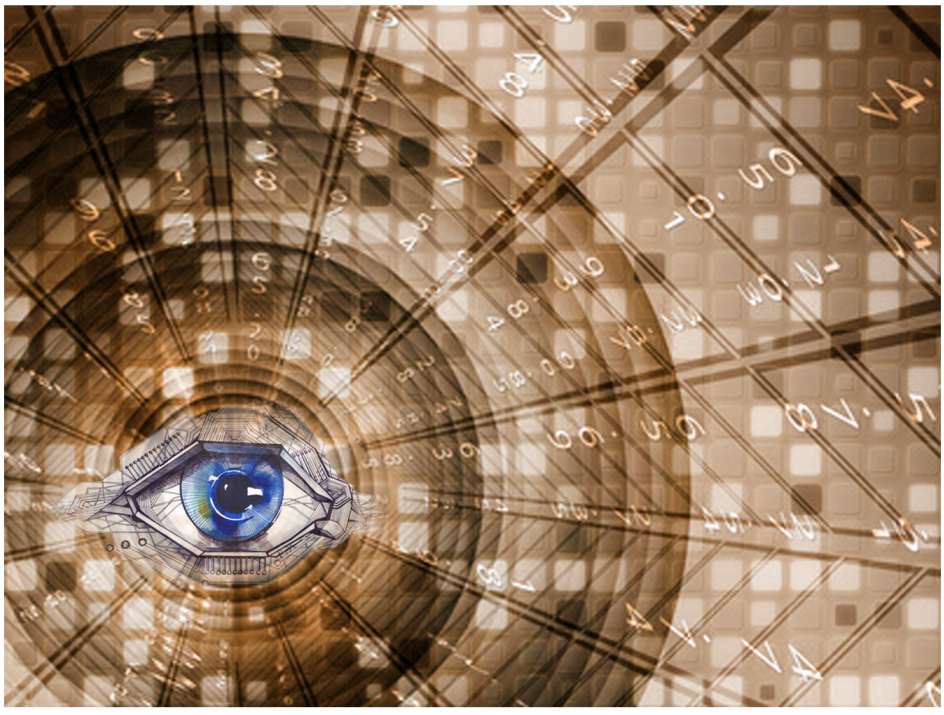
INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

INHESJ

TRAVAUX DES AUDITEURS

Cycle « Sécurité des usages numériques »
Travaux de la 5e promotion (2014-2015)

COMMENT GÉRER L'IDENTITÉ NUMÉRIQUE



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
INHESJ
INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

en partenariat avec le
cigref Réseau de Grandes Entreprises

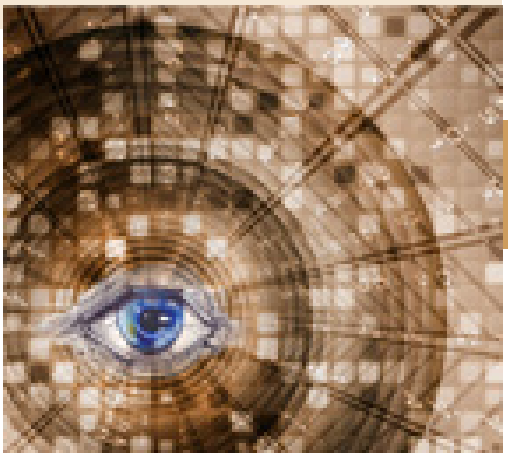
DÉCEMBRE 2015
ISSN 2265-447X

Les auteurs

- Laurent CERISOLA
- Patrick D'HESMIVY D'AURIBEAU
- Arnaud GODET
- Lamia SAOUDI
- Didier TCHENQUELA

Sommaire

Comment gérer l'identité numérique



INTRODUCTION

L'explosion des sources numériques, avec l'avènement de la micro-informatique et d'Internet, a complètement transformé l'univers de la communication ainsi que nos modes de vie. Cette transformation s'est accélérée durant les 10 dernières années, au point d'amener le législateur à revoir des articles du code napoléonien pour y intégrer la signature numérique. Comme pour la signature numérique, l'intégration de l'identité numérique nous force à nous interroger sur les fondements et la nature de l'identité, afin de créer le lien entre le monde virtuel et le monde réel.

En France, Internet est un média deux fois plus influent que la télévision[1] et les actions qui y sont effectuées peuvent désormais influencer et avoir des répercutions dans le monde réel. Tout comme dans le passé, les Etats ont permis le développement des échanges en garantissant l'identité des personnes. De nouveaux modèles devront être trouvés afin de permettre de continuer le développement de la sphère numérique.

Bien que fortement engagée dans la transformation digitale, la France a pris un peu de retard dans le déploiement d'une solution de gestion des identités numériques. Ce retard devrait être comblé avec la mise en œuvre du programme « France Connect » qui devrait se développer fin 2015.

Dans le cadre de ce mémoire, les aspects juridiques, techniques, ainsi que les risques associés à l'identité numérique seront abordés. En effet **l'identité numérique expose les citoyens aux mêmes risques de vol et d'usurpation que pour des biens matériels**, d'autant que la plupart des systèmes actuels d'authentification repose sur des concepts datant du début des années 70. Concepts qui ont depuis démontré leurs faiblesses structurelles et sont de plus en plus faciles à casser selon le principe de la loi de Moore, qui veut que la vitesse des micro-ordinateurs double tous les 18 mois.

[1] Source - Fleishman-Hillard, juin 2010

DÉFINITIONS

L'identité numérique est l'ensemble des informations et des données se rapportant spécifiquement à un internaute. C'est l'image que l'on peut se faire d'une personne, d'un groupe, d'une organisation, ou d'une entité à partir de l'information numérisée qui existe à son sujet. Aujourd'hui chaque utilisateur possède une identité numérique au même titre qu'un état civil.

L'identité web est une sous-section de l'identité numérique. Lorsque nous parlons d'identité numérique, nous parlons en fait de deux choses distinctes :

- l'une d'ordre administratif ;
- l'autre de l'ordre de la personnalité.

Ces deux types d'identité peuvent être abordés soit séparément soit en lien l'une avec l'autre. Cependant, il faut garder à l'esprit qu'il s'agit de deux notions distinctes.

Le développement et l'évolution des moyens de communication, au travers notamment de la multiplication des blogs et des réseaux sociaux, changent le rapport de l'individu à autrui. Ainsi, l'identité numérique permet l'identification de l'individu en ligne et la mise en relation de celui-ci avec cet ensemble de communautés virtuelles qu'est Internet. Dès lors, l'identité numérique peut être divisée en trois catégories :

- **L'identité déclarative**, se réfère aux données saisies par l'utilisateur comme son nom, sa date de naissance, ou autres informations personnelles directement renseignées par l'individu ;
- **L'identité agissante**, est indirectement renseignée par les activités de l'utilisateur sur la toile ;
- **L'identité calculée**, résulte d'une analyse de l'identité agissante par le système, comme le nombre de communautés virtuelles dans lesquelles l'individu évolue ou son nombre d'amis sur les réseaux sociaux.

Identité numérique d'ordre administratif

L'identité numérique administrative est basée sur des informations comme l'adresse, le numéro de téléphone, le numéro d'assurance sociale, un numéro de compte bancaire ou de carte de crédit, et autres renseignements personnels. Elle peut aussi être basée sur des informations apparaissant dans des documents officiels (certificat de naissance, de mariage ou d'adoption, dossier de crédit, dossier criminel, titres de propriété, dossier médical, etc.)

Si cette information est généralement de type textuel ou numérique, elle peut aussi être d'ordre graphique (photographie, radiographie, empreinte digitale ou rétinienne), vidéo (surveillance) ou encore géomatique. Dans les cas énumérés jusqu'ici, elle est associée le plus souvent au nom légal de la personne, dans une relation non équivoque et avérée, qui ne donne pas lieu à l'interprétation.

Il est possible d'interpréter le contenu d'un dossier criminel ou médical. Cela dit, la nature du lien d'appartenance du dossier à la personne ne donne pas lieu à interprétation. Si le lien n'est pas véridique, c'est qu'il y a erreur, falsification ou fraude.

Ce type d'information réside généralement dans des banques de données qui ne sont pas nécessairement d'emblée disponibles via le Web. Cependant, la nature numérique des informations les rend plus vulnérables à des accès élargis, par des canaux administratifs ou criminels, et à une diffusion plus aisée.

D'autre part, les internautes peuvent choisir d'utiliser certaines de ces informations au fil de leurs activités sur le web. Il existe des informations de type administratif qui sont propres au Web, comme les adresses IP et autres informations nécessaires au fonctionnement même du web.

Enfin, il y a le couple « nom d'utilisateur » et « mot de passe » (ou numéro d'identification personnel) qui sert à accéder à des services sur le web. Il peut s'agir d'une institution bancaire, d'un service de courriel, d'un réseau de socialisation, d'une plateforme de jeu, d'un blogue, d'un forum, etc. Cette information peut être associée au nom légal de la personne ou à un pseudonyme.

Identité numérique de l'ordre de la personnalité

L'identité de l'ordre de la personnalité est basée sur de l'information qui révèle les goûts, les opinions, les attitudes, les valeurs, les activités et les relations d'une personne. Ces informations sont constituées de traces que l'internaute laisse sur le web au cours de ses activités en ligne. Ces traces peuvent être de divers ordres. Celles auxquelles on pense en premier sont les traces textuelles, photographiques, ou vidéo que les internautes produisent et mettent en ligne.

Ensuite, il y a les traces qui sont dérivées de l'appartenance de l'internaute à tel groupe, tel service, tel réseau. Un autre type de trace, de plus en plus mis en valeur, est celui des relations déclarées entre des individus. Le cas le plus connu est celui des « amis » sur des réseaux de socialisation tels Facebook. Il existe plusieurs autres cas qui permettent de déceler les relations sociales possibles d'un individu, comme le suivi des signets, des photographies, des vidéos, des « tweets » ou d'autres productions mises en ligne par un internaute.

Ces traces relatives à la personnalité peuvent être interprétées dans les limites d'un service particulier. On observera alors le comportement d'un individu à l'intérieur d'un réseau social. Elles peuvent être observées dans un contexte plus global en considérant l'ensemble des activités en ligne d'un internaute. La procédure type pour cela est de « googler » le nom d'une personne et d'examiner le contenu des résultats de recherche ainsi obtenus.

Il convient cependant de noter que :

- L'identité numérique d'ordre administratif soulève principalement la problématique de la confidentialité des renseignements personnels dépendant de la sécurité de l'information.
- L'identité numérique de l'ordre de la personnalité soulève des questions relatives aux impacts (degré et qualité) du dévoilement personnel souhaitable sur le web.

Il existe aussi la problématique du croisement entre les renseignements administratifs et les informations sur les personnes.

Lieux de l'identité numérique

L'identité numérique se trouve partout où l'on a un *login* et où l'on produit du contenu tel que :

- Les blogs (en tant qu'auteur ou commentateur) ;
- Les forums de discussion ;
- La présentation de soi sur un site de réseautage social ;
- La participation à un média social (par exemple, Wikipedia).

Différentes facettes de l'identité numérique

L'identité numérique est composée de nombreuses informations ou traces pouvant être regroupées en facettes :

- **Les coordonnées** (comment et où joindre la personne), regroupant les données numériques qui permettent de rentrer en contact avec un individu, de l'identifier et de le localiser comme : l'e-mail, le numéro de téléphone, l'adresse IP, les messageries instantanées, les fichiers FOAF et les hCard,
- **Les certificats** (qui atteste de l'identité de la personne) permettant d'authentifier un utilisateur de manière certaine, unique et sécurisée pour transmettre ou recevoir des informations numériques à travers, par exemple, des outils informatiques comme CardSpace, OpenID, ClaimID, Naimz, Thwate, Certinomis…
- **L'expression** (ce que dit la personne) prenant en compte tous les contenus mis en ligne à partir des logiciels, des plateformes, et des services reconnus comme outils de parole, les blogs, Wordpress, Blogging, Overblog,
- **Les avis** (ce qu'apprécie la personne) peuvent concerner un produit (Beaute-test, Ciao, Looneo, etc.), un service (Vacanceo), un site internet (Digg), ou même un contenu rédactionnel.

• **Les hobbies** (ce qui me passionne) se focalisant sur des thèmes divers comme la cuisine, l'automobile, les jeux en ligne, les animaux, etc. Il s'agit souvent des **communautés** de niche échangeant sur une passion partagée ;

• **La connaissance** (ce que sait la personne) qui est transmise à travers les encyclopédies communautaires (**Wikipédia**,) les foires aux questions collaboratives (Google answer), les tutoriels, les blogs spécialisés, etc. ;

• **Les avatars** (ce qui représente la personne) dans un univers virtuel comme dans les **jeux en ligne** (Second Life, World of Warcraft) ou encore dans les comptes numériques (Gravatar) ;

• **L'audience** (qui connait la personne) peut s'étendre à des groupes d'individus (Facebook, Myspace) et des sites de rencontre (Meetic) ;

• **La consommation** (ce qu'achète la personne) reflétant les achats réalisés, le moyen de paiement utilisé, les pages consultées, les produits les plus visités, la fréquence d'achat, la création de profils marchands, l'accumulation de points de fidélité, etc. ;

• **La réputation** (ce qui est dit sur la personne) englobant la notoriété et la fiabilité de l'individu ou de la personne morale sur Internet (Ebay). Des services se sont également spécialisés dans la gestion de la notoriété et de la réputation en ligne, comme Outspoken media ;

• **La profession** (ce que fait la personne) mise en avant à travers les réseaux sociaux professionnels tels que Viadeo ou LinkedIn ;

• **La publication** (ce que partage la personne) recense tous les contenus partagés par les utilisateurs tels que les vidéos (Dailymotion, Youtube, Google video), les photos (Instagram, Flickr), la musique (SoundCloud), les liens (Easylinkr), etc.

Formation de l'identité numérique

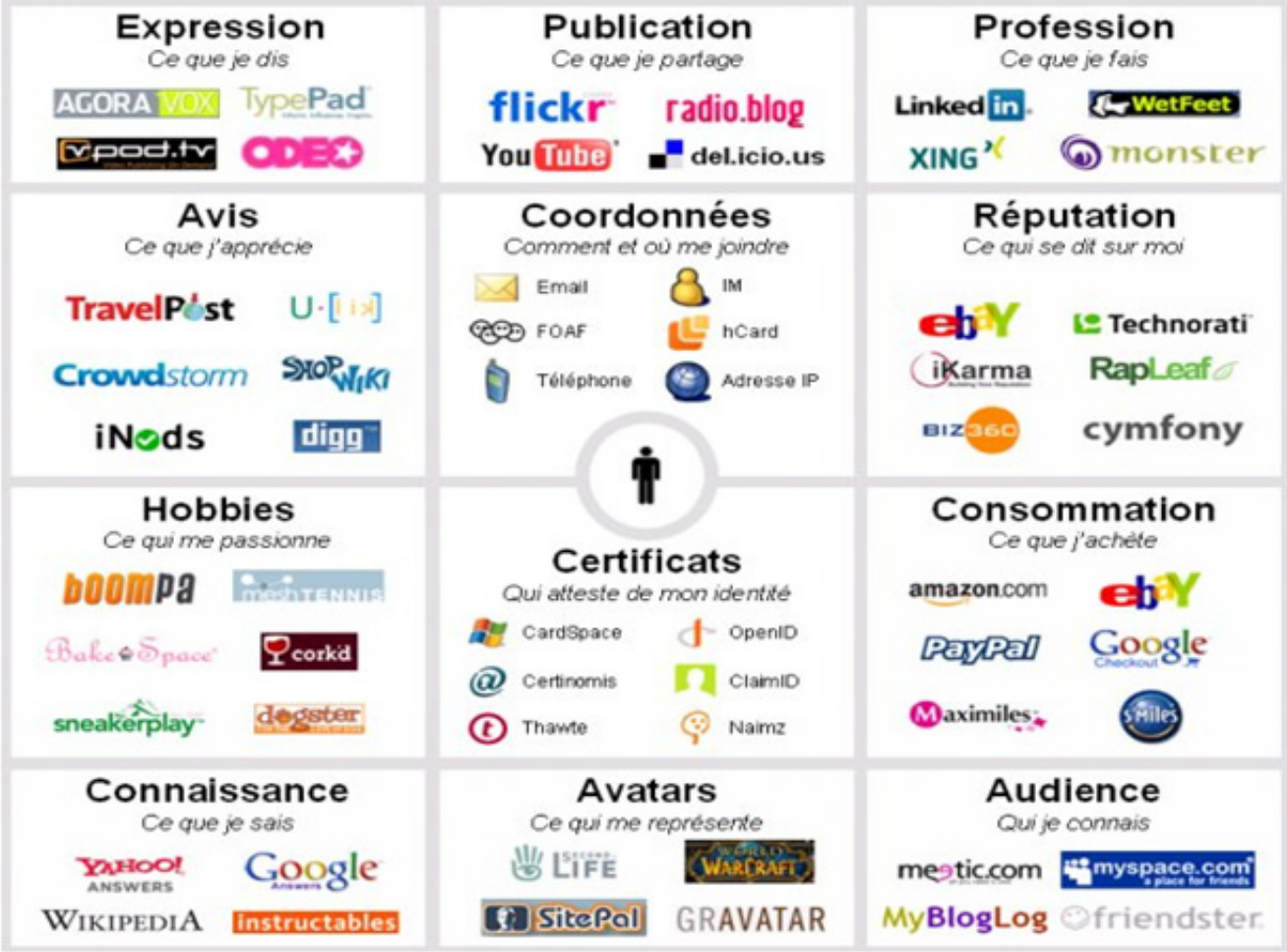
L'IP est une adresse électronique unique sur le réseau qui vous différencie des autres internautes. Cette adresse qui vous caractérise sur Internet est transmise par un serveur qui contient lui-même une information importante : sa géolocalisation. Ainsi, chaque IP donnée est marquée d'une signature géographique. Google s'en sert par exemple pour vous rediriger sur Google.fr.

Dès lors, qu'un réseau comporte des éléments uniques, il est possible de caractériser chacun de ces éléments par une identité propre.

Avec l'évolution du Web, cette identité a inclus davantage de propriétés :

- L'arrivée des forums et des systèmes d'authentification a poussé les utilisateurs à utiliser un pseudonyme ;
- La prolifération des blogs a offert la possibilité (en plus de la liberté d'expression sur le Web déjà possible avec les forums) de tenir un journal plus facilement accessible par les moteurs de recherches pour bénéficier d'une certaine popularité auprès de ses lecteurs ;
- Les plateformes de partage ont permis aux internautes de partager leurs passions par le multimédia (photos, vidéos, musiques) ;
- L'arrivée des réseaux sociaux a parachevé la formation de l'identité numérique en donnant la possibilité de dévoiler entièrement son identité réelle sur le Web ;
- Aujourd'hui, en utilisant les différents services du Web, nous laissons des traces qui peuvent avoir un impact important dans la vie réelle. Ces services, souvent accessibles uniquement sur le Net, sont le reflet de sphères personnelles. Elles poussent les internautes à s'attribuer un mérite par la consommation, dans le but de se prouver son « existence numérique ». Mais cette consommation n'est pas forcement en rapport direct avec un produit ou un service. Elle fait référence à une société d'information.

Vision globale des différentes sphères d'activité d'un internaute



Source : Fred Cavazza, 22 octobre 2006

Les différents outils et services utilisés pour récolter et partager de l'information laissent à leur tour des traces numériques renseignant sur son auteur et même sur son réseau personnel. Les applications Facebook visent à transformer les membres en « ficheurs » en leur proposant de critiquer leurs amis ou de donner des informations privées. Ce type d'application crée une situation inquiétante car certaines données confidentielles peuvent être diffusées par des tiers.

Identifiants numériques

Les identifiants numériques se définissent comme autant de signes caractérisant un individu. Ils sont à la base de la construction de l'identité numérique. Ces identifiants numériques sont le pseudonyme (pseudo), l'e-mail, le nom de domaine Internet, l'URL et l'adresse IP.

■ *Identifiants numériques*

Le mot pseudonyme est fondé sur le radical pseudês (en grec) signifiant menteur. C'est donc au sens littéral, un faux nom. Avec le temps, il a pris le sens de nom d'emprunt. C'est l'individu qui se l'attribue pour l'exercice d'une activité particulière ou pour des raisons fantaisistes. De nombreuses personnalités ont eu, et ont toujours, recours au pseudo. Ainsi, Chaban était le pseudo du résistant Jacques DELMAS pendant la Seconde Guerre Mondiale. Il décida de le conserver et de l'ajouter à son nom pour devenir Jacques CHABAN-DELMAS.

Sur le Web, le recours au pseudo est quasiment obligatoire pour accéder à un grand nombre de services. Identité jetable, elle ne permet pas une complète identification de l'individu, à la différence du nom et du prénom.

Légalement, le pseudo ne doit pas contenir de caractères racistes ou diffamatoires. Il peut être déposé en tant que marque, ce qui signifie que personne n'a le droit d'utiliser un pseudo déposé, excepté la marque dépositaire.

■ *L'e-mail*

Service le plus populaire d'Internet, l'e-mail se divise en deux parties. La partie précédant l'arrobase (@) sert généralement à identifier l'émetteur, alors que la partie le suivant correspond au nom de domaine Internet. Il est associé à un espace de stockage, la boîte de messagerie. Cette dernière contient à-peu-près tous les échanges de l'individu depuis la création de son e-mail. Elle contient aussi bon nombre d'identifiants et mots de passe des sites auxquels il s'est inscrit. On peut comparer l'e-mail à un condensé d'identifiants numériques, c'est donc une mine d'or pour les hackers...

■ *L'adresse IP*

L'adresse IP est plus un identifiant subi qu'une identité numérique. Nous ne détaillerons donc ni sa composante, ni sa fonction, même si celle-ci permet aux spécialistes de masquer ou transformer leur véritable adresse par un jeu de truquage.

■ *Le Système d'identité numérique*

Le « système état civil » regroupe toutes les informations d'un individu (nom, prénom, lieu et date de naissance). Cette carte d'identité donne des droits et des autorisations. Sur Internet, il n'existe pas de tel système global. Chaque service a son propre système d'identité.

Il existe différents services d'authentification comme le projet baptisé OpenID, issu du monde du logiciel libre. Il permet de se connecter avec une seule identité à une multitude de services. C'est un système d'identité décentralisé qui évite à l'individu de créer à chaque fois de nouveaux comptes sur différents services. Toutes les informations de l'individu seraient ainsi regroupées sur une URL du fournisseur d'identité. L'utilisateur doit ensuite fournir cette URL aux services auxquels il souhaite s'inscrire.

L'OpenID regroupe :

- Les identifiants numériques ;
- Un registre en ligne ;
- Une carte d'identité réseau ;
- Des droits et des devoirs numériques.

Données formelles et données informelles

Deux sortes d'informations caractérisent l'empreinte numérique : les données formelles et les données informelles.

- Les données formelles donnent les informations innées et durables d'une personne, comme le nom, le prénom, et tous les identifiants numériques… Elles permettent de classer une personne dans un échantillon (IP, Géolocalisation, tranches d'âges) mais n'offre qu'une liberté limitée de traitement.

- Les données informelles, quant à elles, regroupent les informations générées par l'action d'une personne. Par exemple les commentaires sur un blog, le nombre de posts sur un forum, les inscriptions sur les réseaux sociaux… Elles nécessitent d'être traitées, mais sont difficilement « regroupables » entre plusieurs individus. Elles définissent une personne par son comportement sur le Web et sont facilement accessibles par les moteurs de recherches.

- **Ces deux types de données forment une architecture de données semblable à l'ADN du corps humain. Mais, contrairement à ce dernier, elles peuvent être visibles de tous. En outre, ces données peuvent être transmises pas un tiers et non par l'intéressé : on parle alors de réputation numérique ou d'e-réputation.**

IDENTITÉS NUMÉRIQUES ÉTATIQUES

Historique
(le besoin de fourniture d'identité)

Il est nécessaire, avant de regarder la manière dont l'Etat et d'autres pays ont traité le sujet de l'identité numérique, de rappeler brièvement quelques éléments historiques :

L'identification des personnes est restée pendant longtemps essentiellement basée sur la nécessité de reconnaitre un individu, vivant pour l'essentiel dans une ou plusieurs communautés.

156 ans avant J.C. un individu pouvait être identifié de la façon suivante :

« Environ 30 ans, de taille moyenne, imberbe, les mollets fermes, une fossette au menton, un grain de beauté sur la joue droite, une cicatrice au coin gauche de la bouche ».

Au **XVe siècle, en 1462, on** voit la naissance des documents d'identité par un décret de Louis XI, stipulant que tous les messagers royaux devaient être en possession de papiers d'identité.

Les pèlerins et les compagnons en apprentissage obtiennent alors des sauf-conduits et les vétérans ne sont plus confondus avec les déserteurs. Les indigents, qui ont le droit de demander l'aumône, se voient attribuer des lettres de mendicité pour les distinguer des autres mendiants. Dès ses origines, l'histoire de l'identification est une histoire de privilèges, de libertés et d'entraves. Avec l'avènement de ces documents, les faussaires vont bien évidemment prospérer.

En 1528, le livre des vagabonds fustige ceux qui reproduisent toutes sortes d'actes, signatures ou sceaux, notamment les passeports, certificats de résidence ou lettres de mendicité.

Aux débuts des papiers d'identité, les faussaires n'étaient pas inquiéts d'être accusés de falsification, car ce n'était pas le titulaire d'un document qui était identifié, mais celui qui le délivrait, par un procédé d'identification ancestral : le sceau. Difficile, dans ces conditions, de dire si celui qui présentait un document d'identité en était le détenteur légitime.

En 1938, en Allemagne, le gouvernement national-socialiste impose le port d'une carte d'identification. Deux catégories de la population doivent, sous peine de sanction, être en possession d'un document d'identité avec photo : les hommes de plus de dix-huit ans, et les Juifs. Sur les papiers de ces derniers, un « J » est rajouté en évidence.

L'identification obligatoire qui découle de la bureaucratie ouvre la voie aux futures discriminations et exactions dont les Juifs Allemands seront les victimes.

Après la guerre, cette loi a été amputée de tous ces éléments discriminatoires. **En 1951**, elle est entrée dans les livres de loi de la jeune République fédérale allemande sous le nom de « loi fédérale sur les papiers d'identité ». Au XXIe siècle encore, alors que les pays où l'obligation d'identification est en vigueur sont rares, les citoyens allemands étaient tenus, en vertu de cette loi, d'être en possession de documents pour pouvoir décliner à tout moment leur identité.

Les premiers dispositifs de recensement de la population et d'Etat civil sont liés aux besoins des Etats en matière de mobilisation de troupes militaires, puis de fiscalité, de police et de justice.

Les premiers papiers d'identité apparaissent avec l'évolution des sociétés : le développement des transports et de l'urbanisation, la poussée de l'individualisme, rendent nécessaire de disposer d'un moyen d'identifier les individus sans s'appuyer sur une tierce personne.

En 1921, apparition de la première carte d'identité française, facultative, avec pour but de simplifier les procédures administratives. Uniformisation des dispositifs d'identification délivrés par différents services et départements, suppression du témoignage d'un tiers pour valider les principales démarches.

L'usage de documents d'identité délivrés par l'Etat s'est développé progressivement au-delà des seules relations entre le détenteur et l'administration, lorsque le titulaire doit justifier de son identité dans la vie courante.

En France, contrairement aux idées reçues, la carte nationale d'identité n'est pas obligatoire et chaque Français est libre d'en posséder ou pas. L'article 78-2 du code de procédure pénale permet de justifier de son identité auprès de la police « par tous moyens ». Cela signifie que le témoignage, ou encore un titre de réduction SNCF avec photographie, sont considérés comme des justificatifs acceptables auprès de la police. Mais voyons de plus près de quoi se compose notre carte d'identité.

Aujourd'hui, la carte nationale d'identité et le passeport comportent un composant électronique sécurisé qui inclut :

- Le nom de famille, le ou les prénoms, le sexe, la date et le lieu de naissance du demandeur ;
- Le nom dont l'usage est autorisé par la loi, si l'intéressé en a fait la demande ;
- Le domicile ;
- La taille et la couleur des yeux ;
- Les empreintes digitales ;
- La photographie.

La problématique de la mise en place de l'Identité Numérique en France date de 1974 avec le projet SAFARI, dans lequel chaque citoyen devait être identifié selon un numéro. Le but était d'interconnecter tous les fichiers de l'administration. Ce projet a suscité de vives inquiétudes sur le respect des libertés individuelles et la crainte d'un fichage générale de la population.

A contrario, la loi du 6 janvier 1978 a institué la Commission Nationale de l'Informatique et des Libertés (CNIL) qui prévoit que les données de santé, préférence sexuelle, origines raciales ou ethniques, opinions politiques, philosophiques ou religieuse, et l'appartenance syndicale, sont des données sensibles au sens de la loi (article 8) et font l'objet d'une protection renforcée.

Aujourd'hui, tous les pays de l'Union européenne sont dotés d'une loi Informatique et Libertés et d'une autorité de protection, ce qui, en théorie, pourrait prémunir chaque citoyen d'un état membre de voir son identité recensée sur des listes.

Cependant, l'histoire et les problématiques de réglementation juridique, mais surtout les enjeux de sécurité des Etats et de l'individu, ne pourront empêcher d'apporter une réponse aux besoins imposés par la révolution technologique. Ces éléments doivent attirer notre attention sur les points suivants :

Les besoins originels pour l'Etat de disposer d'une garantie de l'identité d'un individu sont de plus en plus nécessaires, et ce dès la naissance. Données administratives, données médicales ou bancaires, scolarité et examens divers, police, justice, fiscalité, recensement militaire, mais aussi les activités professionnelles telles que le commerce sont assujetties à justification d'une identité, notamment pour les déplacements et les échanges à l'international.

La diversité et le nombre des différents organismes ci-dessus imposent déjà l'emploi de deux à trois moyens de justification de son identité.

- Code PIN de la carte de paiement et du téléphone mobile,
- Digicode d'entrée d'immeuble ou d'alarme ;
- Identifiants et mots de passe de PC, tablettes ;
- Identifiants et mots de passe généralisés dans l'ensemble des services de santé et administrations de l'Etat qui ne communiquent pas entre eux ;
- Applications informatiques et services en tous genres ;
- Sollicitation à créer un compte Facebook pour accéder à un service.

Un internaute français dispose en moyenne de douze comptes numériques distincts sur internet, dont deux adresses de messagerie électronique, deux comptes de réseaux sociaux et quatre comptes sur des sites e-commerce. Autant de moyens pour justifier que vous êtres VOUS et non pas un autre. La difficulté de mémoriser tous ces codes est très grande et conduit l'usager à ne pas les diversifier suffisamment, à les noter sur des supports non sécurisés, comme les Post-It ou encore à les mutualiser entre différentes applications. Par ailleurs, le mot de passe n'a rien de très convivial et sa multiplicité, sa complexité à le préserver et surtout le mémoriser, nous oblige souvent à nous exposer au risque de perte ou de vol. Récemment, lors du piratage de la plateforme informatique de TV5 Monde, nous avons vu qu'un grand nombre de personnes affichent sans crainte sur un Post-It leur mot de passe, même si ce n'est pas cette erreur qui a été pas à l'origine du piratage.

Le souci est donc de préserver ses données personnelles que ce soit au sein de différents Blogs, Wiki, réseaux sociaux... L'évolution de la société et de la technologie numérique, notamment au travers de l'internet, a généré de nouvelles façons de travailler et de jouer, d'effectuer des transactions et d'interagir. Nous sommes entourés d'identités et de données numériques qui doivent être échangées, via des réseaux, par des organisations, des personnes et des objets. Tous ces éléments témoignent aujourd'hui de nos faits et gestes, de nos désirs, de tous les éléments qui nous sont propres et personnels et qui prouvent qui nous sommes vis-à-vis d'une administration, d'une entreprise ou d'un particulier.

La vision de l'identité évolue en fonction de la société. Le déplacement de nombreuses relations entre individus, Etats, entreprises, vers le monde numérique constitue un bouleversement important. Cela impose de se pencher sur la transposition du « papier d'identité », de la multiplicité et de la complexité des moyens d'authentification dans un nouveau contexte numérique.

Les fraudes et abus en tous genres constatés sur la toile, la multitude d'informations, et la nécessité de protéger les données personnelles, impose aux Etats de réfléchir à la manière de mieux gérer l'identité numérique.

La lourdeur mais aussi le coût des processus administratifs doivent être simplifiés, avec pour unique souci de garantir l'identité des individus.

Identité numérique française

■ *Carte Vitale*

La première carte d'identité numérique est la carte vitale.

En France, toute personne est identifiée dès sa naissance par son **numéro d'inscription au répertoire national d'identification des personnes physiques** (NIR). Le NIR, communément dénommé « numéro INSEE » (numéro de sécurité sociale), se compose de 15 chiffres. Il est considéré comme très complet, car il indique le sexe, l'année et le mois de naissance, ainsi que le code chiffré de la commune de naissance et le numéro d'ordre sur le registre des actes de naissance.

Fiable, pratique et sûre, la carte vitale, dont la première version date de 1988, est aujourd'hui présentée à tous les professionnels de santé. Progressivement remplacée par la carte vitale 2 elle a su se substituer à la feuille de soins et a évolué pour contenir plus d'informations. Un système d'opposition électronique a été mis en place pour que les logiciels des officines de pharmacie gèrent une liste nationale et inter-régimes des cartes Vitale en opposition.

Tous ces éléments ne préfigurent pas de la personnalité du titulaire où de ce qu'il est. Par ailleurs, ces données peuvent faire l'objet d'usurpation, être recensées sur des listes à des fins discriminatoire et entraver les libertés de chaque individu.

■ *INES*

En 2005, la France s'est engagée dans un projet de mise en place d'une carte d'Identité Nationale Electronique Sécurisée (INES) contenant des données biométriques (empreintes digitales, photographie, iris de l'œil…) pour vérifier l'identité des demandeurs de titre. Ce projet a lancé un grand débat autour de la question de l'identité biométrique. L'INES aussi baptisé Inept, Nocif, Effrayant et Scélérat par un collectif de plusieurs membres et intervenants extérieurs(11) car il était selon eux susceptible de recenser un individu, de collecter et de stocker ses empreintes dans une finalité de police judiciaire.

Soumis par le ministère de l'intérieur à un débat public, il a permis de dégager un certain nombre de possibilités d'améliorations. Suite au changement de gouvernement, le projet INES a été remplacé par le projet de « **protection de l'identité** » reprenant les contributions issues du débat public.

Ce nouveau projet se décompose ainsi :

1) Un passeport à puce conforme à la réglementation européenne ;

2) Une carte d'identité électronique, proche de celle déjà utilisée en Belgique (6 millions de cartes déjà émises en 2007), Estonie 1 million, Espagne 32 millions en décembre 2012), en Italie et en Suède plusieurs millions chacune, Finlande 150 000. Comme la carte d'identité actuelle, la nouvelle sera facultative ;

3) Un système de gestion commun, utilisant la biométrie pour vérifier l'identité des demandeurs de titres.

La future carte devrait contenir une radio-étiquette contenant l'identité du porteur, et des données biométriques (photo et empreintes digitales), à l'exclusion de toute autre donnée personnelle telle que le numéro de sécurité sociale. Il est prévu que la consultation des données d'identité par les agents de contrôle se fasse sans contact, mais nécessite un code secret, interdisant des contrôles à l'insu du porteur.

La carte devait comporter également en option des clefs électroniques permettant de remplacer les mots de passe sur le web (pour lutter contre le phishing) et de générer une signature numérique.

L'intérêt majeur de cette carte INES est la lutte contre la fraude documentaire ainsi que la possibilité de l'utiliser dans des télé-procédures administratives ou des transactions commerciales.

Deux initiatives rivales semblent se dégager en faveur d'une signature numérique sécurisée :

- IDENUM ;
- La carte d'identité biométrique.

■ *IDENUM*

Le Ministère de l'Industrie et de l'Économie numérique relance un autre dispositif baptisé **IDNum**, supporté par une mini-clé USB ou par la puce d'un mobile, capable d'identifier automatiquement l'utilisateur sur les sites partenaires d'IDNum. Moyennant la confirmation d'un mot de passe, l'identité de l'internaute est immédiatement vérifiée. Ce projet est cependant toujours en attente de la publication de l'étude de préfiguration d'un consortium IDNum lancé en 2010 par Eric Besson Ministre chargé de l'Industrie, de l'Energie et de l'Economie numérique.

Lancé en février 2010, le projet IDNum visait à labelliser des dispositifs d'authentification existants ou à venir (clef USB, carte, certificat, mobile…) proposant un haut niveau de sécurité et reconnus par un large spectre de services en ligne : banques, sites e-commerces, télé services administratifs… Cet identifiant unique devrait faciliter la vie des internautes, qui aujourd'hui gérent en moyenne plus d'une douzaine de login/mots de passe, tout en garantissant un haut niveau de protection de leurs données personnelles.

Le projet, censé déboucher sur des offres fin 2010, a cependant pris du retard et pour le moment, IDNum est avant tout un consortium composé de La Poste, France Télécom, Orange, SFR et de la Fédération française bancaire. Il est vrai que la question centrale, celle du modèle économique (qui paie pour un service estimé à 12 euros par an et par internaute) n'est toujours pas tranchée. C'est du reste pour cela qu'Eric Besson vient de lancer une étude « de préfiguration », confiée au cabinet McKinsey et pilotée par la Caisse des dépôts et consignations, qui doit rendre ses conclusions « sous trois mois et son rapport final à l'automne » afin de « préconiser un modèle économique pour un déploiement à grande échelle ».

Cette étude devra aussi positionner ce projet par rapport aux services gratuits, très simples d'utilisation mais peu sécurisés, proposés par des sites comme Facebook (Facebook connect) évoqué plus loin dans ce document (partie état d'avancement du projet) par rapport à la carte nationale d'identité électronique. Même si officiellement le Gouvernement parle de « complémentarité » on rappellera que la CNIE(6) va proposer des fonctionnalités de signature et d'authentification qui seront gratuites. Pour le moment, la proposition de loi du sénateur Lecerf, qui a pour objectif de garantir une fiabilité maximale aux passeports et aux cartes nationales d'identité a été adoptée par le sénat début juin 2011 mais le parcours législatif est loin d'être terminé. La question est de savoir si les industriels iront plus vite que les parlementaires.

Depuis l'annonce de cette initiative, ce projet rassemble plus de 70 partenaires potentiels aux profils variés : émetteurs de certificats (établissements bancaires, opérateurs de télécommunications), sites de service en ligne accepteurs (commerces en ligne, assureurs, réseaux sociaux professionnels), fournisseurs industriels de solutions (logicielles ou matérielles). Les quatre partenaires présents sont aujourd'hui prêts à proposer, avec l'aide de l'Etat, des offres commerciales dans les prochains mois.

C'est donc un projet complémentaire avec la carte nationale d'identité électronique.

Concernant l'e-administration, le ministre indique que ce projet pourrait toucher l'accès aux fiches d'état-civil, aux extraits d'actes judiciaires, à la récupération de son acte de naissance, ou encore à l'inscription en université ou à un concours. Il pourrait également concerner l'accès aux espaces notariaux dématérialisés ou aux greffes des tribunaux, le dossier médical personnel, la dématérialisation du circuit des crédits à la consommation, ou l'accès simplifié à un coffre-fort électronique.

Le ministère a tenu à préciser que « le projet IDNum est parfaitement complémentaire avec la carte nationale d'identité électronique dont le projet de texte est en lecture au Sénat ». Alors que la CNIE ne devrait être disponible que sous la forme de carte à puce, IDNum permettra de proposer des identités numériques pour des supports complémentaires : clés USB, cartes SIM, téléphones mobiles…

Autre point important, l'utilisation des moyens IDNum restera, comme pour la CNIE, « dans tous les cas totalement volontaire » et « à l'entière discrétion des utilisateurs ». Chaque internaute pourra posséder « plusieurs identités numériques IDNum s'il le souhaite, conformément à l'avis de la Commission Nationale Informatique et Libertés (CNIL) ».

■ *Carte d'identité biométrique*

Le dispositif mettant en place la nouvelle carte d'identité numérique a été publié au journal officiel en mars 2012. Il s'agit de l'adoption par le sénat d'un projet de loi sur la carte d'identité biométrique devant proposer ce service : le titulaire de la carte peut installer sur celle-ci une deuxième puce, support de sa signature numérique, pouvant jouer le rôle d'authentificateur sur les sites administratifs, puis à terme, sur les sites de commerce électronique.

Cette loi précise que la carte d'identité biométrique, mais aussi le passeport des citoyens français, devront comporter plusieurs éléments tels que :

- Le nom de famille, le ou les prénoms, le sexe, la date et le lieu de naissance ;
- Le nom dont l'usage est autorisé par la loi, si l'intéressé en a fait la demande ;
- Le domicile ;
- La taille et la couleur des yeux ;
- Les empreintes digitales ;
- La photographie.

Suite aux navettes parlementaires et à la saisine du Conseil constitutionnel, la Loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité a considérablement réduit les services offerts par ce document d'identité en matière numérique. Les sages ont en effet estimé que la constitution d'un fichier utilisant ces informations n'était pas conforme à la Constitution.

France Connect

La France est devenue en 2014 la première nation Européenne en matière d'administration numérique. Elle entend accélérer sa transformation pour simplifier encore davantage les démarches des particuliers et des entreprises, grâce à Internet, et rendre les services publics plus efficaces et plus réactifs.

Désignée en 2014 par l'Organisation des Nations Unies comme la nation la plus avancée en Europe, et la quatrième dans le monde pour l'administration numérique, la France s'inscrit comme un acteur incontournable dans le domaine. En 2013, le site Légifrance a reçu près de 100 millions de visites et le site service-public.fr plus de 200 millions. Alors que désormais, plus de la moitié de nos concitoyens paient leurs impôts de façon dématérialisée, que 93% effectuent leur demande d'extrait de casier judiciaire en ligne et que 86% des agriculteurs effectuent des demandes d'aide au titre de la Politique agricole commune (PAC) via internet, le Gouvernement, estimant que la grande majorité des français dispose aujourd'hui d'une connexion internet, amplifie considérablement son action et entend imposer la déclaration et le paiement des impôts via internet. Ceci nous montre l'intérêt porté par les citoyens français au besoin de simplification des procédures administratives dans le monde du numérique.

Le 17 septembre 2014, Thierry Mandon a présenté en conseil des ministres le projet du Gouvernement pour faire du numérique l'instrument de la transformation de l'Etat. Ces dernier mois, le Gouvernement a entrepris d'alléger, via le numérique, les charges administratives pesant sur les entreprises, notamment avec l'expérimentation du Marché Public Simplifié (MPS), qui propose aujourd'hui à des entreprises de répondre à certains marchés publics en ne fournissant qu'un numéro de Siret pour s'identifier. Celà sera généralisé au début de l'année prochaine.

L'Etat engage aussi une nouvelle étape de sa stratégie numérique. Le Gouvernement va investir dans la qualité des infrastructures de son système d'information, dans le cadre du système d'information unifié de l'Etat, placé auprès du Premier ministre au cours de l'été.

Début 2015, les choses s'officialisent en matière d'administration en ligne au travers de l'annonce dans les médias de **France Connect**, qui est un système d'identification potentiellement reconnu par toutes les administrations française offrant des services en ligne.

L'objectif du projet encore en développement est ambitieux : créer un système numérique d'identification et d'authentification des citoyens utilisable par plusieurs administrations.

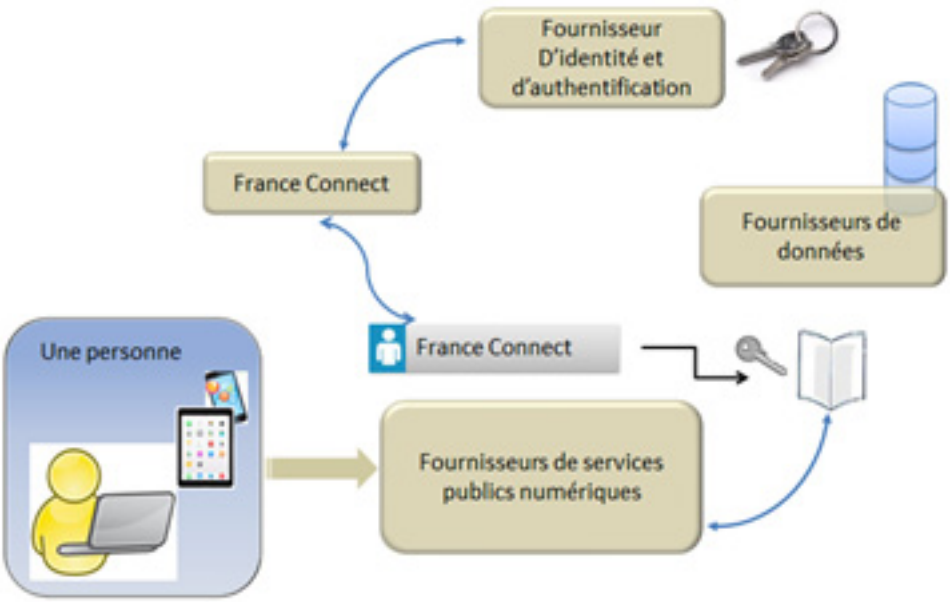
Basé sur un fonctionnement à la manière de Facebook Connect, il permet de s'identifier sur un site partenaire après s'être enregistré sur le réseau social. Un utilisateur n'a donc pas besoin de s'inscrire en passant par un formulaire pour pouvoir profiter du service tiers. Pour ce faire, France Connect promet de fédérer les identités fiscales, administratives ou sociales… d'un usager.

Des discussions avec la CNIL sont en cours sur la circulation des données personnelles.

L'idée n'est donc pas de stocker les informations sur une personne détenues par l'ensemble des administrations, mais uniquement les informations nécessaires, après consentement de l'internaute. Ainsi, pour l'inscription dans une crèche, il suffira de fournir uniquement des données fiscales pour identifier le quotient familial et valider ou non l'inscription (et plus l'intégralité de la feuille d'imposition).

Il ne s'agit donc pas de créer une nouvelle carte d'identité. L'utilisateur devra choisir son fournisseur. Le Directeur des systèmes d'information de l'Etat précise qu'il est question de s'appuyer sur des services comme les FAI, la CAF, Ameli ou bien encore les banques. Le consentement de l'utilisateur sera obligatoire.

Principe de fonctionnement



La Direction interministérielle des systèmes d'information et de communication a déjà commencé à mener des réunions avec la CNIL au sujet de la circulation des informations. Les administrations ne posséderont pas les données mais devront être à même d'authentifier correctement une personne. Ceci pourrait se faire par l'envoi d'un SMS qui permettra à une administration d'identifier la personne.

L'utilisateur devrait également garder la main sur les informations puisqu'il lui reviendra le choix de l'entité qui fournira son identité (impôt, CAF…) auprès d'une administration. Pour ces dernières, France Connect a pour but de les pousser à développer un système de réutilisation des données par un système d'API.

Pour le moment, France Connect est en phase de développement. Ce projet devrait aboutir en janvier 2016, date à laquelle les premières expérimentations débuteront. Il a désormais un objectif clair : mettre en place le dispositif pour la déclaration de revenus en ligne de 2016. A cette date, le site impots.gouv.fr pourrait être compatible avec le système.

Autres Etats

L'Union Européenne a identifié que les emplois des prochaines décennies seront liés à l'économie numérique. Bien que le domaine de l'identité soit une prérogative de chaque Etat Membre, la Commission Européenne a multiplié les projets et les initiatives pour une interopérabilité des services numériques, la protection des données personnelles et de la vie privée. Elle a mis en œuvre une stratégie, dans le cadre de ce qu'elle appelle le *Digital Agenda for Europe*.

Avant d'aborder la manière dont les grands Etats, à l'intérieur et en dehors de l'Union Européenne, ont abordé le sujet de l'identité numérique, il est intéressant de revenir sur les conclusions de la conférence du 9 avril 2015 organisée par la FNTC(7), l'Adelet et Open Peppol(2) à la chambre nationale des huissiers de justice.

Cette conférence, sujet d'échanges entre Opérateurs et administrations a permis de mieux comprendre les différents programmes européens : e-SENS, open PEPPOL et STORK.

En Europe, un mécanisme d'interconnexion européen, MIE ou « Connecting Europe Facility » a pour ambition, avec un budget de 850 millions d'euros, de développer à la fois des infrastructures et des services permettant de fédérer les différents systèmes d'informations nationaux des Etats membres de l'UE, à l'horizon 2020.

La future infrastructure d'identité numérique repose sur la TSL(3), avec un service de référencement géré au niveau central et des systèmes de création ou de validation de signature, comme le service DSS(4) de la DG MARKT. Le principe est celui de systèmes nationaux interagissant avec des services centraux. C'est l'esprit de la Directive des marchés publics, c'est aussi celui du règlement(1) e-IDAS.

Pour la signature électronique, seul le niveau qualifié est retenu selon une politique de certification, elle-même qualifiée. La nouveauté vient de la possibilité de délivrer un cachet électronique à une personne morale et non exclusivement à une personne physique. Faut-il y voir un recul de notre Code Civil ? Concernant les choix technologiques, l'utilisation de certificats sera la règle. Le règlement exclut d'autres systèmes d'authentification alors que le nombre d'applications en ligne ne fait que croître, délivrant quotidiennement et gratuitement des milliers d'identités aux internautes.

Lors de cette conférence, un intervenant de Sealweb a rendu compte du dispositif normatif porté par le CEN et l'ETSI. Le toilettage est rendu nécessaire avec l'homogénéisation d'une centaine de normes. C'est le cadre du mandat M460 de la Commission.

Ces travaux se traduisent par plusieurs avancées notables, une norme sur les puces cryptographiques, une nouvelle famille de normes pour la signature électronique et services associés (horodatage, e-delivery, pérennisation de la signature) etc. Ces développements s'accompagnent aussi de bonnes nouvelles pour les utilisateurs, la création d'un container ASIC de regroupement des documents signés électroniquement qui devrait remédier au risque de perte du fichier détaché de signature ; une normalisation de la TSL européenne pour une meilleure prise en compte des OID(5) par les opérateurs et enfin, la prise en compte par ADOBE de l'intégralité des autorités déclarées dans la TSL alors que son « reader » se limitait jusqu'alors à la vérification de validité de signature aux autorités uniquement référencées par ADOBE lui-même.

E-SENS, dont l'objectif est de lancer des pilotes en Europe dans les domaines des marchés publics, des échanges B2B, de l'e-justice et de la santé, a été présenté au niveau du programme européen. Aujourd'hui porté en France par le SGMAP, il se veut un programme de consolidation de l'ensemble des briques techniques développées dans le cadre des précédents programmes PEPPOL (public procurement) e-CODEX (justice) SPOCS (services aux entreprises) STORK (identité numérique) et ePSOS (santé). Le principe est de réemployer les briques techniques non seulement par soucis d'économie, mais aussi dans un but d'interopérabilité des services entre eux. Plusieurs domaines sont visés, le transport sécurisé de documents entre les administrations (e-Delivery) ; la facture électronique, qui va elle aussi rentrer dans une phase de déploiement généralisé dans le cadre de la nouvelle Directive sur la facture électronique. En France, elle s'appliquera d'abord aux grandes entreprises pour ensuite s'étendre progressivement à la totalité d'entre elles.

Le programme STORK 2.0 a été présenté par OpenTrust. Ce programme rassemble 19 pays et 58 partenaires afin de promouvoir l'e-ID dans les domaines de la santé, le e-learning, la banque en ligne ou les services publics en ligne. La prééminence du pouvoir régalien est arrêtée pour chaque Etat en matière d'identité numérique, ainsi que l'impossibilité d'une identité numérique européenne unique pour les citoyens européens.

Plusieurs représentant de la Banque Mondiale ont rappelé que 40% des enfants dans le monde naissent sans aucune identité dont près de 60% en Afrique sub-Saharienne où le téléphone mobile est plus répandu dans les populations que les moyens d'identification classique, ce qui constituerait le meilleur support de l'identité numérique. Il a également été souligné que l'identité numérique constitue la « killer application » de la lutte contre la pauvreté dans le monde en permettant par exemple de mieux rediriger l'argent public vers les bénéficiaires et mettre en échec la fraude et la corruption ».

Cette conclusion au niveau du programme Européen il parait utile de faire le tour du reste du monde en observant comment les différents Etats ont traité ce sujet.

Petit pays, qui en 2013 a fait le choix du tout numérique, **l'Estonie,** est réputée pour son administration internet. Le pays connait un taux de pénétration d'internet de 78,6 % (un des plus élevés au monde). Il a mis en place pour ses citoyens une e-police, e-santé, e-registre du commerce… L'Estonie souhaite désormais permettre aux citoyens et étrangers entrant dans le pays légalement, de disposer d'une carte d'identité numérique d'e-citoyenneté. A cette carte est associé un code d'identification unique permettant l'accès aux transports, à la bibliothèque, aux services de santé, au vote, au paiement des places de parking. Les possibilités s'étendent tous les six mois. La difficulté pour le citoyens estonien est de rester au courant des évolutions.

Grâce à ce système, les étrangers pourraient avoir accès aux services de l'e-état et cela permettrait de faire un suivi des citoyens estoniens lorsqu'ils partent à l'étranger.

Ce système propre à l'Estonie serait bientôt rendu possible dans d'autres pays. L'Allemagne serait d'ailleurs déjà en train de l'envisager.

Cela pourrait amener des avantages conséquents, faciliter d'accès aux services administratifs ou voter en ligne par exemple. Ce système, comme tout autre pourrait facilement être détourné et utilisé à des fins de surveillance. Il n'y a pas que des avantages dans la mise en place de cette nouvelle technologie. Tous les services administratifs, scolaires, santé etc… fonctionnent dans le monde numérique, cela implique donc une exclusion digitale de toutes les sphères de la société, de tous les citoyens qui n'ont pas les moyens d'avoir Internet.

Mis à part la **Grande Bretagne** (où les citoyens n'ont pas de carte d'identité), la plupart des pays européens ont lancé des initiatives visant à déployer des systèmes de confiance à destination des internautes, aussi bien pour leurs besoins privés que pour leurs relations à l'Etat.

Néanmoins, la grande majorité de ces initiatives est liée à des déploiements de cartes nationales d'identité électroniques. Les autres projets impliquent une subvention étatique ou une obligation réglementaire. Les usages, y compris pour « Suisse ID » qui est le modèle ayant inspiré la réflexion française IDNum, sont largement axés sur l'authentification dans des démarches administratives ou citoyennes.

La Moldavie

Très récemment encore, elle ne disposait pas d'identité et se trouve aujourd'hui grâce à ces programmes dans le peloton de tête des nations où l'e-ID est en passe de devenir une réalité.

L'Espagne

Depuis 2006, 25 millions de cartes d'identité électroniques ont été distribuées, permettant l'accès à 2500 services nationaux. Cependant, l'usage à domicile peine à décoller car il demande l'acquisition par le particulier d'un lecteur spécifique.

Le décret royal du 23 décembre 2005, régissant l'attribution de la carte d'identité dispose : « *à chaque **carte nationale d'identité sera associé un numéro personnel**, qui sera considéré comme identifiant numérique personnel général* ». Par conséquent, tous les titulaires d'une carte d'identité, c'est-à-dire **tous les Espagnols** à partir de l'âge de 14 ans, **sont identifiés par un numéro unique**.

En effet, la loi organique n° 1 du 21 février 1992 relative à la protection de la sécurité des citoyens a rendu obligatoire la détention de la carte d'identité à partir de l'âge de 14 ans.

Ce numéro d'identification fait partie des informations consignées dans les fichiers municipaux de population. Il comporte 8 chiffres ainsi qu'une lettre majuscule constituant une clef de contrôle, et ne présente pas de lien avec les données personnelles. Toutes les personnes résidant en Espagne ont l'obligation de se faire inscrire sur le registre nominal des habitants de la commune où elles sont domiciliées.

Il doit être porté sur tous les documents ou dossiers administratifs (passeport, permis de conduire, permis de pêche ou de chasse, documents fiscaux, inscription à des concours, demande de bourses d'études, etc.), financiers (ouverture de comptes bancaires, de livrets de caisse d'épargne, opérations de bourse, etc.), professionnels (adhésion à un syndicat ou à un ordre professionnel), ainsi que sur la carte de sécurité sociale.

Pour leurs relations avec les services fiscaux, les contribuables utilisent un numéro d'identification fiscal qui est identique au numéro de la carte d'identité.

En revanche, le numéro de sécurité sociale est différent.

La loi 11/2007 du 22 juin sur l'accès électronique des citoyens aux services publics prévoit qu'à partir du 31 décembre 2009, la carte d'identité électronique pourra servir de moyen d'accès universel à tous les services publics, grâce à son système d'identification intégré et de signature électronique.

L'Italie

Une carte de citadin (CRS) est déployée à plusieurs millions d'exemplaires depuis 2007. Elle permet, grâce à un certificat (ainsi qu'une piste magnétique) de s'authentifier pour l'inscription à des jeux en ligne, le paiement des impôts, des prestations de sécurité sociale…

Les personnes physiques sont identifiées par leur numéro d'identification fiscal dit « code fiscal », attribué à la naissance ou lors de l'installation dans le pays.

Le code fiscal ne constitue pas un numéro unique d'identification, mais il est fréquemment utilisé non seulement dans les relations avec l'administration fiscale, mais aussi pour bénéficier des prestations du système national de santé, être embauché comme salarié, conclure un contrat, ouvrir un compte bancaire, etc.

Le code fiscal est composé de 16 caractères alphanumériques. Il est constitué de la façon suivante :

- les trois premières consonnes du patronyme ;
- les trois premières consonnes du (ou des) prénom(s) ;
- les deux derniers chiffres de l'année de naissance ;
- une lettre représentant le mois de naissance ;
- deux chiffres correspondant au jour de naissance pour les hommes et au jour de naissance majoré de 40 pour les femmes ;
- la codification de la commune de naissance, sous forme de quatre chiffres ;
- une clé de contrôle, sous forme d'une lettre.

La modification du code fiscal est envisagée, parce que la codification actuelle n'empêche pas deux personnes d'avoir le même identifiant. Le nouveau numéro, devrait être entièrement numérique, pourrait constituer le futur numéro unique d'identification des personnes, et serait utilisé dans toutes les relations avec les administrations publiques.

Le Portugal

L'entreprise Gemalto, leader de l'identité numérique en Europe a été sélectionnée pour le projet de carte d'identité électronique au Portugal. Ce programme comprend plus de deux millions de cartes par an, avec pour objectif d'être le support d'une multitude de services e-Gouvernement (identification civile, fiscale, santé, électoral etc.). Cette carte, de la taille d'une carte de crédit et répondant à de grandes exigences d'impression sécurisée, sera le document d'identité officiel pour tous les citoyens portugais.

La Suisse

Lancé en mai 2010, « Suisse ID » est destiné à servir de preuve d'identité électronique. Le nombre de prestataires de service (grandes villes et communes, administrations fiscales) dépasse la centaine. Ils sont souvent liés à des opérations administratives : déclarer un changement d'adresse, modification de l'état civil, cyberadministration, décomptes de TVA,…

Au 31 décembre 2010, 271 000 certificats ont été commandés, très majoritairement par des entreprises qui les donnent à leurs salariés.

Il n'existe pas de numéro d'identification unique en Suisse. Toutefois, le numéro d'assuré social n'est pas utilisé uniquement par les organismes de protection sociale. Il sert notamment d'identifiant à l'administration fiscale, aux communes, qui sont chargées de la tenue des fichiers de leurs habitants, aux entreprises privées, pour la gestion de leur personnel, et aux autorités militaires.

Le numéro d'assuré social se compose de 11 chiffres. Il est constitué d'un numéro de base à huit chiffres, qui est suivi d'un numéro d'ordre composé de deux chiffres et d'une clé de contrôle à un chiffre. Le numéro de base est lié aux données personnelles. Les trois premiers chiffres résultent de la codification des premières lettres du patronyme, les deux suivants correspondent à l'année de naissance et les trois suivants constituent la codification de la combinaison du jour et du mois de naissance avec le sexe.

Sauf cas particulier (personne handicapée à la naissance par exemple), le numéro d'assuré social est attribué lorsque l'intéressé atteint l'âge de 20 ans ou lorsqu'il commence à travailler.

La loi du 23 juin 2006 modifiant la loi fédérale sur l'assurance vieillesse et survivants (LAVS) a créé un nouveau numéro d'assuré social à 13 chiffres, dépourvu de toute signification. Ce nouveau numéro sera introduit par étapes à partir du 1er juillet 2008. Il commence par 756, qui est le code de la Suisse, et comprend ensuite neuf chiffres qui ne permettent pas d'identifier l'intéressé, puis une clé de contrôle à un chiffre.

La loi LAVS limite l'utilisation du nouveau numéro d'assuré social comme identifiant. Elle prévoit en effet son utilisation par les services de sécurité sociale et de l'aide sociale, par l'administration fiscale ainsi que par les établissements d'enseignement. En revanche, dans les autres cas, elle subordonne l'emploi du numéro d'assuré social comme numéro d'identification à une autorisation du législateur. Toute personne enfreignant cette règle commettra une infraction pénale et sera passible d'une peine de prison de six mois au plus ou d'une amende pouvant atteindre 30 000 francs suisses (soit environ 28 000 €).

Pour faciliter les transmissions de données entre fichiers publics lorsque celles-ci sont autorisées, la loi fédérale sur l'harmonisation des registres des habitants et d'autres registres officiels de personnes du 23 juin 2006, qui entrera en vigueur le 1er janvier 2008, impose l'utilisation du nouveau numéro d'assuré social.

La Belgique

La Belgique a déployé, de 2004 à 2009 une carte d'identité électronique auprès de 8,3 millions de citoyens. 600 services sont disponibles (prestations sociales, impôts, scolarité...), l'identification pouvant aussi servir pour le commerce électronique. L'État a également favorisé le déploiement et l'usage par des mesures réglementaires : usage obligatoire pour déclarer en ligne ses impôts. La carte d'identité électronique est une carte à puce de même format qu'une carte bancaire. En 2006, une carte du même type a été instaurée pour les enfants de moins de 12 ans : la Kids-ID. Ces cartes sont conformes à la norme ISO/IEC 7816.

Toutes les cartes distribuées depuis 2004 sont électroniques. Tous les Belges ont depuis fin 2009 une carte d'identité électronique, les anciennes cartes plastifiées ayant été remplacées par des cartes d'identité électroniques.

L'Allemagne

L'Allemagne a commencé en novembre 2010 le déploiement de certificats avec le CNIE, qui est une carte à puce sans contact. Les premiers services offerts sont pour l'instant essentiellement administratifs, et les services bancaires sont embryonnaires.

Il n'y a pas de numéro unique d'identification des personnes physiques. Un tel numéro serait incompatible avec la Loi fondamentale, en particulier avec le droit à la libre disposition des données personnelles, considéré par la Cour constitutionnelle fédérale comme dérivé des droits à la dignité et à la liberté, lesquels sont explicitement garantis par les articles 1 et 2 de la Loi fondamentale. Le 15 décembre 1983, dans sa décision relative au recensement, la Cour constitutionnelle fédérale a en effet mis en évidence le droit à la libre disposition des données personnelles, qui confère à chacun le pouvoir de décider de la communication et de l'utilisation par des tiers des données le concernant. À cette occasion, elle a alors expressément affirmé que l'attribution d'un numéro unique d'identification serait inconstitutionnelle.

Depuis le 1er juillet 2007, l'administration fiscale fédérale procède, à partir des données transmises par les services communaux chargés de la tenue des fichiers de déclarations domiciliaires, aux opérations préalables nécessaires à l'attribution d'un numéro permanent d'identification fiscale aux personnes physiques à partir du 1er janvier 2008. Ce numéro se compose de 11 chiffres, le dernier étant une clé de contrôle. Il résulte de la codification de certaines données personnelles (nom, prénom, sexe, date et lieu de naissance, adresse, diplôme universitaire et pseudonyme), mais sa simple lecture ne permet pas de déterminer ces données.

Cet identifiant sera attribué dès la naissance et conservé pendant vingt ans après le décès de l'intéressé. Le code des impôts prévoit qu'il ne doit être utilisé que par l'administration fiscale, et seulement dans le cadre des activités qui lui sont confiées.

Toutefois, le délégué fédéral chargé du contrôle du traitement informatisé des données nominatives et de la liberté de l'information, ainsi que ses homologues des Länder, ont fait part de leur inquiétude, car c'est la première fois qu'un fichier centralise au niveau fédéral les données personnelles et les adresses de toute la population. Cette inquiétude a été renforcée par l'annonce faite par le gouvernement fédéral au début de l'année 2007 de créer un fichier central de déclarations domiciliaires. La réforme constitutionnelle de 2006, qui a transféré à la fédération la compétence exclusive pour légiférer dans certaines matières (notamment la déclaration domiciliaire) alors que cette compétence était auparavant partagée entre la fédération et les Länder permet en effet une telle réforme.

L'Autriche

L'Autriche a mis en place une carte de citoyen avec un certificat de signature électronique, mais l'émission de telles cartes n'est pas réservée à l'État, et les chambres de commerce ou les banques peuvent en émettre. Par ailleurs le support de ce certificat est libre : puce sur carte type bancaire, clef USB, téléphone portable.

Depuis la création du fichier central des déclarations domiciliaires, le 1er mars 2002, toutes les personnes domiciliées en Autriche disposent d'un numéro d'identification, qui est associé aux données de ce fichier.

Ce numéro, dit ZMR(8) (Zentralmelderegister : fichier déclaratif central), se compose de 12 chiffres, qui ne doivent contenir aucun élément signifiant.

Pour chacune des personnes enregistrées, le fichier central contient, outre ce numéro, des informations relatives à l'identité et au domicile. Il est alimenté par les communes, qui ont l'obligation de gérer un registre de leurs résidents.

La loi de 1991 relative à la déclaration domiciliaire prévoit que les informations du fichier central sont accessibles sur autorisation du ministère de l'intérieur non seulement aux administrations, mais aussi aux « partenaires du secteur privé », c'est-à-dire à des personnes ou des établissements privés dont l'activité requiert l'identification répétée des clients : banques, assurances, notaires, avocats, bureaux de recouvrement de créances, etc. Les modalités d'accès à ces informations ainsi que la teneur de celles-ci dépendent du statut du destinataire des données.

Toutefois, afin de garantir la protection des données personnelles et d'empêcher l'interconnexion des fichiers, le numéro ZMR ne peut pas être utilisé comme identifiant personnel ni par les administrations ni par les établissements privés. La loi du 27 février 2004 relative à l'e-gouvernement prévoit en effet que chaque administration doit utiliser pour son secteur propre d'activité un numéro d'identification spécifique et ne doit en aucun cas enregistrer les autres numéros d'identification sectoriels.

En pratique, le numéro ZMR sert à calculer un numéro « source » secret, dont les identifiants sectoriels sont dérivés, le tout selon des procédures très protégées.

Les pays nordiques et pays baltes

Des systèmes ont été déployés dans ces pays traditionnellement en pointe dans les nouvelles technologies :

Au Danemark, le recours au système « NemID(9) »est obligatoire pour les citoyens disposant d'un service de banque en ligne.

Depuis 1968, toutes les personnes qui résident au Danemark sont identifiées par un numéro unique, qui leur est donné dès la naissance ou lors de leur installation dans le pays et qu'elles conservent durant toute leur vie. Ce numéro, dit « numéro CPR(10) » : (*Det centrale personregister*, c'est-à-dire le fichier central des personnes), se compose de **dix chiffres** : les six premiers correspondent à la date de naissance (jour, mois et année), le septième résulte de la codification du siècle de naissance, les huitième et neuvième forment un numéro d'ordre, tandis que le dixième est une clé de contrôle, pair pour les femmes et impair pour les hommes. C'est le ministère de l'intérieur et de la santé qui l'établit pour chaque personne.

Le numéro CPR fait partie des données enregistrées dans le fichier central des personnes, dont la gestion incombe au ministère de l'intérieur et de la santé, et qui est mis à jour par les communes. Ce fichier contient de nombreuses informations sur chaque personne : nom, adresse, état civil, lieu de naissance, nationalité, ascendants et enfants, appartenance religieuse, profession, etc. Chacune de ces informations est très détaillée. Ainsi, les adresses secondaires et les adresses antérieures sont enregistrées.

Les communes, qui exercent de nombreuses compétences, notamment dans le domaine social (gestion des crèches et des écoles primaires, services aux personnes âgées, prestations sociales, etc.), utilisent les données de ce fichier.

La loi sur la protection des données personnelles dispose que les administrations et les établissements publics peuvent utiliser le numéro CPR comme numéro d'identification. La loi sur le fichier CPR autorisant par ailleurs les communes à transmettre les données de ce fichier aux gestionnaires de fichiers publics.

Le numéro CPR est également couramment utilisé comme identifiant dans le secteur privé, par exemple par les banques, mais à condition que les intéressés donnent leur accord.

En Suède, dès 2002, l'Agence suédoise responsable de la gestion publique confiait à des fournisseurs le mandat d'offrir des certificats électroniques aux citoyens. Ces certificats distribués par les six plus grandes banques du pays, par la Poste suédoise et par l'opérateur Telia permettent de signer électroniquement des documents et de s'identifier pour obtenir des services en ligne, y compris de l'administration.

Depuis 1947 tous les résidents sont identifiés par un numéro unique, qui leur est attribué à la naissance ou lors de leur installation dans le pays.

Ce numéro, dit « numéro personnel » se compose de 10 chiffres et d'un symbole (- ou +). Les six premiers chiffres représentent la date de naissance (année, mois, jour), les trois suivants forment un numéro d'ordre, pair pour les femmes et impair pour les hommes, et le dernier est une clé de contrôle. Les six premiers chiffres sont séparés des quatre suivants par un tiret, qui se transforme en signe plus (+) lorsque l'intéressé atteint l'âge de 100 ans. C'est l'administration fiscale qui établit chaque numéro personnel.

Le numéro personnel fait partie des données enregistrées dans le fichier de la population, qui contient de nombreuses informations (nom, date et lieu de naissance, adresse, nationalité, état civil, etc.) et qui, depuis 1991, est géré par l'administration fiscale à partir des indications fournies soit par les intéressés (après la naissance d'un enfant ou un déménagement par exemple) soit par d'autres services administratifs (après un mariage par exemple).

Le traitement des données du fichier de la population est régi par des textes spécifiques, qui prévoient explicitement la transmission des informations à tous les services administratifs. En pratique, une procédure automatique, appelée « Navet », a été mise en place à cet effet.

Le numéro personnel est ainsi utilisé comme identifiant par tous les services administratifs, tant par l'administration fiscale, que par les assurances sociales, le service du permis de conduire, le bureau de conscription de l'armée, etc. Il est également couramment utilisé dans le secteur privé, par exemple par les banques, mais à condition que les intéressés soient d'accord pour le fournir. Les établissements privés ne peuvent pas profiter d'une alimentation automatique de leurs fichiers à partir des données du fichier de la population.

En Norvège, le système « BankID » est une réussite certaine, avec un modèle économique fondé sur une ouverture des marchés de l'acquisition avec un financement par les banques. Les accepteurs (marchands, fournisseurs de services) doivent installer l'application BankID qu'ils obtiennent auprès d'une banque. Les banques doivent collecter les éléments d'identification des accepteurs. La concurrence est libre entre les banques pour acquérir les accepteurs.

Les Etats Unis, pays où il n'existe pourtant pas de carte d'identité, ont défini une « *National Strategy for Trusted Identities in Cyberspace* » afin de sécuriser les services numériques qu'ils ont rendus publics. Ils ont annoncé que leurs sites gouvernementaux mettraient cette politique en pratique, accompagnant ainsi la mise en application par le secteur privé.

En 2015, 85% des identités délivrées par les Etats seront numériques :

En Inde

Un large programme a été lancé il y a quatre ans. La mise en place de l'identité numérique a permis de découvrir que seules 61% des aides aux chômeurs parvenaient aux bénéficiaires prévus. 1,2 milliard d'identités numériques seront délivrées en 2015.

Le projet connu sous le nom de d'Aadhaar est une véritable révolution technologique dont le but est d'améliorer les services publics. Malgré le coût élevé de ce programme, il y a aujourd'hui un accord politique autour de ce projet.

Aadhaar signifie en hindi « socle » ou « soutien ». C'est le nom qui a été donné à la carte d'identité numérique et biométrique dont tous les Indiens seront bientôt dotés. Cette carte devrait servir de support pour l'acheminement des aides sociales aux populations défavorisées. Le programme Aadhaar a été lancé en septembre 2010 sous l'égide de Nandan Nilekani, pionnier de l'informatique en Inde et co-fondateur de la multinationale Infosys. Trois sociétés étrangères dont la société française Morpho (filiale du groupe Safran) participent à ce projet.

Sur la carte Aadhaar est inscrit un numéro à douze chiffres qui est attribué au titulaire. La carte comporte aussi une puce électronique qui contient des informations biométriques : couleur des yeux, empreintes digitales etc. Cette signature digitale est conservée dans une base de données nationale, consultable à distance grâce un lecteur d'empreintes. Il s'agit d'une véritable révolution dans un pays où il n'y avait pas jusqu'ici de notion de carte d'identité. 650 millions de personnes ont déjà été enregistrées dans la base de données, soit la moitié de la population, pour un coût de 400 millions d'euros.

L'intérêt principal de cette carte réside dans l'utilisation que les pouvoirs publics en feront pour apporter une plus grande efficacité dans leur politique sociale. En effet, le gouvernement indien consacre chaque année près de 200 milliards d'euros pour financer les divers programmes sociaux en direction de ses populations défavorisées. Or 85% de ces subventions n'atteignent pas les destinataires, du fait des intermédiaires corrompus.

La carte d'identité numérique permet désormais au destinataire de l'aide gouvernementale d'ouvrir un compte bancaire qui renvoie à son numéro à douze chiffres. C'est sur ces comptes que sont désormais versées directement les allocations. Les cartes de rations pour les denrées de base dont bénéficie une grande partie de la population fonctionneront elles aussi avec ces données numériques et biométriques.

En Tanzani, le projet de protection sociale dispense 5 millions d'identités numériques sur téléphone mobile pour l'attribution de subvention.

Au Nigéria, des audits biométriques ont permis de diminuer de 40% le nombre des pensionnés de l'Etat.

En **Azerbaïjan**, Imza, une solution mobile a été adoptée.

En Jordani, Les distributeurs de billet sont biométriques.

JURIDIQUE

Carte Nationale d'identité

Que contient la carte nationale d'identité aujourd'hui (CNIL- 18 février 2005)

La carte nationale d'identité est le seul document officiel qui ait été créé dans le but exclusif d'authentifier l'identité de son titulaire, et non pour lui ouvrir un droit. Elle mentionne donc des informations relatives à la fois à la personne concernée et à l'autorité qui l'a délivrée. Elle n'est délivrée qu'aux personnes de nationalité française.

La carte d'identité n'est pas obligatoire : elle n'est délivrée que sur demande de la personne concernée. L'on peut apporter la preuve de son identité par tous moyens.

La carte comporte la photographie et la signature du titulaire. **La photographie** fournie à l'appui de la demande de la carte est numérisée, mais à seule fin d'impression sur la carte. A l'origine, elle était directement incorporée dans le titre lui-même, confectionné à partir d'un papier de sécurité enrobé de plastique.

La demande de carte donne lieu au relevé d'une **empreinte digitale**, laquelle ne figure pas sur la carte et ne fait l'objet d'aucun traitement automatisé : elle est seulement conservée dans les dossiers papiers détenus par les préfectures. Elle ne peut être utilisée qu'en vue soit de détecter des tentatives d'obtention ou d'utilisation frauduleuse d'un titre d'identité, soit d'identifier de façon certaine une personne dans le cadre d'une procédure judiciaire.

La carte nationale d'identité est **gratuite** ; elle est valable dix ans, mais, même périmée, elle permet de justifier de son identité tant que la photo est ressemblante.

La carte nationale d'identité sécurisée, telle qu'elle est délivrée dans tous les départements depuis 1995, comporte une bande à lecture optique dans laquelle sont enregistrés le nom de famille, les prénoms, le sexe et la date de naissance de son titulaire, ainsi que le numéro de la carte d'identité concernée. Cette bande n'a jamais été utilisée dans la pratique.

En cas de déménagement, le changement d'adresse est facultatif : il appartient à l'intéressé de demander la délivrance d'une nouvelle carte.

Pour permettre la fabrication et la gestion des cartes nationales d'identité sécurisées, le ministère de l'Intérieur a été autorisé à mettre en œuvre un fichier informatique centralisé. Ce fichier contient les informations relatives au titulaire du document et celles relatives à l'autorité de délivrance de la carte, mais l'empreinte digitale, la photographie et la signature de l'intéressé ne sont pas enregistrées dans ce fichier, qui ne peut faire l'objet d'aucune interconnexion avec d'autres fichiers, ni d'aucune cession.

En cas de vol ou de perte de la carte nationale d'identité sécurisée, les textes prévoient que certaines des informations sont enregistrées dans un fichier central distinct, avec la mention du vol ou de la perte et, le cas échéant, du lieu réel ou supposé où l'événement s'est produit.

Passeport biométrique

■ *Fraude à l'identité*

La mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire, avait considéré qu'il serait utile de confier à **l'ONDRP**, l'Observatoire national de la délinquance et des réponses pénales la mission d'élaborer un outil performant de mesure de la fraude à l'identité.

L'ONDRP s'est attaché, depuis son rapport annuel pour 2007, à présenter les principales mesures disponibles en la matière, en se basant sur l'état 4001 recensant les infractions constatées par les services de police et de gendarmerie, ainsi que sur les données fournies par la direction centrale de la police aux frontières et par le bureau de la nationalité des titres d'identité et de voyage de la direction des libertés publiques et des affaires juridiques du ministère de l'intérieur.

> « *En 2009, près de **13 900 faits constatés** de fraudes documentaires et à l'identité ont été enregistrés par les services de police et les unités de gendarmerie.*
>
> *Sur l'ensemble du territoire français, **4 011 documents frauduleux** français ont été saisis par la police aux frontières (PAF) en 2009. Parmi ces faux documents, on dénombre 1 640 certificats d'acte de naissance, **1 070 cartes d'identité, 1 035 passeports** et 266 permis de conduire.*

De 2004 à 2009, le nombre de signalements de personnes utilisant au moins deux identités a crû de 129,9%. Ce chiffre est obtenu notamment à partir du rapprochement entre l'identité alléguée par la personne interpellée et celle qui est, le cas échéant, associée à ses empreintes dans le fichier automatique des empreintes digitales. Ainsi ***en 2009, 98 350 personnes ont été signalées avec deux états civils différents*** ».

Source : Rapport 2010 de l'Observatoire national de la délinquance et des réponses pénales, novembre 2010, p. 285.

Les chiffres fournis à l'ONDRP par le bureau de la nationalité et des titres d'identité et de voyage du ministère de l'intérieur montrent enfin que le passeport et la carte nationale d'identité restent des titres recherchés par les fraudeurs, **puisqu'en 2009, 351 000 cartes nationales d'identité ont été déclarées perdues ou volées, ainsi que 79 916 passeports**. Ces chiffres sont à rapporter aux 5 millions de CNI et 3 millions de passeports délivrés chaque année et aux 45 millions de CNI et 15 millions de passeports en circulation (Chiffres de 2011).

■ *Première étape: le passeport biométrique*

La création en France d'un titre de voyage biométrique répond à des exigences européennes et internationales.

L'organisation de l'aviation civile internationale et les États-Unis exigent, avant 2015 pour les premiers et depuis le 26 octobre 2006 pour les seconds, l'intégration d'au moins une donnée biométrique dans les documents de voyage, qui peut être la photo numérisée du visage de son titulaire.

Le règlement communautaire du 13 décembre 2004 (n° 2252/2004 du Conseil établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres) , du 13 décembre 2004, modifié par le règlement du 28 mai 2009 (n° 444/2009 du Parlement européen et du Conseil du 28 mai 2009), impose aux États membres la création d'un passeport avec puce électronique, pour les citoyens européens âgés de plus de 12 ans et l'inscription, sur cette puce, de diverses informations (identité, taille, yeux etc.) et des deux données biométriques suivantes : une photographie numérisée du visage et deux empreintes digitales.

Le décret n° 2008-426 du 30 avril 2008 instaurant le passeport biométrique est allé au-delà des prescriptions communautaires. Il a notamment prévu :

- la création d'un fichier central, le fichier « TES » (Titres Electroniques Sécurisés), regroupant l'ensemble des données recueillies pour la confection du titre, notamment les empreintes digitales. Il constitue le premier fichier de ce type et de cette ampleur en France. L'article 19 du décret précité interdit toutefois l'utilisation des empreintes digitales enregistrées dans ce fichier à des fins de police judiciaire. Le fichier ne comporte par ailleurs pas de dispositif de reconnaissance faciale ;
- le recueil de huit empreintes digitales, enregistrées dans la base. Toutefois seules deux empreintes sont inscrites dans la puce électronique du passeport ;
- l'application de l'obligation de disposer d'un passeport biométrique aux enfants âgés de 6 à 12 ans. La France a ainsi utilisé la possibilité de régime transitoire prévue par le règlement européen. Cet âge a été relevé à 12 ans, en application du règlement, à compter du 29 juin 2013, le régime transitoire n'étant appelé à durer que quatre ans.

■ *Base biométrique*

Une fois fixées les finalités de la base biométrique, compte tenu des craintes que suscite un tel dispositif et des risques qu'il présente, toutes les garanties doivent être apportées qu'elle ne pourra être utilisée pour d'autres objets. Les garanties juridiques sont-elles suffisantes ?

La loi « informatique et libertés » soumet les traitements automatisés de données personnelles à un certain nombre d'obligations, protectrices de la liberté individuelle : droit d'accès ou de rectification, contrôle de la CNIL etc.

Le texte qui crée le système de traitement peut prévoir d'autres garanties, interdisant certaines utilisations. Ainsi le décret précité organisant le fichier TES sur les passeports biométriques interdit l'accès des forces de police œuvrant dans le domaine de l'antiterrorisme aux données relatives aux empreintes digitales pour identifier une personne.

De telles garanties sont solides. Cependant, elles ne sont ni définitives, ni absolues : ainsi l'accès aux fichiers est toujours possible dans le cadre d'une procédure judiciaire, sous le contrôle d'un magistrat. De plus, la prohibition peut être levée, ce qui autorise pour l'avenir l'utilisation du fichier pour une autre finalité que sa finalité originelle : c'est ce qui a été proposé par la Commission européenne s'agissant de la base EURODAC qui enregistre les données biométriques des demandeurs d'asile et des personnes appréhendées à l'occasion du franchissement irrégulier d'une frontière extérieure à l'Union européenne.

Carte d'identité électronique

L'intérêt majeur de cette carte d'identité électronique est la lutte contre la fraude documentaire ainsi que la possibilité de l'utiliser dans des téléprocédures administratives ou des transactions commerciales.

En 2005, la France s'est engagée dans un projet de mise en place d'une carte d'identité INES (identité nationale électronique sécurisée) contenant des données biométriques (empreintes digitales, photographie, iris de l'œil…). Ce projet a lancé un grand débat autour de la question de l'identité biométrique.

Ce projet n'est toujours pas mis en œuvre à l'heure actuelle, l'Etat est la seule entité légitime pouvant délivrer des titres d'identités officiels. Ceci s'impose également dans le monde des réseaux numériques.

■ Contours définitifs de la carte d'identité électronique *(Legalis - Décembre 2005)*

Lors des 6ème rencontres parlementaires sur la société de l'information et de l'internet, Philippe Sauzet, directeur du programme Identité nationale électronique sécurisée (INES) au ministère de l'internet, a dévoilé la maquette de la carte d'identité numérique. Ce futur titre sera équipé d'une puce électronique qui comportera un volet régalien et un autre destiné à la partie « services ».

Le premier comprendra, d'un côté, les données lisibles sur la carte ainsi que la taille et la couleur des yeux de la personne et, de l'autre côté, les empreintes digitales numérisées, le tout sécurisé par deux sceaux électroniques du ministère (4096 bits).

La deuxième partie du titre d'identité permettra d'accéder à des services électroniques publics comme privés, grâce à une clé d'authentification et à une clé de signature, qui seront sécurisées par un sceau (2048 bits).

Selon Philippe Sauzet, seule la partie régalienne de la carte devrait être lisible grâce à la technologie sans contact, avec une portée d'un centimètre. Le directeur du programme INES a, par ailleurs, confirmé la création d'une base de données biométriques centralisée. « C'est un élément de sécurisation du système mais les conditions d'accès seront très encadrées. Il n'y aura pas de recherche sur les éléments biométriques sans le recours à l'autorité judiciaire ». Enfin, il a affirmé que le projet « identité numérique » sera facultatif.

INES devait être autorisée par une loi que le ministère de l'Intérieur espèrait voir votée au 1er semestre 2006, pour une **mise en œuvre en 2008**.

Loi du 27 mars 2012 relative à la protection de l'identité

Le 28 mars 2012 le Conseil constitutionnel a censuré les dispositions concernant le fichier central d'empreintes biométriques, considérant qu'elles portent une « atteinte au droit au respect de la vie privée » non « proportionnée au but poursuivi ». Il a également refusé d'autoriser la puce facultative permettant de s'identifier sur internet pour faciliter l'usage des services en ligne.

La loi a été promulguée le 27 mars 2012. Elle a été publiée au Journal officiel le 28 mars 2012.

Saisi le 7 mars 2012 d'un recours déposé par plus de 60 sénateurs et par plus de 60 députés, le Conseil constitutionnel a rendu le 22 mars 2012 une décision censurant trois articles de la proposition de loi.

Le texte définitif de la proposition de loi avait été adopté le 6 mars 2012, l'Assemblée nationale l'ayant adopté en lecture définitive.

La proposition de loi avait été adoptée en nouvelle lecture par l'Assemblée nationale le 1er février 2012 et modifiée par le Sénat le 21 février 2012.

Le texte mis au point par la Commission mixte paritaire avait été rejeté par le Sénat le 26 janvier 2012 après avoir été adopté, avec modification, par l'Assemblée nationale le 12 janvier 2012.

En deuxième lecture, la proposition de loi avait été adoptée par l'Assemblée nationale, avec modification, le 13 décembre 2011 après avoir été modifiée par le Sénat le 3 novembre 2011.

Déposée au Sénat le 27 juillet 2010 par MM. Jean-René Lecerf et Michel Houel, elle avait été adoptée en première lecture par le Sénat le 31 mai 2011 et par l'Assemblée nationale, avec modification, le 7 juillet 2011.

De quoi s'agit-il ?

L'objectif affirmé du texte est de faciliter la lutte contre l'usurpation et la falsification d'identité.

A cette fin il prévoyait, avant la décision du Conseil constitutionnel du 22 mars 2012, la mise en place d'un nouveau type de carte d'identité pouvant intégrer deux types de puces électroniques.

Une première puce obligatoire, appelée « puce régalienne », contiendrait les données d'identité et les données biométriques :

- nom, prénoms, sexe, date et lieu de naissance ;
- nom d'usage autorisé, en cas de demande de l'intéressé ;
- domicile ;
- taille et couleur des yeux ;
- empreintes digitales ;
- photographie.

Une deuxième puce, facultative, aurait été destinée à faciliter l'usage des services en ligne. Elle aurait permis notamment la mise en œuvre de la signature électronique dans le cadre des relations avec une entreprise privée aussi bien qu'avec une administration. Elle devait donc être utilisée dans les démarches administratives, les échanges bancaires ou les transactions commerciales.

Pour permettre au dispositif de fonctionner et assurer l'authentification des données une base centrale devrait être constituée. Cette base, dite « Titres électroniques sécurisés » (TES), serait chargée de « recenser, confronter, vérifier les informations » et devrait notamment permettre un repérage immédiat et précis des doublons, garantie supplémentaire contre les usurpations d'identité ou les falsifications.

La durée de conservation des données devait être fixée par un décret en Conseil d'État, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés (CNIL).

Le Conseil constitutionnel a censuré les dispositions concernant le fichier central d'empreintes biométriques, considérant qu'elles portaient une « atteinte au droit au respect de la vie privée » non « proportionnée au but poursuivi ». Il a également refusé d'autoriser la puce facultative permettant de s'identifier sur internet pour faciliter l'usage des services en ligne.

Données personnelles

Les **données personnelles** correspondent à toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

Les données personnelles permettant l'identification correspondent aux noms, prénoms, adresses (physique et électronique), numéro de téléphone, lieu et date de naissance, numéro de sécurité sociale, numéro de carte de paiement, plaque d'immatriculation d'un véhicule, photo, aux données médicales et génétiques, aux empreintes digitales, à l'ADN et, en général, à toute caractéristique biométrique.

La notion d'identité numérique, composée de plusieurs de ces éléments, rentre dans le cadre des données personnelles, et à ce titre, est protégée par divers instruments juridiques concernant le droit à la vie privée, dont notamment la loi Informatique et libertés de 1978, la directive 95/46/CE ainsi que la Convention n°108.

Lois et textes fondateurs

Loi 78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés

Bien que signée en 1978, l'histoire de la loi Informatique et libertés est environ de dix ans plus ancienne. En effet, dès 1970, le député Michel Poniatowski propose à l'Assemblée nationale la création d'un comité de surveillance et d'un tribunal de l'informatique. Cette suggestion, reprise plus tard par d'autres, est rejetée. Pourtant en 1971, l'INSEE (Institut National de la Statistique et des Etudes Economique), profitant du passage de l'informatique des cartes perforées vers les bandes magnétiques, décida de centraliser à Nantes les répertoires d'identification jusque-là régionaux, par le projet SAFARI (Système automatisé pour les Fichiers Administratifs et le Répertoire des Individus), visant à une interconnexion des fichiers notamment par l'usage du NIR (numéro INSEE de Sécurité sociale). Puis l'administration envisagea de cumuler cette centralisation avec celle à Tours du fichier de la Caisse nationale d'assurance vieillesse (CNAV) et de l'interconnecter avec les fichiers de la carte d'identité, gérée par le ministère de l'Intérieur.

Ce projet perçu comme une entrave grave à la liberté fait scandale lorsque Le Monde titra le 21 mars 1974 : « SAFARI ou la chasse aux Français ». Cette tribune provoqua un tollé politique, auquel dut faire face le tout récent ministre de l'Intérieur Jacques Chirac, qui venait « d'échanger » son poste à l'agriculture avec celui de Raymond Marcellin depuis moins d'un mois. Le projet SAFARI, lancé lors de la présidence de Georges Pompidou, n'a finalement jamais vu le jour.

Mais le 2 avril 1974, Georges Pompidou, décèda de sa maladie de Waldenström (forme de cancer). Valéry Giscard d'Estaing est alors élu président de la République, grâce au soutien de Jacques Chirac et surtout de la popularité de ce dernier auprès du monde rural, acquise lors de son passage à l'Agriculture. Jacques Chirac est nommé Premier ministre et appelle M. Poniatowski au ministère de l'Intérieur. Ce dernier, face à la critique, reprend son idée et crée la Commission de l'informatique et des libertés et met sur pied le projet, qui malgré sa démission en 1977, aboutira à la LIL « loi Informatique et Libertés » du 6 janvier 1978 et à la création de la CNIL (Commission nationale de l'informatique et des libertés).

La LIL, s'applique à la collecte, la conservation et le traitement automatisé de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles, lorsque leur responsable remplit les conditions prévues à l'article 5.

Article 5 modifié par Loi n°2004-801 du 6 août 2004 - art. 1 JORF 7 août 2004 :

I. - *Sont soumis à la présente loi les traitements de données à caractère personnel :*

1° Dont le responsable est établi sur le territoire français. Le responsable d'un traitement qui exerce une activité sur le territoire français dans le cadre d'une installation, quelle que soit sa forme juridique, y est considéré comme établi ;

2° Dont le responsable, sans être établi sur le territoire français ou sur celui d'un autre Etat membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre Etat membre de la Communauté européenne.

II. - *Pour les traitements mentionnés au 2° du I, le responsable désigne à la Commission nationale de l'informatique et des libertés un représentant établi sur le territoire français, qui se substitue à lui dans l'accomplissement des obligations prévues par la présente loi ; cette désignation ne fait pas obstacle aux actions qui pourraient être introduites contre lui.*

La LIL inscrit dès l'article premier l'informatique dans le cadre des droits de l'homme.

Article 1 :

« *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. 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* ».

■ Historique des modifications

Textes modifiant la loi 78-17 du 6 janvier 1978 :

Loi n° 88-227 du 11 mars 1988 (Journal officiel du 12 mars 1988)

Loi n° 92-1336 du 16 décembre 1992 (Journal officiel du 23 décembre 1992)

Loi n° 94-548 du 1er juillet 1994 (Journal officiel du 2 juillet 1994)

Ordonnance n°96-267 du 28 mars 1996

Loi n° 99-641 du 27 juillet 1999, (Journal officiel du 28 juillet 1999)

Loi n° 2000-321 du 12 avril 2000, (Journal officiel du 13 avril 2000)

Ordonnance n°2000-916 du 19 septembre 2000

Loi n° 2001-616 du 11 juillet 2001

Loi n° 2002-303 du 4 mars 2002, (Journal officiel du 5 Mars 2002)

Loi n° 2003-239 du 18 mars 2003 (Journal officiel du 19 mars 2003)

Loi n° 2004-801 du 6 août 2004 (Journal officiel du 7 août 2004)

Loi n° 2006-64 du 23 janvier 2006 (Journal officiel du 24 janvier 2006)

Loi n° 2007-1787 du 20 décembre 2007

Loi n° 2008-696 du 15 juillet 2008

Loi n° 2009-526 du 12 mai 2009 (Journal officiel du 13 mai 2009)

Loi organique n° 2010-704 du 28 juin 2010

Loi n° 2011-334 du 29 mars 2011 (Journal officiel du 30 mars 2011)

Loi n° 2011-525 du 17 mai 2011

Ordonnance n° 2011-1012 du 24 août 2011 (Journal officiel du 26 août 2011)

Loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique (Journal Officiel du 12 octobre 2013)

Loi n° 2014-344 du 17 mars 2014

Textes fondateurs

Directive 95/46/CE sur la protection des données personnelles et loi 2004

Directive 95/46/CE

La Directive 95/46/CE de la Commission Européenne du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données constitue le texte de référence au niveau Européen. Il étend la protection du citoyen et de ses libertés fondamentales plus particulièrement au droit du respect de sa vie privée, en prenant en compte l'augmentation des flux, nationaux et internationaux, de données personnelles au travers de traitement automatisés. La directive vise à harmoniser les normes des différents États-membres en matière de protection des données personnelles, ceci afin de faciliter leur libre-circulation à des fins, notamment, commerciales.

L'art. 2 définit la notion de « données personnelles » ainsi que de « système de traitement de données » et celle de « contrôleur » ou responsable de la bonne tenue des systèmes précités.

Au niveau territorial, la directive s'applique dès que le responsable utilise des équipements situés sur le territoire de l'un des États-membres de l'UE, y compris lorsqu'il est lui-même situé à l'étranger (art. 4). Par ailleurs, des règles spécifiques concernent l'échange de données à des États-tiers (art. 25 et 26). Les pays de l'Espace économique européen (outre les 27 de l'UE, cela inclut l'Islande, le Liechtenstein et la Norvège) ne sont pas considérés comme États-tiers, dans la mesure où la directive a été intégrée dans l'accord sur l'Espace économique européen.

Les données personnelles ne doivent pas être soumises à un traitement automatisé, sauf si celui-ci remplit les exigences posées par trois principes : proportionnalité, transparence, et finalité légitime.

L'art. 28 demande à chaque État-membre d'instituer une autorité de protection des données personnelles, sur le modèle général de la Commission nationale Informatique et libertés (CNIL) établie en France.

L'art. 29 créé un groupe européen, dit G29 (Groupe de travail Article 29 sur la protection des données). Ce groupe a notamment négocié avec les États-Unis les « *International Safe Harbor Privacy Principles* » visant à améliorer la protection des données personnelles des résidents de l'Union européenne traitées aux Etats-Unis, le *Privacy Act* de 1974 n'accordant cette protection, jugée inférieure à celle établie dans l'UE, qu'aux ressortissants américains.

La directive 95/46/CE, largement inspirée de la **Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel** du Conseil de l'Europe de 1981, ne couvre pas la coopération policière et judiciaire en matière pénale, ce qui inclut l'ensemble des fichiers de police, de justice et de renseignements. Par ailleurs, elle ne concerne que la réglementation des Etats-membres ; les données personnelles collectées par des institutions communautaires sont régies par le règlement 45/2001, lequel institua le Contrôleur européen de la protection des données (CEPD). La directive 95/46/CE institua, elle, le G29 afin de coordonner l'activité des différentes autorités de protection des données personnelles.

■ *Loi du 6 août 2004*

La loi de 1978 est modifiée par la loi du 6 août 2004 afin de transposer en droit français les dispositions de la directive 95/46/CE sur la protection des données personnelles. La loi de 1978 modifiée est complétée par son décret d'application n°2005-1309 en date du 20 octobre 2005. Cette transposition modifie de manière substantielle le texte de 1978, en élargissant le domaine des données qualifiées de personnelles (article 2), simplifie leurs régimes juridiques et alourdit les sanctions aux articles 226-16 à 226-24 du Code pénal. De plus, les pouvoirs d'enquête, d'investigation et de sanctions de la CNIL sont renforcés.

La nouvelle loi harmonise partiellement les règles de déclaration des fichiers entre secteur privé et secteur public. Le régime général pour le secteur public n'est plus de demander une autorisation à la CNIL, mais de faire une simple déclaration de ces fichiers, comme c'était déjà le cas pour le secteur privé. Le demandeur doit alors attendre le récépissé de la CNIL avant l'utilisation effective du fichier.

Toutefois, la distinction entre personne publique et personne privée n'a pas totalement disparu. La loi du 6 août 2004 prévoit en effet une procédure nouvelle de demande d'avis imposée aux organismes du secteur public pour la création de certains fichiers contenant des données sensibles. La procédure d'autorisation demeure pour les entreprises privées et s'étend à de nouvelles catégories de données. Les fichiers devant faire l'objet d'une demande d'autorisation sont, entre autres, ceux qui utilisent le numéro de sécurité sociale.

Cette simplification de la loi ne va pas sans poser de problèmes, la simple déclaration à la CNIL, contrairement à une demande d'autorisation, ne permet plus à cette dernière de protéger les citoyens de manière proactive quand des fichiers contenant des données personnelles sont créés et utilisés de manière irrégulière.

La France sera la dernière à transposer la directive européenne de 1995, qui modifia profondément la loi, en remplaçant notamment le terme « d'informations nominatives », par celui de « données à caractère personnel ».

Convention n°108 pour la protection des données personnelles (1981)

Convention 108

La Convention du 28/04/1981 est signée par les états membres du Conseil de l'Europe. Le but de la présente Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelle que soit sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant (protection des données).

La Convention est le premier instrument international contraignant qui a pour objet de protéger les personnes contre l'usage abusif du traitement automatisé des données à caractère personnel, et qui réglemente les flux transfrontaliers des données.

Outre des garanties concernant le traitement automatisé des données à caractère personnel, elle proscrit le traitement des données « sensibles » relatives à l'origine raciale, aux opinions politiques, à la santé, à la religion, à la vie sexuelle, aux condamnations pénales, etc... , en l'absence de garanties offertes par le droit interne. La Convention garantit également le droit des personnes de connaître les informations stockées à leur sujet et d'exiger le cas échéant des rectifications.

Seule restriction à ce droit : lorsque les intérêts majeurs de l'Etat (sécurité publique, défense, etc...) sont en jeu.

La Convention impose également des restrictions aux flux transfrontaliers de données dans les Etats où n'existe aucune protection équivalente.

Protocole Additionnel du 8/11/2001

Ce protocole vient renforcer la Convention en y ajoutant deux articles:

Article 1 : Autorités de contrôle

1. Chaque Partie prévoit qu'une ou plusieurs autorités sont chargées de veiller au respect des mesures donnant effet, dans son droit interne, aux principes énoncés dans les chapitres II et III de la Convention et dans le présent Protocole.

a. A cet effet, ces autorités disposent notamment de pouvoirs d'investigation et d'intervention, ainsi que celui d'ester en justice ou de porter à la connaissance de l'autorité judiciaire compétente des violations aux dispositions du droit interne donnant effet aux principes visés au paragraphe 1 de l'article 1 du présent Protocole.

b. Chaque autorité de contrôle peut être saisie par toute personne d'une demande relative à la protection de ses droits et libertés fondamentales à l'égard des traitements de données à caractère personnel relevant de sa compétence.

3. Les autorités de contrôle exercent leurs fonctions en toute indépendance.

4. Les décisions des autorités de contrôle faisant grief peuvent faire l'objet d'un recours juridictionnel.

5. Conformément aux dispositions du chapitre IV et sans préjudice des dispositions de l'article 13 de la Convention, les autorités de contrôle coopèrent entre elles dans la mesure nécessaire à l'accomplissement de leurs missions, notamment en échangeant toute information utile.

Article 2 : Flux transfrontières de données à caractère personnel vers un destinataire n'étant pas soumis à la juridiction d'une Partie à la Convention

1. Chaque Partie prévoit que le transfert de données à caractère personnel vers un destinataire soumis à la juridiction d'un Etat ou d'une organisation qui n'est pas Partie à la Convention ne peut être effectué que si cet Etat ou cette organisation assure un niveau de protection adéquat pour le transfert considéré.

2. Par dérogation au paragraphe 1 de l'article 2 du présent Protocole, chaque Partie peut autoriser un transfert de données à caractère personnel:

a. si le droit interne le prévoit :

- pour des intérêts spécifiques de la personne concernée,

- lorsque des intérêts légitimes prévalent, en particulier des intérêts publics importants,

b. si des garanties pouvant notamment résulter de clauses contractuelles sont fournies par la personne responsable du transfert, et sont jugées suffisantes par les autorités compétentes, conformément au droit interne.

Le traité de Lisbonne modifiant le traité sur l'Union européenne et le traité instituant la Communauté européenne est entré en vigueur le 1er décembre 2009. Par conséquent, à partir de cette date, toute mention des Communautés européennes doit être lue comme **l'Union Européenne**.

Droit à l'image

Si l'identité numérique peut être définie comme les identifiants choisis ou attribués par les tiers (pseudo, mot de passe, nom de famille, numéro de Sécurité Sociale), elle s'étend surtout à ce que les autres perçoivent : c'est-à-dire l'image.

L'identité numérique faisant partie du monde multimédia, qui inclut l'image, l'identifiant est donc indissociable de l'image. Avec la montée des réseaux sociaux, il est très difficile de contrôler son image sur Internet.

La loi comporte aujourd'hui plusieurs textes pour protéger l'image des personnes ou des entreprises.

Premièrement, l'article 9 du Code civil concerne l'atteinte à la vie privée en établissant que « chacun a droit au respect de sa vie privée ».

L'article 226-1 du Code pénal prévoit une peine d'un an d'emprisonnement et de 45 000 euros d'amende « le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui ». Cependant, le dernier alinéa du texte prévoit également que cette violation d'image ne doit pas avoir été accomplie accomplie « au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire » sinon le tribunal estime que le consentement a été exprimé. Cela signifie donc qu'une photo prise en soirée dans un lieu privé et déposée sur les réseaux sociaux le lendemain sans l'accord des personnes sera considérée comme avoir été prise avec un consentement implicite puisque les personnes ne s'y sont pas opposées. Le texte sera donc difficilement applicable ici.

Enfin, l'article 228-8 du Code pénal prévoit une peine « d'un an d'emprisonnement et de 15 000 euros d'amende le fait de publier, par quelque voie que ce soit, le montage réalisé avec les paroles ou l'image d'une personne sans son consentement, s'il n'apparaît pas à l'évidence qu'il s'agit d'un montage ou s'il n'en est pas expressément fait mention ».

Droit à l'oubli

Il existe aujourd'hui un paradoxe quant à l'utilisation d'Internet. Les internautes expriment de plus en plus leur inquiétude d'être fichés mais diffusent dans le même temps de plus en plus d'informations (parfois intimes).

Le droit à l'oubli est donc une véritable problématique concernant Internet puisqu'il s'agit d'un droit à ce que les éléments relatifs au passé d'une personne, qu'ils soient exacts, inexacts ou devenus obsolètes puissent être retirés des contenus en ligne, ou rendus difficilement accessibles, afin de pouvoir sortir de la mémoire collective et tomber dans l'oubli.

Il n'existe pas actuellement de droit à l'oubli en tant que tel mais des moyens sont présents dans le cadre juridique actuel pour permettre l'oubli (prescription, suppression de condamnation du casier judiciaire, réhabilitation…).

L'article 6 de la loi Informatique et Libertés relatif aux conditions de licéité des traitements de données à caractère personnel précise que la durée de conservation des données ne doit pas excéder la durée nécessaire aux finalités pour lesquelles les données sont collectées et traitées.

Par ailleurs, l'article 40, inséré dans la section relative aux droits des personnes à l'égard des traitements de données à caractère personnel dispose, notamment, que toute personne peut exiger l'effacement de données la concernant, inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Il existe actuellement un projet de règlement européen qui devrait consacrer le principe d'un « droit à l'oubli » numérique pour permettre aux internautes de mieux maîtriser leur vie en ligne. Ce nouveau droit devra s'exercer tout en respectant la liberté d'expression, du droit de la presse et du devoir de mémoire. La CNIL a d'ailleurs lancé en mai 2013 une consultation publique sur la question du droit à l'oubli, c'est la « possibilité offerte à chacun de maîtriser ses traces numériques et sa vie - privée comme publique - en ligne ».

Pour Alex Türk, président de la CNIL, ce premier pas est historique, mais demeure insuffisant tant que la valeur juridique contraignante de ces principes n'est pas définie.

Chartes du droit à l'oubli numérique

Initiées en France par la secrétaire d'État chargée de la Prospective et du Développement de l'économie numérique, Nathalie Kosciusko-Morizet, deux chartes du droit à l'oubli numérique ont été signées en 2010 :

- le 30 septembre 2010 : Charte du Droit à l'oubli numérique dans la publicité ciblée : il s'agit des données personnelles collectées passivement, sans que l'internaute en ait vraiment conscience ;
- le 13 octobre 2010 : Charte du Droit à l'oubli numérique dans les sites collaboratifs et moteurs de recherche : il s'agit des données personnelles publiées activement par l'internaute. La CNIL, Facebook et Google ont participé à la réflexion, mais n'ont pas signé la charte.

LOPPSI 2: Loi d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure

Usurpation d'identité

La loi 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure est une loi française qui concerne la gestion de la police et de la gendarmerie pour la période 2009-2013. Ce texte, appelé LOPPSI 2 en référence à la LOPSI de 2002 avec le même objet et portant presque le même nom sans « Performance », a été élaboré par les ministres de l'Intérieur Michèle Alliot-Marie puis Brice Hortefeux.

Le texte concerne en particulier la lutte contre la criminalité générale, la récidive, la délinquance routière, la « cyber-pédopornographie », l'instauration d'un couvre-feu pour les mineurs. Il donne également de nouveaux pouvoirs à la police et prévoit d'en déléguer aux polices municipales et aux entreprises de sécurité privée. Cette loi crée en particulier un nouveau **délit d'usurpation d'identité**.

Chapitre 2, Article 2 : Lutte contre la Cybercriminalité

Après l'article 226-4 du code pénal, il est inséré un article 226-4-1 ainsi rédigé :

> « *Art. 226-4-1.-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* ».

Cette peine est applicable notamment lorsqu'une personne utilise votre identité sur les réseaux sociaux pour diffuser des informations erronées. Attention, cette infraction nécessite un dépôt de plainte au commissariat ou à la gendarmerie.

Jusqu'à l'adoption de la LOPPSI 2 du 14 mars 2011, il n'existait pas d'infraction propre à l'usurpation d'identité. La fraude à l'identité était réprimée à travers plusieurs types d'infractions différentes, soit à titre autonome, soit comme un élément constitutif de ces infractions.

Ainsi **l'article 434-23 du code pénal punit de cinq ans d'emprisonnement et de 75 000 euros d'amende** 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. La fausse déclaration relative à l'état civil d'une personne, lorsque celle-ci a eu ou aurait pu avoir le même effet contre un tiers, est également punie des mêmes peines. Ces peines se cumulent, le cas échéant, avec celles encourues au titre de l'infraction à l'occasion de laquelle l'usurpation d'identité a été commise.

A l'époque, des critiques de la presse internationale (*Der Spiegel et The Register*) qualifiaient cette loi comme étant la plus répressive du monde en matière de cybercriminalité, la France passant alors devant l'Australie, déjà réputée pour sa sévérité en la matière.

Dès 2009 cette loi a suscité de nombreux doutes sur son contenu et sa supposée efficacité, comme ceux exprimés par la CNIL qui avait rendu son avis sur ce projet de loi le 24 juillet 2009:

> « *Nous sommes inquiets par ce projet de loi. Nous redoutons une utilisation excessive de ce système d'espionnage par la police, qui pourrait mettre en danger la protection des sources journalistiques. Le cadre de mise en œuvre de la captation des données informatiques doit être plus clairement défini. Nous demandons aux parlementaires de présenter des amendements pour mieux encadrer ce projet* ».

Cet article intitulé : « L'usurpation d'identité numérique : un nouveau délit pour rien ? ». en témoigne.

Système PHAROS

Cette mesure cohabite avec un autre système : PHAROS, « Plate-forme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements » ouvert à tous. C'est un outil pour porter à la connaissance des forces de l'ordre tous les cas de criminalité liée aux nouvelles technologies.

Cette plateforme est intégrée à l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication. Ce service appartient à la Direction Centrale de la Police Judiciaire, composante de la Police nationale.

- 137 456 signalements en 2014.
- 120 000 signalements en 2012
- 78 000 signalements en 2010
- 18 000 signalements sur les 6 premiers mois de 2009 (aucun lié à des cas d'usurpation d'identité)

Projets en cours

Projet de règlement européen sur la protection des données à caractère personnel

Ce projet de règlement vise à renforcer les règles de l'Union Européenne en matière de protection des données. Il a pour vocation de se substituer à la directive 95/46/CE du 24 octobre 1995.

La réforme comprend deux propositions législatives : un projet de règlement définissant un cadre général au sein de l'Union Européenne pour la protection des données et un projet de directive relative à la protection des données à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ainsi que d'activités judiciaires connexes.

Le projet se caractérise tout d'abord par la modification de l'instrument juridique utilisé pour consacrer les règles. Reposant jusqu'à présent sur une directive européenne, la réforme a pour vocation d'utiliser le vecteur d'un règlement européen. La particularité d'un règlement européen est de créer un même droit dans toute l'Union européenne et d'être valable uniformément et intégralement dans tous les États membres.

Le texte est actuellement en cours de discussion au Parlement européen, où il fait l'objet d'amples débats (le pré-rapport présenté en janvier 2013 par M. Albrecht, rapporteur à la Commission Libertés civiles, justice et affaires intérieures du Parlement européen, a ainsi fait l'objet de plusieurs milliers de propositions d'amendements).

Ce projet de règlement est présenté par les parlementaires européens comme l'un de ceux ayant généré la plus importante opération de lobbying jamais vue dans le cadre de l'adoption d'un texte européen. De très nombreux professionnels s'inquiètent en effet des contraintes nouvelles que le projet de règlement risque de leur imposer dans le cadre de la mise en oeuvre de traitements de données personnelles.

Sur le fond, l'adoption du projet apparaît indispensable. Le contexte de l'internationalisation des flux rend en effet nécessaire, au-delà des aspects purement juridiques, que l'Europe parle d'une seule voix sur le plan politique face aux autres États du monde qui n'entendent pas à-priori se conformer à un cadre aussi protecteur que celui défini en Europe. L'adoption d'un règlement permettra ainsi à l'Union européenne de disposer d'un outil harmonisé qui lui donnera la possibilité de peser plus lourdement dans le cadre de négociations internationales, par exemple concernant un éventuel traité impliquant les États-Unis ou les pays de la zone Asie/Pacifique.

La mise en œuvre du nouveau texte, une fois celui-ci adopté, impliquera une importante mise à niveau de la part de nombreux organismes publics ou privés afin de se conformer aux nouvelles obligations qui seront définies.

Ce règlement entend conférer aux individus de nouveaux droits comme décrit dans les articles suivants :

L'article 11 introduit l'obligation, pour les responsables du traitement, de fournir des informations transparentes, facilement accessibles et intelligibles, s'inspirant notamment de la résolution de Madrid relative à des normes internationales en matière de protection des données à caractère personnel et de la vie privée.

L'article 12 oblige le responsable du traitement à prévoir des procédures et des mécanismes permettant à la personne concernée d'exercer ses droits, notamment les moyens d'effectuer une demande par voie électronique, la fixation d'un délai de réponse à la demande de la personne concernée et la motivation des refus.

L'article 13 prévoit des droits en faveur des destinataires inspirés de l'article 12, point c), de la directive 95/46/CE et étendus à tous les destinataires, y compris les responsables conjoints du traitement et les sous-traitants.

L'article 14 précise les informations que le responsable du traitement est tenu de fournir à la personne concernée et ajoute par rapport aux articles 10 et 11 de la directive 95/46/CE, notamment la durée de conservation, le droit d'introduire une réclamation, les transferts internationaux et la source des données. Il reprend également les dérogations prévues dans la directive 95/46/CE, par exemple l'absence d'obligation d'information si la législation prévoit expressément l'enregistrement ou la communication des données. Cela pourrait, par exemple, s'appliquer aux procédures engagées par une autorité de concurrence, une administration fiscale ou douanière, ou un service chargé des questions de sécurité sociale.

L'article 15 confère à la personne un **droit d'accès aux données** à caractère personnel la concernant, tout comme le faisait l'article 12, point « a » de la directive 95/46/CE, en y ajoutant de nouveaux éléments tels que l'obligation d'informer les personnes de la durée de conservation, de leur droit à rectification et à l'effacement et de leur droit de réclamation.

L'article 16 confère à la personne un **droit à rectification**, sur la base de l'article 12, point b), de la directive 95/46/CE.

L'article 17 lui confère, quant à lui, un **droit à l'oubli numérique** et à l'effacement. Il développe et précise le droit d'effacement prévu à l'article 12, point «b», de la directive 95/46/CE et fixe les conditions du droit à l'oubli numérique, notamment l'obligation qui est faite au responsable du traitement ayant rendu publiques des données à caractère personnel d'informer les tiers de la demande de la personne concernée d'effacer tout lien vers ces données ou les copies ou reproductions qui en ont été faites. Il intègre aussi le droit de limiter le traitement dans certains cas, en évitant le terme équivoque de « verrouillage ».

L'article 18 confère à la personne concernée un nouveau droit, le **droit à la portabilité** des données, c'est-à-dire celui de transmettre des données d'un système de traitement automatisé à un autre, sans que le responsable du traitement ne puisse y faire obstacle. À titre de condition préalable et pour améliorer l'accès des personnes physiques aux données à caractère personnel les concernant, il prévoit le droit d'obtenir ces données du responsable du traitement dans un format électronique structuré et couramment utilisé.

L'article 19 confère à la personne concernée un **droit d'opposition**. Il est fondé sur l'article 14 de la directive 95/46/CE, auquel il apporte quelques modifications, notamment en ce qui concerne la charge de la preuve et son application au marketing direct.

L'article 20 porte sur le **droit de la personne concernée** à ne pas être soumise à une mesure fondée sur le profilage. Il est inspiré de l'article 15, paragraphe 1, de la directive 95/46 relatif aux décisions individuelles automatisées, qu'il complète et assortit de garanties supplémentaires, et tient compte de la recommandation du Conseil de l'Europe concernant le profilage.

L'article 21 précise dans quelle mesure l'Union ou les États membres peuvent maintenir ou introduire des limitations aux principes énoncés à l'article 5 et aux droits de la personne concernée prévus aux articles 11 à 20 et à l'article 32. Cette disposition repose sur l'article 13 de la directive 95/46/CE et sur les exigences découlant de la charte des droits fondamentaux et de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, telles qu'elles ont été interprétées par la Cour de justice de l'Union européenne et par la Cour européenne des droits de l'homme.

Projet de loi numérique du Gouvernement

Projet préparé par Mme Lemaire, Secrétaire d'État chargée du Numérique, auprès du ministre de l'Économie, de l'Industrie et du Numérique.

Extrait d'une intervention de Mme Lemaire du 25 avril 2014 lors de la **Conférence de Paris sur l'open data et le gouvernement ouvert :**

« *La révolution numérique, comme ont coutume de l'appeler les journalistes, est en marche, elle touche toutes les strates de la société, les citoyens comme les entreprises ou les territoires.* ***L'État et l'ensemble des acteurs publics ont la responsabilité, je dirais même le devoir, de s'insérer pleinement dans ce mouvement***.

La prochaine transposition en droit français de la directive européenne PSI (Public Sector Information) concernant la réutilisation des informations du secteur public nous offre tout à la fois un cadre juridique et une opportunité majeure d'évolution et d'affirmation de notre volonté.

Je souhaite qu'à cette occasion, plusieurs principes soient réaffirmés et gravés dans le marbre législatif :

- *Le fait que, par défaut, une donnée publique se doit d'être ouverte et que toute fermeture soit explicitement expliquée, justifiée et réversible ;*
- *Le principe fondateur de la gratuité des données publiques qui ne sauraient faire l'objet de redevances que sur des motifs d'intérêt général ;*
- *La définition et l'inscription dans les pratiques administratives d'un bloc d'informations et de données publiques faisant l'objet d'une obligation de publication ;*
- *Le renforcement, enfin, des pouvoirs de la CADA et du pouvoir de saisine de la commission du secret statistique, avec l'assurance que la hiérarchie des normes soit appliquée strictement en la matière.*
- *Le gouvernement prépare un projet de loi sur le numérique qui sera précédé d'une concertation ouverte confiée au CNNum (Conseil National du Numérique) qui débutera dans les tout prochains jours. Je ne doute pas que ces questions seront abordées à cette occasion.*

Le gouvernement souhaite également aller plus loin dans son soutien aux démarches innovantes portées par tous les acteurs.

Les discussions de ce matin ont aussi mis en lumière la nécessité de la pédagogie. Ainsi, il est nécessaire de rappeler parfois quelques évidences:

- *Open data et big data ne sont pas synonymes ;*
- *L'ouverture des données publiques n'équivaut pas à la divulgation de données personnelles ;*
- *L'open data n'est pas une simple affaire de techniciens ou de spécialistes, mais bien une question politique, culturelle, citoyenne et économique.*
- *L'utilisation de données personnelles pour valider des modèles ou des algorithmes, je pense par exemple à des données liées à la santé, est possible dans un cadre très contraint, protecteur des libertés des individus et sous le couvert d'organisations de confiance* ».

Propositions de la CNIL

Projet de loi numérique : propositions rendue publiques sur les évolutions de la loi informatique et libertés, 13 janvier 2015, Isabelle FALQUE-PIERROTIN - Présidente de la CNIL et du G29

Le Gouvernement a annoncé en février 2013 son intention de déposer un projet de loi sur le numérique. La CNIL a engagé une réflexion qui l'a conduite à présenter en mars 2014 plusieurs propositions d'évolution législative. A l'occasion des débats organisés par le Conseil national du numérique, elle a décidé de verser ces propositions au débat public.

Les propositions rendues publiques concernent les quatre principaux acteurs de l'écosystème « informatique et libertés » : la personne, les entreprises, les pouvoirs publics et la CNIL.

Ces propositions sont organisées autour de cinq axes :

1) Le renforcement de l'effectivité des droits pour les personnes

2) La simplification des formalités et des règles applicables pour les entreprises

3) L'amélioration du cadre juridique de certains traitements publics

4) Le renforcement des relations entre la CNIL et les pouvoirs publics

5) L'adaptation des pouvoirs de la CNIL, notamment en vue de renforcer l'efficacité et la crédibilité de la politique de contrôle et de sanction.

Les propositions de modifications législatives doivent notamment tenir compte de deux éléments :

- *Le projet de règlement européen : les modifications éventuelles de la loi informatique et libertés devront naturellement être compatibles avec le règlement à venir dont l'adoption définitive est attendue au cours de l'année 2015.*
- *La cohérence avec les autres pays de l'Union : la législation sur les données personnelles ayant une portée économique croissante, les modifications éventuelles ne doivent pas créer de distorsion entre pays de l'Union, mais les bonnes pratiques doivent être valorisées car elles sont un élément de compétitivité.*

Enfin, la discussion autour d'une réforme du cadre juridique fixé par la loi pourrait être utilement complétée par une réflexion sur la constitutionnalisation du droit à la protection des données personnelles.

Il y a quelques années, on vantait internet pour sa capacité à déconcentrer, l'intelligence se trouvait aux extrémités, elle était distribuée. Désormais on s'inquiète de voir que les fleurons de l'internet qui ont profité de cela succombent à la tentation du centre qui capte et retient la valeur. Le constat est d'autant plus paradoxal que cette valeur est désormais produite par la donnée et donc par l'individu. C'est pourquoi, il me parait si important que l'on puisse redonner de la maîtrise aux individus sur leurs données, pour redonner à l'internet cette fluidité. Beaucoup d'innovations existent en la matière, juridiques, techniques ou commerciales.

C'est par exemple le sens du projet de règlement européen sur la protection des données qui entend conférer aux individus de nouveaux droits comme le droit à la portabilité des données. Ce droit, c'est la capacité pour tout un chacun d'aller chercher son profil de réseau social, ses données de consommation pour recréer de la concurrence au niveau individuel.

Cependant ne soyons pas naïfs, les individus seuls ne peuvent pas tout. La complexité des algorithmes est telle, la vitesse de calcul sur les big data est si importante qu'il faut responsabiliser les acteurs eux-mêmes et doter le régulateur de la capacité d'intervenir avec plus d'efficacité encore.

Le projet de loi numérique que prépare Mme Lemaire contribuera, je le souhaite, à aller en ce sens et instaurer cette loyauté dans la relation entre les individus et les entreprises en permettant par exemple de donner à la CNIL des pouvoirs coercitifs à la hauteur des enjeux, de travailler sur la transparence des algorithmes ou sur les clauses contractuelles.

CNIL

Création de la CNIL

Le 6 janvier 1978, le Parlement instaurait non seulement la loi informatique et libertés mais aussi l'autorité de contrôle permettant sa bonne application : la CNIL (Commission Nationale de l'Informatique et des Libertés), premier organisme étatique à avoir été qualifié d'autorité administrative indépendante (AAI). Les AAI, plus ou moins indépendants du pouvoir exécutif, ont souvent un pouvoir de sanction ou de réglementation, ce qui en fait des organismes quasi-juridictionnels, on parle aussi « d'autorités régulatrices ».

Missions de la CNIL

Grâce à la loi Informatique et Libertés de 1978, vous bénéficiez de droits spécifiques que vous pouvez, dans la plupart des cas, faire valoir vous-mêmes.

Tout citoyen peut s'adresser à la CNIL pour :

- **Adresser une plainte** en cas de violation de la loi informatique et libertés (non-respect de vos droits, faille de sécurité, défaut d'information, absence de déclaration...)
- **Accéder aux informations contenues dans des fichiers de police ou de gendarmerie**.
- **Demander les coordonnées d'un responsable de fichier** auprès de qui exercer ses droits.

La CNIL peut :

- Intervenir auprès du responsable de fichier que vous désignez
- Contrôler sur place les organismes qui exploitent des données personnelles
- Prononcer des sanctions
- Dénoncer à la Justice des infractions graves.

Tout citoyen peut porter plainte directement auprès du procureur de la République en vue de faire condamner pénalement le non-respect par les responsables de fichiers de ses droits.

Les délais de traitement de votre plainte peuvent être importants en raison notamment du grand nombre de saisines que la CNIL reçoit, près de 6 000 par an.

■ *Droit d'accès*

Accès Direct

Vous pouvez demander directement au responsable d'un fichier s'il détient des informations sur vous (site web, magasin, banque...), et demander à ce que l'on vous communique l'intégralité de ces données. L'exercice du droit d'accès permet de contrôler l'exactitude des données et, au besoin, de les faire rectifier ou effacer.

***Que dit la loi* :**

Le droit d'accès « direct » est prévu par les **Articles 39, Article 41, Article 42 de la loi du 6 janvier 1978 modifiée**. En exerçant son droit d'accès, la personne peut **s'informer des finalités du traitement, du type de données enregistrées, de l'origine et des destinataires des données, des éventuels transferts de ces informations vers des pays n'appartenant pas à l'Union Européenne**.

Les limites au droit d'accès :

Si un responsable de traitement estime qu'une demande est manifestement abusive, il peut ne pas y donner suite. En revanche si l'affaire est portée devant un juge il devra apporter la preuve du caractère manifestement abusif de la demande en cause.

L'exercice du droit d'accès ne doit pas porter atteinte au droit d'auteur.

Pour certains fichiers, la loi n'autorise pas un particulier à accéder directement aux informations contenues. Il pourra cependant y accéder de manière indirecte par l'intermédiaire de la CNIL.

Accès Indirect

Vous ne pouvez pas demander directement aux services de police, de gendarmerie, de renseignement, à l'administration fiscale d'accéder aux données vous concernant dans leurs fichiers. C'est ce qu'on appelle le « droit d'accès indirect ».

Le magistrat de la CNIL doit se déplacer auprès des services concernés afin de vérifier les enregistrements dont vous faites peut-être l'objet. **Le délai moyen de traitement est ainsi de 2 mois à 4 mois**.

Que dit la loi :

Le droit d'accès « indirect » est prévu par les articles **41 et 42 de la loi du 6 janvier 1978 modifiée**. L'un des membres de la CNIL, magistrat ou ancien magistrat, est chargé de **procéder en votre nom à la vérification du ou des fichier(s) concerné(s) : Traitement d'Antécédents Judiciaires, Système d'Information Schengen, fichiers de renseignement, fichier des comptes bancaires (FICOBA)**...

Les limites au droit d'accès indirect :

Le « droit d'accès indirect » ne vous ouvre pas un droit à communication des données. Elles ne peuvent vous être communiquées qu'en accord avec le responsable du fichier (et du procureur de la République pour le Traitement des Antécédents Judiciaires -TAJ -) qui peut s'y opposer pour des motifs liés à la finalité du fichier, la sûreté de l'Etat, la défense ou la sécurité publique. **En cas de refus de communication, la CNIL vous indiquera les voies de recours qui vous sont ouvertes pour contester cette décision**.

■ *Droit de rectification*

Toute personne peut demander la rectification des informations inexactes la concernant. Le droit de rectification complète le droit d'accès. Il permet d'éviter qu'un organisme ne traite ou ne diffuse de fausses informations sur vous.

Que dit la loi :

L'article 40 de la loi du 6 janvier 1978 modifiée permet à toute personne de rectifier, compléter, actualiser, verrouiller ou effacer des informations qui la concernent lorsqu'elles sont :

- Erronées ;
- Inexactes ;
- Incomplètes ;
- Périmées ;
- Ou les données dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Les limites au droit de rectification :

Attention, **le droit de rectification ne s'applique pas aux traitements littéraires, artistiques et journalistiques**.

Les cas particuliers :

Les personnes décédées : les héritiers d'une personne décédée peuvent exiger du responsable d'un traitement de prendre en considération le décès et/ou de procéder aux mises à jour nécessaires.

Pour les fichiers de police, de gendarmerie, de renseignement, FICOBA, soumis au droit d'accès indirect via la CNIL, vous ne pouvez pas solliciter la rectification auprès des services concernés. Le magistrat de la CNIL est également chargé de procéder aux rectifications nécessaires vous concernant.

■ *Droit d'opposition*

Toute personne a la possibilité de s'opposer, pour des motifs légitimes, à figurer dans un fichier. En matière de prospection, notamment commerciale, ce droit peut s'exercer sans avoir à justifier d'un motif légitime. **Vous pouvez vous opposer à ce que les données vous concernant soient diffusée, transmises ou conservées**.

Que dit la loi :

L'Article 38 de la loi du 6 janvier 1978 modifiée permet à toute personne physique de s'opposer :

- **pour des motifs légitimes**, à ce que des données la concernant fassent l'objet d'un traitement (c'est-à-dire qu'elles soient collectées, enregistrées, diffusées, communiquées, ou conservées etc.) ;
- **sans frais**, à ce que des données la concernant soient utilisées à des fins de prospection commerciale.

Ce droit peut s'appliquer dans différents cas, par exemple :

- **en refusant de voir ses données transmises ou commercialisées**, notamment au moyen d'une case à cocher dans les formulaires de collecte d'informations personnelles ;
- **en refusant de fournir des renseignements lors d'une collecte** non obligatoire de données ;
- en demandant la **suppression des données personnelles enregistrées** dans des fichiers commerciaux ;
- en demandant la **suppression de commentaires, photos, diffusés** sur des sites ou réseaux.

Les limites au droit d'opposition :

Le droit d'opposition est un droit personnel qui ne peut être étendu aux informations relatives à des tiers, même s'il s'agit de membres de votre famille, sauf les cas de représentation de mineurs ou de majeurs protégés.

Le droit d'opposition n'existe pas pour de nombreux fichiers du secteur public comme, par exemple, ceux des services fiscaux, des services de police, des services de la justice, de la sécurité sociale...

L'organisme est en droit de refuser d'accepter votre demande d'opposition. Les décisions de refus doivent être motivées par le responsable du traitement, sauf lorsque la demande est manifestement abusive. En cas d'absence de réponse (refus tacite), vous pouvez saisir la CNIL et les tribunaux.

■ *Droit au déréférencement*

Les internautes peuvent saisir les moteurs de recherche de demandes de déréférencement d'une page web associée à leurs nom et prénom.

Que dit la loi :

Dans un récent arrêt (C-131/12, 13 mai 2014), la Cour de justice de l'Union européenne a confirmé que les moteurs de recherche sont responsables de traitements. A ce titre, ils doivent respecter le droit européen à la protection des données personnelles. Désormais les personnes disposent d'un droit à demander le déréférencement d'informations en lien avec leur identité.

Toute personne résidant en France peut saisir la CNIL à la suite d'un refus de déréférencement.

Les limites au droit au déréférencement :

Le déréférencement consiste à supprimer certains résultats figurant dans la liste de ceux affichés par un moteur de recherche après une requête effectuée sur la base de données relative à une personne.

Cette suppression ne signifie pas l'effacement de l'information sur le site internet source. Le contenu original reste ainsi inchangé et est toujours accessible via les moteurs de recherche en utilisant d'autres mots clés de recherche ou en allant directement sur le site à l'origine de la diffusion.

Si le moteur de recherche estime qu'une demande est manifestement abusive, il peut ne pas y donner suite.

Sanctions Pénales

En cas de non-respect de la loi, plusieurs sanctions sont envisageables.

1. Par la CNIL :
   - Avertissement
   - Injonction à cesser le traitement ou retrait de l'autorisation
   - Verrouillage de certaines données
   - Recours au Premier ministre ou à la justice pour prendre les mesures nécessaires afin de faire cesser le traitement
   - Amende d'un maximum de 300 000 €

2. Par un tribunal :
   - 5 ans d'emprisonnement (articles 226-16 et suivant du code pénal)
   - Annulation d'un licenciement prononcé sur la base de preuves obtenues par un traitement qui n'a pas été déclaré à la CNIL

Sanctions Pénales s'appliquant à la loi informatique et libertés de 1978, quelques exemples clés:

Art. 226-16

Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

Art. 226-16-1

Le fait, hors les cas où le traitement a été autorisé dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 précitée, de procéder ou faire procéder à un traitement de données à caractère personnel incluant parmi les données sur lesquelles il porte le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

Art. 226-18

Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

Art. 226-18-1

Le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.

Quelques statistiques sur les jugements rendus par la CNIL ces **9 dernières années, de 2006 à 2014** inclus, sur un total de **114 dossiers traités en jugement** :

- Avertissements, public et non public : 50
- Interruption de traitement : 2
- Non-lieux et relaxes : 7
- Sanctions Pécuniaires : 55 (1 montant inconnu)
- 1€ à 10 000€ : 34
- >10k à 50 000€ : 18
- >50k à 100 000€ : 1 (Affaire Google délibération de 2011 sur la Géolocalisation)
- >100k à 150 000€ : 1 (Affaire Google délibération de 2014 → recours au Conseil d'état en cours)

BIOMÉTRIE

Avis de la CNIL (Octobre 2011) sur la Loi du 27 Mars 2012

Depuis le début des années 2000, plusieurs projets de cartes d'identité biométriques et électroniques ont vu le jour. La CNIL a ainsi été saisie par le ministère de l'intérieur de trois avant-projets de loi et s'est prononcée, en particulier en juillet 2008, sur un projet de loi relatif à la protection de l'identité. Celui-ci n'ayant pas été déposé sur le bureau de l'Assemblée nationale, la délibération n° 2008-306 du 17 juillet 2008 n'a pas été rendue publique.

La CNIL estime nécessaire, conformément à ses missions générales de conseil et d'information prévues par l'article 11 de la loi « Informatique et Libertés », de faire connaître son analyse en la matière. La présente note d'observations, examinée en séance plénière de la Commission le 25 octobre 2011, s'appuie tout particulièrement sur les décisions qu'elle a déjà rendues s'agissant des passeports biométriques (**délibération n°2007-368** du 11 décembre 2007), des cartes d'identité électroniques et biométriques (notamment **délibération n° 2008-306** précitée), et plus généralement en matière de biométrie, d'administration électronique et de téléservices.

La Commission rappelle que **les données biométriques ne sont pas des données à caractère personnel « comme les autres »**. Elles présentent en effet la particularité de permettre à tout moment l'identification de la personne concernée sur la base d'une réalité biologique qui lui est propre, permanente dans le temps et dont elle ne peut s'affranchir.

La nécessité de prêter une attention particulière aux données biométriques doit être renforcée lorsque la biométrie utilisée est dite « à trace », comme les empreintes digitales par exemple. Celles-ci ont en effet la particularité de pouvoir être capturées et utilisées à l'insu des personnes concernées, comme par exemple à des fins d'usurpation d'identité.

Il en est de même pour les caractéristiques du visage. En effet, si celles-ci ne donnent pas lieu à dépôt de traces, l'association entre vidéoprotection et dispositifs de reconnaissance faciale aboutit à un résultat similaire en créant des traces informatiques en lieu et place des traces physiques laissées par les empreintes digitales.

Pour approfondir : dossier

Cette spécificité des données biométriques a pour conséquence d'accroître le niveau d'exigence quant à leur utilisation. En particulier, deux principes fondateurs du droit à la protection des données à caractère personnel doivent être impérativement respectés :

- **le principe de finalité** : les traitements de données doivent poursuivre des finalités « déterminées, explicites et légitimes » (article 6-2° de la loi « Informatique et Libertés ») et les données concernées ne doivent pas être utilisées à d'autres fins que celles qui ont été définies ;

- **le principe de proportionnalité** : les dispositifs envisagés doivent être strictement proportionnés au regard des objectifs du traitement. Plus précisément, les données traitées doivent être « adéquates, pertinentes et non excessives » au regard des finalités attribuées au traitement (article 6-3°), leur durée de conservation dans le traitement ne doit pas excéder la durée nécessaire à ces finalités (article 6-5°) et elles ne doivent être rendues accessibles qu'aux destinataires ayant un intérêt légitime à les connaître.

la Commission s'est prononcée à de multiples reprises sur des projets de traitements biométriques mis en œuvre dans le cadre de la délivrance de titres d'identité ou de voyage, tout particulièrement dans le cadre de son avis sur les passeports biométriques. **La finalité du système des passeports biométriques**, autorisé par le décret n° 2005-1726 du 30 décembre 2005 modifié, est uniquement d'ordre administratif. Ce traitement a ainsi pour seul objectif de mieux sécuriser la délivrance de ces titres et en particulier de lutter contre la fraude à l'identité.

Dans son avis du 11 décembre 2007, la Commission a rappelé qu'elle a toujours considéré comme **légitime le recours à des dispositifs de reconnaissance biométrique pour s'assurer de l'identité d'une personne, dès lors que les données biométriques sont conservées dans un support individuel** exclusivement détenu par la personne concernée. **La Commission a estimé que l'introduction dans les titres d'identité et de voyage d'un composant électronique contenant des données biométriques est proportionnée par rapport à l'objectif de renforcement de la sécurité de l'établissement et de la vérification des titres**. En ce qui concerne spécifiquement les passeports, la législation européenne fait d'ailleurs obligation aux Etats membres de délivrer de tels passeports.

L'analyse de la Commission a cependant été différente en ce qui concerne la création de la base de données biométriques centralisée. la Commission a considéré que, si légitimes soient-elles, les finalités invoquées ne justifiaient pas la conservation, au plan national, de données biométriques telles que les empreintes digitales et que les traitements ainsi mis en œuvre seraient de nature à porter une atteinte excessive à la liberté individuelle.

En outre, **la proportionnalité du traitement en base centrale des empreintes digitales des demandeurs de titre a fait l'objet de réserves de la part de la Commission. La création d'une base centralisée de données biométriques de grande ampleur comporte des risques importants et implique des sécurités techniques complexes et supplémentaires.**

La CNIL a également souligné que **le recueil de huit empreintes digitales et leur conservation en base centrale ne résultaient pas des prescriptions du règlement communautaire relatif aux passeports. Un dispositif biométrique de lutte contre la fraude ne peut être pleinement efficace que si les documents d'état civil produits par les demandeurs pour se faire enregistrer dans le système sont fiables**. Or, aucune mesure particulière n'était prévue par le ministère de l'intérieur afin de sécuriser ces « documents sources ».

Au regard de l'ensemble de ces éléments, **la Commission a estimé que la conservation sous forme centralisée des huit empreintes digitales des demandeurs de passeport semblait disproportionnée au regard de l'objectif de lutte contre la fraude documentaire.**

Sur la nouvelle proposition de loi la CNIL se positionne :

La délivrance de tels documents doit cependant, selon la Commission, être assortie de garanties complémentaires. Celles-ci pourraient porter en premier lieu sur **l'âge minimal de collecte des identifiants biométriques** : pour la CNIL, la détermination de cet âge n'est **pas seulement un élément technique mais une question de principe** méritant un large débat.

La Commission estime que la comparaison entre la donnée biométrique enregistrée dans le composant et l'empreinte lue en direct sur un lecteur pourrait se faire dans la carte elle-même. La mise en œuvre de cette **technique**, dite « *match on card* », serait susceptible d'apporter une garantie supplémentaire à la protection des données à caractère personnel, en **évitant toute possibilité de copie externe**.

Dans le cadre de la proposition de loi relative à la protection de l'identité, le système projeté a pour seul objectif de mieux sécuriser la délivrance de ces titres et en particulier de lutter contre la fraude à l'identité. Dès lors, il s'agirait uniquement de créer un fichier administratif, semblable au traitement déjà mis en œuvre relatif aux passeports biométriques, et en aucun cas de constituer un outil de police judiciaire à la disposition des services de police et de gendarmerie.

Il convient cependant de **s'assurer que le traitement créé ne peut être utilisé à d'autres fins** que la sécurisation de la délivrance des titres d'identité et de voyage, par exemple en le prévoyant expressément dans la loi. De même, l'interdiction de procéder à l'interconnexion avec tout autre traitement de données à caractère personnel, à l'exception des fichiers de passeports et de cartes d'identité volés ou perdus, pourrait être prévue dans le texte de la proposition de loi.

Il conviendrait également de **s'assurer qu'un tel système ne soit pas détourné de sa finalité** par un recours systématique aux réquisitions judiciaires, qui sont possibles sur tout traitement de données à caractère personnel, en application des dispositions du code de procédure pénale.

En ce qui concerne la proportionnalité de cette base centrale d'éléments biométriques, la Commission relève qu'il **existe des modalités de lutte contre la fraude qui apparaissent tout à la fois efficaces et plus respectueuses de la protection de la vie privée des personnes**, en particulier celles qui s'attachent à sécuriser les « documents sources » à produire pour la délivrance de titres d'identité.

Dans ces conditions, la Commission estime, tout comme dans le cadre de son avis sur le projet de loi présenté en 2008 par le ministère de l'intérieur, que **la proportionnalité de la conservation sous forme centralisée de données biométriques, au regard de l'objectif légitime de lutte contre la fraude documentaire, n'est pas à ce jour démontrée**.

Si une telle base centralisée de données biométriques était néanmoins envisagée, des garanties supplémentaires de nature à assurer la protection des données personnelles des citoyens français devraient être introduites.

Sur la possibilité de mettre en œuvre des dispositifs de reconnaissance faciale, la Commission considère que la mise en œuvre par l'Etat de dispositifs de reconnaissance faciale des personnes présente des risques importants pour les libertés individuelles, notamment dans le contexte actuel de multiplication du nombre des systèmes de vidéoprotection, de leur interconnexion et de leur interopérabilité.

Sur les fonctions électroniques de la carte nationale d'identité, **de telles fonctions électroniques appellent des garanties particulières, dans la mesure où elles pourraient permettre la constitution d'un identifiant unique pour tous les citoyens français ainsi que la constitution d'un savoir public sur les agissements privés**. C'est pourquoi le dispositif projeté doit empêcher la collecte excessive de données, le suivi des personnes sur internet ainsi que l'usurpation de l'identité numérique.

Enfin, des mesures techniques de nature à garantir l'absence de constitution d'un identifiant unique (la création d'identifiants sectoriels spécifiques à chaque prestataire) ainsi que la sécurité des communications entre la carte d'identité et les lecteurs d'une part, entre la carte, les fournisseurs de téléservices et le tiers certificateur d'autre part, devraient également faire l'objet de spécifications techniques détaillées.

Proposition du Sénat

Suite aux recommandations de la CNIL, une proposition visant à limiter l'usage des techniques biométriques, texte n° 361 (2013-2014) de M. Gaëtan GORCE et plusieurs de ses collègues, a été déposée au Sénat le 12 février 2014. Suite aux travaux de la commission des lois et à la revue en séance publique, un texte a été adopté par le Sénat (n° 124 (2013-2014)) et déposé Texte adopté par le Sénat en Séance publique le 27 Mai 2014 :

Article 1er

Après le II de l'article 25 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, il est inséré un II bis ainsi rédigé :

« II bis. - Pour l'application du 8° du I, ne peuvent être autorisés que les traitements dont la finalité est la protection de l'intégrité physique des personnes, la protection des biens ou la protection d'informations dont la divulgation, le détournement ou la destruction porterait un préjudice grave et irréversible et qui répondent à une nécessité excédant l'intérêt propre de l'organisme les mettant en œuvre. »

Article 2 (nouveau)

Les responsables de traitements de données à caractère personnel dont la mise en œuvre est régulièrement intervenue avant l'entrée en vigueur de la présente loi disposent, à compter de cette date, d'un délai de trois ans pour mettre leurs traitements en conformité avec les dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dans leur rédaction issue de la présente loi.

Les dispositions de la loi n° 78-17 du 6 janvier 1978 précitée, dans sa rédaction antérieure à la présente loi, demeurent applicables aux traitements qui y étaient soumis jusqu'à ce qu'ils aient été mis en conformité avec les dispositions de la loi n° 78-17 du 6 janvier 1978 précitée, dans leur rédaction issue de la présente loi, et, au plus tard, jusqu'à l'expiration du délai de trois ans prévu au premier alinéa du présent article.

Ce texte, n° 1972, a été transmis à l'Assemblée nationale le 27 mai 2014. Il n'y a pas encore d'information sur la lecture de ce texte par l'Assemblée Nationale.

eSignature

■ eIDAS

Source, Février 2015 :

Après 15 ans d'application de la directive 1999/93/CE sur la signature électronique, le législateur Européen a estimé que cette directive était insuffisante, suite au constat notamment que l'Union Européenne ne disposait encore d'aucun cadre transnational et intersectoriel complet de nature à garantir des échanges électroniques sûrs, fiables et aisés, qui recouvre tant l'identification et l'authentification électroniques que les services de confiance autres que la signature électronique.

Pour combler cette lacune, ce législateur a adopté le 23 juillet 2014 **le règlement (applicabilité directe qui permet une harmonisation plus efficace) n° 910/2014** sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, qui abroge par la même occasion la directive 1999/93/CE.

L'objectif principal de ce Règlement consiste à mettre en place un cadre juridique en vue de susciter la confiance accrue dans les transactions électroniques au sein du marché intérieur. S'il est vrai que ce règlement abroge la directive de 1999, il en reprend néanmoins la plupart de ses dispositions, moyennant quelques modifications, et complète celles-ci par de nouvelles dispositions relatives, d'une part, à la reconnaissance mutuelle au niveau de l'UE des schémas d'identification électronique notifiés et, d'autre part, aux services de confiance complémentaires à la signature électronique (le cachet, « sceau » électronique sécurisé dédié aux personnes morales, l'horodatage et le service d'envoi recommandé électroniques ainsi que l'authentification de site Internet).

Désormais, les règles applicables au sein de l'Union européenne seront les mêmes pour tous et d'application directe en droit national. Les prestataires et utilisateurs ne devraient généralement plus être confrontés à des différences entre les législations nationales, à des différences dans la qualité des contrôles ou à des spécificités nationales dans le domaine des services publics. Les EM sont tenus de reconnaître les moyens d'identification électronique notifiés conformément au Règlement. Ils sont également tenus d'accepter les services de confiance « qualifiés » et de leur reconnaître les effets juridiques consacrés par le Règlement.

Le Règlement prévoit que, si on utilise une signature électronique « *qualifiée* » (signature créée par des dispositifs logiciels (de cryptologie par exemple) et/ou matériels (une carte à puce par exemple) eux-mêmes qualifiés), son effet juridique est équivalent à celui d'une signature manuscrite. Le Règlement ne va pas plus loin dans l'harmonisation. En d'autres mots, il appartient au droit national de définir l'effet juridique produit par la signature manuscrite, et donc celui de la signature électronique qualifiée, effet qui peut varier d'un EM à l'autre…

Le Règlement est entré en vigueur le 17 septembre 2014, à savoir le vingtième jour suivant sa publication le 28 août 2014 au Journal Officiel de l'Union européenne. Ceci étant, il faudra attendre le 1er juillet 2016 pour observer d'un point de vue concret les changements fondamentaux apportés par le Règlement.

Ce règlement apparaît plus comme une boîte à outils juridique à disposition des prestataires et utilisateurs que comme un instrument contraignant incontournable. Il crée un cadre qui stimule tant l'innovation que l'offre de services de confiance et l'utilisation de moyens d'identification électronique. Enfin, il établit un système présentant un niveau de sécurité technique et juridique élevé, contribuant à renforcer la confiance des utilisateurs.

Loi sur le terrorisme (surnommée LOPPSI 3)

Adoptée par l'Assemblée Nationale le 29 octobre 2014, le projet de loi est définitivement adopté le 4 novembre 2014 par le Parlement, par un ultime vote du Sénat. La loi est promulguée le 13 novembre 2014. Articles relatifs aux données informatiques, et par extension, aux données personnelles et donc à l'identité numérique :

Art.10 et 11 Des perquisitions dans le *cloud* et des déchiffrements facilités

Avec cet article, la police ou la gendarmerie vont plus facilement pouvoir effectuer des perquisitions dans le « *cloud* » depuis leurs locaux. Jusqu'à présent, ces procédures étaient possibles, mais uniquement depuis le lieu d'une perquisition physique. Si les données dans le *cloud* sont protégées, pas de problème. Les officiers de police judiciaire pourront requérir toute personne susceptible d'avoir connaissance des mesures appliquées pour les verrouiller. Elles devront leur remettre les informations permettant d'accéder à ces informations. Si elles ne répondent pas, elles seront susceptibles de se voir infliger une amende de 3 750 euros (Ces mesures sont déjà en partie effectives).

Dans le même sens, l'article 11 compte bien faciliter la mise au clair des informations chiffrées. Un officier de police judiciaire, sur autorisation du juge d'instruction ou du procureur, pourra désormais directement faire appel à une personnalité qualifiée pour espérer obtenir ces informations.

Art. 11 bis Le vol de données informatiques est adopté

L'art. 11 bis est adopté également. Ajouté en Commission des lois, il compte sanctionner désormais le vol de données en cas de piratage informatique. Plutôt que vol, supposant la soustraction d'une chose plutot que sa copie, le texte va punir celui qui détient, extrait, reproduit ou transmet une donnée acquise suite à la pénétration dans un système informatique. Le rapporteur et député PS Sébastien Pietrasanta profite de ce texte sur le terrorisme pour augmenter l'échelle des peines en matière de piratage informatique. Accéder ou se maintenir, frauduleusement, dans un système informatisé sera puni de deux ans de prison et 100 000 euros d'amende (contre 30 000 euros actuellement). Extraire, simplement détenir, reproduire ou transmettre, supprimer ou modifier une donnée vaudra à son auteur jusqu'à 3 ans de prison, 375 000 euros d'amende (contre 45 000 euros aujourd'hui). Entraver ou fausser le fonctionnement d'un système, en introduisant par exemple frauduleusement des données, sera sanctionné de 5 ans de prison et 500 000 euros d'amende (contre 75 000 euros d'amende actuellement). Si le système visé est mis en œuvre par l'État, l'échelle restera à 7 ans de prison, mais passera à 750 000 euros d'amende, contre 100 000 aujourd'hui.

Quand ces infractions informatiques auront lieu en bande organisée, la peine sera portée à 10 ans d'emprisonnement et 1 million d'euros d'amende. Ce régime sera également activable en cas d'importation, détention, offre, cession, mise à disposition d'un outil dédié au piratage informatique, non justifié par la recherche ou la sécurité informatique.

Art. 13 Généralisation des enquêtes sous pseudonyme

Cet article généralise les enquêtes sous pseudonyme pour toute une série d'infractions graves. Ils pourront alors participer sous un pseudonyme aux échanges électroniques, entrer en contact avec les personnes susceptibles d'être les auteurs de ces infractions, récupérer des éléments de preuves, sans pouvoir cependant inciter les personnes contactées à commettre ces infractions.

Art. 15 Le délai d'effacement dans les interceptions de sécurité étendu à 30 jours

L'article 15 étend le délai d'effacement des données glanées lors d'une interception de sécurité. Normalement, ces enregistrements doivent être détruits dans les 10 jours. Bernard Cazeneuve veut porter ce délai maximal à 30 jours. Précisons que les retranscriptions sont conservées aussi longtemps que nécessaire. C'est le premier ministre qui donne son feu vert à ces procédures sur demande motivée du ministre de l'Intérieur, du budget ou celui de la défense. Les demandes sont motivées par la volonté de glaner des renseignements touchant la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, la prévention du terrorisme, la prévention de la criminalité et de la délinquance organisées ou la prévention de la reconstitution ou du maintien de groupements dissous.

Mort numérique

Source CNIL, 31 octobre 2014 : Mort numérique ou éternité virtuelle : que deviennent vos données après la mort ?

De nombreux internautes s'interrogent sur le devenir des données concernant leurs proches ou eux-mêmes après la mort. C'est dans ce contexte qu'a émergé le concept de « mort numérique », potentiellement porteur d'interrogations juridiques mais également sociétales.

Sensible à la dimension humaine de cette thématique et soucieuse d'assurer une protection effective de l'identité individuelle, la CNIL ouvre le débat des enjeux de la mort numérique.

Le développement de nouveaux modes d'exposition de soi en ligne a conduit à faire vivre son identité après la mort de multiples façons : il peut s'agir d'entretenir le souvenir d'un défunt, de créer un avatar qui dialoguera avec les vivants ou de laisser des messages ainsi que des biens dématérialisés (fleurs ou bougies) à ses héritiers ou ses proches.

Ainsi, de nombreux sites proposent de faire vivre la personne après la mort, de rendre visible sa dernière « demeure » sur la toile, de proposer une tombe virtuelle, d'organiser un testament numérique ou enfin, de gérer ses identités numériques post-mortem.

Dès lors, comment concilier le droit à l'oubli numérique et les possibilités d'atteindre l'éternité numérique offertes par la vie en ligne ? D'ici quelques années, la majorité des personnes décédées se sera dotée d'une identité numérique post-mortem.

En effet, à défaut d'effacement programmé par la personne concernée, le profil d'un défunt continue d'exister, d'être visible sur la toile et d'être référencé par les moteurs de recherches.

■ Mort sous l'angle « Informatique et libertés »

Que les données concernent des personnes vivantes ou des personnes décédées, la CNIL, interlocuteur naturel des internautes en matière de protection des données personnelles, veille à ce que l'informatique ne porte atteinte, ni à l'identité du défunt, ni à la vie privée de ses héritiers.

Sur le plan de la loi Informatique et Libertés, la question de la mort numérique invite à s'interroger sur la prise en compte par les réseaux de la mort d'une personne, mais également sur le respect de ses droits ainsi que sur leur application effective par ses héritiers.

Les droits d'accès, de modification, et de suppression prévus par la loi sont des droits personnels qui s'éteignent à la mort de la personne concernée. La loi ne prévoit pas la transmission des droits du défunt aux héritiers : un héritier ne peut donc, sur le fondement de la loi Informatique et Libertés, avoir accès aux données d'un défunt. La loi autorise toutefois les héritiers à entreprendre des démarches pour mettre à jour les informations concernant le défunt (enregistrement du décès par exemple).

Pourtant, les familles des personnes disparues qui s'adressent à la CNIL veulent pouvoir accéder aux données concernant le défunt, ou exigent au contraire leur suppression. Dans ce contexte souvent douloureux, la Commission fait face à des problématiques aussi bien techniques que juridiques. Chargée de veiller au respect des durées de conservation des données conformément à la finalité poursuivie, elle s'intéresse à l'effacement, la suppression, le déréférencement ou la désindexation des données des personnes décédées.

Toutefois, la prise en compte de l'intérêt des héritiers n'est pas évidente en l'absence d'expression de la volonté du défunt. Afin de pallier cette carence, les grands acteurs de l'Internet, tels Google et Facebook proposent désormais des fonctionnalités permettant de paramétrer « la mort numérique ».

■ Enjeux de la régulation de la mort numérique

L'encadrement juridique de la mort numérique ne devrait pas reposer sur les seules conditions générales d'utilisation des sites, d'autant plus que de nombreuses questions n'ont parfois pas de réponses.

Dans quelles conditions les héritiers peuvent-ils récupérer les données du défunt ? Si rien n'est prévu dans les conditions générales d'utilisation des sites, quels sont les héritiers qui pourront demander la mise à jour ou la suppression des données ? Comment résoudre les conflits entre des héritiers qui n'ont pas toujours la même perception de la volonté post-mortem du défunt (si un héritier souhaite accéder aux données alors qu'un autre souhaite les supprimer) ?

La Commission a été invitée à plusieurs reprises à se prononcer sur le cadre juridique de la conservation et l'archivage des données des personnes décédées, sur leur accessibilité et leur réutilisation.

Cependant la régulation de la mort numérique ne se limite pas à la seule protection des données personnelles des défunts ou de la vie privée de leurs ayants-droits. Le droit des contrats ainsi que le droit des successions devront sans doute évoluer pour répondre à ces nouveaux besoins exprimés par les utilisateurs et anticiper la problématique de la mort en ligne.

À la veille de l'adoption d'un règlement européen consacrant de nouveaux droits (le droit à l'oubli ou le droit à la portabilité des données), il semble nécessaire d'introduire dans les débats la question de la prise en compte de la mort par les réseaux sociaux et ses conséquences pour les personnes.

La CNIL n'ayant pas vocation à arbitrer l'équilibre qui doit être trouvé entre les besoins de suppression de toutes traces de l'identité après la mort, et la volonté d'atteindre l'immortalité numérique en continuant à faire vivre l'identité au-delà de la mort.

Cependant, il apparaît essentiel que les autorités de protection des données, en concertation avec les pouvoirs publics, les professionnels de l'Internet, les acteurs de la société civile et les citoyens, ouvrent la discussion sur ce sujet qui tend à devenir une problématique incontournable de « l'âge numérique ».

SOLUTIONS TECHNIQUES

BYOID (*Bring Your Own IDentity*)

Dès le début des années 70[1] avec l'arrivée des premiers systèmes multi-utilisateurs, le problème de l'authentification se posa en informatique. Ce problème fût à l'époque solutionné par la création du couple utilisateur/mot de passe qui permet, sur la base d'un identifiant unique (le nom d'utilisateur ou login) public, connu de tous les autres utilisateurs et d'un secret (le mot de passe). Cependant avec l'expansion de la micro-informatique en entreprise ayant abouti à la création de nombreuses applications spécialisées (il n'est pas rare pour les grandes entreprises d'avoir plusieurs centaines d'applications mises à disposition des utilisateurs et s'exécutant sur des serveurs) et l'avènement d'internet avec sa myriade de sites web, le système du couple utilisateur/mot de passe est mis à mal.

En effet ce système souffre de plusieurs faiblesses structurelles :

1) Il est difficile de retenir un grand nombre de secrets. Du fait du nombre grandissant de couples utilisateur/mot de passe à retenir, nombre d'utilisateurs utilisent très fréquemment le même secret à plusieurs endroits ce qui fait mécaniquement diminuer la valeur du secret. En effet tout piratage de l'un des sites ou toute divulgation du secret permet l'usurpation des accès sur l'ensemble des sites. Cette faiblesse a également vu l'arrivée de comportements déviants consistant à noter ses identifiants (couple utilisateur/mot de passe) sur un support tiers (cahier, agenda, fichier texte, …) ;

2) Les mots de passe utilisés sont souvent triviaux. Nombre d'utilisateurs ayant peu conscience de la valeur du secret de leurs identifiants choisissent généralement un secret trivial. Cet état de fait fût porté à l'attention du grand public dès 1995 avec le film « *Hackers*[2] » de Lain Softley qui mettait en avant les 4 mots de passes les plus utilisés de l'époque (*secret, sex, love et god*). Cette faiblesse, désormais utilisée par tous les logiciels de cassage de mot de passe qui permettent d'utiliser des dictionnaires de mot de passes (pouvant contenir plusieurs centaines de milliers de mot de passe) afin de diminuer le temps nécessaire à la révélation du mot de passe ;

[1] Sortie en 1972 le système HP 3000 est considéré comme le premier système multi-utilisateur
[2] Film sorti en 1995 également connu sous le titre francophone « Hackers : Les Pirates du cyberespace »

3) Il est possible de partager son secret avec un tiers et par là même son identité. Que ce soit de façon volontaire (partage du secret avec une tierce personne) ou involontaire (piratage du mot de passe, capture des touches du clavier, …), il est possible avec ce système pour un tiers de prendre l'identité d'un utilisateur.

En dépit de ses faiblesses le système utilisateur/mot de passe est encore le plus utilisé. Néanmoins afin de réduire ses faiblesses, différents dispositifs techniques et organisationnels peuvent être mise en place :

- Changement régulier du secret (mot de passe). Cette pratique, que certains attribuent au « mot de semestre » de la franc-maçonnerie, vise à limiter la valeur du secret et donc de l'exposition de la prise d'identité dans le temps. Effet sur les premiers systèmes UNIX l'empreinte résultant de la transformation du mot de passe par la fonction de hachage était connu de tous les utilisateurs. Il était donc possible de trouver l'ensemble des mots de passe du système avec un temps suffisamment long ;
- Complexité de mot de passe renforcé. De nombreux systèmes et sites web sont désormais équipés de mécanismes permettant de renforcer la robustesse du mot de passe. Ces derniers vous obligent en général à créer un mot de passe de plus de 8 caractères contenant des caractères alphanumériques ainsi que des éléments de ponctuation ;
- Utilisation de deux facteurs d'authentification. Ce changement de paradigme permet de ne plus faire reposer l'identification sur le seul secret en y ajoutant généralement la possession d'un objet (Carte à puce, token, SMS reçu sur téléphone, …). Ce type de mécanisme est notamment utilisé pour les cartes bancaires disposant de puce, où la carte est l'objet possédé et le code à 4 chiffres le secret.

Les outils d'authentification uniques, dit de « *Single Sign-On* » (SSO), ont émergé afin d'améliorer l'expérience utilisateur (ayant beaucoup de mots de passe différents à retenir au sein d'un même système d'information). Ces outils permettent à un utilisateur d'accéder à plusieurs systèmes, applications ou sites web à partir d'une même base d'authentification et ne nécessitent qu'une seule et unique authentification pour avoir accès à l'ensemble des ressources. Bien qu'améliorant l'expérience utilisateur en prévenant un rejet de la sécurité liée à des contraintes d'identification trop fortes et par là même réduisant les risques d'utilisation de mot de passe faible et de partage intra-applicatif, ces outils augmentent l'impact de la perte du mot de passe. En effet si les identifiants sont connus d'un tiers, ce dernier aura alors accès à un grand nombre de ressources (Cet aspect est régulièrement mentionné sous la formulation : « il a les clés du château »).

Ce paradoxe d'augmentation et de réduction des risques est généralement adressé par la mise en place de mots de passe plus complexes ou de mécanismes d'authentification multi-facteurs.

La complexification de la gestion des identités (incluant l'authentification), devenue un maillon essentiel du développement d'Internet qui propose de plus en plus de services payants et/ou réservés à des membres, a poussé l'émergence de nouveaux services de fédération des identités également appelés « *Bring Your Own IDentity* » (en référence au « *Bring Your Own Device* » sorti à la même période).

La plupart des grands acteurs web fournissent désormais des services de délégations d'identités qui offrent les avantages suivants aux applications/sites qui les mettent en place :

- La gestion du mécanisme d'authentification (parfois multi-facteur) est à la charge du fournisseur d'identité, ce qui permet la mise en place d'un accès à la sécurité renforcé sans besoin lourd de déploiement ;
- Les systèmes mis en place offrent pour la majorité des fonctionnalités semblables aux services de SSO, ce qui permet à l'utilisateur de s'authentifier une seule fois pendant une période donnée sur l'ensemble des applications/sites web ;
- En plus du système d'authentification, certains fournisseurs proposent des API (Interfaces de programmation) supplémentaires permettant d'utiliser directement leurs services sur le site web du client.

En sus des protocoles de délégation décrits dans la partie V.3.3 (Fédération d'identité), majoritairement utilisés par des acteurs de taille importante, la délégation d'authentification s'effectue généralement au travers des API de délégation suivantes :

- OAuth en passe de devenir un standard communément mis en place par les différents grands acteurs du marché. Ce protocole est soutenu par la fondation OpenSocial regroupant Google, LinkedIn, Hi5, Orkut, Friendster, Viadeo, MySpace, Netlog, VZ.net, Yahoo!;
- AuthSub mis en place par Google ;
- BBAuth (*Browser-Based Authentication*) mis en place par Yahoo!;
- Facebook Auth mis en place par Facebook ;
- FlickrAuth mis en place par Flickr ;
- OpenAuth mis en place par AOL ;
- Windows Live ID mis en place par Microsoft.

Dans une interview, Edward Snowden révélait que la plupart des mots de passe de 8 caractères (standard actuel communément admis comme fiable) pouvait être cassés très rapidement par la NSA. Cette révélation met à mal une fois de plus la viabilité à long terme du couple identifiant/mot de passe, et la gestion individuelle de ce dernier au profit de fournisseur d'authentification pour l'ensemble des acteurs d'Internet. Néanmoins l'utilisation de la délégation d'authentification au sein des réseaux d'entreprise doit être sérieusement étudiée (doit-on donner les « clés du château » et la machine pour les produire à un tiers ?) avec une analyse de risque avant d'être mise en place.

Méthodes d'identification

L'authentification reste une des questions les plus importantes de l'identité numérique, simplement parce que c'est par là que tout commence.

L'authentification vise à vérifier l'identité dont une entité (personne ou machine) se réclame. L'authentification est toujours précédée ou combinée avec une identification qui permet à cette entité de se faire reconnaître du système par un élément dont on l'a doté : un identifiant.

En résumé, s'identifier c'est communiquer un identifiant présumé, s'authentifier c'est apporter la preuve que l'entité s'est vue attribuer cet identifiant.

L'authentification vise soit :

- à contrôler l'accès à des informations, des locaux, plus généralement des biens, d'un système d'information, en étant dans ce cas associée à une fonction d'attribution de privilèges particuliers liés à l'identité ;
- à garantir une imputabilité avec vérification forte de l'identité affichée, par exemple pour la journalisation d'actions, la facturation, l'authentification de données, etc. ;
- à assurer une combinaison de ces fonctions d'attribution de privilèges et d'imputations.

Dans tous les cas, l'utilisation de mécanismes d'authentification sûrs est nécessaire à la réalisation de ces objectifs.

La phase de vérification fait intervenir un protocole d'authentification. On en distingue trois sortes :

- L'authentification simple : l'authentification ne repose que sur un seul élément ou « facteur » ;
- L'authentification forte : l'authentification repose sur deux facteurs ou plus ;
- L'authentification unique : (Single Sign-On ou SSO) permet à un utilisateur de ne procéder qu'à une seule authentification pour accéder à plusieurs services informatiques.

■ Authentification simple

Classiquement, les systèmes utilisent un mode d'authentification simple impliquant l'utilisation d'un des trois composants suivants :

Ce que l'entité connaît : Cette technique d'authentification se base sur une information ou chaîne d'informations, qu'en principe, seul l'entité connaît (mot de passe, code PIN, phrase-clé, date d'un fait marquant, etc.…

Cette méthode d'authentification a montré ses limites :

On connait les conseils qui prévalent classiquement dans ce domaine. Une rapide recherche sur Google fait remonter les conseils suivants :

- Taille minimum : au moins 8 caractères ;
- Ne pas utiliser de mots issus d'un dictionnaire ;
- Mixer chiffres, lettres et symboles spéciaux ;

Ces conseils ne sont pas mauvais et restent valables. Mais la technologie et les techniques utilisées par les pirates n'ayant de cesse de se perfectionner, ils ne sont plus suffisants.

De plus la multiplicité des comptes utilisateurs que nous possédons nous pousse a réutiliser les mêmes identifiants et parfois le même mot de passe sur plusieurs sites.

Cette réutilisation d'identifiants est un risque très important car elle fait dépendre la sécurité de notre vie digitale du maillon le plus faible. En effet, imaginons que j'aie les mêmes identifiants sur Gmail et sur un site de commerce électronique, lambda.com : si les informaticiens de lambda.com ne sont pas très consciencieux, que le site se fait pirater, mon mot de passe peut être découvert. Et voilà des hackers en possession de l'identifiant et du mot de passe de mon compte Gmail !

Ce que l'entité détient : Cette technique se base sur la présentation d'un composant que seul l'utilisateur possède (une clé magnétique, une clé USB, un PDA, une puce (RFID, carte), un smartphone, un token : générateur de mot de passe synchronisé).

Le risque de ce genre de facteur d'authentification vient du fait qu'il est sujet à la perte, ou pire, au vol.

Ce que l'entité est : la Biométrie. Le terme biométrie se réfère à toute caractéristique physique qui permet d'authentifier un individu en tant que personne (empreinte digitale, rétinienne, palmaire, forme du visage, caractéristiques de la voix, etc.).

L'un des freins au développement de la généralisation de la biométrie n'est autre que son coût. Les systèmes de reconnaissance biométriques fiables représentent un investissement conséquent.

Aucun label CNIL n'a été développé autour des matériels biométriques.

Certains problèmes viennent du fait :

- que les données biométriques ne sont pas confidentielles ;
- qu'il est impossible de les modifier en cas de compromission.

Il s'avère que le corps subit, comme tout organisme vivant, de légères modifications : on vieillit, on subit des traumatismes. Dans ce cas, les mesures changent. Les fabricants cherchent ainsi à diminuer le taux de faux rejets tout en maintenant au plus bas les taux de fausses acceptations.

Cette authentification à un facteur n'offre plus le niveau de sécurité requis pour assurer la protection de biens informatiques sensibles. Elle est sujette a de nombreuses attaques, attaque par force brute, attaque par dictionnaire, écoute du clavier informatique (*keylogger*), par voie logicielle (cheval de troie...), écoute du réseau lorsque le protocole utilisé est dépourvu de chiffrement (http, telnet , ftp, LDAP, etc ..), Hameçonnage (*phishing*), etc.

■ Authentification forte

Le principe de l'authentification forte est de combiner l'utilisation d'au moins deux facteurs d'authentification de nature distinctes afin de rendre la tâche plus compliquée à un éventuel attaquant.

On peut considérer que l'authentification forte est une des fondations essentielles pour garantir :

- L'autorisation ou contrôle d'accès (qui peut y avoir accès) ;
- La confidentialité (qui peut le voir) ;
- L'intégrité (qui peut le modifier) ;
- La traçabilité (qui l'a fait).

Les solutions technologiques les plus courantes permettant une authentification forte sont les suivantes :

Mot de passe à usage unique/One Time Password (OTP)

Cette technologie est fondée sur un secret partagé unique. Grâce au partage de ce dénominateur commun, il est alors possible de générer des mots de passe à usage unique (*One-Time-Password*). Du fait que ce type de technologie utilise un secret partagé, il n'est pas possible d'assurer la non-répudiation. La plupart du temps ce mode d'authentification est couplé à un mot de passe, ou code PIN, permettant la génération du mot de passe unique.

OTP préétablis :

La liste à rayer ou TAN (*Transaction Authentication Number*). Il s'agit de rentrer un OTP (*One-Time Password*) provenant d'une liste de codes fournie par exemple par la banque. Cette liste est considérée comme un authentifieur.

Matrix card authentication ou authentification à carte matricielle. Il s'agit de rentrer un OTP provenant d'une carte matricielle fournie. Ce système utilise les coordonnées en Y et en X. La carte matricielle est considérée comme un authentifieur.

Utilisation des SMS. Ce système utilise la technologie des SMS. L'utilisateur reçoit un OTP directement sur son téléphone portable. Le téléphone portable est considéré comme un authentifieur.

Mot de passe à usage unique fondé sur le temps

Cette méthode utilise, en plus du secret partagé, un dénominateur commun qui est le temps. Chaque partie est synchronisée sur le temps universel (UTC). On utilise alors un Code PIN comme deuxième facteur d'authentification. Ces authentifieurs sont définis comme une technologie dite synchrone. Chaque minute, par exemple, un nouveau « ***Token Code*** » sera affiché, le *One Time Password*.

L'exemple le plus connu est SecurID de la société RSA Security.

Certificat numérique

Un certificat numérique peut être vu comme une carte d'identité numérique. La grande force du certificat est qu'il peut servir à :

- Identifier et authentifier une personne physique ou morale ;
- Echanger des clés de chiffrement pour sécuriser des échanges ;
- Signer un document électronique.

Le chiffrement

Le principe du certificat repose sur l'utilisation d'algorithmes de chiffrement asymétriques utilisant une paire de clefs, l'une publique, l'autre privée.

Dans ce cas, la clef de chiffrement est différente de la clef de déchiffrement.

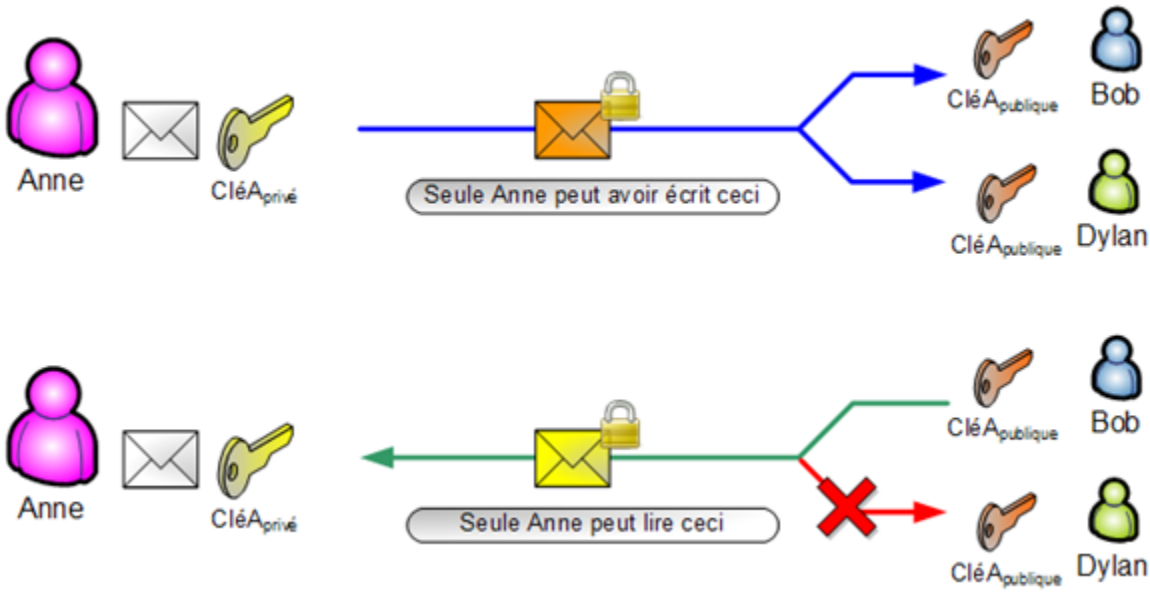


Figure 1: Chiffrement asymetrique

La signature électronique

La signature électronique repose sur l'utilisation successive d'une fonction de hachage et de chiffrement asymétrique.

Une fonction de hachage permet de convertir une chaîne de caractères de longueur quelconque en une chaîne de caractères de taille fixe. Cette chaîne de caractères de taille fixe est appelée empreinte.

La fonction de hachage doit fournir une unique empreinte. Dans les faits, il est impossible d'obtenir une empreinte unique sachant que l'empreinte est de taille fixe inférieure à celle de la chaine initiale. Néanmoins une bonne implémentation d'une fonction de hachage tend à viser ce résultat.

La fonction doit également permettre le calcul rapide de l'empreinte à partir d'un texte initial.En revanche, il est impossible de retrouver le texte à partir de son empreinte.

Chiffrer un document avec une clé privée engendre une signature numérique du document, car seul le propriétaire de la clef privée a été capable de le chiffrer. La signature est infalsifiable car c'est la clef privée qui l'a générée au moment de la signature. La signature n'est pas réutilisable car elle fait partie intégrante du document. Le document est immuable car la moindre falsification sur le document provoquerait une erreur lors du déchiffrement de celui-ci. Cependant, au lieu de signer le document lui-même, il est préférable de signer l'empreinte du document car elle est de taille fixe et comme les chances d'avoir deux documents différents ayant la même empreinte est très faible, signer l'empreinte est aussi fiable que de signer le document tout entier.

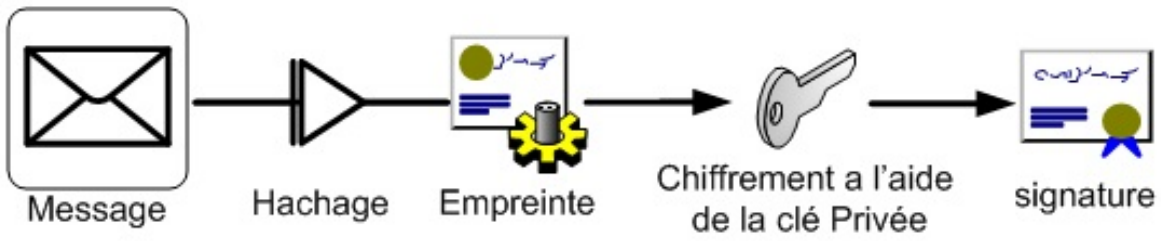


Figure 1: Chiffrement asymetrique

Pour vérifier l'identité de l'émetteur, il suffit de calculer, à partir du document original, l'empreinte par la fonction de hachage et de déchiffrer la signature de l'émetteur avec sa clef publique. Si les deux empreintes sont identiques, alors nous avons vérifié l'identité de l'émetteur et par la même occasion, l'intégrité du document.

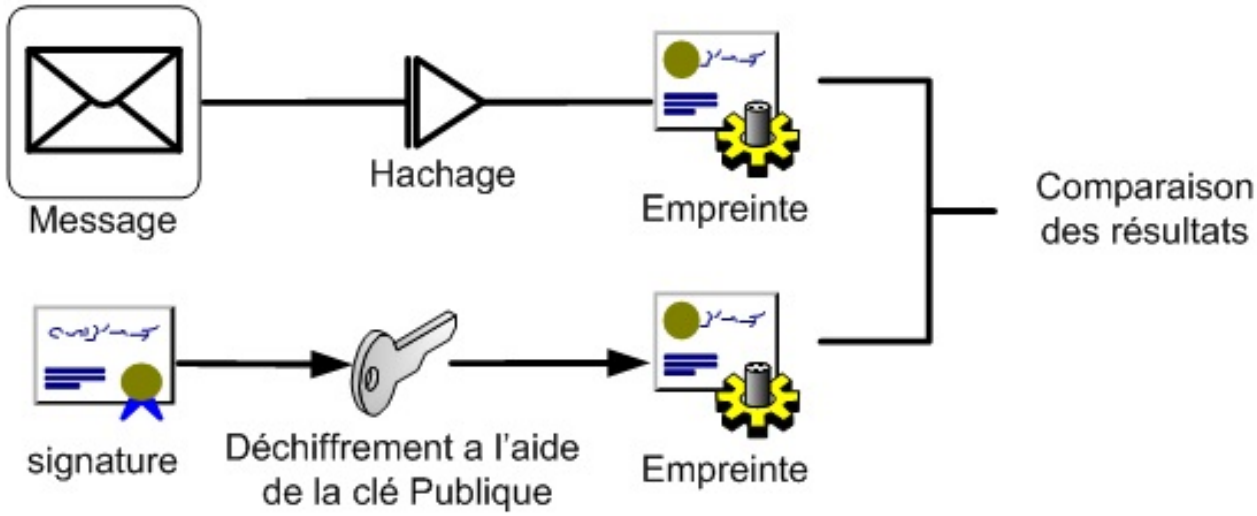
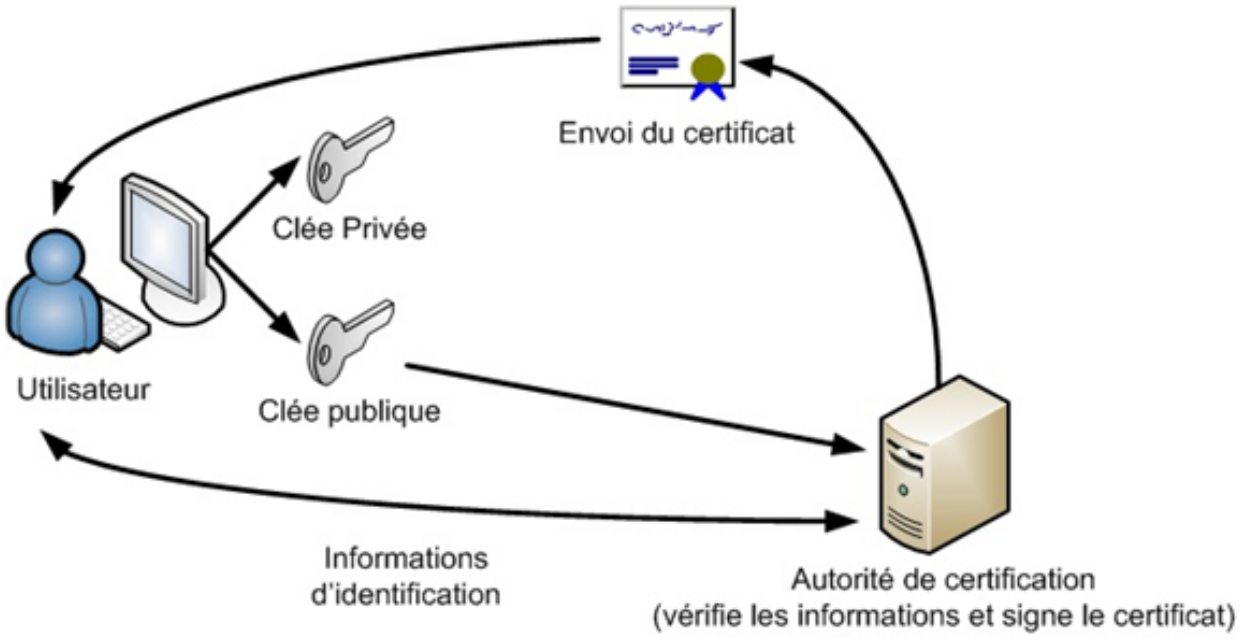


Figure 3: Vérification de l'identité et de l'intégrité

La structure du certificat

Un certificat électronique est un ensemble de données contenant :

- Au moins une clé publique ;
- Des informations d'identification (nom, date de naissance, adresse mail, etc...) ;
- Au moins une signature, apposée par une autorité permettant de prêter confiance à l'exactitude des informations du certificat.



Les certificats électroniques sont l'une des mises en œuvre de la signature électronique. Ils permettent d'authentifier l'émetteur d'un document, d'un message ou d'une transaction électronique. Il fait intervenir un tiers de confiance (nommé Autorité de Certification, ou AC) qui, sur réception d'une demande de certificat, vérifie que la clef publique de l'émetteur correspond bien à son identité. Ensuite, l'AC crée un certificat (généralement au format X.509) contenant des informations d'identité sur l'émetteur et sur elle-même, puis signe ce certificat.

■ Authentification unique

Le principe de l'authentification unique (*Single Sign On*) repose sur la gestion centralisée de l'authentification. Les différents fournisseurs de services délèguent à un système tiers l'authentification des utilisateurs. Une fois reconnu par le système une première fois, ces derniers disposent d'un accès libre à toutes les applications ayant intégré des fonctions de SSO.

Les objectifs sont multiples :

- simplifier pour l'utilisateur la gestion de ses mots de passe : plus l'utilisateur doit gérer de mots de passe, plus il aura tendance à utiliser des mots de passe similaires ou simples à mémoriser, abaissant par la même occasion le niveau de sécurité que ces mots de passe offrent face aux risques de piratage ;
- simplifier la gestion des données personnelles détenues par les différents services en ligne, en les coordonnant par des mécanismes de type méta-annuaire ;
- Renforcer la sécurité du système car elle permet aux sites partenaires, susceptibles d'utiliser des systèmes potentiellement faillibles, de déléguer l'authentification d'un utilisateur au système d'authentification forte, centralisé et maitrisé par le SI de l'organisme ;
- Possibilité d'étendre facilement les services offerts : gestion des mots de passe, fédération, contrôle d'accès, transmission d'informations de session.

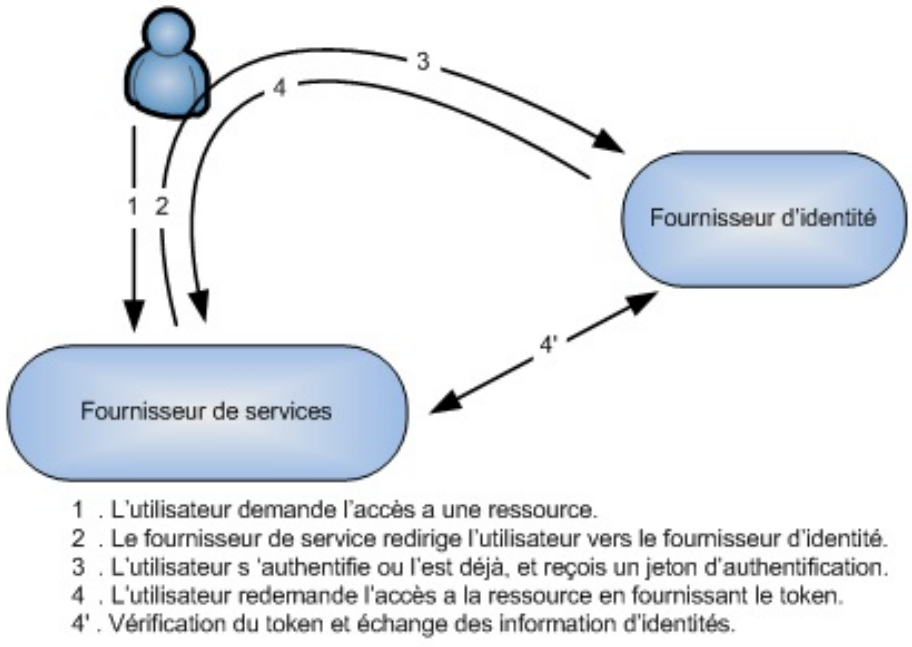


Figure 4: fédération d'identité

Comme SSO donne accès à de nombreuses ressources une fois l'utilisateur authentifié (il a les « clés du château »), les pertes peuvent être lourdes si une personne mal intentionnée a accès aux informations d'identification des utilisateurs. Avec l'authentification unique, une attention particulière doit donc être prêtée à ces informations, et des méthodes d'authentification fortes doivent être combinées (par exemple, l'usage d'une carte à puce).

Solution logicielle

Elle consiste à télécharger le certificat directement sur un périphérique de stockage (Disque, Clé USB, Carte SD/micro SD, carte à mémoire simple).

L'utilisateur est responsable du stockage du certificat et de la clé privée.

Le certificat et surtout la clé doivent être chiffrés, le mécanisme de déverrouillage est assuré par le *middleware*.

La machine de l'utilisateur joue alors le rôle d'environnement de confiance.

Pour le stockage des certificats et la clé privée, il est possible d'utiliser une carte à mémoire personnalisée qui fournit en plus un système de protection en logique câblée : ce système peut être une zone protégée en écriture après destruction d'un fusible, une zone protégée en lecture et écriture par un code confidentiel. Le problème de ce type de carte est que, par principe, il est toujours possible d'accéder aux données qu'elle contient et donc de copier la clé privée.

Solution matérielle

Dans ce type de solution, un microprocesseur effectue les opérations cryptographiques. Le terminal n'accède jamais aux clés. Le support peut alors se présenter sous la forme d'une clé USB, d'une carte à puce ou d'une carte SIM.

La carte à microprocesseur est un véritable micro-ordinateur avec son microprocesseur, de la mémoire RAM (*Random Acess Memory*) allouée aux calculs, et de la mémoire allouée aux données. Elle est généralement munie d'un système d'exploitation COS (*Chip Operating System)* aussi appelé le masque ou « *Hard Mask* » qui est stocké dans la ROM (*Read Only Memory*) au moment de sa conception et ne peut donc pas être modifié durant la vie de la carte.

Pour les cartes avec contact, les composants sont logés sous la partie visible de la puce que l'on appelle contacts. Ceux-ci permettent d'établir tous les échanges entre la puce et l'extérieur, que ce soit pour l'alimentation ou les échanges de données.

Enfin, les cartes sans contact possèdent les mêmes caractéristiques fonctionnelles que les cartes à microprocesseur; elles sont alimentées par induction (l'induction est un principe physique qui permet de transformer l'énergie mécanique, le mouvement, placée dans un champ magnétique en énergie électrique) et équipées d'une antenne pour communiquer à des distances de quelques centimètres par radiofréquence (13,56 MHz principalement).

Le principe d'authentification est le suivant :

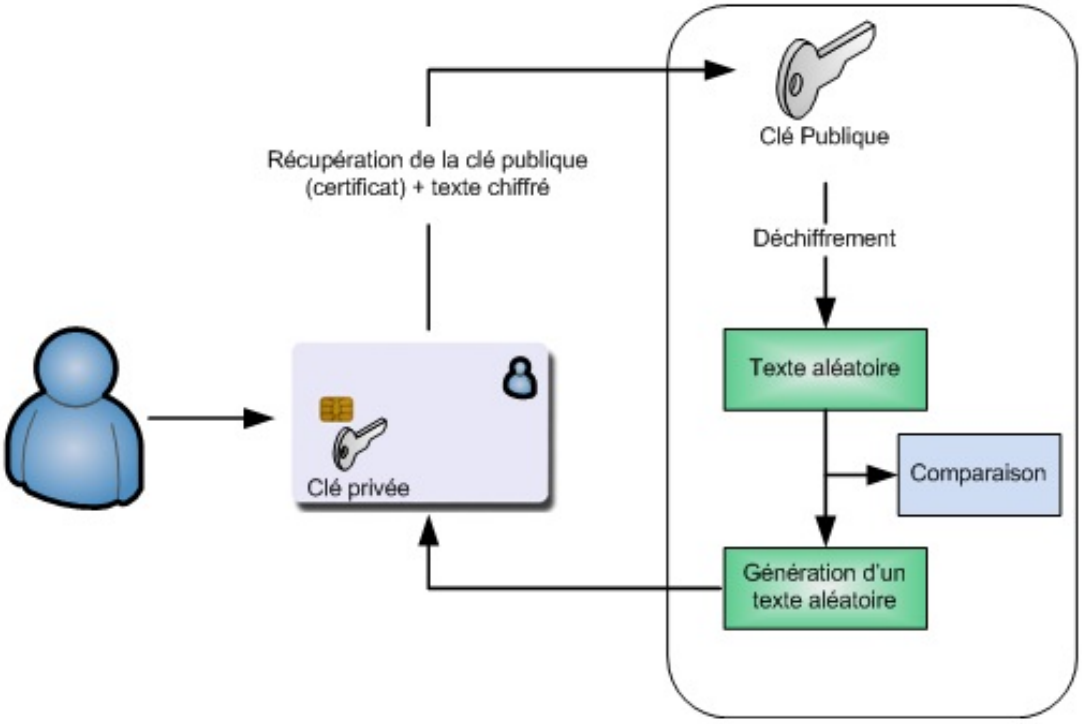


Figure 5: Authentification par carte à puce

Un certificat proposé sur un support matériel est, toujours plus sûr car on ne peut pas le copier. Il est souvent plus pratique car il est possible de l'utiliser sur des sites différents et il n'est pas perdu en cas de problèmes avec l'ordinateur.

Normes

Certificats

Les certificats électroniques respectent des standards spécifiant leur contenu de façon rigoureuse. Les deux formats les plus utilisés aujourd'hui sont :

- X.509 dont plusieurs RFC définissent les propriétés et usages (RFC 2459, RFC 5280)
- OpenPGP défini dans la RFC 48802.

La différence notable entre ces deux formats est qu'un certificat X509 ne peut contenir qu'un seul identifiant, que cet identifiant doit contenir de nombreux champs prédéfinis, et ne peut être signé que par une seule autorité de certification. Un certificat OpenPGP peut contenir plusieurs identifiants, lesquels autorisent une certaine souplesse sur leur contenu, et peuvent être signés par une multitude d'autres certificats OpenPGP, permettant alors de construire des toiles de confiance.

Carte à puce

Les principaux standards en matière de carte à puce sont le fruit des travaux de l'Organisation internationale de normalisation (l'ISO) : la norme ISO/CEI 7816 (en) est découpée en 15 parties, et est complétée par la norme ISO 14443 (en) pour les communications sans contact.

Il existe également d'autres organismes de normalisation. Les principaux sont :

- ETSI : pour les cartes de téléphones mobiles ;
- EMVCo : consortium bancaire regroupant Visa, MasterCard et JCB ;
- ECMA : pour la communication en champ proche (NFC), depuis normalisée par l'ISO/CEI 18092 et CEI 21481

Fédération d'identité

La fédération d'identités se repose sur SAML (*Security Assertion Markup Language*, normalisé, dans sa version 2.0, en mai 2005 par l'OASIS) comme standard pour le format des assertions d'authentification et d'attributs entre les IdP et les SP. SAML définit le format du message XML, appelé assertion, ainsi qu'un ensemble de profils. Ces profils sont des cas d'utilisation détaillés qui présentent la cinématique d'échange des messages, les paramètres attendus et renvoyés.

Toutes les solutions de fédération d'identités s'appuient sur des techniques de base, employées par les méthodes d'authentification unique : redirections HTTP, cookies, Web services, SSL.

Les relations de confiance techniques entre les fournisseurs s'appuient généralement sur des certificats x509 ou des clés symétriques. Plusieurs spécifications de frameworks de fédération d'identité sont aujourd'hui disponibles (cette multiplicité n'en facilite d'ailleurs pas l'adoption) : ID-FF de Liberty Alliance et Shibboleth d'Internet2 (qui est à l'origine à la fois une spécification et une implémentation) ont convergé pour former SAMLv2 qui connaît à ce jour le plus grand succès sur le marché.

WSFederation est un standard concurrent soutenu par plusieurs fournisseurs, dont Microsoft. WS-Federation utilise le format de jeton SAML pour communiquer les assertions d'identité, mais est incompatible avec les fédérations basées sur SAML. Gartner estime que WSFederation est utilisé dans 10 à 25 % des fédérations en production, la majorité étant des entités centrées sur Microsoft qui se fédèrent entre elles.

OpenID connect est une couche d'authentification basée sur OAuth 2.0, un dispositif d'autorisation. Ce standard est géré par la fondation OpenID.

Les assertions SAML sont basées sur les couches SOAP, XML Encryption et XML Signature.

SOAP est le protocole d'encapsulation standard des messages XML, utilisé principalement par les Web services.

XML Encryption est le protocole standard de chiffrement des messages XML. Il a la particularité de pourvoir chiffrer la globalité du message ou simplement un sous-ensemble précis. Cela permet d'avoir, par exemple, un document XML en clair avec des valeurs d'attributs chiffrées.

XML Signature est le protocole standard de signature des messages XML. Tout comme XML Encryption, il permet de cibler l'élément à signer. Plusieurs intervenants peuvent ainsi signer une partie différente du document XML.

RISQUES

Vol d'identité

Perte du contrôle d'identité numérique ! A quoi sommes-nous exposés ?

L'identité numérique n'est pas seulement composée du prénom et du nom d'un individu. Elle concerne aussi d'autres données personnelles.

Rappelons-en quelques-unes :

- Adresse privée ;
- Date de naissance ;
- Téléphone privé ;
- E-mail personnel ;
- Identifiant et mot de passe ;
- Nom de jeune fille ;
- Numéro de carte de crédit.

Grâce aux moteurs de recherche tels que Google ainsi qu'aux multiples informations souvent personnelles semées inconsciemment sur la toile aux travers des réseaux sociaux, tels que Myspace ou Facebook, mais aussi Skype par exemple, nous savons qu'il est très aisé de réunir les données qui sont dispersées sur plusieurs sites.

Cependant, l'assemblage des données personnelles et des traces est une porte ouverte au vol de d'identité. L'usurpation de l'identité numérique est en plein expansion en Europe, elle constitue même un revenu illégal non négligeable dans certaines régions d'Afrique. Elle touche également des millions d'américains et de canadiens chaque année. Avec des informations comme le nom, l'adresse et la date de naissance, il est possible de se faire passer pour quelqu'un d'autre à des fins plus que malhonnêtes.

Chaque année en France, il y aurait plus de 120 000 personnes victimes de vol de leur identité numérique. (Source : Arte, émission futur Mag du 31/1/2015). En France, du point de vue juridique, l'usurpation d'identité est considérée comme un délit et passible d'un an de prison à l'inverse des Etats-Unis où elle est considérée comme un crime.

Voici des exemples de ce qu'il est possible de faire dans certains pays avec quelques données personnelles trouvées sur Internet, ou tout simplement dans votre boite aux lettres, voire votre poubelle.

- Ouvrir un compte bancaire à votre nom pour contracter des emprunts, faire des chèques sans provision, demander des cartes de crédit ;
- Acheter des véhicules, voyager… ;
- Ouvrir des lignes téléphoniques ;
- Créer de faux papiers d'identité ou des passeports ;
- Organiser un mariage blanc en votre nom ;
- Etc.

Grâce aux informations disponibles sur votre identité personnelle, on peut également tenter de deviner votre mot de passe, ou trouver des réponses aux questions secrètes servant à sécuriser l'accès aux sites bancaires ou administratifs. Ces questions sont souvent d'ordre privé, telles que « Quel est le nom de votre animal de compagnie ? » Pour connaitre la réponse, il n'y a pas besoin de pirater votre ordinateur. C'est possible en réunissant les informations que vous avez mises à disposition inconsciemment sur les différents sites communautaires ou blogs que vous fréquentez.

Différentes techniques permettent de voler vos informations personnelles et de se faire passer pour vous :

- Le *phising* (12) ;
- Le *pharming* (13) ;
- Le *spoofing* (14).

Il y a deux ans, Matt Honan, journaliste au magazine Wired, a vu toute sa vie digitale effacée. Son identifiant Apple et ses comptes Google, Twitter et Amazon se sont retrouvés en danger en l'espace d'une heure. Le pirate tweetait des remarques désobligeantes à partir de son compte Twitter et a nettoyé son Iphone, ipad et MacBook.

Il y a quelques mois, un utilisateur de Reddit situé au Royaume-Uni s'est aperçu qu'un pirate avait volé une bonne somme d'argent en effectuant un grand nombre d'opérations financières sur son compte PlayStation. Au point que ce mois-là, l'utilisateur n'était plus en mesure de payer son loyer. Ces deux incidents sont des exemples de ce qui peut arriver lorsque les noms d'utilisateur et mots de passe tombent entre de mauvaises mains.

L'identité numérique est également fragilisée au travers des différentes failles de sécurité exploitées par les pirates. En Avril 2014, des chercheurs ont découvert une des plus grosses vulnérabilités qu'internet n'ait jamais connu : Le bug Heartbleed. Il provient d'une faille critique liée à OpenSSL, un célèbre système de cryptage. La faille permet à des pirates de duper les serveurs OpenSSL et d'accéder aux informations personnelles chiffrées.

Depuis, les experts ont mis en garde le public en conseillant de changer les mots de passe de leurs comptes les plus importants. Toutefois, ces évènements soulèvent la question de savoir si oui ou non il existe un avenir aux couples nom d'utilisateur/mot de passe traditionnels. (1) Extrait du JDN Business Insider du 28 aout 2014.

L'identité numérique protégée par mot de passe est aujourd'hui de plus en plus vulnérable. En aout 2014 le New-York Times a révélé le vol de 1,2 milliards de login et mots de passe par des hackers russes, selon les chercheurs en sécurité de Hold Security. Ce serait le plus grand vol de données de l'histoire d'Internet. Plus grand que celui de Target ou du Playstation Network. Le mot de passe est un moyen médiocre pour assurer notre sécurité.

Plus près de nous, en mars 2015 un adolescent, élève d'un collège de Castres dans le Tarn a usurpé l'identité de son principal et contacté le rectorat pour demander les codes d'accès au système d'information du collège.

Mais le principal, interloqué par la réception de plusieurs mails du rectorat lui renvoyant ses codes d'accès (Espace Numérique de Travail), a décidé de porter plainte au commissariat pour « accès frauduleux dans un système de traitement automatisé de données », comme le rapporte La Dépêche du Midi. En effet, le proviseur n'avait jamais perdu ses codes d'accès au portail informatique permettant aux collégiens et aux familles d'accéder en ligne aux informations liées à la scolarité de l'élève.

On le voit ici, la jungle du numérique peut être impitoyable à l'égard de nos données professionnelles mais aussi personnelles convoitées par une multitude d'individus.

La sécurité des documents personnels est tout aussi vulnérable. Vous avez, par exemple, égaré votre carte d'identité. Vous en déclarez la perte. Le Commissariat de police vous remet une déclaration de perte. Avec cette déclaration, deux photos et un justificatif de domicile, vous obtenez un nouveau titre d'identité.

Une personne malveillante peut effectuer cette opération et demander un nouveau titre à l'aide d'un simple justificatif de domicile qu'elle aura dérobé dans votre boite aux lettres ou dans votre poubelle. Cela lui permet d'usurper votre identité en obtenant un « vrai » titre comportant l'identité d'un tiers. Elle pourra ainsi en toute impunité commettre des infractions, louer un appartement ou prendre des engagements financiers, en laissant au tiers l'obligation d'en assumer les conséquences.

Premières étapes pour retrouver son identité

Si vous vous retrouvez dans ce genre de situation, vous aurez à démontrer que vous êtes bien VOUS, et que vous n'êtes pas l'auteur des actes frauduleux réalisés par l'usurpateur. C'est alors un parcours du combattant durant lequel vous devrez faire face à de graves préjudices.

Encore une fois, les vulnérabilités de violation de l'identité numérique sont multiples, tant dans le monde numérique que dans la vie réelle où l'on risque de voir quelqu'un prendre un jour votre place et agir frauduleusement à votre encontre.

La première étape pour retrouver son identité peut se faire par le biais du site Internet du ministère de la justice qui permet aujourd'hui de demander en ligne un extrait de casier judiciaire (Bulletin N°3).

Avec un petit nombre d'informations (nom, prénom, date de naissance, lieu de naissance, adresse), vous recevrez ce document dans un délai d'environ huit jours. Ce dispositif semble apporter un grand nombre d'avantages pour l'internaute, mais il apporte également son lot d'insécurité.

Vous pouvez également demander par téléphone un extrait d'acte de naissance à votre mairie de naissance, en ne donnant que très peu d'informations. Ce document est une pièce essentielle à tout dossier de création d'identité numérique, que ce soit une Carte Nationale, un passeport, ou l'inscription à un service social.

Ces procédures simples apportent facilité d'usage et gain de temps. En revanche, rien ne garantit encore une fois qu'un tiers ne les utilise à votre insu en s'appropriant votre identité.

Comment l'état gère la situation :

En France, l'Etat a pris la mesure du risque associé au vol d'identité et sécurise les étapes de la délivrance de ces documents : enregistrement de la demande et remise du document en main propre (un agent de l'état physiquement au contact du demandeur), usage éventuel de la biométrie pour éviter de donner plusieurs titres (sous des identités différentes) à la même personne.

L'Etat dispose ainsi d'un moyen très sûr pour produire des identités numériques de haute qualité.

Vol des données personnelles

Deux sortes d'informations caractérisent l'empreinte numérique : les données formelles et les données informelles.

- Les données formelles donnent des informations innées et durables d'une personne, comme le nom, le prénom, et tous les identifiants numériques… Elles permettent de classer une personne dans un échantillon (IP, Géolocalisation, tranches d'âges) mais n'offrent qu'une liberté limitée de traitement.
- Les données informelles, quant à elles, regroupent les informations générées par l'action d'une personne (commentaires sur un blog, nombre de posts sur un forum, inscriptions sur les réseaux sociaux…) Elles nécessitent d'être traitées mais sont difficilement « regroupables » entre plusieurs individus. Elles définissent une personne par son comportement sur le Web et sont facilement accessibles par les moteurs de recherches
- ***Ces deux types de données forment une architecture de données semblable à l'ADN du corps humain. Mais contrairement à ce dernier elles peuvent être visibles de tous. En outre ces données peuvent être transmises par un tiers et non pas par l'intéressé : on parle alors de réputation numérique ou d'e-réputation.***

Problématique d'usurpation d'identité/Diffamation

E-réputation

La formation d'une identité numérique visible par le réseau amène des problématiques importantes en termes de confidentialité des données et de gestion des données.

La capacité de stockage des serveurs Web comme ceux de Google étant immense et ses données inscrites dans le temps, un nouveau terme est apparu pour désigner ce phénomène peu connu de la majorité des utilisateurs d'Internet : « la persistance du Web ». Les serveurs stockent des données cachées qui peuvent nuire à la vie privée des personnes ou à l'image d'une entreprise. Le Web garde donc de nombreuses traces de dérapages attribués à l'inconscience de la jeunesse et viennent bafouer, selon la CNIL (Commission Nationale de l'Informatique et des Libertés) le « droit à l'oubli » :

> « ***le danger de ce système est surtout qu'il produit un traçage dans le temps, et ce que j'ai dit à 20 ans sur Internet pourra m'être reproché quand j'en aurai 50. Du coup, on ne maîtrise plus tout-à-fait sa liberté de pensée et d'expression. Pour la CNIL, c'est une négation de ce que nous appelons le « droit à l'oubli*** ».
>
> Alex Türk Président de la CNIL, TF1.lci.fr, interview de Henri Seckel - le 20/05/2008

Les résultats de Google peuvent être surprenants. Il peut s'agir d'anciens messages laissés sur un forum, de profils sur des réseaux sociaux, de photos et vidéos publiées sur des plateformes de partage ou de blogs. Ces éléments peuvent constituer un frein à l'emploi et/ou au développement social.

En effet, la réputation d'une personne ou d'une entreprise peut se jouer sur un Buzz. Les Buzz utilisent tous les canaux de communication, mais Internet est très souvent le premier utilisé. On peut expliquer ce choix par la nature du média Web. En termes de réactivité, les capacités du réseau Internet ne sont plus à prouver :

- Le temps de publication d'un article relève de la seconde contrairement au journal papier qui met plusieurs heures ;
- Le JT de 20h sera toujours à 20h alors qu'un blog est disponible 24h/24h ;
- Les radios n'interrompront pas leur programme (sauf exception) alors que le Web possède des millions de programmes indépendants.

■ Enjeux de la réputation en ligne

Sur Internet la réputation dépend non seulement de vous mais également des autres. Le Web est un réseau qui contient encore des réseaux (réseaux sociaux, plateformes communautaires…).

La notation des membres sur eBay montre un premier signe du jugement de l'autre. Elle altère la confiance que porte la communauté sur un membre, donc sa réputation. La conséquence de cette mauvaise réputation affectera la vente de ses produits.

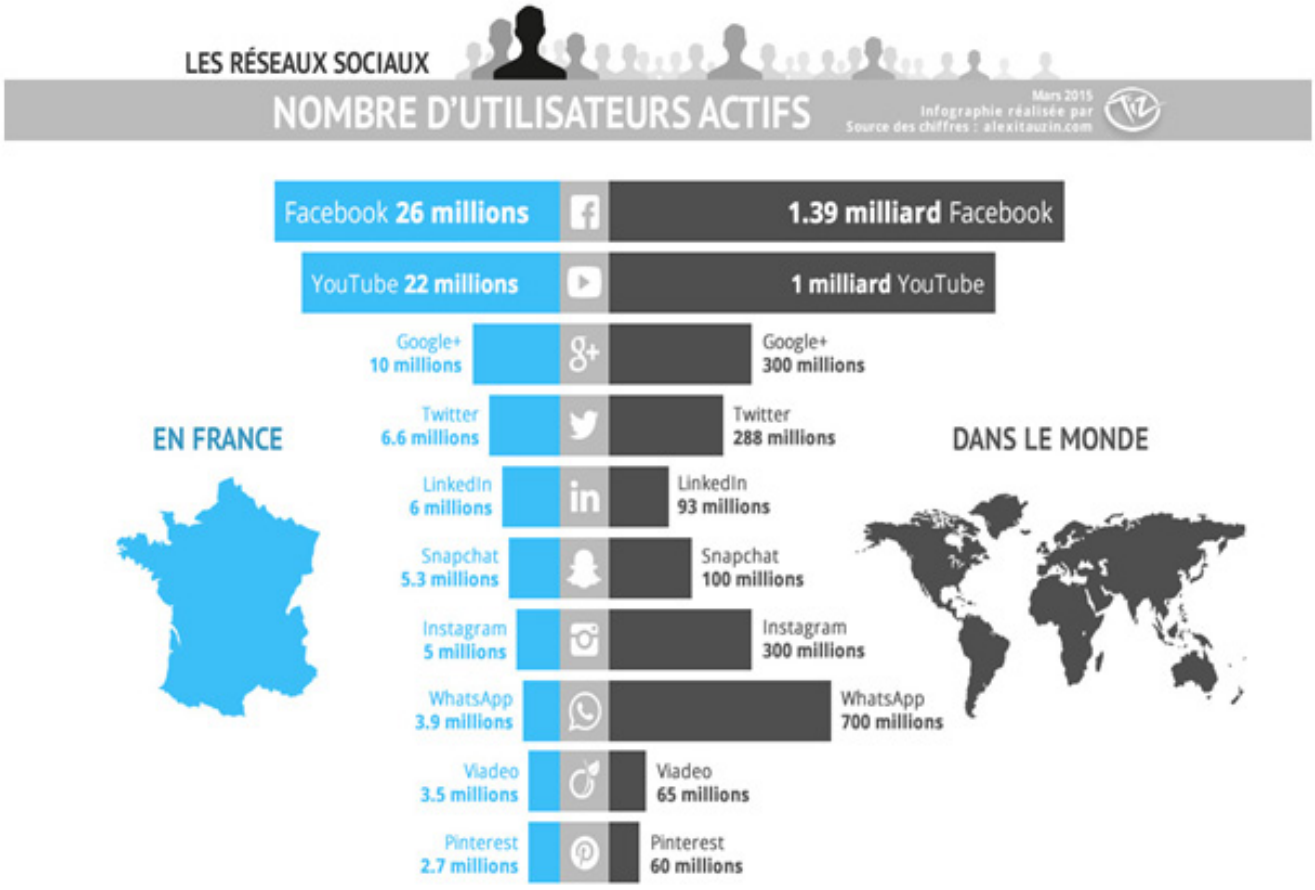
En faisant l'analogie avec une entreprise qui dégage une partie de son chiffre d'affaires via le e-commerce, les conséquences peuvent être ainsi catastrophiques. Les entités du réseau peuvent être des personnes connues, inconnues tout comme des entreprises ou des associations. On peut également penser aux pays comme la Chine, vivement critiquée par les bloggeurs avant les médias traditionnels.

De nombreux exemples de personnalités politiques ont connu des mésaventures sur le Web. On peut prendre l'exemple de Nicolas SARKOZY (vidéo avec les pécheurs, conférence de presse après le déjeuner avec Mr POUTINE, salon de l'agriculture…). À l'étranger, un ministre Belge vantant les valeurs familiales a vu une vidéo de lui en train de consommer des produits illicites « buzzer » sur le net. On peut également citer le scandale Laure MANAUDOU, et plus récemment le cas Marc L., livre autobiographique publié par le magasine Le Tigre, aux dépens d'un internaute en s'inspirant des données publiées sur son profil Facebook.

■ Entreprise, des enjeux différents

La gestion de la réputation est un phénomène connu des entreprises mais avec l'explosion des services Web 2.0 comme les systèmes de notations, les commentaires, les plateformes de partage et d'outils d'évaluation de services, ce phénomène s'est considérablement amplifié. Quelle que soit leur taille, toutes les entreprises sont concernées par la problématique de l'e-réputation.

De nombreuses études ont montré que les internautes passaient énormément de temps avec les médias sociaux et les réseaux sociaux en particulier. Selon une étude Comscore, parmi les 47 millions d'internautes que compte la France, « 37,8 millions d'entre eux visitent des réseaux sociaux soit 80% environ ». Et Facebook est de loin la première plateforme communautaire en France.



Mars 2015 – sources des chiffres : Alexitauzin.com

Les entreprises ont donc tout intérêt à y créer leur(s) page(s) et à y rassembler leur(s) communauté(s) de fans. Elles commencent à prendre conscience de l'importance d'être présentes sur les médias sociaux et allouent davantage de budget pour aller en ce sens.

« ***43% des entrepreneurs français sondés admettent s'être développés et avoir gagné de nouveaux clients grâce aux médias sociaux. Et plus des 3/4 des entreprises françaises estiment qu'ignorer les médias sociaux dans sa stratégie marketing sera une cause d'échec*** » - étude Régus

Outre faire la promotion de son activité, être présente sur les réseaux sociaux permet à l'entreprise de faire de la veille, de trouver des prospects, de créer un climat de confiance avec sa communauté et de surveiller la concurrence.

Les informations se transmettent deux fois plus vite via Internet, et les contenus sont rapidement indexés dans les moteurs de recherche. Donc les informations sur une entreprise ou un individu remontent deux fois plus vite dans les SERP. Et aucune entreprise n'est à l'abri d'un « *bad buzz* » produit par le simple commentaire négatif d'un internaute vu plus de 10 000 fois !

L'enjeu est de taille pour les entreprises si elles souhaitent surveiller ce qui se dit sur elles et réagir en conséquence.

Cette introduction consacrée à l'identité numérique sur le Web ne doit pas faire oublier qu'avant que celle-ci n'existe « son ancêtre » permettait d'identifier un individu de manière beaucoup plus rudimentaire. Nous parlons bien sur de tous autres moyens permettant de vous identifier.

En effet, derrière chaque identité se cache un individu. Cet individu doit être par principe reconnu de manière formelle et sans équivoque au travers de la carte d'identité mais aussi du passeport, ou de la carte vitale.

Au travers de l'histoire, la définition de l'identité a su évoluer avec l'aide des évolutions technologiques et des choix stratégiques des grands pays de notre monde.

Failles de sécurité liées à la fourniture d'ID

■ Attaque du certificat

Le système de certificats ne présente pas de vulnérabilité technique théorique, sous réserve que toutes ses étapes soient correctement implémentées.

Le principal risque peut provenir de la compromission des gestionnaires du système (autorités de certification et gestionnaire de clés). Le contrôle des demandeurs de certification peut être insuffisant ou compromis, permettant à des attaquants de faire certifier des clés publiques frauduleuses. Des clés privées peuvent être volées chez le diffuseur final ou chez les autorités de certification.

Les attaques des diffuseurs ou autorités de certification peuvent être électroniques ou conventionnelles (intrusion physique, corruption...). Ainsi, le virus Stuxnet utilisé contre le programme nucléaire iranien exploitait plusieurs certificats volés.

Une autre vulnérabilité vient de l'utilisation de la fonction de Hachage.

L'intégrité d'un algorithme de hachage utilisé pour signer un certificat est un élément critique de sa sécurité. Les faiblesses des algorithmes de hachage peuvent conduire à des situations dans lesquelles les attaquants peuvent falsifier des certificats. Comme de nouvelles attaques apparaissent régulièrement et que les améliorations technologiques les rendent plus faciles à mettre en œuvre, l'utilisation d'algorithmes dépassés n'est pas conseillée, l'utilisation de md5 est à proscrire depuis 2009, SHA-1 sera abandonné au 1/1/2017. Il est donc important de choisir un algorithme de hachage le plus robuste possible. Le renouvellement des cartes tous les 5 a 7 ans semble indispensable afin de conserver un niveau de sécurité correct.

■ Attaque du support

Une attaque sur une carte à puce vise toujours un des composants de l'architecture suivants :

- Le code exécutable ;
- Les données ;
- Le secret permettant d'accéder au système.

Lire le code exécutable n'est pas dommageable à moins qu'il ne soit secret ce qui est fortement déconseillé. D'après le Principe de Kerckhoffs « La sécurité d'un système cryptographique ne doit pas dépendre de la préservation du secret de l'algorithme. La sécurité ne repose que sur le secret de la clé ».

La modification du code exécutable est très sensible parce qu'elle permet de prendre le contrôle de tout ou partie de la carte puisque le COS (*Chip Operating System*) gère toutes les données et les algorithmes contenus sur la carte.

Le risque lié à la lecture ou à la modification de données (qu'elles soient cryptographiques, personnelles ou sensibles) est évident.

La modification de secret peut permettre à l'attaquant de prendre le contrôle de la carte. Cette technique est utilisée aussi dans les attaques de type DFA (*Differential Fault Analysis*)

On appelle attaque physique, toute attaque menée sur la puce en tant que composant matériel électronique. Ces attaques supposent une connaissance approfondie de l'architecture d'une carte à puce.

Les attaques physiques sont elles-mêmes rangées en deux sous-catégories :

- les attaques invasives ;
- Les attaques non-invasives.

Attaques invasives

Les attaques invasives sont des attaques menées en général par des experts. Elles requièrent du matériel au coût très élevé. Pour ce type d'attaque, il faut tout d'abord isoler le composant électronique. Pour cela, l'attaquant met à nu le circuit imprimé, que ce soit chimiquement ou physiquement (cela revient à « casser » la protection en plastique qui entoure le circuit.

Ensuite, l'attaquant doit avoir des connaissances électroniques pour comprendre l'architecture de la puce et pour contourner les protections électroniques. Cela passe par la reconstitution de circuits à l'aide d'un FIB (*Focus Ion Beam*). Un FIB est un outil utilisé en électronique permettant de réaliser des microcircuits, la lecture ou la modification de bits par LASER. Ce sont des attaques de *Reverse-engineering*. L'attaquant va tenter de récupérer le maximum d'informations sur le circuit pour en déduire les algorithmes utilisés, la manière dont ils ont été implémentés, les sécurités mises en place, pour enfin peut-être tenter de récupérer tout ou partie de la clé.

Solution contre les attaques invasives

Pour se prémunir des attaques invasives, la solution consiste à détecter l'attaque afin de bloquer dans un premier temps l'activité de la puce et dans un deuxième temps d'envisager le suicide logique de la puce afin qu'aucune donnée n'ait été transmise. Pour cela, deux solutions sont adoptées aujourd'hui, l'une est physique l'autre est logique.

Une solution physique consiste à placer la puce sous des couches de métal sur lesquels on place des détecteurs d'activité anormale. Ceux-ci sont sensibles à la température, aux UV, aux rayons X, et communiquent à la puce toute opération suspecte. C'est alors que la puce se bloquera voire provoquera sa mort logique.

Une solution logique supplémentaire pour éviter les attaques invasives est d'introduire régulièrement dans les calculs des contrôles d'intégrité permettant de s'assurer que les données n'ont pas été modifiées par l'extérieur. Cette technique est également utilisée pour se prémunir des attaques par injection de fautes (DFA).

Attaques non-invasives

Les attaques non-invasives exploitent les canaux cachés du microprocesseur. Dans ce type d'attaque, on va mesurer un paramètre physique extérieur de la puce pendant son activité. On ne touche donc pas à l'intégrité physique de la puce. Ce paramètre physique peut être le temps de calcul, le courant, ou le champ électromagnétique émis par la puce.

Ces attaques sont typiquement des attaques à clair connu c'est-à-dire que l'attaquant va soumettre au chiffrement de la puce un ensemble de messages bien choisis. Pendant que la puce chiffrera ces messages l'attaquant relèvera les données du paramètre physique mesuré. Une fois ces paramètres récupérés, l'attaquant par analyse directe des données ou par analyse statistique en déduira des données sur la clé.

Dans ces attaques on retrouve la «*Timing Attack*» qui exploite le temps d'exécution d'une puce, la SPA (*Simple Power Analysis*) et la DPA (*Differential Power Analysis*) qui mesure le courant consommé par la puce pendant son activité, la SEMA (*Simple Electro Magnetic Analysis*) et la DEMA (*Differential Electro- Magnetic Analysis*) qui exploitent le rayonnement électromagnétique dû à l'effet inductif produit par le courant passant dans les circuits de la puce. Dans les attaques SPA et SEMA l'analyse des données est directe alors qu'elle est statistique pour les attaques DPA et DEMA.

Solutions contre les attaques non-invasives

Les attaques non-invasives consistent essentiellement à déterminer l'activité de la puce pour en déduire des informations secrètes. Cela passe par l'analyse de paramètres physiques (tels que le temps d'exécution, le courant, le champ magnétique...), qui s'avèrent être un réel canal subliminal d'informations. Les contre-mesures à ce type d'attaques vont consister soit à brouiller l'information qui passe par ces canaux soit à atténuer ou éliminer le signal émis.

Pour brouiller l'information l'encarteur possède plusieurs techniques néanmoins semblables :

- Le chiffrement interne des bus et des mémoires
- La génération d'activité aléatoire

Chiffrer les bus et les mémoires signifie que les données ne transitent jamais en clair, même à l'intérieur de la puce et que seul le COS est en mesure de lire ces informations. Par conséquent, toute attaque par analyse d'activité sera vaine dans la mesure où l'attaquant ne récupèrera que des données chiffrées. Il existe une technique dans le même esprit que cette dernière qui consiste à appliquer pseudo-aléatoirement un masque binaire permettant de chiffrer ces mêmes données. L'idée est de se rapprocher du principe du *One Time Pad,* sans la contrainte d'échange de clés grandes, en générant du pseudo-aléa à partir d'une clé courte.

Générer de l'activité aléatoire, c'est introduire des opérations leurres et aléatoires que la puce effectuera en parallèle pour induire l'attaquant en erreur. Ce brouillage est algorithmique. En pratique, la puce effectue des calculs aléatoires en parallèle et cache les opérations réellement effectuées par la puce dans le cadre cryptographique.

Restent enfin les techniques qui visent à atténuer le signal émis par la puce dans ces canaux parallèles : celles-ci reposent sur le *hardware* et l'encarteur va pour cela essentiellement chercher à minimiser la consommation de la puce, de sorte que les attaques par analyse de courant ou de champs magnétiques soient plus difficilement réalisables. L'encarteur réduit également la taille des composants et dispose des couches de métal pour protéger la puce.

NOS PRÉCONISATIONS

Nous avons pris le parti de ne pas donner de recommandations techniques autres que celles liées à l'utilisation de standard. Il nous semble primordial, une fois la solution choisie dans son ensemble, d'effectuer une analyse de risque approfondie qui fera émerger les menaces et ainsi permettra d'adapter les moyens techniques pour répondre à ces menaces.

Dans le cadre d'un projet unifié de gestion de l'identité numérique française, nous recommandons que l'état fournisse, en plus de ses services actuels de gestion d'identité, les services suivants :

- Délégation d'authentification ;
- Signature électronique pour des documents/transactions officielles et civiles ;
- Vérification d'âge minimum ;
- Fédération d'identité.

Les parties ci-après décrivent un projet global visant à fournir à l'ensemble des citoyens français une meilleure gestion de leur identité numérique et également à aider les sites internet dans leur gestion quotidienne. Ce projet est un ensemble cohérent, dont certaines parties peuvent cependant être prises indépendamment.

Fourniture de service d'authentification

Dans le cadre de la mise en place d'un système de gestion des identités numériques, l'état pourrait offrir des services d'authentification à destination d'autres entités que les services gouvernementaux.

La fourniture de ce type de service par l'état français à destination des entreprises, associations, collectivités locales, permettrait notamment de :

- Mettre en place un système de protection des mineurs.
- Protéger la vie privée des citoyens (Google)
- Faciliter les activités de renseignement
- Mettre en avant et aider à mieux sécuriser les données des entreprises françaises

La mise en place d'un système de protection des mineurs peut être la volonté d'une politique de renforcement de contrôle des accès à des contenus déconseillés à certaines tranches de la population. Dans le cadre de la fourniture de services d'authentification, la France pourrait proposer des API (interfaces de programmation) permettant de valider l'appartenance d'une personne à une tranche d'âge. Cette fonctionnalité représenterait une véritable avancée dans le domaine de la protection des mineurs face aux contenus inappropriés, qui pour l'instant ne se fonde que sur la base déclarative de la personne.

La majorité des services internet qui utilisent l'authentification déléguée se basent sur les systèmes de Google ou Facebook. Ces géants américains sont connus pour pister les utilisateurs et leur modèle économique ne repose que sur leur capacité à connaitre les utilisateurs et à leur proposer des publicités ciblées. Afin de mieux protéger les citoyens français face à ce genre de surveillance numérique et d'atteinte à leur vie privée, la mise en place de services d'authentification étatiques permettrait de ne pas alimenter les bases de connaissances de ces géants.

De plus en fournissant des services d'authentification, et sous réserve d'accord de la CNIL, les services régaliens seraient en mesure de suivre les activités de personnes sous surveillance. Il convient cependant d'apporter une vigilance particulière lors de la mise en place de ce service afin de ne pas permettre à des tiers de pouvoir pister des citoyens. Pour ce faire nous recommandons que le service fournisse pour chaque site/outil/forum, désirant utiliser l'authentification déléguée de l'état, un identifiant unique différent qui ne permettrait pas de pister l'utilisateur.

Les services de délégation d'authentification permettront aux entreprises françaises d'avoir une base de sécurité pour la gestion des utilisateurs, facile à implémenter et à maintenir. Cette facilité représentera un véritable avantage économique face à des concurrents ne bénéficiant pas de ce type de services. De plus les entreprises seront en mesure d'avoir une attestation fiable de l'identité de la personne et ainsi de réduire le risque de fraude. La mise en place de ce service pourra également permettre à la CNIL d'optimiser ces contrôles en ayant une meilleure connaissance des systèmes manipulant des données de citoyens français.

Protection de la carte d'identité support de l'identité numérique

Pour être sécurisée et viable dans le temps, la carte d'identité utilisée pour l'authentification numérique doit inclure l'authentification multi-facteurs. Dans le cadre de ce rapport, nous prenons comme hypothèse que la future carte d'identité embarque les facteurs d'authentification suivants :

- Certificats numérique stockés dans la puce ;
- Un cryptogramme visuel changeant ;
- Biométrie palmaire.

La puce doit prendre en charge plusieurs certificats numériques, afin de pourvoir offrir les fonctionnalités suivantes :

- Signature numérique simple permettant d'attester de la validité de la carte d'identité. Cette fonctionnalité pourra être utilisée par des tiers non gouvernementaux nécessitant de vérifier l'identité des personnes ;
- Signature numérique complexe uniquement accessible des forces de l'ordre, permettant d'attester de la validité de la carte d'identité présentée ;
- Certificat contenant les informations personnelles de l'utilisateur (nom, prénom, adresse, numéro de sécurité sociale) nécessitant un code connu uniquement de l'utilisateur. Ce système pourra être utilisé chez un nouvel employeur afin de simplifier les démarches administratives et de permettre, après accord de la CNIL aux autorités étatiques, de mieux cibler les contrôles ;
- Signature numérique simple permettant d'identifier la carte émettrice. Ce système sera utilisé pour les transactions par internet en complément du cryptogramme visuel changeant ;
- Signature numérique forte permettant d'authentifier la personne (à coupler avec un code et/ou une empreinte digitale) permettant de signer numériquement des actes (impôts, notaire, sécurité sociale, …)

Le cryptogramme visuel changeant, tel qu'actuellement testé sur les cartes bancaires, en remplacement du cryptogramme visuel statique (CVV : 3 chiffres se trouvant au verso des cartes bleue VISA) permet d'ajouter un second facteur d'authentification pour l'utilisation de la carte comme moyen d'authentification sur Internet. Ce système permet de prévenir les attaques par rejeux au cas où le premier système d'authentification serait compromis.

L'utilisation de systèmes de signature et de certificats numériques doit être effectuée selon les standards de sécurité actuels, tels que décrit dans la partie V.3 (Normes). De plus pour améliorer le niveau de sécurité, ils devront être accompagnés de la mise en place de plusieurs infrastructures à clés publiques (ou PKI) permettant la révocation rapide de carte perdue/volée ou du système compromis.

Vol et usurpation d'identité

Afin de prévenir l'usurpation d'identité numérique, il est important de mettre en place les infrastructures à clés publiques décrites dans la partie précédente. En plus de prévenir les usurpations d'identité numérique, ces infrastructures pourront permettre de lutter efficacement contre l'utilisation frauduleuse de la carte d'identité si cette dernière a été perdue ou dérobée. De plus, comme ce système ne permet d'avoir qu'une seule carte valide par citoyen, il prévient également les abus causés par le vol d'identité qui consiste à prendre l'identité d'une personne en se faisant faire des papiers officiels grâce à une déclaration de perte et à un certificat de naissance.

Il est également indispensable que toute utilisation de la carte d'identité comprenne l'authentification par 2 facteurs distincts, (carte et code secret) afin de réduire les risques de vol d'identité numérique. De plus la mise en place de plusieurs mécanismes d'authentification permettra d'amoindrir les impacts d'une vulnérabilité touchant l'un de ces mécanismes. En effet si la carte ne comprend qu'un mécanisme unique et qu'une vulnérabilité est découverte sur ce dernier, alors l'ensemble du système deviendrait caduque et permettrait le vol en masse des identités numériques des citoyens français.

Business case

Essayons de montrer macroscopiquement le coût économique de la solution que nous préconisons. Certains chiffres dans les coûts de fabrication sont issus de sources officielles et d'autres sont issus d'estimations (*) ou d'éléments rapportés par des tiers (**).

Dans le cadre d'un business case, il convient généralement de produire les coûts et les bénéfices chiffrés de la solution. Dans le cas présent, les bénéfices sont difficiles à quantifier et sont basés sur des estimations à plus ou moins 30%, qu'il conviendra d'affiner une fois la phase de conception générale terminée.

■ Coûts

Coûts de la carte à puce

Le tableau ci-après représente les coûts estimés pour la fabrication et la distribution de la nouvelle carte d'identité.

	Coût unitaire	Quantité	Coût global (10ans)	Coûts lissé sur 10 ans
Carte d'identité ou même format que le permis de conduire à puce	14€**	40 M	560 M€	56 M€ / an
Cryptogramme visuel changeant	2€	40 M	80 M€	8 M€ / an
Ajout de la biométrie palmaire	1€	40 M	40 M€	4 M€ / an
Total	**17€**		**680 M€**	**68 M€ / an**

Coûts de l'infrastructure numérique de fournisseur de service d'authentification

Le tableau ci-après représente les estimations pour la mise à disposition des services d'authentification sur Internet. Prenons les hypothèses suivantes :

- L'état se porte acquéreur des équipements informatiques et ces derniers sont amortis sur 5 ans ;
- Le nombre de demandes d'authentification simultanée ne dépasse pas les 200 000 avec un temps moyen de résolution de l'authentification de 4s ;
- Les ressources nécessaires à l'authentification dans 5 ans (en prenant en compte les avancées technologique) correspondront aux même ratios que ceux actuels.

	Coût unitaire	Quantité	Coût global (10ans)	Coûts lissé sur 10 ans
Plateforme d'hébergement (Intégration inclue)	20 M€	2	40 M€	4 M€ / an
Bande passante internet et service anti DDoS	1 M€ / an	10	10 M€	1 M€ / an
Maintien en condition opérationnelle	600 k€ /an	10	6 M€	0,6 M€ / an
Total	**17€**		**56 M€**	**5,6 M€ / an**

Promotion et dotation des forces de l'ordre

Il n'est malheureusement pas possible d'estimer correctement ces deux parties car :

- La promotion publicitaire nécessaire pour faire connaitre le système dépendra avant tout de la volonté politique de mettre en avant cette avancée et aussi des tarifs et moyens négociés par l'Etat avec les différents média (ces derniers chiffres/tarifs ne sont pas publics)

- La dotation en équipements des forces de l'ordre ne peut être également chiffrée car ces derniers dépendront des technologies choisies au niveau de la puce et du système de certificat/signature. Le prix des terminaux de lecture pouvant varier selon un facteur 15 en fonction des choix technologiques, nous ne pouvons fournir dans le cadre de ce rapport une estimation fiable. Nous conseillons cependant que cette dernière soit intégrée à la fin de l'étude sur le choix des technologies à adopter.

■ Bénéfices

Les bénéfices liés à l'amélioration de la sécurité de la carte d'identité (prévention des vols et des usurpations) sont difficilement quantifiables pécuniairement tout comme ceux liés à l'utilisation d'un système d'authentification unifié pour tous les services en ligne de l'état.

D'après le rapporteur Bernard Farriol, le travail au noir représentait en 2013, 10,8% du PIB français. Un système d'identité numérique unifié avec une clé unique permettant de relier les comptes bancaires au numéro de sécurité sociale pourrait permettre de mieux cibler les contrôles et de réduire la fraude.

D'après les chiffres 2014 de la FEVAD (Fédération E-commerce et Vente A Distance), le e-commerce représente 51,1 milliard d'euros de chiffre d'affaires et 87 000 emplois directs. La mise en place d'une stratégie de développement du numérique ainsi que les systèmes d'authentification mis à disposition des professionnels pourrait permettre aux e-commerce de gagner jusqu'à un point de croissance.

CONCLUSION

L'identité d'un individu s'est dématérialisée dans le temps. Il ne s'agit plus aujourd'hui de décrire ou de formaliser par écrit ce qu'est un individu pour affirmer qu'il est bien lui, mais de réunir de manière beaucoup plus complexe, à l'aide des nouvelles technologies tout ce qui vous caractérise sans la moindre erreur. Nous pensons qu'il est du devoir des Etats d'assurer la sécurité en ligne de leurs citoyens comme ils le font dans le monde réel.

L'identité numérique est également un enjeu de rayonnement de la France à l'international. En effet plusieurs pays commencent à se doter de systèmes pour gérer l'identité numérique. Dans ce cadre la France, qui a été reconnue première nation Européenne en matière d'administration numérique en 2014, peut jouer un rôle majeur dans l'identité numérique. Nous sommes convaincus que seul l'Europe sera en mesure d'imposer des standards et une alternative étatique aux systèmes gérés par des multinationales.

Néanmoins l'intégration d'un projet global autour de l'identité numérique, tel que proposé dans nos recommandations, demande de nombreuses modifications de textes de loi et pose des interrogations face aux abus éventuels qu'un système d'identité unifié pourrait permettre. En effet, il est d'ores et déjà possible de quasiment tout savoir de la vie d'un individu en étudiant ses relevés de carte bancaire, ses journaux de connexion internet ainsi que les informations dont dispose la sécurité sociale. Les nouveaux textes proposés devront d'abord recevoir l'aval de la CNIL et du conseil constitutionnel avant de permettre la mise en œuvre du projet.

De notre point de vue, l'identité numérique est un sujet clé complexe que la France se doit d'adresser afin de maintenir son *leadership* numérique parmi les Etats européens. Ce projet apporte de nouvelles opportunités ainsi que des risques qu'il convient d'adresser avec précaution pour permettre à ce projet d'être un vecteur de croissance et de développement pour l'économie numérique française.

GLOSSAIRE

- (1) e-IDAS Electronic identification and trust services
- (2) Le réseau PEPPOL, est un réseau sécurisé ouvert reposant aujourd'hui sur une centaine de points d'accès en Europe
- (3) TSL, *Trusted services list* ou liste de confiance européenne des autorités de certifications qualifiées pour délivrer des certificats attestant de l'identité numérique dans chaque Etat Membre
- (4) DSS, Digital Signature Service est une solution de création de signature reposant sur un logiciel développé par la DG MARKT dans le cadre de la Directive services (2006/123/EC) et supportant les formats avancés types CADES/ XADES ou PADES
- (5) OID, organisation délivrant de l'identité numérique (il y en a 147 actuellement déclarées)
- (6) CNIE, Carte Nationale Identité Electronique
- (7) FNTC, regroupe une centaine d'acteurs du monde du numérique. C'est une Fédération de professionnels fournisseurs et/ou utilisateurs de services numériques où l'on côtoie de très anciennes institutions, des entreprises de tailles variées, des start-ups et des experts (avocats, consultants,…)
- (8) ZMR, (Zentralmelderegister) : pour, fichier déclaratif central
- (9) NemID , est une solution d'identification sur internet utilisée par les banques et plusieurs entreprises privées, au Danemark
- (10) CPR, (Det centrale personregister) : équivaut au fichier central des personnes

• (11) (Ligue des droits de l'Homme – LDH ; Syndicat de la magistrature – SM ; Syndicat des avocats de France – SAF ; l'Association française des juristes démocrates – AFJD ; l'association « Imaginons un réseau Internet solidaire » – IRIS)

• (12) Le phising générerait tous les ans des dizaines de millions d'euros de fraude. Cette technique consiste à envoyer un mail à un utilisateur en se faisant passer pour une institution ou une entreprise. L'e-mail ressemble à l'identique à un e-mail officiel et il invite l'utilisateur à se rediriger vers un faux site où il lui est demandé de saisir des informations confidentielles le concernant pour X raisons

• (13) Le pharming est un véritable acte de piratage. L'auteur du délit pirate un nom de domaine, par exemple le site d'une banque, et redirige les victimes vers un site frauduleux pour soutirer leurs coordonnées bancaires. La victime n'y voit que du feu

• (14) Le spoofing est lui une variante qui consiste à pirater l'adresse IP d'une machine pour se l'approprier et ainsi récupérer des données confidentielles. C'est ce qui est arrivé à la société SONY avec le piratage de son service le Playstation Network. Les hackers ont eu accès à 75 millions de numéros de cartes bancaires. Cette affaire à couté cher à SONY, aussi bien financièrement qu'au niveau de son image.

INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

INHESJ

TRAVAUX DES AUDITEURS

Cycle « Sécurité des usages numériques »
Travaux de la 5e promotion (2014-2015)

COMMENT GÉRER L'IDENTITÉ NUMÉRIQUE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre
INHESJ
INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

en partenariat avec le
cigref Réseau de Grandes Entreprises

DÉCEMBRE 2015
ISSN 2265-447X