée Digi-ID, et un mobile équipé d'une fonctionnalité optionnelle appelée Mobile-ID).

- Pour SuisseID, le générateur produit toujours un seul et même pseudonyme, à partir de trois supports (carte à puce, clé USB et mobile).
- En Autriche, tous les supports remplissent le même rôle fonctionnel de générer les pseudonymes spécifiques à chaque secteur à partir de la même identité civile, de la même manière. Quel que soit le support utilisé, l'utilisateur est toujours représenté par le même pseudonyme dans un secteur donné.
- L'Allemagne fait figure d'exception en déployant l'identité numérique à partir d'une seule carte à puce, mais son portage sur le mobile semble être en cours.

En Autriche et en Allemagne, le générateur produit *n* pseudonymes en fonction du secteur, ce générateur pouvant être attaché à un seul ou plusieurs supports.

Les pseudonymes multiples sont implémentés par défaut en Autriche et en Allemagne. À l'inverse, pour pouvoir cloisonner les usages avec la SuisseID, l'utilisateur de ce système doit acquérir plusieurs générateurs : souscrire un contrat supplémentaire avec un enrôlement distinct, et acheter un (ou plusieurs) support supplémentaire associé à ce contrat.

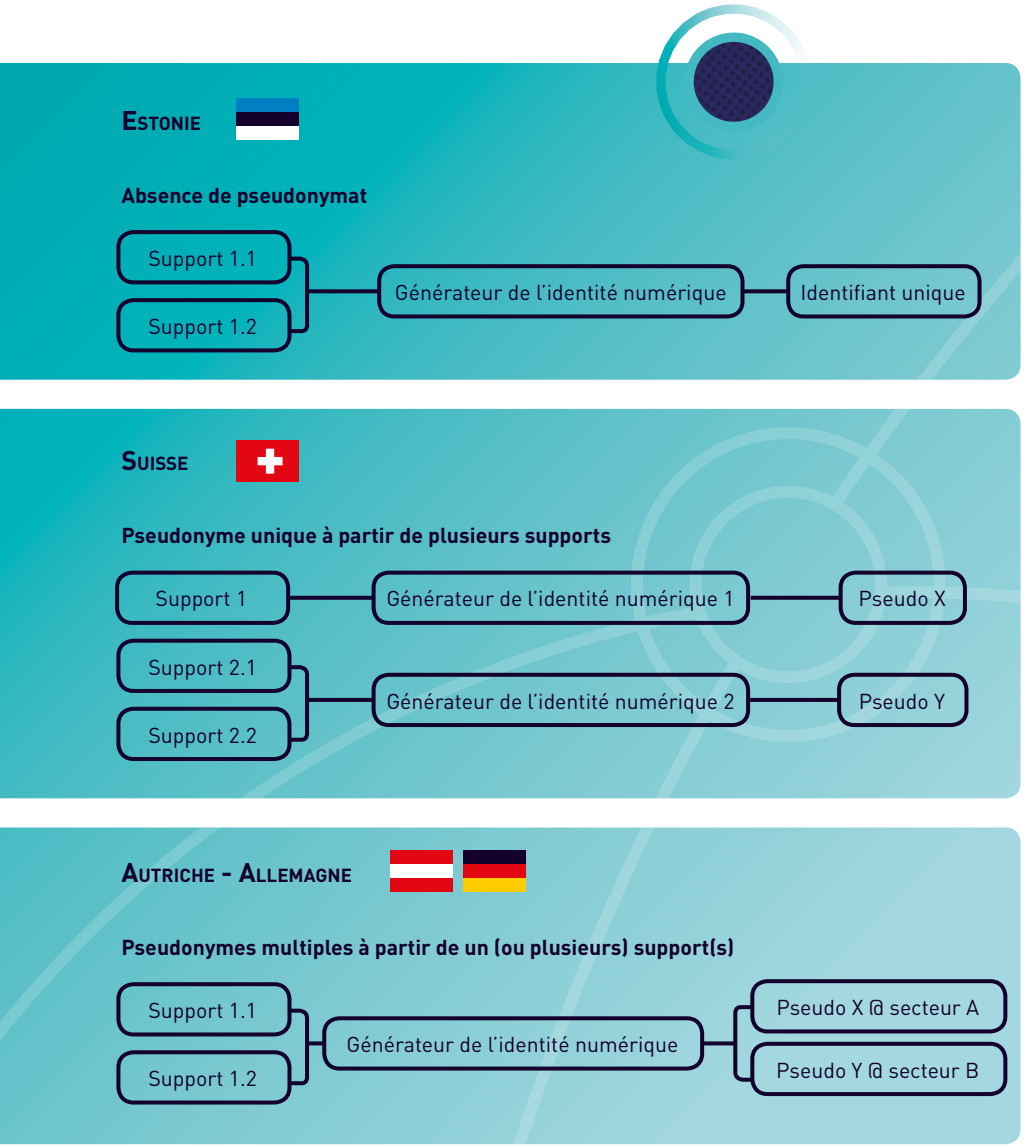


Figure 8. Les trois modèles du générateur de l'identité numérique

8.3. **Niveaux de protection offerts par les systèmes de gestion des identités numériques**

En fonction du schéma d'authentification choisi, le rôle des acteurs et le niveau de protection des données personnelles diffèrent.

En **Estonie**, le rôle du fournisseur d'identités est réduit à la délivrance de l'identité numérique et à sa révocation, l'authentification se faisant directement entre l'utilisateur et le fournisseur de services. Cette approche est caractéristique des infrastructures classiques à clés publiques dites « PKI » (*Public Key Infrastructure*). De ce fait, il n'y a pas *a priori* d'instance centrale qui aurait connaissance de tous les attributs de l'utilisateur ou des connexions de l'utilisateur aux fournisseurs de services. Cependant, en raison de la présence d'un identifiant unique, il est tout à fait possible de tracer l'utilisateur. Par ailleurs, la divulgation sélective des attributs n'est pas implémentée.

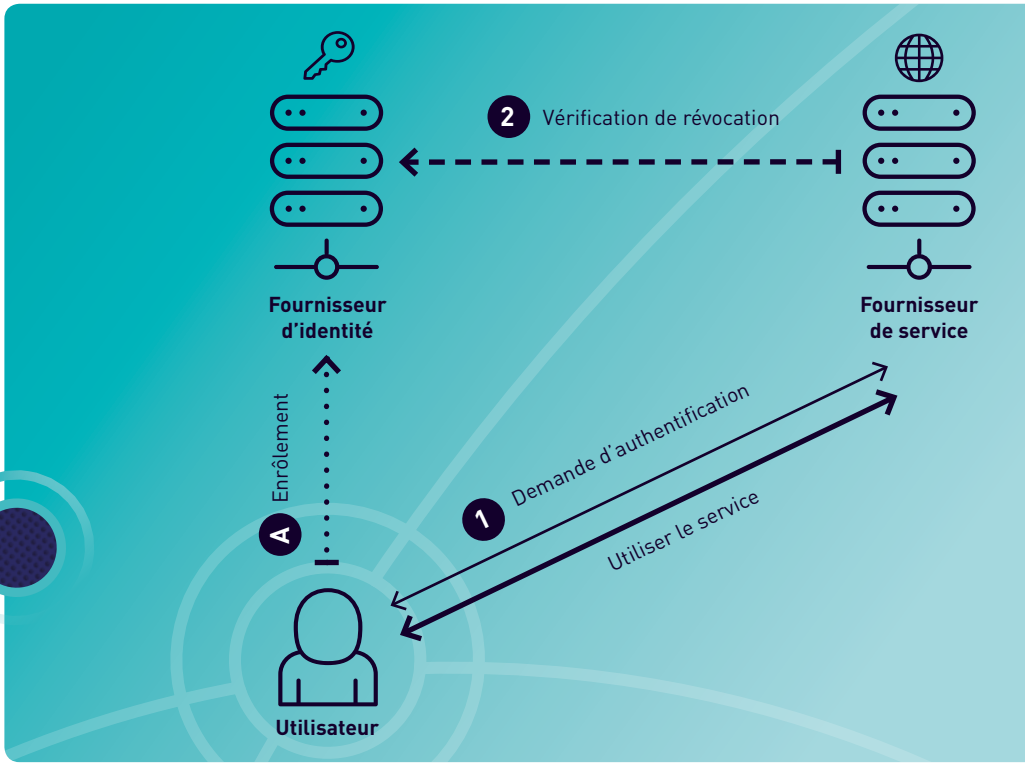


FIGURE 9. Le système estonien (identifiant unique utilisé dans les secteurs public et privé *via* les cartes à puce et les téléphones mobiles)

En **Autriche**, le fournisseur d'identités acquiert un rôle plus important, en raison même du mécanisme de pseudonymes sectoriels. Il est sollicité par les fournisseurs de services à chaque demande d'authentification pour générer le pseudonyme sectoriel. Les fournisseurs de services sont donc incapables de remonter de manière univoque à l'identité civile, ou de savoir qu'un même utilisateur s'est connecté à un fournisseur de services d'un autre secteur. Le fournisseur d'identités a connaissance de toutes les connexions de l'utilisateur. Par ailleurs, le fournisseur d'identités connaît peu d'attributs liés à l'utilisateur, ceux-ci étant essentiellement gérés par les fournisseurs de services. La divulgation sélective des attributs n'est donc pas implémentée.

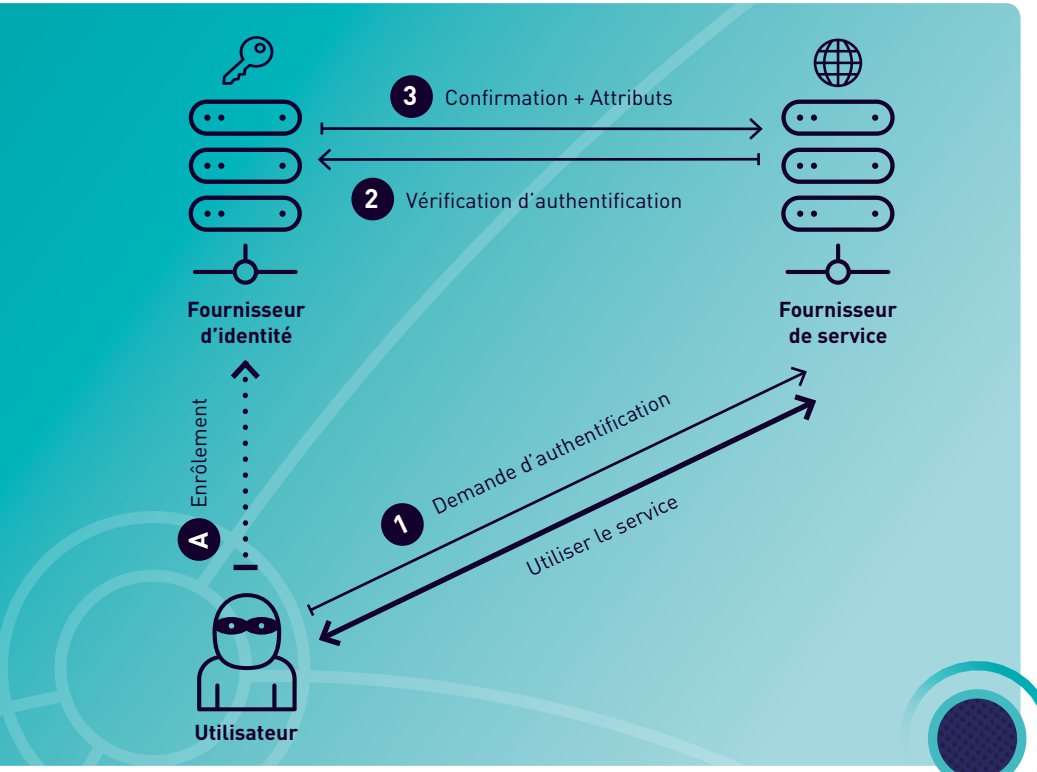


FIGURE 10. Le système autrichien (pseudonymes sectoriels utilisés dans les secteurs public et privé *via* les cartes à puce et les téléphones mobiles)

En **Suisse**, le rôle central du fournisseur d'identités est encore plus prononcé. Contrairement au modèle autrichien, l'instance centrale et ses « satellites » connus sous le nom de fournisseurs d'attributs additionnels détiennent plus de données personnelles (telles que profession libérale ou personne morale) que ce que contient le support de l'identité numérique lui-même. Pour limiter la divulgation de ces données, toutes les demandes d'attributs de la part du fournisseur de services sont contrôlées par l'utilisateur *via* un tableau de bord. Enfin, l'utilisateur est toujours aussi exposé au risque que le fournisseur d'identités trace ses différentes activités, puisque toutes les demandes d'attributs font appel à cette instance centrale. Le moyen nécessaire (mais pas toujours suffisant) de limiter ce risque consiste pour la personne à avoir en sa possession plusieurs générateurs d'identités numériques.

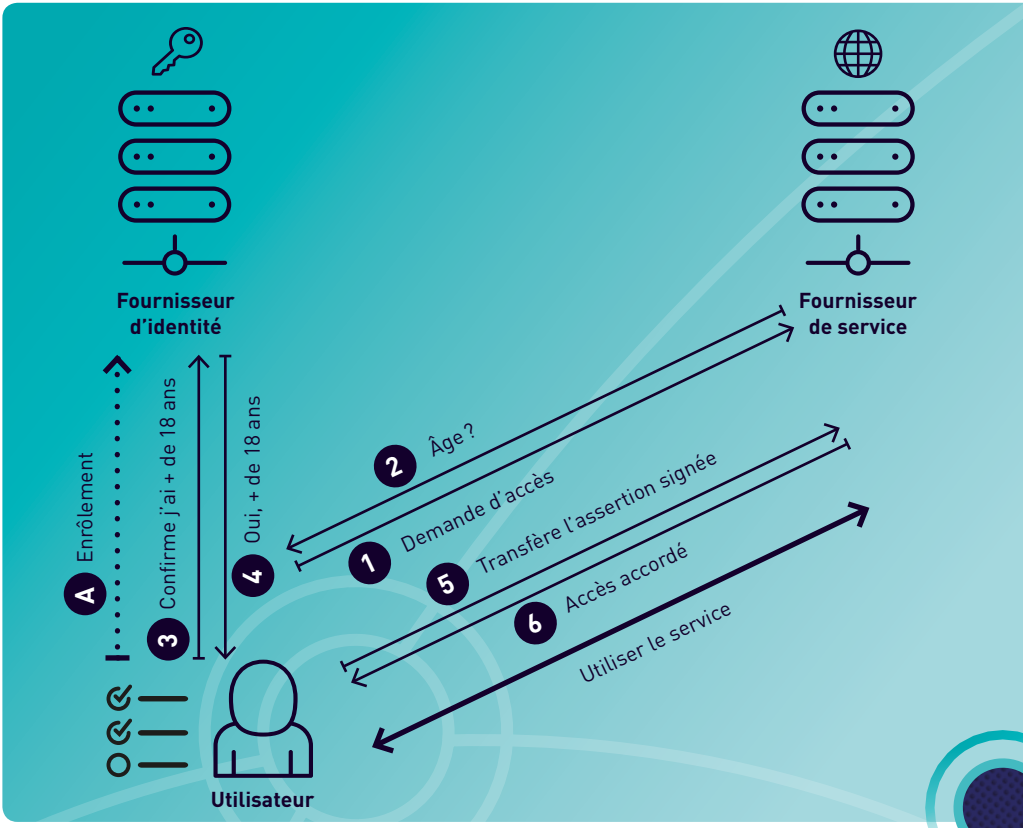


FIGURE 11. Le système suisse (pseudonymes optionnels et divulgation sélective utilisés dans les secteurs public et privé *via* les cartes à puce, les téléphones mobiles et les clés USB)

En **Allemagne**, où la génération des pseudonymes sectoriels est largement inspirée du système autrichien, un mécanisme supplémentaire a été introduit pour limiter la connaissance des actions de l'utilisateur par une instance centrale. Ici, l'autorité de délivrance ne s'occupe que de la gestion des listes de révocation, à la fois pour les utilisateurs et les fournisseurs de services (seuls les services sur liste blanche sont autorisés). Ces listes sont transmises à une entité appelée eID-Server, implémentée à l'interface entre l'utilisateur et le fournisseur de services. L'eID-Server joue le rôle de fournisseur d'identités décentralisé sur chaque fournisseur de services, il n'a donc qu'une vision partielle des activités de l'utilisateur. Une fois authentifié, l'utilisateur peut sélectionner, *via* un tableau de bord, les attributs à divulguer au fournisseur de services. Enfin, une clé d'authentification partagée par un groupe de cartes permet de prouver la validité de l'identité sans que le fournisseur de services puisse tracer l'utilisateur.

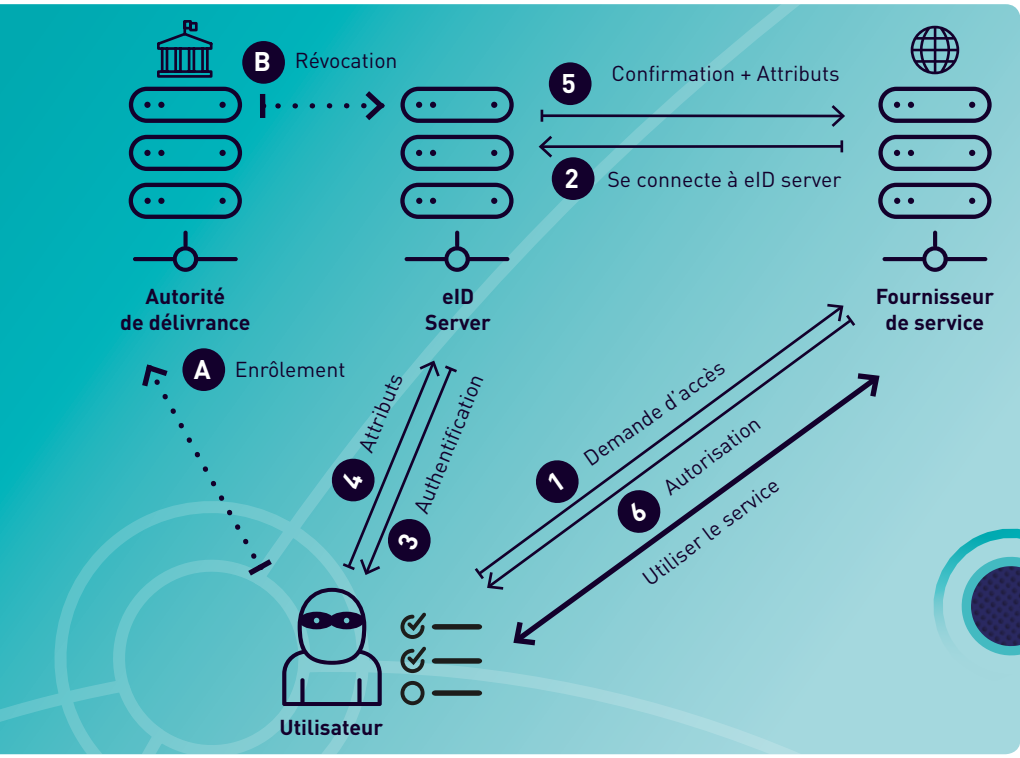


FIGURE 12. Le système allemand (pseudonymes optionnels et divulgation sélective utilisés dans les secteurs public et privé *via* les cartes à puce, les téléphones mobiles et les clés USB Allemagne)

8.4. **Conclusion**

La stratégie adoptée dans le cadre de SuisseID cherche à gérer les risques pesant sur les données personnelles des utilisateurs provenant des fournisseurs de services plutôt que du fournisseur d'identités. Ce choix se traduit par une solution élégante et flexible, présentant un niveau de complexité technique raisonnable.

La démarche mise en place par l'Allemagne place la protection des données personnelles au cœur même de son système. Cette priorité se traduit par une architecture relativement complexe et coûteuse. Cependant, les utilisateurs sont réticents à utiliser l'identité numérique générée à partir de la carte nationale d'identité dans le cadre de transactions commerciales[69]. En effet, ce que nous avons appelé le « modèle du générateur de l'identité » (*cf.* fiche 8.2), à savoir l'articulation entre un mécanisme sophistiqué perçu comme une boite noire et un support physique unique, conduit à ce que les utilisateurs ne perçoivent pas le niveau de protection offert par l'ensemble du système. Ces derniers n'adhèrent simplement pas à l'idée qu'un seul support physique soit capable de produire des pseudonymes différents de manière fiable.

S'il fallait envisager des pistes pour améliorer l'adoption de ces systèmes, il faudrait prendre en compte le niveau de protection tel qu'il est en pratique perçu par l'utilisateur. À titre d'illustration, l'infrastructure déjà en place en Allemagne pourrait permettre à l'utilisateur d'acquérir plus d'un générateur d'identités numériques pour améliorer la « protection perçue ». Cette solution impliquerait de dissocier les générateurs supplémentaires de la fonctionnalité « carte nationale d'identité électronique » et donc de modifier le cadre juridique. De manière symétrique, la SuisseID pourrait être dotée de générateurs de pseudonymes multiples ce qui impliquerait de refondre complètement l'infrastructure technique.

De tels aménagements, dont on ignore le coût financier, permettraient peut-être de remédier au manque de confiance des utilisateurs dans les systèmes techniques. Ils tendraient vers le cloisonnement des identités entre les contextes d'usage (*cf.* fiche 1), et offriraient au citoyen plus d'initiatives dans la gestion active de son environnement numérique.

69 Harbach, M., Fahl, S., Rieger, M., Smith, M. (2013). On the Acceptance of Privacy-preserving Authentication Technology: The Curious Case of National Identity Cards, *in Privacy Enhancing Technologies*, De Cristofaro, E., Wright, M. (Eds.), Springer.

Fiche 9. L'identité numérique en France

Armen Khatchatourov
et Claire Levallois-Barth

En France, l'institutionnalisation des identités numériques a connu plusieurs épisodes. Son histoire en cours d'écriture comporte tour à tour des initiatives à l'échelle nationale, des projets pilotes et plus récemment un projet à grande échelle qui a pour ambition de créer un « intermédiaire » entre l'État, les fournisseurs d'identités et les services publics, voire à terme les services privés. Ce projet, actuellement en cours de déploiement, s'inscrit dans la démarche européenne portée par le règlement (UE) n° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (*Electronic IDentification And trust Services* – eIDAS) qui prendra effet au 1er juillet 2016 (*cf.* fiche 10)[70].

9.1. **Le programme public INES**

Le programme public d'Identité Nationale Électronique Sécurisée, connu sous le nom d'INES, a été lancé en 1999 par le ministère de l'Intérieur. Il comprenait deux volets :

- un passeport doté d'une puce comportant des données biométriques : ce volet a donné lieu au passeport électronique déployé par l'Agence Nationale des Titres Sécurisés (ANTS) ;
- une carte d'identité électronique offrant un accès à des services web, notamment d'administration électronique.

Il est difficile de déterminer les raisons exactes de l'abandon en juin 2005 de ce deuxième volet, soumis par le ministère de l'Intérieur à un débat public. Pierre Piazza a montré que la création d'un collectif opposé au projet a incité le gouvernement à se prononcer en faveur de son retrait, d'autant plus que la CNIL avait émis des signaux répétés de prudence[71]. Ce retrait semble également lié à la priorité accordée au volet passeport au regard des moyens financiers disponibles[72].

Suite au changement de gouvernement intervenu mi-2005, le projet INES a été remplacé par le projet de « protection de l'identité ».

---

70 Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juill. 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE : JOUE L 257/73 du 28 août 2014.

71 Piazza, P. (2006). Les résistances au projet INES, *Cultures et Conflits*, n° 64.

72 Lacouette-Fougère, C. (2008). *Les métamorphoses d'INES. Trajectoire d'un programme public innovant : la carte nationale d'identité électronique*, Mémoire à l'IEP Paris, Master Recherche Politique et sociétés en Europe, Lascoumes, P. (Dir.), 29 sept. 2008. http://www.laurent-mucchielli.org/public/Memoire_Clement_Lacouette-Fougere_Vallegee.pdf

9.2. **Le projet de « protection de l'identité »**

Ce deuxième projet de carte nationale d'identité électronique, initialement prévu en 2009, consistait à introduire une carte comportant deux puces électroniques. Il a donné lieu à une proposition de loi censurée partiellement par le Conseil constitutionnel.

La première puce dite « régalienne » sans accès à internet était lisible uniquement par des agents de l'État habilités, à l'aide d'un équipement dédié tout comme pour le passeport à puce. Cette puce comportait le jeu de données d'identification et de données biométriques, dont les empreintes digitales. Il était prévu de stocker l'ensemble de ces informations dans la base centrale des titres sécurisés gérée par l'ANTS.

La deuxième puce facultative dite « vie quotidienne » était destinée à « s'identifier sur les réseaux de communications électroniques et de mettre en œuvre la signature électronique »[73], aussi bien pour l'administration électronique (par exemple pour effectuer une déclaration fiscale) que pour les services commerciaux privés. Elle comportait les données d'état civil « classiques » (nom, prénom, adresse) ; il est intéressant de noter que l'on retrouve ce concept (et presque le même jeu des données identifiantes) sous le nom d'« identité-pivot » dans le cadre du projet France Connect (*cf.* 9.4 ci-après) et du règlement eIDAS.

La loi relative à la protection de l'identité a été partiellement censurée par le Conseil constitutionnel en 2012, principalement pour deux motifs[74]. La première raison se rapporte à la « puce régalienne » et au fichier biométrique adjacent ; le Conseil juge à cet égard que la création d'une base centrale nationale constitue une « *atteinte au droit au respect de la vie privée qui ne peut être regardée comme proportionnée au but poursuivi* »[75].

La seconde raison concerne la puce « vie quotidienne ». À cet égard, le Conseil a dénoncé l'imprécision entourant les conditions de son implémentation, le texte ne mentionnant « *ni la nature des* « données » *au moyen desquelles ces fonctions [d'identification sur les réseaux de communications électroniques et de la signature électronique] peuvent être mises en œuvre ni les garanties assurant l'intégrité et la confidentialité de ces données* »[76].

---

73 Art. 3 de la proposition de loi relative à la protection de l'identité. Texte adopté n° 883 adopté le 6 mars 2012 par l'Assemblée nationale, session ordinaire de 2011-2012.

74 Décision n° 2012-652 DC du 22 mars 2012 du Conseil constitutionnel sur la loi relative à la protection de l'identité, http://www.conseil-constitutionnel.fr/decision/2012/2012-652-dc/decision-n-2012-652-dc-du-22-mars-2012.105165.html

75 Considérant 11 de la décision n° 2012-652 DC : « *En effet, l'objectif qui était de préserver l'intégrité des données nécessaires à la délivrance des titres d'identité et de voyage était bien justifié par un motif d'intérêt général. Cependant, la nature des données enregistrées, l'ampleur de ce traitement, ses caractéristiques techniques qui autorisaient l'interrogation à des fins de police administrative ou judiciaire et les conditions de sa consultation portaient au droit au respect de la vie privée une atteinte disproportionnée au but poursuivi.* »

76 Considérant 14 de la décision n° 2012-652 DC.

Il est à noter que les discussions à l'Assemblée nationale évoquaient également une « confusion des genres » entre les rôles des acteurs institutionnels. En particulier, le ministère de l'Intérieur délivrant de fait la deuxième puce pour l'utilisation des services commerciaux privés, cet usage apparaissait alors comme inapproprié[77].

Parallèlement aux discussions parlementaires était lancé le projet pilote IdeNum.

9.3. **Le projet pilote IdeNum**

Démarré en 2010, suspendu et ensuite relancé en 2013, le projet IdeNum visait à expérimenter des formes de collaboration entre les secteurs public et privé pour la fourniture des identités numériques. Cofinancé lors de la deuxième phase par le Plan d'investissement d'avenir *via* la Caisse des dépôts et par des actionnaires privés (Solocal Group, le groupe La Poste, SFR et Euro Information – Crédit Mutuel), il a donné lieu à la création de la société IdeNum qui ambitionnait de mettre en place « *une gamme de solutions [...] selon les usages et les niveaux de sécurité requis* »[78]. Ainsi, l'objectif n'était pas de créer « *des identifiants numériques mais un label qui [certifierait que tel ou tel] identifiant permet bien de récupérer des données qualifiées suffisantes pour s'identifier à un autre service* ».

Après une phase d'expérimentation au cours de laquelle SFR agissait en qualité de fournisseur d'identités[79], le projet a été arrêté au cours de l'été 2015.

IdeNum a alors rejoint le projet France Connect, ce qui devrait permettre à ce dernier de bénéficier de l'expérience acquise, en particulier sur un point qui nous semble important, celui du dialogue avec les acteurs privés afin d'élaborer des modèles d'affaires pérennes.

9.4. **Le projet France Connect**

Lancé en 2014, France Connect s'inscrit dans une démarche globale de l'État plateforme portée par le Secrétariat général pour la modernisation de l'action publique (SGMAP). Selon Guillaume Blot, chef du service Architecture et urbanisation de la Direction interministérielle des systèmes d'information et de communication (DISIC), « *une des caractéristiques de l'État plateforme, qui est la figure même de la transformation des services publics, est d'admettre la donnée comme un bien commun. Il s'agit ici de faciliter la circu-*

77 Assemblée nationale, XIIIe législature, Session extraordinaire de 2010-2011, compte rendu intégral, deuxième séance du jeudi 7 juillet 2011 : http://www.assemblee-nationale.fr/13/cri/2010-2011-extra/20111008.asp

78 http://www.usine-digitale.fr/article/identifiant-numerique-unique-idenum-nkm-en-a-reve-fleur-pellerin-l-a-fait.N194954

79 http://atelier.sfr.fr/beta-tests/venez-tester-idenum-votre-identite-numerique-qui-simplifie-vos-demarches-sur-internet

lation des données entre les administrations tout en redonnant à l'usager la maîtrise des données échangées quand il s'agit de données personnelles. Ceci impose de disposer d'un mécanisme d'identification et d'authentification numérique des usagers reconnu par les fournisseurs de services publics »[80].

Comment fonctionnera France Connect ?

Le projet sert à la fois de « porte d'entrée » vers un écosystème composé de France Connect, de fournisseurs d'identité (notamment l'assurance maladie et son site internet AMELI, La Poste), de fournisseurs de services (les services des impôts, des mairies, etc.) et de fournisseur d'attributs (la Direction générale des finances publiques, l'URSSAF). Le même acteur peut tour à tour jouer le rôle de fournisseur de services et de fournisseur dit de « données ». Le fournisseur de données est ainsi proche de ce que nous appelons un fournisseur d'attributs dans le présent Cahier.

France Connect, actuellement en cours d'expérimentation, devrait être opérationnel en 2016. Concrètement, lorsqu'un utilisateur se connectera en ligne *via* le bouton France Connect, il sera authentifié par le fournisseur d'identités de son choix (par exemple AMELI), qui à son tour confirmera l'identité au fournisseur de services. La personne pourra ensuite utiliser le service.

Exemple d'un usager souhaitant demander une place en crèche pour son enfant, et dont les tarifs dépendent du niveau d'imposition :

- soit l'usager envoie lui-même au service communal de la petite enfance un avis d'imposition dématérialisé émis par la DGFIP (Direction générale des finances publiques) ;
- soit le service de la petite enfance accède directement aux informations requises *via* une interface proposée par la DGFIP sous réserve d'avoir préalablement identifié et authentifié l'usager à l'aide de France Connect.

À terme, France Connect ambitionne d'offrir aux usagers la possibilité de se connecter à toutes les administrations à l'aide d'un seul bouton. Quel que soit le canal de communication (poste fixe, *smartphone*, etc.), la traçabilité et la transparence des données manipulées

80 Interview de Guillaume Blot, chef du service architecture et urbanisation de la Direction interministérielle des systèmes d'information et de communication (DISIC) et de Jean-Jacques Leandri, expert auprès du groupe de travail eIDAS, secrétariat général pour la modernisation de l'action publique (SGMAP), réalisé par Armen Khatchatourov, juillet 2015.

lors des démarches en ligne devraient être assurées à la fois vis-à-vis des usagers et des autorités administratives.

Ainsi, France Connect ne se positionne pas comme un fournisseur d'identités, mais comme un intermédiaire mettant en relation les différents acteurs. Sa vocation est de faciliter les démarches entreprises par les citoyens, et non de devenir une carte nationale d'identité électronique.

De manière générale, un certain nombre de fournisseurs d'identités publics (AMELI, DGFIP) sont appelés à participer à cet écosystème. Des fournisseurs d'identités privés, comme des opérateurs de télécommunications ou des banques, sont également susceptibles de rejoindre le système. Ils devront pour cela respecter le cahier des charges publié par France Connect.

Concernant les fournisseurs de services, Guillaume Blot précise qu'*« il serait intéressant d'ouvrir France Connect à des services privés. L'usager effectue, en moyenne, quatre à cinq fois par an des démarches auprès des services publics. Cependant, si France Connect s'ouvre à la sphère privée, le besoin d'informations administratives est démultiplié (par exemple, une banque en ligne demandant un justificatif fiscal dans le cadre d'un prêt). Une telle ouverture pose des questions juridiques, techniques (par exemple la robustesse du service sous charge accrue) et budgétaires »*.

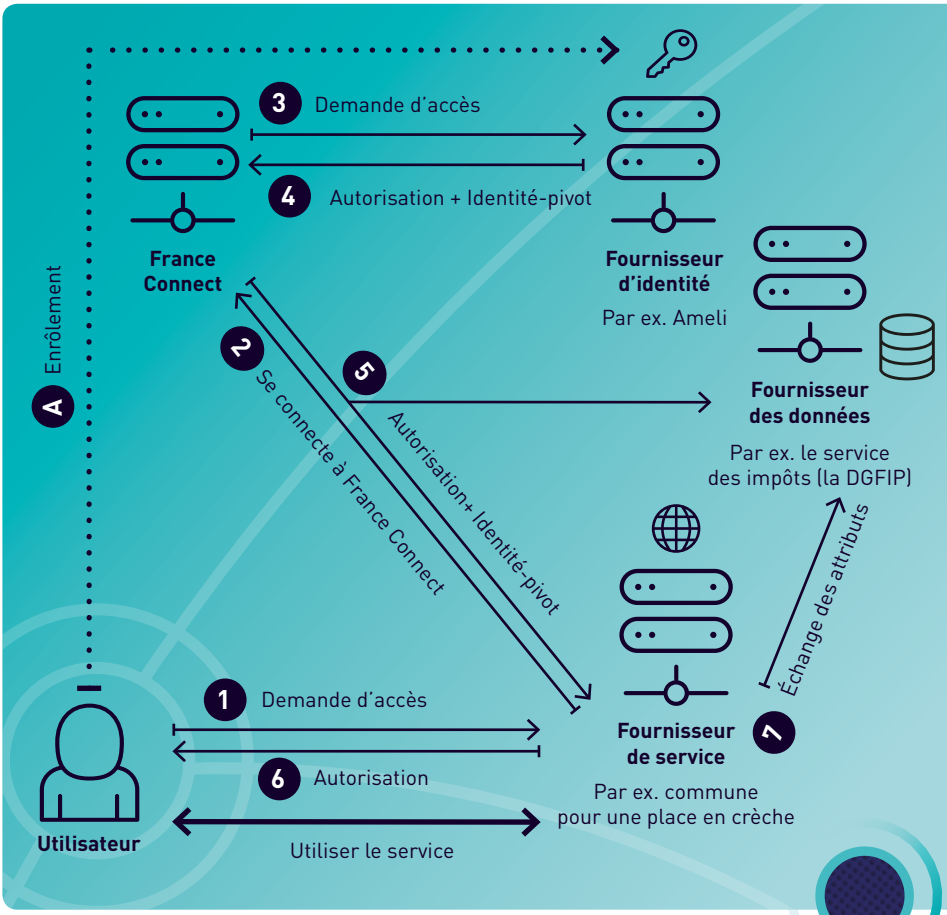


FIGURE 13. **France Connect**

Quel est le positionnement de France Connect par rapport au règlement eIDAS et à l'interopérabilité avec les identités numériques délivrées par les autres États membres de l'Union européenne ?

France Connect a été conçu en lien avec le règlement eIDAS, qui consacre la reconnaissance mutuelle des identités électroniques entre les États membres (*cf.* fiche 10). La France ne devrait notifier auprès de la Commission européenne que des moyens d'identification

fédérés dans France Connect. Une fois publiés au Journal officiel de l'UE, ces moyens seront reconnus et acceptés par l'ensemble des États de l'UE.

En ce qui concerne l'accès des services publics français par les citoyens européens, la mise en œuvre de l'interopérabilité sera assurée *via* l'articulation entre France Connect et les moyens d'identification des États membres dont ils sont originaires.

En ce qui concerne l'utilisation de services étrangers par les citoyens français, France Connect invitera l'utilisateur à s'authentifier lors de chaque accès auprès d'un des fournisseurs d'identités qu'il aura labellisés. Cette labellisation nécessitera de coordonner les niveaux de garantie « substantiel » ou « élevé » présentés par les fournisseurs d'identités opérant depuis le territoire français et ceux opérant dans chaque État membre de l'UE.

Quelles sont les mesures envisagées pour la protection des données personnelles ?

Selon Guillaume Blot, France Connect « *met en place plusieurs mécanismes de protection des données personnelles même s'il n'y a pas de mécanisme de pseudonymat à proprement parler. Ceci est motivé par le fait que les services d'e-administration demandent en règle générale d'avoir ce que nous appelons l'identité pivot (nom, prénom, date et lieu de naissance, sexe) ou au moins des éléments partiels de cette identité pivot. La démarche est donc celle de minimisation des données échangées. Il faut préciser que les données qui transitent par France Connect se limitent à cette identité pivot et ne sont pas conservées après la déconnexion de l'utilisateur.* »

France Connect ne comprend pas dans son état actuel de divulgation sélective fine pour la transmission de l'identité pivot. Il semble cependant que des évolutions dans ce sens soient prévues. Dans son état actuel, le projet comporte déjà un premier un mécanisme d'information et de contrôle par l'utilisateur. Ainsi, « l'usager a la capacité, si nécessaire, d'autoriser — ou pas — l'accès par le fournisseur de services publics aux données le concernant et détenues par un fournisseur de données. L'usager est également informé des échanges de données le concernant, à l'aide d'une fonction « historique » qui liste à la fois les autorisations et les échanges de données »[81].

Il est également prévu que France Connect puisse vérifier les données d'identité de l'utilisateur. Pour ce faire, France Connect vérifiera auprès du Répertoire national d'identification des personnes physiques (RNIPP) les informations composant l'identité pivot. Conformément au principe de proportionnalité, France Connect n'accèdera pas au Numéro d'identification personnel (NIR dit « numéro de sécurité sociale »), mais obtiendra simple-

81 Interview de Guillaume Blot et de Jean-Jacques Leandri, précitée.

ment la confirmation ou non qu'une telle personne est bien présente et enregistrée sans ambiguïté.

Quel est l'avenir de France Connect ?

Le projet France Connect semble rencontrer un certain écho auprès des services publics et de certaines communautés de développeurs. En témoigne par exemple la participation de trente équipes de développeurs lors d'un hackathon organisé les 18 et 19 juin 2015 visant à proposer des applications pilotes pour les services publics qui seront fournis aux usagers.

Si ce premier volet semble être en bonne voie, France Connect devra néanmoins faire face à des difficultés classiques étudiées dans le domaine de la diffusion des innovations, difficultés relatives à son ergonomie, à son « acceptation » par les utilisateurs, mais aussi à la méfiance, justifiée ou non, de ces derniers[82].

En ce qui concerne le deuxième volet, à savoir l'extension de France Connect à un écosystème incluant les services privés, on ignore pour l'instant si les acteurs privés qui sont censés jouer le rôle de fournisseurs d'identité trouveront des modèles d'affaires leur permettant de s'engager avec l'ampleur nécessaire.

82 Sur ces questions, nous renvoyons à Khatchatourov, A., Laurent, M., Levallois-Barth, C. (2015). Privacy in Digital Identity Systems: Models, Assessment, and User Adoption, in Electronic Government, Lecture Notes in Computer Science, Springer.

Fiche 10. La réglementation mise en place par l'Union européenne en matière d'identification électronique et des services de confiance (règlement eIDAS)

Claire Levallois-Barth

Le règlement (UE) nº 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (*Electronic IDentification And trust Services* - eIDAS) a été adopté le 23 juillet 2014[83]. Cette fiche décrit les deux types de services ainsi régulés : les services d'identification électronique et les services de confiance. Elle s'interroge sur la façon dont ce cadre complexe est actuellement mis en œuvre.

Abrogeant la directive dite « Signature électronique »[84] avec effet au 1er juillet 2016, le règlement eIDAS s'inscrit dans la mise en œuvre de la stratégie numérique pour l'Europe. Il vise à mettre en place un cadre transnational et intersectoriel complet pour les transactions électroniques des autorités publiques, des citoyens et des entreprises. À cette fin, **deux types de services sont couverts : les services d'identification électronique et les services de confiance**.

Le traitement de données personnelles étant intrinsèque à la création et à l'utilisation de ces services, ceux-ci doivent être conformes à la législation en vigueur, actuellement la directive 95/46/CE Protection des données, et lorsqu'il sera prochainement adopté au nouveau règlement Données personnelles (*cf.* fiche 6). Le règlement eIDAS précise par ailleurs que « *l'utilisation de pseudonymes dans les transactions électroniques n'est pas interdite* ». Pour autant, leur utilisation ne doit pas empêcher les États membres d'exiger l'identification d'une personne en vertu du droit national ou du droit de l'Union européenne. Ce faisant, le règlement couvre le cas de l'authentification pseudonymisée (*cf.* fiche 7). Dans tous les cas, les données traitées doivent être considérées comme des données personnelles lors de l'utilisation de pseudonymes.

L'objectif poursuivi ainsi que les modalités de répartition des compétences entre l'Union européenne et les États membres expliquent principalement la complexité du cadre mis en place.

10.1. Quelles sont les conditions de reconnaissance mutuelle des services d'identification électronique ?

La réglementation en matière d'identité relevant de la compétence des États membres, le but n'est pas d'établir un système européen de gestion de l'identité électronique (par

83 Règlement (UE) nº 910/2014 du Parlement européen et du Conseil du 23 juill. 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE : JOUE L 257/73 du 28 août 2014.

84 Directive 1999/93/CE du Parlement européen et du Conseil du 13 déc. 1999 portant sur un cadre communautaire pour les signatures électroniques : JOUE L 13 du 19 janv. 2000, p. 12.

exemple en créant une carte d'identité européenne électronique) ou d'obliger les États à mettre en place des systèmes d'identification électronique.

> Le but recherché est de fixer des règles d'interopérabilité afin que les systèmes nationaux acquièrent une dimension paneuropéenne.

Les obligations imposées concernent uniquement les services publics transfrontaliers, les États devant encourager le secteur privé à utiliser, sur une base volontaire, les moyens d'identification électronique relevant du règlement.

➔ Ainsi, un État qui prévoit une possibilité d'authentification doit s'assurer que cette solution est accessible aux utilisateurs du secteur public établis hors de ses frontières dans les mêmes conditions que celles appliquées sur son territoire.

> **Identification électronique :** « *le processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale* » (art. 3 [1] du règlement [UE] n° 910/2014 eIDAS)
> **Authentification :** « *un processus électronique qui permet de valider l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité d'une donnée sous forme électronique* » (art. 3 [5] du règlement [UE] n° 910/2014 eIDAS)

Concrètement, la reconnaissance obligatoire des moyens d'identification électronique s'effectue selon une procédure en trois étapes qui sera mise en place en 2018.

Étape 1. La Commission européenne définit un **cadre d'interopérabilité**, *via* des actes d'exécution. Déclaré neutre du point de vue technologique (ce qui signifie qu'il ne devra pas opérer de discrimination entre les solutions techniques nationales) et fondé sur des normes européennes et internationales, ce cadre doit « *facilite [r] la mise en œuvre du principe du respect de la vie privée dès la conception* » (*Privacy by design*). Il comporte notamment des références aux exigences techniques et à un ensemble de **données d'identification personnelle**, à savoir « *un ensemble de données permettant d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant une personne morale* ».

Étape 2. Les États membres ont la possibilité de **notifier** à la Commission européenne **le ou les schémas d'identification électronique interopérables utilisés au**

niveau national. Ce schéma doit répondre aux exigences d'au moins un des trois niveaux de garantie définis par la Commission européenne : garantie « faible », « substantielle », « élevée ».

Le niveau de garantie dépend du niveau de fiabilité que le moyen d'identification électronique accorde à l'identité revendiquée ou prétendue d'une personne. Il tient compte notamment des processus de preuve et de vérification d'identité, de l'entité délivrant les moyens d'identification et des contrôles mis en œuvre.

Garantie	Fiabilité	Objectif
FAIBLE	Accorde un degré limité de fiabilité de l'identité revendiquée ou prétendue d'une personne	Réduire le risque d'utilisation abusive ou d'altération de l'identité
SUBSTANTIELLE	Accorde un degré substantiel de fiabilité de l'identité revendiquée ou prétendue d'une personne	Réduire substantiellement le risque d'utilisation abusive ou d'altération de l'identité
ELEVÉE	Accorde un degré de fiabilité plus élevé	Empêcher l'utilisation abusive ou l'altération de l'identité

FIGURE 14. Règlement eIDAS : niveaux de garantie des services d'identification électronique

La notification des schémas nationaux est libre : l'État peut notifier la totalité ou bien une partie du schéma ou refuser de le faire. Toutefois, les moyens d'identification notifiés doivent être exigés pour accéder au minimum à un service fourni par un organisme public relevant de l'État membre. Ces moyens peuvent être fournis selon trois modes : par l'Etat lui-même, *via* un mandat délivré par cet Etat ou indépendamment de l'État. Dans ce dernier cas, le moyen doit avoir été reconnu par l'État : rien ne s'oppose donc à ce qu'un État membre notifie un service d'identification fourni par une multinationale américaine.

Étape 3. La liste des systèmes nationaux notifiés et les informations essentielles afférentes sont **publiées** au Journal officiel de l'UE. Cette publication rend effectives la reconnaissance et l'acceptation mutuelles d'une solution d'identification de niveau « substantiel » ou « élevé » par l'ensemble des États de l'UE.

➔ Concrètement, si un État A exige une identification électronique élevée pour accéder à un service en ligne fourni par un organisme public, cet Etat doit reconnaître le moyen d'identification élevé délivré par l'Etat B. L'État A reste libre de reconnaître ou non un moyen d'identification notifié par l'État B de niveau « faible ».

Afin d'assurer un fonctionnement pérenne du système, un mécanisme de coopération entre les États membres est prévu. En cas de dommage causé intentionnellement ou par négligence, chaque type de responsabilité (celle de l'État, celle de la partie qui délivre le moyen d'identification et celle qui le gère) s'applique conformément aux dispositions nationales, par exemple les dispositions relatives à la définition des dommages ou à la charge de la preuve.

10.2. **Quel est le cadre juridique pour les services de confiance ?**

Les cinq services de confiance

Le règlement instaure un cadre juridique concernant l'utilisation de cinq services de confiance normalement fournis contre rémunération : les signatures électroniques, les cachets électroniques, les horodatages électroniques, les services d'envoi recommandé électronique et de certificats relatifs à ces services, les certificats pour l'authentification de sites internet. Chaque service dispose de deux ou trois niveaux de confiance. Les États sont libres de recourir à ces services et de définir d'autres types de services de confiance reconnus au niveau national.

Services	Niveaux de confiance		
Signature électronique (Personne physique)	**SIMPLE**	**AVANCÉE**	**QUALIFIÉE : RECONNUE ET ACCEPTÉE DANS TOUS LES ÉTATS MEMBRES**[85]
Cachet électronique (Personne morale)			
Horodatage électronique	**SIMPLE** (garantie de non-répudiation)	**QUALIFIÉ : RECONNUE ET ACCEPTÉE DANS TOUS LES ÉTATS MEMBRES :** le service bénéficie d'effets juridiques identiques au même service ramené au papier, lorsqu'il existe	
Service d'envoi recommandé électronique	**SIMPLE**	**QUALIFIÉ :** le service bénéficie d'effets juridiques identiques au même service ramené au papier, lorsqu'il existe[86]	
Authentification de sites internet			

FIGURE 15. **Règlement eIDAS : niveaux de confiance pour les services**

Seuls les services de confiance fournis au public et ayant des effets sur des tiers doivent remplir les exigences fixées par le règlement. En particulier, le règlement eIDAS ne couvre pas :

- la fourniture de services utilisés exclusivement dans des systèmes fermés au sein d'un ensemble défini de participants et donc inopposables aux tiers, par exemple les systèmes institués par des entreprises ou des administrations publiques pour gérer les procédures internes ou un système d'identification entre une banque et ses clients ;
- les aspects relatifs à la conclusion et à la validité des contrats ou autres obligations juridiques lorsque des exigences d'ordre formel sont posées par le droit national ou de l'Union européenne. Ainsi, les parties à une transaction pourront éventuellement déroger aux dispositions du règlement sur la base d'un contrat contenant des stipulations sur la preuve et la signature[87].

85 Exigences définies par l'annexe IV pour les certificats.

86 Exigences définies par l'annexe I pour les certificats qualifiés, par l'annexe II pour les dispositifs de création de signature électronique, et l'annexe III pour les certifications.

87 Caprioli, E. A., Agosti, P. (2013). La régulation du marché européen de la confiance numérique : enjeux et perspectives de la proposition de règlement européen sur l'identification électronique et les services de confiance, *CCE* 2013, n° 2, étude 3.

La signature électronique

La signature électronique reste l'apanage d'une personne physique. Elle compte trois niveaux : « simple », « avancé » et « qualifié ». Les dispositifs de création de signature électronique qualifiée et les certificats qualifiés de signature électronique sont reconnus dans tous les États membres s'ils répondent aux exigences des annexes I et II du règlement. Une fois certifiés par des organismes publics ou privés nationaux, ces dispositifs figurent sur une liste gérée par la Commission européenne. Ils produisent alors un effet juridique « équivalent à celui d'une signature manuscrite ». Néanmoins, ils ne bénéficient pas du même effet juridique dans l'UE, cet effet étant défini par chaque État.

Le cachet électronique

Le cachet électronique est réservé aux personnes morales.

> **Cachet électronique** : « *des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières* » (art. 3 [25] du règlement [UE] n° 910/2014 eIDAS)

D'une part, le cachet électronique sert à prouver qu'un document électronique a été délivré par une personne morale comme les factures électroniques, les offres de crédit ou les bulletins de paie ; d'autre part, il permet d'authentifier tout bien numérique d'une personne morale, tel un code logiciel ou un serveur. Le cachet compte lui aussi trois niveaux : simple, avancé et qualifié. Le **cachet électronique qualifié** bénéficie d›une présomption d'intégrité et d'exactitude de l'origine des données. Il est reconnu dans tous les Etats membres s'il satisfait aux exigences posées par le règlement eIDAS, notamment son annexe III.

Les trois autres services de confiance comprennent deux niveaux : « simple » (le service bénéficie d'une simple garantie de non-répudiation) et « qualifié » (le service bénéficie d'effets juridiques identiques au même service fourni sous forme papier).

L'horodatage électronique

Horodatage électronique : «*des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant*» (art. 3 [33] du règlement [UE] n° 910/2014 eIDAS)

L'horodatage électronique qualifié bénéficie d'une présomption d'exactitude de la date et de l'heure qu'il indique et d'intégrité des données. Il est reconnu dans tous les États membres s'il satisfait aux exigences fixées par le règlement.

Les services d'envoi recommandé électronique

Services d'envoi recommandé électronique : «*un service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée*» (art. 3 [36] du règlement [UE] n° 910/2014 eIDAS)

Les données envoyées et reçues au moyen d'un tel service bénéficient d'une présomption quant à leur intégrité, à leur envoi par l'expéditeur identifié et à leur réception par le destinataire identifié. À cette fin, le service qualifié doit, pour exclure toute modification indétectable des données, utiliser une signature électronique avancée ou un cachet électronique avancé.

Services d'authentification de sites internet

Enfin, le règlement fixe les obligations minimales de sécurité et de responsabilités applicables aux prestataires et aux **services d'authentification de sites internet.** La fourniture et l'utilisation de ces services se font uniquement sur une base volontaire. Les certificats qualifiés d'authentification d'un site internet doivent satisfaire les conditions fixées par l'annexe IV du règlement. Ainsi, un visiteur peut s'assurer que le site internet est géré par une entité véritable et légitime.

Les obligations et responsabilités des prestataires de services de confiance

Le règlement distingue deux types de prestataires : le prestataire non qualifié et le prestataire qualifié. Dans les deux cas, le prestataire doit prendre les mesures adéquates pour gérer les risques liés à la sécurité. En particulier, il est soumis à une obligation de notification de toute atteinte à la sécurité ou de perte d'intégrité « ayant une incidence importante sur le service de confiance fourni ou sur les données personnelles qui y sont conservées ». La notification devra être effectuée dans un délai de 24 heures auprès de l'organe de contrôle (en France, l'ANSSI) et, le cas échéant, auprès des autres organismes concernés (organisme national compétent en matière de sécurité de l'information, autorité chargée de la protection des données, etc.) ainsi qu'aux personnes bénéficiant du service de confiance et susceptibles de subir un préjudice.

Le prestataire qualifié est soumis à des exigences renforcées. Il doit en particulier vérifier tous les attributs spécifiques de la personne physique ou morale à laquelle il délivre le certificat qualifié, tenir à jour une base de données relative aux certificats et fournir des informations précontractuelles à ses clients. Il doit bénéficier d'un système d'assurance responsabilité adéquat, assurer la continuité du service et prendre des mesures appropriées en ce qui concerne les preuves à produire en justice.

Conformément aux principes de non-discrimination et de neutralité technologique, la qualification ne conditionne pas l'efficacité juridique et la recevabilité d'une signature, d'un cachet, d'un horodatage ou d'un envoi recommandé électroniques comme moyens de preuves en justice. Il est possible de **recourir à des services non qualifiés** qui ne peuvent pas être refusés comme moyens de preuve. Cependant, l'interopérabilité est réduite. En outre, l'utilisateur ne bénéficie pas d'une présomption « légale » de fiabilité. En effet, si les prestataires de services de confiance sont **responsables des dommages** causés intentionnellement ou par négligence à toute personne en raison d'un manquement à leurs obligations, la charge de la preuve diffère :

- le prestataire qualifié est présumé responsable, à moins qu'il ne prouve que les dommages ont été causés sans intention ni négligence de sa part ;
- à l'inverse, la faute du prestataire non qualifié doit être prouvée par l'utilisateur qui invoque l'existence d'un préjudice.

Du côté du prestataire qualifié, la qualification constitue la reconnaissance d'un niveau « élevé » de fiabilité technique. L'objectif est qu'elle soit perçue comme un signe de confiance qui prendra la forme d'un label mis en œuvre par la Commission européenne.

10.3. **Quel rôle et quels pouvoirs pour les organes de contrôle ?**

Afin de renforcer la confiance, chaque État membre doit désigner un « **organe de contrôle** ». En France, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) contrôle *a posteriori* les prestataires non qualifiés. Elle accorde le statut de prestataire qualifié après examen d'un rapport d'audit délivré par un organisme d'évaluation de la conformité. Le prestataire peut fournir son service qualifié lorsque son statut est mentionné sur les listes nationales de confiance. Il doit, par la suite, transmettre, au minimum tous les deux ans, un rapport d'audit. L'ANSSI peut exiger que tout manquement soit corrigé et, à défaut de correction, retirer le statut de qualifié.

Pour les entreprises établies dans plusieurs États membres, le principe du guichet unique s'applique : un seul organe de contrôle est compétent pour contrôler les activités d'un prestataire dans l'ensemble de l'UE, celui du pays du principal lieu d'établissement de l'entreprise. Cet organe doit coopérer avec ses homologues européens et avec les autorités de protection des données personnelles. Particulièrement, il les informe des résultats des audits faisant apparaître une violation des règles de protection des données personnelles.

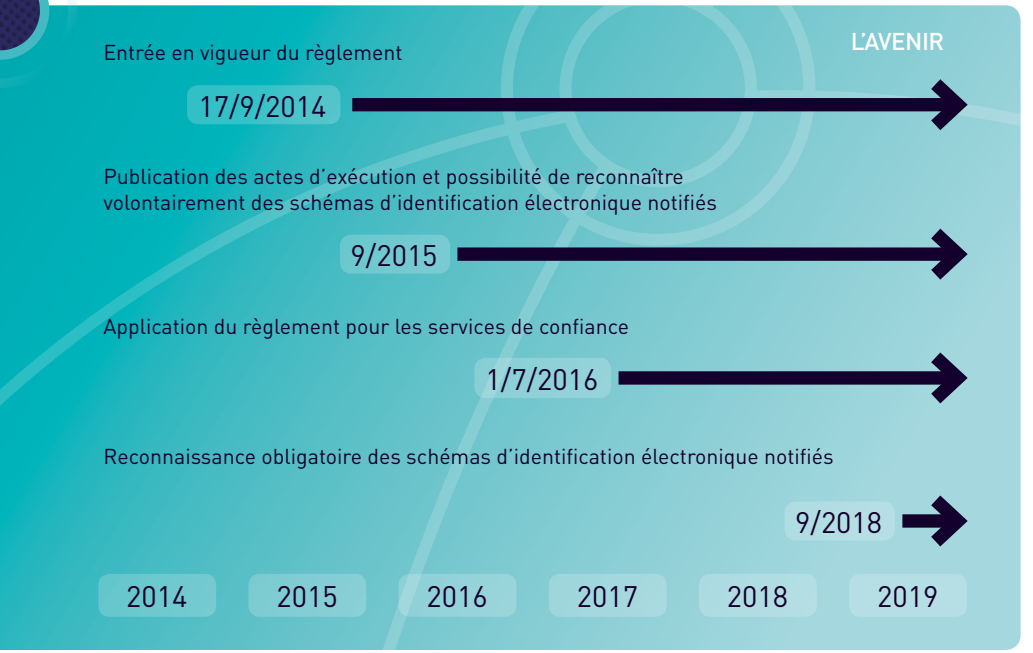


FIGURE 16. **Règlement eIDAS : chronologie de mise en œuvre**

Le règlement eIDAS est un texte de base, un socle nécessitant d'être décliné sous plusieurs formes :

- des **actes d'exécution** : le règlement eIDAS prévoit explicitement que certaines de ses dispositions soient précisées par la Commission européenne *via* des actes d'exécution. Afin de permettre aux États membres de rester associés, l'adoption de ces actes est strictement encadrée. Conformément à l'article 291 du Traité sur le fonctionnement de l'Union européenne, la Commission doit soumettre chaque projet d'acte d'exécution à un comité composé d'experts représentant des États membres ; ce processus d'adoption de mesures d'exécution des actes législatifs est désigné sous le terme de « comitologie » ;
- des **normes**, en cours d'élaboration[88] ;
- des **déclinaisons nationales**, avec des niveaux variés de protection des données personnelles. Selon des chercheurs de l'Université de Londres, le système GOV.UK Verify présenterait de graves problèmes en termes de protection des données personnelles, notamment parce que l'identification des citoyens s'appuie sur le croisement de fichiers opéré par des opérateurs publics et privés[89]. Soulignons ici que, contrairement aux autres pays de l'UE, le Royaume-Uni n'a pas signé la Charte des droits fondamentaux de l'Union européenne.

Cette structure en forme de « poupées russes » explique le manque de visibilité. Elle se révèle d'autant plus complexe à mettre en œuvre que le règlement est difficile à appréhender compte tenu de son aspect technique et de son champ d'application. La façon dont les quelque quatre-vingts normes sont élaborées n'est guère transparente. Les enjeux sont pourtant de taille. Il s'agit, par exemple, de garantir qu'un prestataire qualifié sera en mesure de fournir un accès aux données liées à une signature électronique dans 30 ans ou d'assurer le séquestre électronique de données pendant 100 ans. Surtout, le règlement eIDAS laisse une large place, une trop large place selon certains, aux actes d'exécution. La Commission européenne en a adopté sept et est compétente pour en adopter vingt autres, si elle l'estime nécessaire.

---

88 Pour aller plus loin : *Publication des spécifications techniques en matière d'identification électronique (eIDAS)*, http://www.ssi.gouv.fr/agence/publication/publication-des-specifications-techniques-en-matiere-didentification-electronique-eIDAS. On peut également se reporter à : ISO/IEC 24760, *A framework for identity management*, ISO/IEC 29115, *Entity authentication assurance framework*, ISO/IEC 9798, *Entity Authentication*, ISO/IEC 29100, *Privacy Framework*.

89 Brandão, L., Christin, N., Danezis, G., Anonymous (2015). Toward Mending Two Nation-Scale Brokered Identification Systems, *Proceedings on Privacy Enhancing Technologies* 2015(2):1–22.

Services d'identification électronique	Services de confiance
Cadre d'interopérabilité[90]	Format des signatures électroniques et des cachets électroniques avancés[91]
Modalités de coopération entre les États membres[92]	Format des signatures électroniques et des cachets électroniques avancés[93]
Niveaux de garantie des schémas nationaux d'identification électronique[94]	Format du label européen[95]
	Listes de confiance[96]

FIGURE 17. **Règlement eIDAS : mesures d'exécution**

Enfin, eIDAS est étonnamment silencieux en ce qui concerne l'application des principes fondamentaux régissant la protection des données personnelles (*cf.* fiche 6). Il aurait dû évoquer les droits des personnes concernées, notamment le droit d'information qui conditionne la validité du consentement. Surtout, il ne fait guère référence aux principes de proportionnalité et de minimisation des données personnelles. Ce point est d'autant plus important que les solutions d'identification électronique déjà mises en place dans certains États membres obligent le plus souvent l'utilisateur à divulguer toutes les informations contenues dans son moyen d'identification, par exemple dans sa carte d'identité électro-

90 Règlement d'exécution (UE) 2015/1501 de la Commission du 8 sept. 2015 sur le cadre d'interopérabilité visé à l'article 12, § 8, du règlement (UE) n° 910/2014 : JOUE L 235 du 9 sept. 2015, p. 1.

91 Décision d'exécution (UE) 2015/1506 de la Commission du 8 sept. 2015 établissant les spécifications relatives aux formats des signatures électroniques avancées et des cachets électroniques avancés devant être reconnus par les organismes du secteur public visés à l'article 27, § 5, et à l'article 37, § 5, du règlement (UE) n° 910/2014 : JOUE L 235 du 9 sept. 2015, p. 57.

92 Décision d'exécution (UE) 2015/296 de la Commission du 24 fév. 2015 établissant les modalités de coopération entre les États membres en matière d'identification électronique conformément à l'article 12, § 7, du règlement (UE) n° 910/2014 : JOUE L 53 du 25 fév. 2015, p. 14.

93 Décision d'exécution (UE) 2015/1506 de la Commission du 8 sept. 2015 établissant les spécifications relatives aux formats des signatures électroniques avancées et des cachets électroniques avancés devant être reconnus par les organismes du secteur public visés à l'article 27, § 5, et à l'article 37, § 5, du règlement (UE) n° 910/2014 : JOUE L 235 du 9 sept. 2015, p. 57.

94 Règlement d'exécution (UE) 2015/1502 de la Commission du 8 sept. 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, § 3, du règlement (UE) n° 910/2014 : JOUE L 235 du 9 sept. 2015, p. 7.

95 Règlement d'exécution (UE) 2015/806 de la Commission du 22 mai 2015 établissant les spécifications relatives à la forme du label de confiance de l'Union pour les services de confiance qualifiés : JOUE L 128 du 23 mai 2015, p. 13

96 Décision d'exécution (UE) 2015/1505 de la Commission du 8 sept. 2015 établissant les spécifications techniques et les formats relatifs aux listes de confiance visées à l'article 22, § 5, du règlement (UE) n° 910/2014 : JOUE L 235 du 9 sept. 2015, p. 26.

nique. En réalité, le règlement est construit sur le concept d'identification et ne se réfère pas à l'authentification, entendue comme la possibilité d'accéder à des ressources sans pour autant être identifié de manière univoque[97].

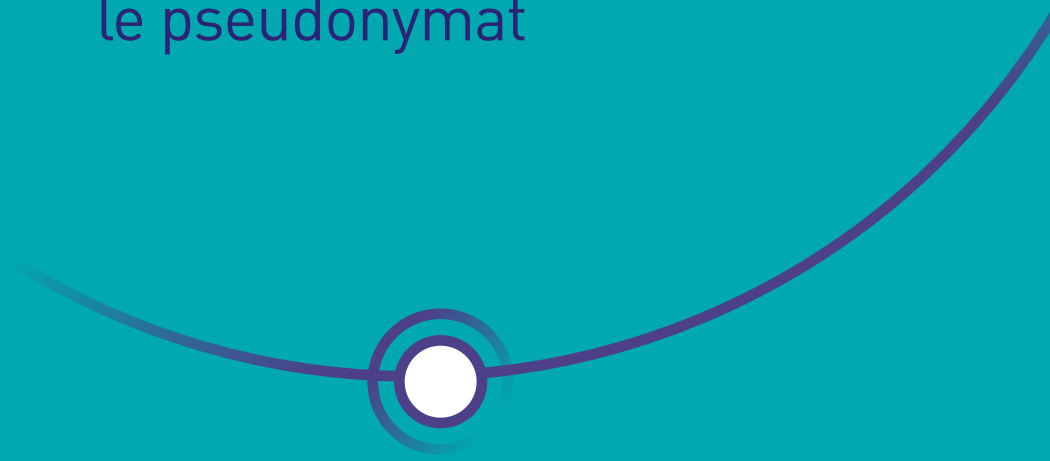
De façon inquiétante, on retrouve cette logique dans le règlement d'exécution (UE) 2015/1501 sur le cadre d'interopérabilité qui définit un « *ensemble minimal de données d'identification personnelle représentant de façon univoque une personne physique* »[98]. Cet ensemble comprend obligatoirement les nom et prénom, la date de naissance et surtout un identifiant unique « qui soit aussi persistant que possible dans le temps » créé par l'État membre expéditeur. En gardant à l'esprit que « *l'utilisation d'un identifiant personnel unique pour des finalités et contextes variés a été jugé inconstitutionnel en Allemagne, Hongrie, Portugal* »[99], il est permis d'avoir des doutes sur la validité juridique de cette mesure d'exécution.

97 Zwingelberg H., Schallaböck, J. (2013). *The Proposal for a Regulation on Electronic Identification and Trust Services under a Privacy and ABC4Trust Perspective*, https://abc4trust.eu/index.php/pub/deliverables/176-h2-4.

98 Règlement d'exécution (UE) 2015/1501, précité, Annexe « Exigences relatives à l'ensemble minimal de données d'identification personnelle représentant de manière univoque une personne physique ou morale, visé à l'article 11 »

99 Gomes de Antrade, N. N. (2012). Towards a European eid Regulatory Framework: Challenges in Constructing a Legal Framework for the Protection and Management of Electronic Identities, *in European Data Protection: In Good Health?* Gutwirth, S., Leenes, R., De Hert, P., Poullet, Y., (Eds.), Springer.

Fiche 11. Les preuves d'identités ou d'attributs préservant le pseudonymat



Maryline Laurent
et Nesrine Kaâniche

Actuellement, les solutions développées par les différents pays européens sont à elles seules insuffisantes pour garantir la multi-identité et protéger de façon optimale les données personnelles (*cf.* fiche 8). Cette fiche propose une alternative consistant à déployer des schémas de preuves d'identité ou d'attributs, à côté des schémas d'authentification.

À la différence des schémas d'authentification déjà déployés en Europe, les schémas de preuves respectueux du pseudonymat apportent la propriété d'inassociabilité (*cf.* fiche 3). Leur objectif est d'empêcher les fournisseurs de services et le fournisseur d'identités d'établir un lien entre un utilisateur et ses activités, et ce, même si l'utilisateur se connecte plusieurs fois au même fournisseur de services. À ce titre, les schémas de preuves sont complémentaires des schémas d'authentification, car certains services ne nécessitent pas de connaître l'identité réelle d'une personne.

Les schémas de preuves respectueux du pseudonymat[100] prennent place dans un contexte de transactions numériques. Ils permettent de fournir à une entité la preuve de l'identité d'une personne ou la garantie que cette personne répond à certains critères (être majeur, être titulaire du permis de conduire avec un nombre de points suffisants…), tout en conservant le pseudonymat de la personne et en ne dévoilant que le strict minimum des attributs qui lui sont associés. Plus précisément, ils visent à garantir :

- aux citoyens la préservation de leur pseudonymat ;
- aux fournisseurs de services la vérification des éléments fournis par ces mêmes citoyens, bénéficiaires du pseudonymat. Lors de cette vérification, les fournisseurs ne doivent prendre connaissance d'aucune donnée personnelle non nécessaire comme la véritable identité de la personne physique, ou bien certaines valeurs de ses attributs ;
- aux pouvoirs publics la possibilité de lever le pseudonymat et d'identifier la personne physique associée à la preuve sous réserve de certaines conditions prévues par un cadre légal, par exemple à l'occasion de litiges ou d'enquêtes judiciaires.

Les solutions émergentes s'intéressent principalement aux deux premières caractéristiques, mais ne répondent pas avec conviction et souplesse à la situation où le pseudonymat doit être levé.

Nous proposons par la suite de décrire les éléments fondamentaux des schémas de preuves avec leurs propriétés techniques, puis les solutions existantes et les défis de demain.

---

100 Pour des questions de cohérence du vocabulaire utilisé entre droit et sciences informatiques, il est fait référence au pseudonymat plutôt qu'à l'anonymat, mais gardons à l'esprit comme souligné dans la section « Le pseudonymat et l'anonymat sont-ils un leurre ? », que la communauté scientifique privilégie le terme « anonymat ». De plus, pour éviter les anglicismes, le terme « preuves » est utilisé alors que « *credential* » serait plus adapté techniquement.

11.1. Les différents types de preuves

Dans le contexte d'une transaction électronique, les trois preuves suivantes sont d'intérêt :

- **les preuves d'identité** : le fournisseur de services a besoin de s'assurer que l'utilisateur qui se présente sous un pseudonyme est bien une personne physique réelle ;
- **les preuves de consentement** : le fournisseur de services a besoin de recueillir le consentement de l'utilisateur avant de collecter ses données personnelles et de les traiter. L'idée est de permettre au fournisseur de conserver la preuve de consentement et de la faire valoir en cas de litige ;
- **les preuves d'attributs** : le fournisseur a besoin de s'assurer que l'utilisateur est âgé de plus de 18 ans, dispose d'un permis de conduire, est de nationalité française, réside en Île-de-France, a plus de trois enfants mineurs à charge… Une preuve de ces attributs lui est nécessaire, sans qu'il ait besoin d'avoir connaissance de l'identité réelle de l'utilisateur, ni de sa date de naissance, ni de son adresse précise. La preuve ne doit divulguer que le strict minimum des attributs requis pour l'obtention du service afin de respecter le principe de proportionnalité mentionné par la directive 95/46/CE Protection des données (*cf.* fiche 6).

11.2. Les propriétés attendues des schémas de preuves

Les schémas de preuves s'intéressent aux cinq propriétés suivantes :

- **le pseudonymat** garantit que les schémas de preuve ne révèlent pas l'identité réelle de l'utilisateur concerné ;
- **la non-falsification** correspond à l'impossibilité pour une entité illégitime d'émettre une preuve valide auprès d'un vérifieur ;
- **l'inassociabilité** (*unlinkability*) garantit que la preuve originale émise par l'émetteur ne peut pas être associée à la preuve dégradée (générée par l'utilisateur) ou que plusieurs preuves dégradées émises par un même utilisateur ne peuvent pas être reliées entre elles ;
- **la révocation** est la possibilité d'exclure un utilisateur du système pour l'empêcher de bénéficier du service de preuves ;
- **la divulgation minimale** permet à l'utilisateur de sélectionner un sous-ensemble des attributs spécifiés dans la preuve originale pour ne prouver au vérifieur au travers de la preuve dégradée que la véracité des attributs sélectionnés.

11.3. L'architecture fonctionnelle associée classiquement aux schémas de preuves

Les preuves nécessitent techniquement la mise en place d'une architecture fonctionnelle s'appuyant sur plusieurs acteurs aux rôles définis et sur leurs interactions. L'ensemble est communément appelé dans le domaine technique « schémas de preuves ».

Ces schémas reposent sur une architecture faisant intervenir tout au plus cinq acteurs remplissant les fonctions suivantes :

- **l'émetteur** émet pour le compte d'un utilisateur une preuve complète ; ce rôle est typiquement attribué au fournisseur d'identités ;
- **l'utilisateur** souhaite accéder à un service avec des garanties de pseudonymat et recourt à un système/service pour générer, à partir d'une preuve complète, une preuve dégradée qu'il transmet au vérifieur ;
- **le vérifieur ou fournisseur de services** demande à l'utilisateur de fournir une preuve d'identité ou d'attributs afin d'en vérifier sa validité ;
- **l'inspecteur (ou les pouvoirs publics)** est une entité de confiance qui lève le pseudonymat en cas de nécessité ;
- **l'autorité de révocation** révoque les utilisateurs du système pour les empêcher de continuer à utiliser le schéma de preuves.

Tout schéma de preuves doit nécessairement faire intervenir les trois premiers acteurs, les deux derniers étant optionnels. Notons qu'il est possible de fusionner certains acteurs, comme l'émetteur avec l'autorité de révocation ou le vérifieur. Néanmoins, afin de garantir le pseudonymat, il n'est pas permis de fusionner l'émetteur avec l'inspecteur.

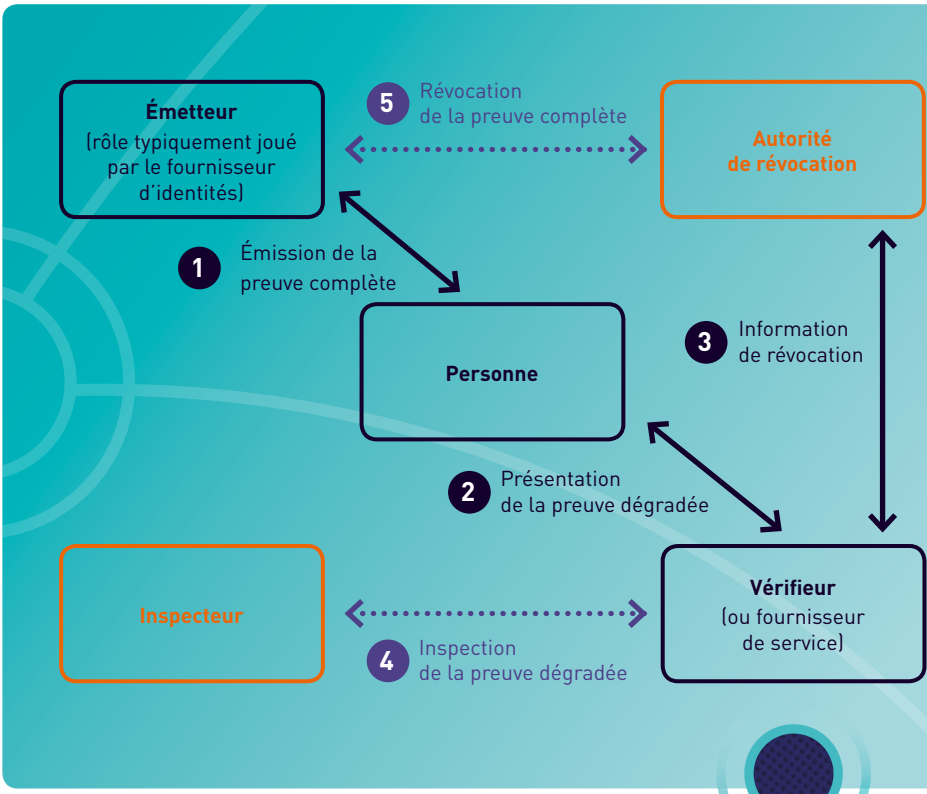


FIGURE 18. Architecture générique d'un schéma de preuves

11.4. Les solutions existantes

Actuellement, les solutions les plus connues sont « Idemix » de IBM et « U-Prove » de Microsoft. Elles trouvent leur origine dans les schémas conçus par Brands[101] et Camenisch-Lysyanskaya[102] en 2000 et 2002 respectivement. Depuis, elles ont été enrichies et améliorées. Tandis qu'« Idemix » satisfait les cinq propriétés attendues d'un schéma de preuves, « U-Prove » ne garantit pas totalement la propriété d'inassociabilité, ce qui permet au fournisseur de services d'identifier un même utilisateur au cours de ses différentes connexions.

101 Brands, S. A. (2000). Rethinking Public Key Infrastructures and Digital Certificates : Building in Privacy, MIT Press, Cambridge, MA, USA.

102 Camenisch, J., Lysyanskaya, A. (2002). A Signature Scheme with Efficient Protocols, SCN, Lecture Notes in Computer Science, vol. 2576, Springer.

Notons qu'« Idemix » fait partie de la solution technique retenue par le projet européen ABC4Trust et le projet pilote néerlandais IRMA.

Ces deux solutions reposent sur des principes cryptographiques et nécessitent des calculs lourds, ce qui explique qu'aujourd'hui elles ne soient pas industrialisées. En effet, les performances obtenues sur une carte à puce (de type MULTOS)[103] sont de l'ordre de la seconde, ce qui est au-delà des temps de réaction communément admis dans les transactions électroniques.

11.5. **Les défis de demain**

Afin de construire une infrastructure numérique de confiance, les schémas de preuves sous pseudonymat occupent une place importante. Encore faut-il relever plusieurs défis techniques, dont les suivants :

- concilier au sein d'un même schéma de preuves les propriétés de préservation de pseudonymat, de levée de pseudonymat, de révocation et de divulgation minimale ;
- atteindre des performances raisonnables de telle sorte que les calculs nécessaires puissent s'exécuter en très grand nombre sur des serveurs centralisés, ou que des terminaux de faible puissance puissent générer des preuves dégradées ;
- enrichir les schémas de preuves pour qu'ils prennent en compte les exigences définies par les nouvelles réglementations européennes, en particulier le futur règlement général sur la protection des données qui devrait être adopté en principe mi-2016.

Les recherches actuellement entreprises au sein de la Chaire Valeurs et Politiques des Informations Personnelles s'intéressent en particulier à définir des schémas de signatures peu coûteux en calculs et respectueux des propriétés de préservation de pseudonymat, de levée de pseudonymat, de révocation et de divulgation minimale.

103 Mostowski, W., Vullers, P. (2012). Efficient U-prove Implementation for Anonymous Credentials on Smart Cards, in Security and Privacy in Communication Networks, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Rajarajan, M., Piper, F., Wang, H., Kesidis, G. (Eds.), vol. 96:243–260, Springer. — Vullers, P., Alpar, G. (2013). Efficient Selective Disclosure on Smart Cards Using Idemix. In Policies and Research in Identity Management, IFIP Advances in Information and Communication Technology, vol. 396:53–67, Springer.

Conclusion

Armen Khatchatourov,
Claire Levallois-Barth
et Pierre-Antoine Chardel

Nous constatons aujourd'hui le développement de l'usage des identités numériques sous diverses formes, allant des identités « déclaratives » sur les réseaux sociaux en ligne jusqu'aux initiatives régaliennes, notamment au niveau européen. Si ces dernières sont majoritairement orientées vers le secteur public, elles sont aussi conçues pour être adoptées par les acteurs du secteur privé, pour des usages aussi variés que les achats en ligne ou les transports. Ce phénomène s'explique notamment par le fait qu'il semble de prime abord plus « commode » d'utiliser une même identité, avec un même système d'authentification, dans des contextes différents.

Or, comme il a été souligné dans ce Cahier, l'utilisation d'une identité unique dans des secteurs d'activité foncièrement différents n'est pas sans risque pour le respect des libertés fondamentales, libertés que le législateur français a entendu protéger notamment en adoptant en 1978 la loi Informatique et Libertés. Pour diminuer ces risques, il est possible de recourir à des systèmes de gestion des identités pseudonymisées, et à l'utilisation des identités multiples. Pour autant, on constate que la pseudonymisation n'est pas toujours suffisamment élaborée : certains acteurs peuvent procéder, *a posteriori*, à l'unification des identités d'une même personne en l'absence de tout consentement et ainsi regrouper ses données personnelles.

Dans un contexte où l'usage de l'identité numérique ne cesse de se développer, il convient d'en résumer les enjeux et de s'interroger sur les solutions qui permettraient de construire des systèmes qui ne conduisent pas à une traçabilité globale du citoyen. Il en va de l'intérêt de tous, notamment de l'État s'il entend maintenir sa souveraineté, mais aussi des entreprises pour lesquelles il est important d'obtenir la confiance de leurs clients.

Du point de vue du droit, les textes juridiques existants (la directive 95/46/CE Protection des données transposée en France *via* la loi Informatique et libertés) affichent une volonté claire d'assurer un « niveau élevé » de protection des données personnelles. Ces textes sont en cours de révision (*cf.* le projet de règlement européen Données personnelles) afin de renforcer de façon effective la protection actuellement offerte.

Cette approche, nous l'espérons, devrait permettre de corriger certains points faibles afin de remettre l'utilisateur au cœur du système technique et économique. Parmi les faiblesses actuelles, on note la difficulté d'une réelle manifestation de volonté de la personne. En pratique, un consentement n'est pas toujours réalisable : dans certains cas, l'utilisateur n'a pas d'autre choix que d'accepter les conditions proposées ; dans d'autres, le coût cognitif qui lui est demandé est beaucoup trop important[104]. Cette situation peut conduire à

104 *Cf.* par exemple Turow, J., Hennessy, M., & Draper, N. (2015). *The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers And Opening Them Up To Exploitation*. Annenberg School of Communication.

un déséquilibre des forces entre l'utilisateur et le détenteur de données. Les dispositions légales en cours d'adoption pourront-elles pallier ce déséquilibre ? Certains pensent que les démarches législatives actuelles restent insuffisantes[105]. On note cependant que le projet de règlement renforce la définition du consentement[106] et en précise les conditions[107]. Notamment, le responsable de traitement doit être en mesure de démontrer que la personne a bien donné son consentement conformément au principe de responsabilité.

Au chapitre de la mise en œuvre, les difficultés concernent également l'application du principe de transparence. Alors que l'avènement de notre monde numérique entraine un accroissement sans précédent de l'utilisation et du transfert ultérieur des données personnelles par des moyens de plus en plus complexes, il est difficile pour l'utilisateur de connaître ou de comprendre ce phénomène et encore plus d'exercer un certain contrôle sur la circulation de ses données. Le respect de son obligation d'information par le responsable de traitement est pourtant vital, car il conditionne la possibilité pour les individus de faire valoir leurs droits.

Si ces derniers n'ont pas connaissance de l'existence même du traitement, comment peuvent-ils devenir les acteurs de leur propre protection ? Comment peuvent-ils exercer leur (futur) droit à la portabilité des données ou leur droit à l'oubli, par exemple auprès de leur fournisseur d'identité ? Quand bien même pourraient-ils le faire, comment pourraient-ils s'assurer que ce fournisseur est digne de confiance en l'absence d'indicateurs fiables ? À cet égard, le renforcement de l'obligation d'information[108] et la mise en place de schémas de certification et de labels nous paraît constituer une réponse intéressante, susceptible de renforcer la transparence et de conférer un avantage compétitif aux produits et services labellisés.

---

105 À ce sujet, on consultera notamment : Koops, B.-J. (2014). *The trouble with European data protection law*, *International Data Privacy Law*, 4(4), pp. 250-261. — Mantelero, A. (2014). The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics, *Computer Law & Security Review*, 30(6), pp. 643–660. — Blume, P. (2014). The myths pertaining to the proposed General Data Protection Regulation, *International Data Privacy Law*, 4(4), pp. 269–273. Pour une discussion critique de « notice and consent », *cf.* notamment Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press.

106 Art. 4 (8) de la proposition de règlement Données personnelles du 28 janvier 2016 qui définit le consentement comme « *toute manifestation de volonté, libre, spécifique, informée et non ambigüe par laquelle la personne concernée accepte, par une déclaration ou par un acte positif univoque, que des données à caractère personnel la concernant fassent l'objet d'un traitement* » (traduction libre).

107 Art. 7 de la proposition de règlement Données personnelles du 28 janvier 2016. On peut également se référer au considérant 25 de la proposition ainsi qu'au le considérant 32 qui précise : « *Le consentement ne doit pas être considéré comme donné librement si la personne concernée ne dispose pas d'une véritable liberté de choix et n'est pas en mesure de refuser ou de se rétracter sans subir de préjudice* » (traduction libre).

108 Voir art. 12 de la proposition de règlement Données personnelles du 28 janvier 2016.

Il convient également d'encourager des démarches complémentaires, qui permettraient de décliner les principes légaux de façon contextuelle, opérationnelle et compréhensible à la fois pour les entreprises et le grand public. Cette déclinaison, qui est loin d'être aisée, doit s'exercer à la fois au niveau des politiques publiques (par exemple à travers la publication de guides de « bonnes pratiques »), des acteurs économiques (*via* notamment la promotion de ces pratiques par l'intermédiaire des associations professionnelles) et des utilisateurs.

Les solutions à apporter revêtent également des aspects techniques. Le moyen principal est de recourir à des identités multiples à travers les pseudonymes « inassociables ». Il convient toutefois de garder à l'esprit que le pseudonymat n'apporte qu'une réponse partielle au problème de traçabilité des utilisateurs. En outre, les solutions techniques se heurtent à un double obstacle.

Tout d'abord, comme le montre l'exemple de l'identité numérique régalienne en Allemagne, les solutions techniques protectrices des libertés individuelles demandent des investissements significatifs de la part des pouvoirs publics et éventuellement des entreprises. Par ailleurs, les changements technologiques remettent constamment en question leur efficacité. L'exemple par excellence est celui du croisement des données au sein du *big data*, croisement qui permet d'identifier l'individu de plus en plus précisément, alors même que celui-ci utilise de multiples identités numériques. Par conséquent, il importe de mettre en place les procédures internes adéquates afin de vérifier régulièrement l'efficacité des solutions implémentées, tout au long du cycle de vie des identités numériques.

Pour inciter les acteurs, et en particulier les acteurs économiques, à adopter des solutions protectrices des libertés individuelles, il faut mettre en évidence que les utilisateurs sont demandeurs de solutions pseudonymisées. En effet, si l'on suppose que le consommateur choisit une identité numérique selon le contexte de la transaction, on peut alors concevoir que ce choix soit guidé par la possibilité de rester « anonyme » et que la pseudonymisation influence positivement le taux d'utilisation et par conséquent le volume de transactions. À l'heure actuelle, il est difficile de tirer des conclusions, car il semble que cette corrélation dépende encore une fois du contexte sociotechnique. Certains travaux, comme ceux de Balgobin et al. (2015)[109] vont dans le sens d'une corrélation positive entre la protection des données personnelles offerte par les systèmes et leur taux d'utilisation : garantir l'anonymat lors d'une transaction permet d'acquérir des produits que l'on n'aurait

109 Balgobin, Y., Bounie, D., Quinn, M., Waelbroeck, P. (2015). *Payment Instruments, Financial Privacy and Online Purchases*, document de travail.

pas achetés. D'autres, comme ceux de Khatchatourov et al. (2015)[110], vont plutôt dans le sens d'une absence de corrélation dans le contexte des identités numériques fortes.

Finalement, les identités numériques soulèvent des enjeux fondamentaux relatifs à la société dans son ensemble. En effet, si la possibilité de construction active des identités multiples par les utilisateurs n'est pas préservée, l'autonomie des citoyens et l'exercice de leur libre arbitre, corolaires d'une posture citoyenne active s'en trouveront menacés. Par conséquent, une tendance à l'unification des identités qui s'installerait de manière durable risquerait de réduire la possibilité de voix hétérogènes, en remettant en cause l'équilibre fragile entre une certaine transparence et une possibilité de dissimulation pourtant nécessaire à l'épanouissement de chacun dans l'espace public[111].

Nous comprenons donc en quoi les mesures technologiques en faveur de l'identité unique renvoient à des choix non seulement politiques, mais aussi éthiques. Quelle vision de la société entendrons-nous porter avec de telles mesures ? Un défi majeur consistera à développer des solutions qui demeureront respectueuses de la construction de nos identités. Il faudra pour cela une véritable volonté de la part des Etats et des entreprises, dont les choix influencent de façon déterminante l'évolution de la société et la possibilité de stimuler (ou bien au contraire de neutraliser) le sens de l'agir commun. Une telle volonté de prendre soin de la qualité de l'être-ensemble devra passer, non seulement par des initiatives législatives et techniques appropriées, mais aussi par la mobilisation de la société civile, au moyen notamment d'une éducation au numérique qui serait en mesure de permettre une sensibilisation de l'ensemble des citoyens à ces enjeux si considérables pour l'avenir de nos sociétés démocratiques.

110 Khatchatourov, A., Laurent, M., Levallois-Barth, C. (2015). Privacy in Digital Identity Systems: Models, Assessment, and User Adoption, *in Electronic Government, Lecture Notes in Computer Science*, Springer.

111 Nous renvoyons sur ce point à : Pierre-Antoine Chardel, Brigitte Frelat-Kahn, Jan Spurk (dir.), *Espace public et reconstruction du politique,* Presses des Mines, 2015.

Bibliographie

Akerlof, G.A., Kranton, R.E. (2000). Economics and Identity, *Quarterly Journal of Economics*, 115(3).

Balgobin, Y., Bounie, D., Quinn, M., Waelbroeck, P. (2015). *Payment Instruments, Financial Privacy and Online Purchases*, document de travail.

Balgobin, Y., Bounie, D., Waelbroeck, P. (2015). *Quelle acceptation par les Français du partage de leurs données personnelles ?*, document de travail.

Blume, P. (2014). The myths pertaining to the proposed General Data Protection Regulation, *International Data Privacy Law*, 4(4).

Bounie, D., Bourreau, M., Gensollen, M., Waelbroeck, P. (2008). *Do Online Customer Reviews Matter ? Evidence from the Video Game Industry*, Telecom ParisTech Working Paper N° ESS-08-02. http://ssrn.com/abstract=1091449.

Bounie, D., Eang, B., Sirbu, M. A., Waelbroeck, P. (2012). *Online Price Dispersion : An International Comparison*. http://ssrn.com/abstract=1625847

Brandão, L., Christin, N., Danezis, G., Anonymous (2015). Toward Mending Two Nation-Scale Brokered Identification Systems, *Proceedings on Privacy Enhancing Technologies* 2015(2).

Brands, S. A. (2000). *Rethinking Public Key Infrastructures and Digital Certificates : Building in Privacy*, MIT Press, Cambridge, MA, USA.

Cabral L., Hortascu A., (2010). The Dynamics of Seller Reputation : Theory and Evidence from eBay, *Journal of Industrial Economics*, Vol. 58.

Camenisch, J., Lysyanskaya, A. (2002). A Signature Scheme with Efficient Protocols, *SCN, Lecture Notes in Computer Science,* vol. 2576, Springer.

Caprioli, E. A., Agosti, P. (2013). La régulation du marché européen de la confiance numérique : enjeux et perspectives de la proposition de règlement européen sur l'identification électronique et les services de confiance, *CCE,* 2013, n° 2, étude 3.

Caprioli, E. A., Mattatia, F., Vuillet-Tavernier, S. (2011). L'identité numérique, *Cahier de droit de l'entreprise* 2011, n° 3, entretien 3.

Cavoukian, A. (2009). *Privacy by Design: The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario, Canada. https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf.

Chardel, P.-A., Frelat-Kahn, B., Spurk, J. (dir.) (2015). *Espace public et reconstruction du politique,* Paris, Presses des Mines.

Chauvet, D. (2014). *La vie privée. Étude de droit privé*, th. Paris-Sud.

Cohen, J. (2012). *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*, Yale University Press.

Colin, N., Verdier, H. (2014). *L'âge de la multitude. Entreprendre et gouverner après la révolution numérique,* Paris, Armand Colin.

De Hert, P., Gutwirth, S. (2009). Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionlisation in Action, *in Reinventing Data Protection* ?, Gutwirth, S., Poullet, Y., Hert, P., Terwangne, C., Nouwt, S. (Eds.), Springer.

De Montjoye, Y.-A., Hidalgo, C.A., Verleysen, M., Blondel, V.D. (2013). Unique in the Crowd: The Privacy Bounds of Human Mobility, *Nature,* srep. 3, 1376 ; DOI:10.1038/srep01376, http://www.nature.com/articles/srep01376

Goffman, E. (1973). *La mise en scène de la vie quotidienne*, t. 1 La présentation de soi, Paris, Éditions de Minuit, coll. « Le Sens Commun ».

Gomes de Antrade, N. N. (2011). Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization, *in Computers, Privacy and Data Protection: An Element of Choice*, Gutwirth, S., Poullet, Y., De Hert, P., Leenes, R., (Eds.), Springer.

Gomes de Antrade, N. N. (2012). Towards a European eid Regulatory Framework: Challenges in Constructing a Legal Framework for the Protection and Management of Electronic Identities, *in European Data Protection: In Good Health?* Gutwirth, S., Leenes, R., De Hert, P., Poullet, Y., (Eds.), Springer.

Guattari, F. (2006). Entretien avec Jacques Robin : Révolution informatique, écologie et re-composition subjective, *Multitudes,* nº 24.

Harbach, M., Fahl, S., Rieger, M., Smith, M. (2013). On the Acceptance of Privacy-preserving Authentication Technology: The Curious Case of National Identity Cards, *in Privacy Enhancing Technologies*, De Cristofaro, E., Wright, M. (Eds.), Springer.

Hui K.L., Png I.P.L. (2006). The Economics of Privacy, *in Handbooks in Information Systems*, Hendershott, T. (Ed.), Elsevier.

Khatchatourov, A., Laurent, M., Levallois-Barth, C. (2015). Privacy in Digital Identity Systems: Models, Assessment, and User Adoption, *in Electronic Government, Lecture Notes in Computer Science*, Springer.

Kirman, A. (2004). The Structure of Economic Interaction: Individual and Collective Rationality, *in Cognitive Economics: An Interdisciplinary Approach*, Bourgine, P., Nadal J.-P. (Eds.), Springer, Ch. 18.

Koops, B.-J. (2014). The trouble with European data protection law, *International Data Privacy Law*, 4(4).

Lacouette-Fougère, C. (2008). *Les métamorphoses d'INES. Trajectoire d'un programme public innovant : la carte nationale d'identité électronique*, Mémoire à l'IEP Paris, Master Recherche Politique et sociétés en Europe, Lascoumes, P. (Dir.), 29 sept. 2008. http://www.laurent-mucchielli.org/public/Memoire_Clement_Lacouette-Fougere_Vallegee.pdf

Le Lamy Droit du numérique (2015). Wolters Kluwer.

Laurent, M., Bouzefrane, S. (Eds.) (2015). *La gestion des identités numériques*, Londres, ISTE, ISBN : 978-1-78405-056-6 (papier), ISBN : 978-1-78406-056-5 (ebook),

Levallois-Barth, C. (2014). Global Privacy Governance and Legal Issues, *in Cahier de prospective The futures of privacy,* Dartiguepeyrou, C. (Ed.), Fondation Télécom, Institut Mines-Télécom.

Mantelero, A. (2014). The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics, *Computer Law & Security Review*, 30(6).

Mostowski, W., Vullers, P. (2012). Efficient U-prove Implementation for Anonymous Credentials on Smart Cards, *in Security and Privacy in Communication Networks, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, Rajarajan, M., Piper, F., Wang, H., Kesidis, G. (Eds.), vol. 96:243–260, Springer.

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press.

Piazza, P. (2006). Les résistances au projet INES, *Cultures et Conflits*, nº 64.

Purtova, N. (2015). The illusion of personal data as no one's property, *Law, Innovation and Technology*, 7:1.

Ricœur, P. (1990.) *Soi-même comme un autre*, Le Seuil.

Rochelandet, F. (2010). Économie des données personnelles et de la vie privée, Paris, La Découverte, coll. «Repères».

Rochfeld, J. (2013). *Les grandes notions du droit privé*, 2e éd., PUF, coll. «Thémis droit».

Salanskis, J.-M. (1996). *Husserl*, Paris, Les Belles Lettres.

Salanskis, J.-M. (1998). *Heidegger*, Paris, Les Belles Lettres.

Sen, A. (2002). *Rationality and Freedom*, Harvard, Harvard Belknap Press.

Turow, J., Hennessy, M., & Draper, N. (2015). *The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers And Opening Them Up To Exploitation*. Annenberg School of Communication.

Vullers, P., Alpar, G. (2013). Efficient Selective Disclosure on Smart Cards Using Idemix. *In Policies and Research in Identity Management, IFIP Advances in Information and Communication Technology*, vol. 396:53–67, Springer.

Zarsky, T., Gomes de Andrade, N. N. (2013). Regulating Electronic Identity Intermediaries: The 'Soft eid' Conundrum, *Ohio State Law Journal*, Vol. 74, No. 6. http://ssrn.com/abstract=2368986.

Zhao, S., Grasmuck, S., Martin, J. (2008). Identity Construction on Facebook : Digital Empowerment in Anchored Relationships, *Computers in Human Behavior*, 24(5). http://doi.org/10.1016/j.chb.2008.02.012

Zwingelberg H., Schallaböck, J. (2013). *The Proposal for a Regulation on Electronic Identification and Trust Services under a Privacy and ABC4Trust Perspective*, https://abc-4trust.eu/index.php/pub/deliverables/176-h2-4.

Compléments de lecture

Blanchot, M. (1971). La terreur de l'identification, *in L'amitié*, Paris, Gallimard.

Cammilleri-Subrenat A., Prouvèze R., Verdier-Büschel I. (Dirs.) (2012). *Nouvelles technologies et défis du droit en Europe – L'imagerie active au service de la sécurité globale*, Bruylant, coll. «Travaux du CERIC».

Certeau, M. de. (1980). *L'invention du quotidien*, t. I, Arts de faire. Folio Essais.

Chardel, P.-A. (Dir.) (2014). *Politiques sécuritaires et surveillance numérique*, Paris, CNRS Editions.

Citton, Y. (2012). *Renverser l'insoutenable*. Paris, Seuil.

Crettiez, X., Piazza P., (Dir.) (2006). *Du papier à la biométrie. Identifier les individus,* Paris, Presses de Sciences Po.

Debet, A., Massot, J., Metallinos, N. (2015). *La protection des données à caractère personnel en droit français et européen*, L.G.D.J.

Deleuze, G. (1990). Post-scriptum sur les sociétés de contrôle, *in Pourparlers 1972 – 1990*, Paris, Les éditions de Minuit.

Delmas-Marty, M. (2010). *Libertés et sûreté dans un monde dangereux*, Paris, Editions du Seuil.

Detlev, Z., Dholakia, N. (2004). Consumer Subjectivity in the Age of Internet: The Radical Concept of Marketing Control through Customer Relationship Management, *Information and Organization*, 14(3). DOI : 10.1016/j.infoandorg.2004.01.002.

Detlev, Z, Dholakia, N. (2004). Whose Identity is it Anyway? Consumer Representation in the Age of Database Marketing, *Journal of Macromarketing*, 24(1). DOI: 10.1177/0276146704263920.

Gutmann, D. (2000). *Le sentiment d'identité*, LGDJ, coll. « Bibliothèque de droit privé ».

Guattari, F. (1992). *Chaosmose*. Galilée.

Mattelart, A. (2007). *La globalisation de la surveillance. Aux origines de l'ordre sécuritaire*, Paris, La Découverte.

Piolle, G. (2015). Protection des données personnelles dans le système d'information, *in Techniques de l'ingénieur - Sécurité des SI : organisation dans l'entreprise et législation* TIB458DUO (h5455), Éditions TI publisher.

Rouvroy, A., Berns, T. (2013). Gouvernementalité algorithmique et perspectives d'émancipation : le disparate comme condition d'individuation par la relation. *Réseaux*, 31 (177).

Voirol, O. (2011). L'intersubjectivation technique : de l'usage à l'adresse, *in Communiquer à l'ère numérique : regards croisés sur la sociologie des usages*, Denouël, J., Granjon, F. (Eds.), Paris, Presses des Mines.

Lexique

Authentification pseudonymisée : mécanisme permettant à l'utilisateur d'être authentifié et d'accéder à des services sans révéler son identité civile.

Communautés d'expériences : communautés médiatées à travers un support comme un site web ou un réseau social et permettant d'échanger des informations et des connaissances entre ses membres.

Certificat électronique : un document électronique permettant de rendre public le lien entre une entité et sa clé cryptographique publique, la confiance dans ce lien reposant sur la crédibilité de l'autorité émettrice du certificat.

Ciblage publicitaire : cherche à cibler une offre commerciale en fonction de l'intention d'achat d'un prospect ; le reciblage est dynamique et permet de suivre un prospect au cours de son parcours de navigation web ou mobile.

CNIe : Carte nationale d'identité électronique, document d'identité comportant habituellement toutes les caractéristiques de la carte nationale d'identité (CNI) classique et y ajoutant les moyens d'authentification électroniques, habituellement sous forme de carte à puce.

Credential : un élément d'information servant à prouver l'identité d'une personne et prenant la forme d'un mot de passe statique ou jetable, d'une signature électronique, etc. Très souvent, le mot de passe statique prédomine dans les usages courants, l'internaute détenant en moyenne cinq mots de passe pour accéder à ses comptes en ligne.

Discrimination par les prix : cherche à optimiser le prix de vente en fonction de la disponibilité à payer d'un client.

Divulgation minimale : dans le contexte des schémas de preuve, mécanisme permettant de sélectionner un sous-ensemble d'attributs spécifiés dans la preuve originale pour ne prouver au travers de la preuve dégradée que la véracité des attributs sélectionnés.

Divulgation sélective des attributs : mécanisme qui permet à l'utilisateur de divulguer le minimum nécessaire d'attributs pour réaliser une transaction électronique. Ce mécanisme peut être réalisé de manière automatisée ou pas, les deux approches pouvant être combinées. La première approche (divulgation sélective automatisée) est réalisée par le système qui confirme que l'utilisateur a plus de 18 ans sans divulguer la date de naissance, ou indique le département de résidence sans divulguer l'adresse exacte. La deuxième approche consiste à donner à l'utilisateur, à l'aide d'un tableau de bord ou d'un ensemble de cases à cocher, le choix de communiquer ou pas telle ou telle information.

Donnée à caractère personnel (donnée personnelle) : « *toute information concernant une personne physique identifiée ou identifiable (personne concernée) ; 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* » (art. 2a) de la **directive européenne 95/46/CE** Protection des données).

e-réputation : permet de résoudre des problèmes d'asymétries d'information lorsque l'on effectue une transaction avec une personne que l'on ne connaît pas.

eID : identité numérique (pour *electronic identity*), terme générique désignant une représentation de l'utilisateur dans l'environnement numérique. Dans la littérature anglophone en informatique, ce terme est utilisé essentiellement dans les contextes où il s'agit de l'identité régalienne ou assimilée.

Étude d'impact sur la vie privée (EIVP ou PIA pour *Privacy Impact Assessment*) : procédure visant à mesurer l'impact des systèmes techniques réels sur la protection de la vie privée et des données personnelles, avant leur déploiement et tout au long de leur cycle de vie.

Identité idem : correspond à un regard porté sur l'individu de l'extérieur, qui le considère comme une somme de caractéristiques stables.

Identité ipse : correspond à l'individu tel qu'il se rapporte à lui-même.

Identifiant unique : identifiant numérique associant de manière univoque et persistante dans le temps l'identité civile de l'utilisateur et l'identifiant numérique.

Identité pivot : le jeu minimum des attributs liés à l'identité de la personne permettant son identification.

Moyen d'authentification : tout moyen permettant à un utilisateur de s'authentifier auprès d'un service en ligne avant d'y accéder, comme le couple *login*/mot de passe, les certificats électroniques ou bien des équipements dédiés comme les cartes à puce ou le lecteur d'empreintes.

NIR : Numéro d'inscription au répertoire national d'identification des personnes physiques (RNIPP). Ce numéro correspond au numéro de sécurité sociale.

Non-falsification : impossibilité pour une entité illégitime d'émettre une preuve valide auprès d'un vérifieur.

Pseudonyme : alias ou nom d'emprunt pour dissocier l'identité civile correspondant à l'identifiant numérique, dans le but garantir à son propriétaire les propriétés d'anonymat et d'inassociabilité (*unlinkability*). Une même personne peut disposer de plusieurs pseudonymes. Le pseudonyme peut être soit choisi par la personne (nom d'emprunt), soit généré automatiquement de manière logicielle (par exemple, un nombre aléatoire « persistant »). Dans le contexte des schémas de preuve, mécanisme garantissant que les schémas de preuve ne révèlent pas l'identité réelle de la personne concernée.

Recommandations personnalisées : permettent de résoudre des asymétries d'information lorsque l'on ne connaît pas la qualité d'un bien ou d'un service *a priori*.

Révocation : procédure visant à empêcher d'utiliser un moyen d'authentification auprès d'un service, ou de bénéficier du service de preuves. La procédure est similaire à une mise en opposition des moyens de paiement dans le sens où une instance tierce interdit l'utilisation de services pour un moyen d'authentification donné.

RNIPP (Répertoire national d'identification des personnes physiques) : le RNIPP est un instrument de vérification de l'état civil des personnes nées en France. Sa consultation permet de préciser si une personne est vivante ou décédée et de connaître son Numéro d'inscription au répertoire (NIR). Le RNIPP permet la certification de l'état civil pour les organismes de sécurité sociale, l'administration fiscale, la Banque de France, pour le répertoire des entreprises SIRENE. Il permet la gestion du fichier électoral. Ce fichier ne peut être utilisé à des fins de recherche des personnes (source : CNIL).

Signature électronique : un élément d'information servant à prouver l'authenticité d'un document ou d'un flux de données. La signature est générée sur ce document ou flux à l'aide de la clé cryptographique privée de l'entité émettrice. La vérification de la signature nécessite la connaissance de la clé publique complémentaire et publiée dans le certificat électronique.

Inassociabilité (*Unlinkability*) : incapacité à relier au moins deux informations distinctes (enregistrements, messages, URL, actions, identifiants) relatives à un individu ou à un groupe d'individus. Dans le contexte des schémas de preuve, l'inassociabilité garantit que la preuve originale émise par l'émetteur ne peut pas être associée à la preuve dégradée (générée par la personne) ou bien que plusieurs preuves dégradées émises par une même personne ne peuvent pas être reliées entre elles.

Index

A

Acceptation 83
Accountability 61
Analyses d'impact 61
Anonymat 9, 32, 42
Anonymisation 54
Associabilité 69, 75, 110
Attributs 8, 52
Authentification 30, 47, 65, 110
Autodétermination informationnelle 25
Autonomie 8, 14
Autorité de délivrance 46

C

Carte nationale d'identité électronique 22, 47, 87
Ciblage publicitaire 39
CNIL 52
Communautés d'expériences 40
Confidentialité 57
Consentement 56, 60
Construction de l'identité 4, 14
Contextes 6, 15
Contextual privacy 15
Credential 30
Cycle de vie d'une identité 46

D

Data protection by design 9
Démocratie 8
Directive 95/46/CE 52, 54
Discrimination par les prix 39
Divulgation sélective des attributs 68
Données périphériques 34
Données personnelles 9, 22, 52, 66
Données sensibles 41, 58

Droit à la portabilité 60
Droit à la protection des données personnelles 66
Droit à l'oubli numérique 26, 60
Droit au respect de la vie privée 66
Droits de la personne 57
Durée de conservation 56

E

eIDAS 10, 86, 91, 96
Empreintes numériques (fingerprinting) 33
Enrôlement 46
E-réputation 38
Espace public 3
Etat civil 18

F

Federal Trade Commission 65
Fédération d'identités 90
Finalités 56
Fournisseur de services 46, 68
Fournisseur d'identités 46, 55, 70
Fournisseurs d'attributs 46

G

G29 32, 52
Générateur d'identité numérique 83

H

Hachage 76

I

Identifiant de portée générale 59
Identifiant unique 7, 107
Identification 30, 96
Identité civile 4
Identité-idem 12, 18
Identité-ipse 12, 21

Identité numérique en Allemagne 82
Identité numérique en Autriche 80
Identité numérique en Estonie 79
Identité numérique en Suisse 81
Identité régalienne 5, 16, 18, 96
Identités multiples 15, 25, 43, 69
Identité « souple » 16
Individualisation 18

J

Jeu à somme nulle 65

L

Légitimation 56
Loi Informatique et libertés 23, 52

M

Multitude 4

N

Numérisation 4

P

Privacy by design 35, 60, 64
Protection des données dès la conception 65, 67
Protection des données par défaut 65, 67
Pseudonymat 9, 20, 32, 69, 75, 110
Pseudonymes sectoriels 69, 76
Pseudonymisation 61

Q

Qualité des données 56

R

Recommandations personnalisées 39
Règlement Données personnelles 59, 65
Réseaux sociaux 3, 14, 49
Responsabilité 54
Responsable du traitement 54, 59

Ressources 3, 33
Retargeting 40

S

Schémas de preuves 112
Sécurité 57
Services de confiance 99
Sous-traitant 55
Subjectivité 3
Systèmes de gestion des identités numériques 8, 9, 46, 54, 68, 71

T

Tiers de confiance 46
Transfert de données personnelles 57

U

Unification de l'identité 15

V

Vie privée 52, 66
Vol d'identité 23

Table des illustrations

Figure 1. *Idem* et *Ipse* 13

Figure 2. Illustration des multiples manières dont les données périphériques sont diffusées 34

Figure 3. Gestion de l'identité numérique : exemple d'implémentation de la carte nationale d'identité électronique 48

Figure 4. Gestion de l'identité numérique : exemple type d'un réseau social 49

Figure 5. Exemples types de données personnelles 53

Figure 6. Principes clés de protection des données personnelles 55

Figure 7. Tableau comparatif des systèmes de gestions des identités numériques déployés en Europe 73

Figure 8. Les trois modèles du générateur de l'identité numérique 78

Figure 9. Le système estonien (identifiant unique utilisé dans les secteurs public et privé via les cartes à puce et les téléphones mobiles) 79

Figure 10. Le système autrichien (pseudonymes sectoriels utilisés dans les secteurs public et privé via les cartes à puce et les téléphones mobiles) 80

Figure 11. Le système suisse (pseudonymes optionnels et divulgation sélective utilisés dans les secteurs public et privé via les cartes à puce, les téléphones mobiles et les clés USB) 81

Figure 12. Le système allemand (pseudonymes optionnels et divulgation sélective utilisés dans les secteurs public et privé via les cartes à puce, les téléphones mobiles et les clés USB Allemagne) 82

Figure 13. France Connect 91

Figure 14. Règlement eIDAS : niveaux de garantie des services d'identification électronique 98

Figure 15. Règlement eIDAS : niveaux de confiance pour les services 100

Figure 16. Règlement eIDAS : chronologie de mise en œuvre 104

Figure 17. Règlement eIDAS : mesures d'exécution 106

Figure 18. Architecture générique d'un schéma de preuves 113

La Chaire de recherche « Valeurs et Politiques des Informations Personnelles »

Lancée par l'Institut Mines-Télécom en mars 2013, la Chaire regroupe une équipe pluridisciplinaire de chercheurs travaillant à la fois sur les aspects juridiques de régulation et de conformité, techniques de sécurité des systèmes et des données, économiques de partage des informations personnelles et philosophiques de responsabilisation et d'anticipation des conséquences sociétales.

Elle bénéficie du soutien de six mécènes : le Groupe Imprimerie Nationale, BNP Paribas, Orange, LVMH (mécènes fondateurs), Dassault Systèmes et Deveryware (mécènes associés), de la collaboration de la Commission nationale de l'informatique et des libertés (CNIL) et du support de la Fondation Télécom.

La Chaire est coordonnée par Claire Levallois-Barth, maître de conférences en droit à Télécom ParisTech et a été cofondée avec Maryline Laurent, professeur en sciences de l'informatique à Télécom SudParis, Patrick Waelbroeck, professeur en sciences économiques à Télécom ParisTech et Pierre-Antoine Chardel, professeur en philosophie à Télécom École de Management.

La Chaire Valeurs et Politiques des Informations Personnelles se propose d'aider les entreprises, les citoyens et les pouvoirs publics dans leurs réflexions sur la collecte, l'utilisation et le partage des informations personnelles, à savoir les informations concernant les individus (leurs vies privées, leurs activités professionnelles, leurs identités numériques, leurs contributions sur les réseaux sociaux, etc.), incluant celles collectées par les objets communicants qui les entourent. Ces informations fournies par les personnes, ou traces de leurs activités et interactions, posent en effet de nombreuses questions en termes de valeur sociale, valeur économique, politique de contrôle et politique de régulation.

Les travaux de la Chaire sont conduits selon cinq axes de recherche transdisciplinaires :

- les identités numériques ;
- la gestion des informations personnelles ;
- les contributions et traces ;
- les informations personnelles dans l'internet des objets ;
- les politiques des informations personnelles.

En plus de la publication d'articles de recherche et la participation aux colloques et conférences, la Chaire organise régulièrement des évènements ouverts à tous, pour sensibiliser le grand public sur ces enjeux majeurs du monde numérique.

→ **www.informations-personnelles.org**

Rencontres organisées par la Chaire en lien avec la thématique des identités numériques (évènements ouverts au public)

26 mars 2015 • **Internet des objets et *Privacy by design***

avec **Bernard Benhamou**, fondateur du portail de services mobiles Proxima Mobile et coordinateur de la première conférence ministérielle européenne sur l'internet des objets, et **Olaf Avenati**, designer graphique et numérique, enseignant à l'ESAD de Reims ; animée par Armen Khatchatourov.

17 juin 2014 • **Quelles pistes concrètes pour la réappropriation des informations personnelles par le citoyen ?**

avec **Daniel Kaplan**, cofondateur et délégué général de la Fondation pour l'internet Nouvelle Génération, et **Benjamin Sonntag**, entrepreneur et informaticien dans le monde du logiciel libre et de GNU/Linux, cofondateur de La Quadrature du Net ; animée par Armen Khatchatourov.

1er avril 2014 • **Traitement des informations personnelles dans les enquêtes**

avec **Eric Freyssinet**, colonel de gendarmerie, polytechnicien (X92) et maître **Olivier Itéanu**, avocat à la cour d'appel de Paris, président d'honneur de l'internet Society France, administrateur et secrétaire général d'Eurocloud France ; animée par Claire Levallois-Barth.

28 janvier 2014 • **Acceptation sociale massive de la surveillance : quelles sont les alternatives possibles à la passivité des usagers ?**

avec **Dominique Cardon**, sociologue au Laboratoire des usages d'Orange Labs et chercheur associé au Centre d'études des mouvements sociaux (CEMS/EHESS), et **Jean-Gabriel Ganascia**, professeur à l'université Pierre et Marie Curie (Paris VI), philosophe, expert en intelligence artificielle et éthique des nouvelles technologies ; animée par Pierre-Antoine Chardel.

15 octobre 2013 • **La vie privée en contexte, regards croisés Asie - Amérique du Nord**

avec **Helen Nissenbaum**, *Professor of Media, Culture and Communication and professor of Computer Science, Steinhardt School of Culture, Education and Human Development, New York University* et **Bregham Dalgliesh**, *Associate Professor, College*

of Arts and Sciences, University of Tokyo, Research Fellow, Interdisciplinary research group ETOS, Institut Mines-Télécom ; animée par Pierre-Antoine Chardel.

17 septembre 2013 • **Les enjeux européens de gestion des identités numériques**
avec **Amandine Jambert**, service de l'expertise informatique de la CNIL, et **Gabriel Periès**, professeur de sciences politiques à Télécom École de Management (Institut Mines-Télécom) ; animée par Claire Levallois-Barth.

17 juin 2013 • **Les frontières redéfinies du privé et du professionnel à l'ère du numérique : quelles conséquences pour les informations personnelles ?**
avec **maître Isabelle Renard**, avocate associée du cabinet Racine, et **Antonio A. Casilli**, maître de conférences en *Digital Humanities* à Télécom Paristech (Institut Mines-Télécom) ; animée par Claire Levallois-Barth.

Ateliers organisés par la Chaire en lien avec la thématique des identités numériques (évènements internes réservés aux partenaires)

27 mars 2014 • **Identités multiples**

Animé par Armen Khatchatourov, cet atelier a porté sur l'analyse comparative des pays européens qui ont implémenté des dispositifs de l'identité numérique à l'échelle nationale, avec une attention particulière aux questions de la protection des données personnelles, de la gestion des identités multiples et d'un éventuel usage professionnel des dispositifs en question.

8 décembre 2014 • **Approche critique des identités numériques : usages, technologies et aspects réglementaires**

Armen Khatchatourov a présenté l'évaluation critique des usages des systèmes de gestion des identités numériques dans les pays européens, ainsi qu'une analyse critique du règlement eIDAS du point de vue des flux des données personnelles, aujourd'hui et dans le futur proche en lien avec les évolutions techniques en cours. Claire Levallois-Barth a analysé le contenu du règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (eIDAS). Enfin, Didier Chaudun, vice-président de l'Alliance pour la confiance numérique (ACN), a exposé les réflexions menées à l'ACN sur les identités numériques.

18 juin 2015 • **Les métamorphoses de l'identité à l'ère numérique : enjeux éthiques et sociophilosophiques**

Animé par Pierre-Antoine Chardel et Armen Khatchatourov, cet atelier a déployé l'approche philosophique des identités numériques. Cet atelier a évalué à la fois les origines historiques et les conséquences sociétales des politiques aujourd'hui à l'œuvre dans le domaine des identités numériques. Il a proposé des outils conceptuels originaux pour la compréhension des mutations contemporaines.

Contributeurs

Claire Levallois-Barth, maître de conférences en droit à Télécom ParisTech, coordinatrice de la Chaire. Elle s'intéresse à l'évolution de la protection des libertés et droits fondamentaux à l'ère numérique. Elle se concentre en particulier sur la question de la protection des données personnelles, notamment dans le contexte du *big data*, ainsi que sur la gestion des identités numériques.

Pierre-Antoine Chardel, professeur de philosophie sociale et d'éthique à Télécom École de Management, cofondateur de la Chaire. Responsable de l'équipe de recherche « Ethique, Technologies, Organisations, Société » (ETOS) de Télécom École de Management, il s'intéresse aux relations intersubjectives et aux pratiques sociales dans la société technologique, et à l'émergence de sens dans la métamorphose numérique.

Maryline Laurent, professeur en sciences de l'informatique à Télécom SudParis, cofondatrice de la Chaire, est responsable de l'équipe R3S (Réseaux, Systèmes, Services, Sécurité) du laboratoire UMR 5157 SAMOVAR. Elle s'intéresse aux problématiques de sécurité et de vie privée dans les environnements de *cloud*, de systèmes miniaturisés et à la gestion des identités numériques.

Patrick Waelbroeck, professeur en sciences économiques à Télécom ParisTech, cofondateur de la Chaire. Ses travaux portent sur l'économie de l'innovation, l'économie de la propriété intellectuelle, l'économie de l'internet et des données personnelles. Il enseigne l'économie de l'internet et des données.

Armen Khatchatourov, ingénieur de recherche à Télécom École de Management et docteur en philosophie de la technique. En articulant l'approche théorique et l'ingénierie, il s'intéresse à la manière dont les technologies numériques affectent notre sentiment de soi et aux conséquences sociétales de ces technologies.

Delphine Chauvet, post-doctorante en droit à Télécom ParisTech, a soutenu sa thèse sur « La vie privée. Étude de droit privé » à l'Université Paris-Sud et est chargée d'enseignement à l'Université Paris 2 Panthéon-Assas.

Nesrine Kaâniche, post-doctorante en sciences informatiques à Télécom SudParis, a soutenu sa thèse sur « La sécurité des données stockées dans environnement *Cloud*, basée sur des mécanismes cryptographiques ». Elle s'intéresse à la cryptographie au service de la protection de la vie privée.

Avec la participation de **Stéphane Menegaldo**, chargé de communication.

Le numérique permet à l'individu, en fonction des contextes dans lesquels il évolue, de choisir la manière dont il entend se présenter aux autres et de nouer des relations, par exemple en tant que « père », « fan de musique » ou « demandeur d'emploi ». Cependant, un mouvement inverse consiste à ramener les multiples pratiques d'une personne qui se présente sous différentes identités à une identité unique. Il s'observe à la fois dans les secteurs privés et publics.

Ce Cahier examine donc la manière dont la France et les pays de l'Union européenne entendent mettre en place des systèmes de gestion des identités à l'échelle de la société. Il s'agit ici notamment d'améliorer la sécurité des moyens d'identification utilisés par les citoyens et de simplifier leurs démarches administratives. Dans le même temps, ce mouvement renforce la transparence des différentes facettes de l'individu et augmente les risques de surveillance.

Quels sont les effets de cette tendance à l'unification des identités à la fois du point de vue philosophique, éthique, juridique, économique et informatique ? Cette unification est-elle souhaitable ? Dans quels cas ? Comment les États et les entreprises entendent-ils nous identifier ? Comment s'assurer que la personne dispose de la marge de manœuvre nécessaire pour se présenter et nouer des relations avec autrui de façon autonome ? Le pseudonymat constitue-t-il une réponse appropriée ?

Conçu comme un outil d'accompagnement, ce Cahier s'adresse à la fois aux citoyens, aux entreprises et aux pouvoirs publics.

Les partenaires de la Chaire Valeurs et Politiques des Informations Personnelles

Mécènes fondateurs

GROUPE Imprimerie Nationale

BNP PARIBAS

orange™

LVMH

Mécènes associés

DASSAULT SYSTEMES

DEVERYWARE
TRUSTED LOCATION-BASED SOLUTIONS

Partenaire qualifié

CNIL
Commission Nationale de l'Informatique et des Libertés

Maquette : *implica CR&A* - Mars 2016