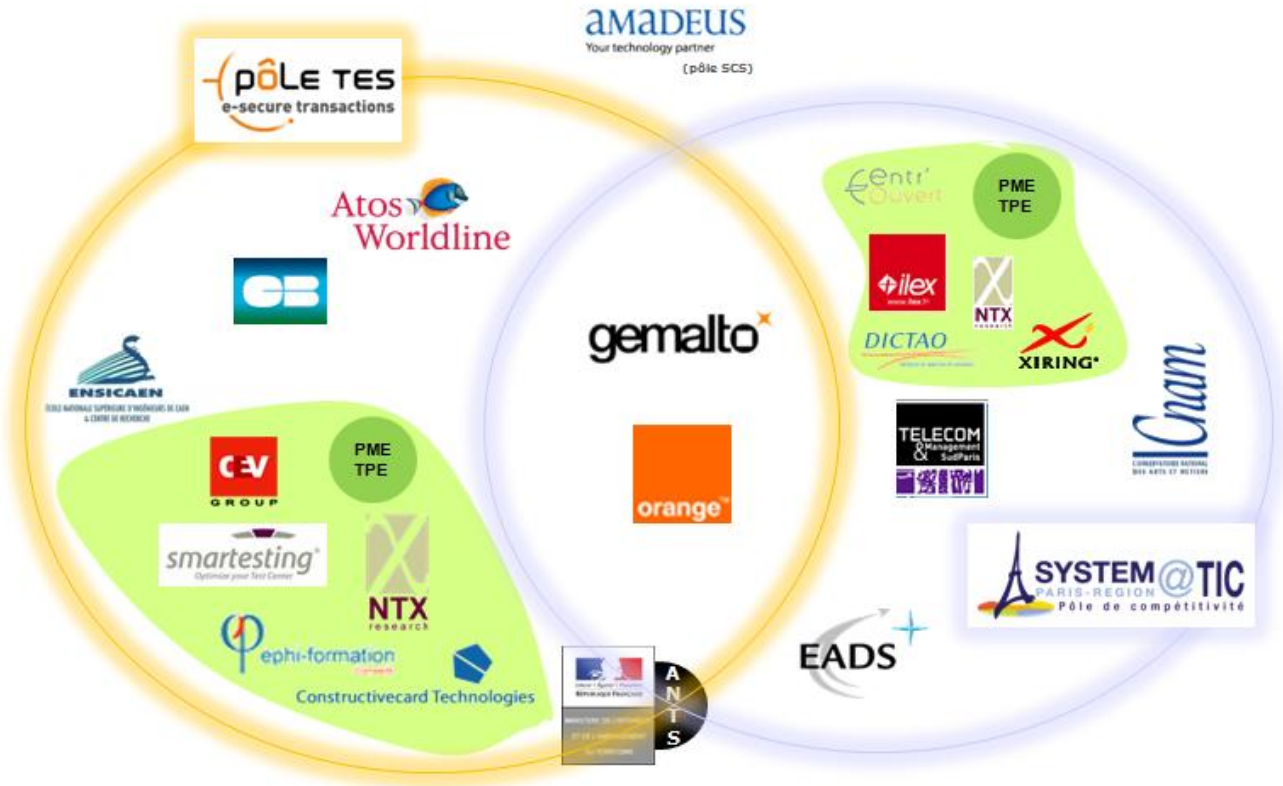

**LIVRE BLANC**

# GESTION DES IDENTITES

## ANALYSE DES CONTEXTES JURIDIQUE,

## SOCIO-ECONOMIQUE ET SOCIETAL

## MEMBRES DU CONSORTIUM




**Informations sur le projet** : http://www.fc2consortium.org

### UN PROJET LABELLISE PAR

SYSTEM@TIC PARIS-REGION Pôle de compétitivité — pôle tes e-secure transactions

### UN PROJET FINANCE PAR

DGE — MAIRIE DE PARIS — Basse-Normandie — 92 Conseil général des Hauts-de-Seine — îledeFrance

# SOMMAIRE

# INTRODUCTION

Futur pivot de confiance de la vie numérique, la gestion des identités est à la croisée des besoins en matière de transactions électroniques sécurisées et des échanges numériques de confiance.
Le projet FC² - fédération de cercles de confiance et usages sécurisés de l'identité numérique - en est une illustration qui présente des enjeux multiples : accompagner les citoyens, protéger les libertés individuelles, innover technologiquement, forger une filière industrielle.
L'un des enjeux fondamentaux d'un tel projet est de garantir à l'utilisateur la confidentialité de ses données personnelles ainsi que le respect d'un nombre de droits et de règles juridiques.

De manière générale, la gestion des identités numériques consiste à dématérialiser la gestion des différentes données personnelles des individus (ou des données identifiant des organisations), avec différents niveaux de sécurisation : faible pour des usages simples ou plus fort pour des usages complexes, qui peuvent nécessiter la « certification » et donc la signature électronique des données par un tiers de confiance.

La fédération d'identités peut quant à elle se définir comme la gestion d'un ensemble d'identités par un ensemble d'organisations distinctes et inscrites dans un même « cercle de confiance » ou des cercles distincts. Elle permet aux utilisateurs de se connecter une seule fois en utilisant un seul identifiant pour avoir accès à plusieurs services. Elle permet ainsi d'échapper à la complexité de la multitude des identifiants, et d'éviter une fastidieuse saisie répétée d'identifiants.

Techniquement, la fédération d'identité tient en deux éléments :

- la délégation de l'authentification qui consiste à authentifier l'utilisateur depuis le service d'authentification d'un tiers ;
- la propagation des attributs utilisateurs qui permet de transmettre un identifiant reconnu et des attributs de comptes internes.

Une telle plate-forme pose des problématiques telles que celles du consentement de la personne, de la conservation des données personnelles, des responsabilités des acteurs ou plutôt de leur partage des risques, d'autant plus que l'on sort de la stricte identité de consommateur puisque l'intervention de personnes publiques met en jeu le profil de « citoyen ». Personnes publiques, personnes privées, institutions mixtes coexistent et l'e-administration est au cœur du projet.

Par ailleurs, la question de l'acceptabilité d'un tel service de gestion d'identité reste ouverte, sur le plan sociétal et socio-économique. Si les utilisateurs expriment des besoins en matière de simplicité ou « d'expérience utilisateur », ils semblent moins nombreux à l'heure actuelle à demander une sécurité accrue dans la gestion de leurs données personnelles, et sont peu conscients des risques potentiels. Dans ce contexte, dans quelle mesure les utilisateurs sont-ils prêts à utiliser de nouvelles méthodes d'authentification et surtout de nouveaux concepts et outils de gestion d'identité ?

Afin d'éclairer les travaux du projet sur des questions au demeurant très incertaines étant donné le caractère encore balbutiant des applications de gestion électronique d'identité, ce livrable réalise une analyse synthétique du contexte juridique d'une part, et des aspects sociétaux et socio-économiques d'autre part. L'analyse se situe, au-delà du contexte français (qui comporte certaines particularités sur le plan juridique), dans la mesure du possible au niveau européen.

# 1. CONTEXTE JURIDIQUE DE L'IDENTITE NUMERIQUE

Réalisée dans le contexte du projet FC², pour les besoins des membres du consortium, cette analyse n'a pas vocation à être exhaustive.

Elle a pour objectif de clarifier le contexte juridique du projet, de dresser un état des lieux synthétique des questions juridiques liées à la gestion des identités numériques, et de proposer un certain nombre de recommandations pour la bonne mise en œuvre du projet.

## 1.1 DEFINITIONS STRUCTURANTES

### 1.1.1 IDENTITE DES PERSONNES

- au cœur de la personne, l'identité est une notion hautement sensible et symbolique, à tel point qu'elle n'a aucune définition juridique globale.
- dans le dictionnaire de l'académie française, l'identité, dans le domaine juridique, correspond à "la personnalité civile d'un individu, légalement reconnue ou constatée, établie par différents éléments d'état civil et par son signalement". elle se réduit donc largement à la sphère « régalienne », comme dans la notion de carte ou document *d'identité*. cette définition omet ainsi d'autres domaines d'utilisation, dans la sphère marchande en particulier.
- selon le contexte, la définition de l'identité varie. elle n'est pas la même selon que l'on se place sur un plan philosophique, sociologique ou encore économique.
- il n'existe pas qu'une seule identité. tous les individus sont dotés de plusieurs identités, qui sont constituées d'une somme de données personnelles rattachées à l'individu. celui-ci peut donc utiliser différentes identités selon le contexte, et peut souhaiter que ces identités ne soient pas directement reliées entre elles.

La définition suivante s'applique également à l'identité dite « régalienne » de la personne : « L'identité d'une personne peut être vue comme un « ensemble de composants grâce auxquels il est établi qu'une personne est bien celle qui se dit ou que l'on présume telle (nom, prénoms, nationalité, filiation) »[1]. Elle peut être légalement reconnue ou constatée.

Plus globalement, l'identité peut se définir comme «l'ensemble des attributs qui caractérise un individu et qui permet d'identifier une personne, un principal grâce à ses caractéristiques physiques (taille, poids, couleur des yeux), son état civil (nom, prénom, date et lieu de naissance, adresse de son domicile), ses données numériques (adresse de courrier électronique, numéro de téléphone mobile), ses préférences ou encore ses habitudes»[2].

Au-delà, on peut considérer de manière générale que l'identité d'une personne, multiple, est composée d'ensembles de données personnelles liées à cette personne, mais ne permettant pas nécessairement de l'identifier directement par son état civil.

[1] Thierry PIETTE-COUDOL, L'identité des personnes, les certificats et la signature électronique, Communication Commerce électronique n° 1, Janvier 2005, étude 2
[2] Vision d'architecture "Liberty Alliance" – Réf. LibertyAllianceADAEV1.0.1.sxw - Agence pour le développement de l'administration électronique, octobre 2004

### 1.1.2 IDENTITE NUMERIQUE

L'identité numérique est la déclinaison dématérialisée de l'identité d'une personne dans le monde « virtuel » du web.
Dans les relations sur Internet, l'identité numérique est souvent requise pour s'identifier ou passer des contrats sur des sites marchands. Aujourd'hui, celle-ci est fournie en règle générale par la simple introduction du nom de la personne ou d'un pseudo.

Tandis que l'identité est une expression fondamentale de la personnalité – le « je suis » - qui permet à un individu d'affirmer son existence pour être reconnu par les autres, ce que l'on appelle « l'identification » est « une marque de défiance par rapport à l'expression de son identité par une personne »[3].
L'identification est une opération qui tend à rendre objective l'identité, par le contrôle d'éléments vérifiables : date et lieu de naissance, filiation, statut matrimonial. C'est avec le développement des services d'identité judiciaire au début du siècle passé que des « éléments de signalement ont été rajoutés aux documents d'identification : photographie, couleur des yeux, empreinte digitale ».[4]

Dans les temps passés, les méthodes d'identification n'étaient pas tout à fait fiables et une même personne pouvait, sans exagération, vivre sous plusieurs identités, ce que Maître Renard illustre ainsi : « Jean Valjean, condamné à dix neuf ans de bagne pour avoir volé un pain, deviendra le riche Monsieur Madeleine, avant de changer de nouveau d'identité pour échapper à l'implacable Javert. »[5]

Cette situation a sensiblement évolué aujourd'hui avec le progrès des techniques d'identification dans tous les domaines, et ce même si rien n'empêche l'obtention en France de vrais-faux papiers sur présentation de faux justificatifs. Pourtant, certaines circonstances, telles que l'exercice des droits civils ou encore la conclusion de contrats d'importance ou dont le paiement est différé, imposent un niveau de fiabilité plus élevé quant à l'identité des personnes impliquées. Cela est tout aussi vrai dans les relations sur Internet.

### 1.1.3 DONNEES PERSONNELLES

C'est un ensemble de données personnelles qui composent l'identité (numérique) d'une personne. Nom de famille, prénoms, sexe, date et lieu de naissance etc. constituent des données personnelles. Le « profil » lui, est tout ou partie des données personnelles d'un individu. Ainsi un « profil » client est la personne telle qu'on la connaît d'après les informations dont on dispose la concernant. Le « profil » citoyen est constitué des données administratives sur la personne, ou fournies par l'Administration.

La Convention 108 du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, dont le but est de « garantir, sur le territoire de chaque partie, à toute personne physique, quelles que soient 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») », est un texte important pour la définition des données personnelles. Dans son article second (a), elle précise : les «données à caractère personnel» sont « toute information concernant une personne physique identifiée ou identifiable (personne concernée)»[6] .

[3] http://ec.europa.eu/justice_home/fsj/privacy/
[4] d'après Maître Isabelle Renard
[5] *http://www.isabelle-renard.com/vie-privee-tracabilite.php*
[6] Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, site du conseil de l'Europe ;
http://conventions.coe.int/Treaty/FR/Treaties/Html/108.htm

La loi Informatique et Libertés va plus loin en précisant que le terme « identifiable » est un potentiel : « Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. » L'acception de « toute autre personne » est ici très vaste.

Le rapport Truche[7] (contrairement au rapport Carcenac[8]) a traité tôt de l'identité électronique, du risque d'une société de surveillance concomitante à la société de l'information, ainsi que de l'usage de la cryptographie. Le rapport éclaire sur le fait que, pour l'identité numérique du citoyen, le numéro d'identification INSEE ne peut servir d'identifiant unique et que son utilisation en dehors du cadre social ou médical est sévèrement encadré par la loi. Ainsi chaque ministère a développé son propre système d'identification lié à la manière dont sont organisés ses propres fichiers. Au contraire, certains pays européens, ainsi que les Etats-Unis, ont opté pour un identifiant unique (souvent le numéro de sécurité sociale) lié à un certain nombre de données personnelles propres à l'individu, et lui permettant de s'identifier facilement pour un grand nombre d'usages.

En outre, la protection des données personnelles est fortement liée au respect de la vie privée. La source de ce droit se trouve dans l'article 9 du code civil. Il s'agit d'un droit subjectif, le droit au respect de la vie privée, ou encore, le droit, pour tout individu, de choisir ce qu'il veut dévoiler de lui-même et les personnes auxquelles il désire que soient communiquées les informations relatives à sa personne et à son identité. C'est pour garantir le respect de cette faculté que le législateur réglemente strictement la collecte, la conservation ou la diffusion des données personnelles ou nominatives[9].

### 1.1.4 ATTRIBUTS

Un attribut est un élément constitutif de l'identité. Juridiquement, il s'agit tout simplement des données personnelles (voir ci-dessus).

Selon le dictionnaire de l'Académie Française, un attribut est ce « qui est propre et particulier à un être, à quelqu'un ou à quelque chose[10] ». Le Larousse en donne la définition suivante : « une propriété distincte, mesurable, physique ou abstraite appartenant nommément à une entité (individu ou autre) ».

Les attributs peuvent prendre des formes très variées :

- état civil de la personne (nom, prénom, date de naissance, etc.) ;
- qualités (ex. diplôme, nationalité, fonction, employeur)
- coordonnées postales, téléphoniques, e-mail, etc. ;
- coordonnées bancaires ;
- données de fidélité ;
- les certificats qui sont délivrés par des organismes, des services ;
- les contenus publiés à partir d'outils d'expression (ex. blogs, avis, wikis) ;
- les achats (ou ventes) réalisés chez certains marchands ;
- les données diffusées au travers de réseaux sociaux, sites de rencontre ou mondes virtuels ;
- les informations fournies par des services de gestion de notoriété et de réputation ;
- etc.

[7] "Données personnelles et administration électronique" 26 février 2002, foruminternet.org
[8] Rapport Carcenac, "Pour une administration électronique citoyenne" 2001
[9] M. Braibant, Données personnelles et société de l'information : Doc. Française. 1998.
[10] Dictionnaire de l'Académie Française,1932-5, 8eme édition

### 1.1.5 CERCLES DE CONFIANCE

Il est nécessaire de bien distinguer les définitions technique et juridique d'un « cercle de confiance ».

Juridiquement, un cercle de confiance est constitué d'un réseau de partenaires commerciaux, principalement des fournisseurs de services et des fournisseurs d'identité et d'attributs. Ces acteurs ont passé des accords de partenariat bilatéraux les obligeant notamment à privilégier leurs partenaires dans leurs relations clients-fournisseurs, par exemple pour la fourniture de données d'identité. La nature de ces accords peut être contractuelle ou prendre une autre forme.

Il peut exister une multitude de cercles de confiance utilisant le même service de gestion d'identité, à l'intérieur d'un même cercle, ou bien en relation avec d'autres cercles ou des acteurs indépendants.

### 1.1.6 TECHNIQUES D'IDENTIFICATION

Il n'est pas aisé de déterminer une hiérarchie des techniques d'identification puisque l'utilisation d'une ou de plusieurs de ces techniques demeure variable et discrétionnaire.

De manière générale, les moyens d'identification et de vérification d'identité les plus utilisés à l'heure actuelle sont les suivants :

- **l'utilisation des données biométriques** : traditionnellement, la comparaison visuelle de la personne avec sa photographie sur un titre d'identité.
- **l'usage du nom** : la preuve du nom est normalement apportée par la carte nationale d'identité, même si celle-ci risque la fraude. afin de limiter les risques de falsification des cartes et permettre une identification électronique des citoyens, le ministère de l'intérieur a lancé en 2005 le programme ines[11]. ce dernier a été profondément remanié pour tenir compte du débat public de 2005. ayant changé de contenu, il a changé de nom : il s'agit désormais du programme de protection de l'identité (ppi). le projet va de pair avec la mise à disposition des citoyens de moyens d'identification et d'outils de signature électronique comme composantes de leur carte nationale d'identité électronique (cnie). or, la signature électronique fait d'ores et déjà l'objet d'une réglementation précise et détaillée sur le territoire national.
- **les numéros d'identification** tels que le numéro de sécurité sociale ou le numéro de permis de conduire sont aussi utilisés afin d'identifier une personne. ces numéros ont généralement été émis par des organismes publics afin de répondre aux besoins de la gestion d'un grand nombre de dossiers administratifs. ils sont couramment associés à une carte (jetons physiques). le système d'identification reposant uniquement sur des numéros d'identification peut présenter de grandes lacunes au plan de la sécurité, particulièrement lorsqu'il est utilisé à des fins d'identification par une autre organisation que l'organisme émetteur. en france, la quantité importante de fraudes qui existent au niveau des numéros et cartes de sécurité sociale en est un exemple.

[11] Le programme INES (Identité Nationale Electronique Sécurisée), émis par le Ministère de l'Intérieur, de la Sécurité Intérieure et des Libertés Locales, version 2 du 1er mars 2005. Il consistait à fusionner les procédures de demande de carte d'identité et de passeport, améliorer la gestion des titres dans de nouvelles applications, délivrer des titres conformes aux exigences internationales, offrir des moyens d'identification et de signature électroniques aux citoyens.

- **le recours à un tiers** : le recours à un tiers constitue une façon communément utilisée afin de vérifier l'identité d'une personne. fréquemment utilisée dans le cadre de transactions à distance, l'idée du recours à un tiers, tel le notaire, a donné naissance aux autorités de certification. le recours à des jetons physiques est également un moyen très répandu afin de vérifier l'identité d'une personne.
- **les jetons physiques** : la carte plastique représente l'une des formes de jetons physiques que l'on qualifie de jeton passif. les jetons passifs sont communément renommés pour donner lieu à une importante contrefaçon. le jeton passif est généralement associé à différents autres moyens d'identification et de vérification d'identité tel un numéro, le nom, la signature ou la photographie. on distingue enfin les jetons dits actifs. la carte à microprocesseur est un exemple de jeton actif.
- **les codes secrets** : plusieurs systèmes informatiques reposent enfin sur des codes secrets afin d'identifier des individus comme les codes d'accès (login) et le nip (numéro d'identification personnel, ou pin) utilisé par les cartes bancaires. les codes secrets utilisés seuls posent plusieurs problèmes au plan de la gestion et de la sécurité (oubli, confusion, dévoilement involontaire, etc.). ces difficultés sont accentuées lorsque le code est inscrit et transmis en clair, augmentant ainsi les chances d'interception et d'utilisation non autorisée. les codes secrets peuvent aussi être associés à un jeton actif. dans ce cas leur niveau de sécurité s'en trouve évidemment accru de façon significative puisque le code seul, bien que compromis, ne sera pas suffisant pour activer une fonction.

Il n'existe pas de moyen d'identification qui soit parfait et la simplicité et l'universalité des différents moyens d'identification et de vérification d'identité sont souvent inversement proportionnelles au niveau de fiabilité offert par ceux-ci au plan de l'identification.

L'identification est un processus destiné à réduire l'incertitude, en procurant la quantité optimale d'information à l'égard d'une personne afin de pouvoir procéder à la transaction avec un niveau de risque acceptable. Elle vise en premier lieu à rassurer les parties : définir et caractériser afin de mieux repérer. Se basant sur des mécanismes de sécurisation concrets, le but est en partie psychologique : inspirer confiance et sécurité.

Toutefois, il existe une gradation des besoins en matière d'identification : bon nombre des transactions que nous faisons dans la vie courante ne supposent pas un niveau très élevé de certitude quant à l'identification. Il en va de même de la plupart des transactions dont le paiement s'effectue sur place et en argent comptant.

Mais l'identification sur le net ne va pas sans exagération. Comportant des éléments physiquement attachés au porteur, elle concrétise l'idée d'objectivisation de l'identité et établit une certaine certitude qui dérange certains. Peu importent les pseudonymes, l'individu a le sentiment d'être identifié de façon unique par des caractéristiques qu'il n'a pas le pouvoir de modifier, et grâce à des procédés divers. La tendance à l'interconnexion croissante des fichiers contenant des renseignements sur une même personne renforce ce phénomène, car l'individu ignore quel usage il en est fait malgré les garde-fous imposés par le code pénal, le code des postes et communications électroniques, et la CNIL.

La « traçabilité » des données personnelles est par ailleurs le plus grand obstacle du point de vue de la CNIL. En conséquence, la Directive européenne Signature électronique[12], dans son attendu 25, légitime l'utilisation d'un pseudonyme dans la mesure où celui-ci contribue à une protection des données. Ainsi, pour être formé

[12] Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques

régulièrement, produire des effets juridiques fondés en droit et avoir une certaine valeur probante, un acte juridique a seulement besoin d'être imputé à quelqu'un, c'est-à-dire d'établir le lien entre lui et son auteur sans vraiment devoir exposer un élément particulier de son identité. Ce mécanisme d' « anonymisation » ou de « pseudonymisation » s'inscrit dans la tendance à la protection des données et vient contrecarrer, du moins contribuer à contrôler, le déploiement de l'identité numérique.
A ce sujet, la réaction de certains demeure préoccupante. Réclamer que l'anonymat soit promu au rang de droit constitutionnel, de droit de l'homme afin de protéger l'individu mais également installer durablement la confiance dans les réseaux numériques peut laisser perplexe sur cette question de confiance : comment la gagne t-on ? En identifiant l'utilisateur aussi bien que le professionnel ? En cachant son identité (voire leurs identités) ?

## 1.2 DROIT APPLICABLE ET PORTEE DES TEXTES

Cet inventaire des branches du droit concernées par le sujet de l'identité numérique a pour finalité de cerner le champ des règles de droit à prendre en compte dans le cadre du projet FC² (droits, obligations, sanctions). Il devra être tenu à jour et complété s'il s'avérait qu'il ne comportait pas les branches de droit requises.

### 1.2.1 DROIT SUR L'INFORMATION

Les différentes branches de droit sur l'information comprennent :

- les règles de l'état civil
- les règles sur la nationalité (code de la nationalité)
- les traités européens notamment traité de schengen, et la constitution française
- les droits fondamentaux de la personne résultant tant de la convention européenne des droits de l'homme du conseil de l'europe que de la jurisprudence de la cour de justice des communautés européennes et des cours et tribunaux français
- les conventions sur les droits d'auteur et autres droits de propriété intellectuelle
- les lois sur les archives
- la convention n°108 du conseil de l'europe sur le traitement automatique de données personnelles et le droit à la vie privée
- la loi informatique et libertés
- loi pénale sur les secrets professionnels et secrets de l'instruction
- lois dérogeant aux secrets et protection de la vie privée dans le cadre de la lutte contre le terrorisme et le blanchiment
- loi sur les données administratives : accès aux documents administratifs
- loi sur la signature électronique et code civil art. 1617 et suivants
- loi sur la sécurité financière
- loi sur la sécurité quotidienne
- loi sur les données publiques

### 1.2.2 DROIT A L'INFORMATION

Les différentes branches de droit à l'information comprennent :

- loi informatiques et libertés
- convention n°108 du conseil de l'Europe
- loi sur l'accès aux documents administratifs
- déclaration des droits de l'homme et liberté d'expression
- loi sur la transparence administrative
- droits de propriété intellectuelle
- droit de la consommation et notamment loi sur l'économie numérique
- droit de la concurrence et réglementation des échanges d'informations commerciales
- droit à et de l'interopérabilité (code de la propriété intellectuelle…)

### 1.2.3 DROITS ET OBLIGATIONS POUR REPRODUIRE LES INFORMATIONS

- informations protégées par un secret (vie privée ou secret professionnel)
- informations propriété d'un tiers ou dont les droits d'utilisation n'ont pas été donnés par voie contractuelle, réglementaire ou législative
- informations dont la diffusion ou publications sont interdites par contrat ou par la loi
- informations dont la diffusion ou publications sont soumises à des conditions contractuelles ou législatives
- informations de libre parcours mais où les droits d'adaptations sont réservés (protection de droits d'adaptation que certains acteurs du web prennent pour représenter des données pourtant appartenant au domaine public)
- conditions réglementaires, contractuelles et législatives de publication ou diffusion particulières, notamment soumises à l'autorisation ou l'absence d'oppositions de la personne visée par les informations (secrets, qu'ils soient bancaires ou médicaux)
- informations ou données personnelles dont la communication est soumise aux conditions de la loi informatiques et libertés.

### 1.2.4 FOCUS SUR LA LOI INFORMATIQUES ET LIBERTES

Il est utile de s'arrêter sur la loi Informatique et libertés[13], car elle structure les process et les architectures :

- recueil préalable du consentement de la personne fichée dont les données sont collectées, stockées et communiquées à sa demande ;
- demande (ou autorisation) authentifiée(s) de la personne visée par les données pour les transmettre à un tiers ;
- limitations au stockage centralisé des données personnelles, et contrôles d'accès aux données personnelles stockées ;
- respect de l'intégrité des données par utilisation de mesures de sécurité ;
- recommandations de la cnil au sujet des « cookies », sur la nécessité d'informer au préalable les utilisateurs et la possibilité pour ceux-ci de paramétrer leur navigateur afin de s'opposer à l'enregistrement de cookies.

#### 1.2.4.1 DEPLOIEMENT DE L'IDENTITE NUMERIQUE : TRAITEMENT DES DONNEES PERSONNELLES

La loi Informatique et Libertés modifiée, ainsi que la directive 95/46/CE 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, traitent de la question du traitement des données personnelles.

D'autre part, la loi relative à la sécurité quotidienne (LSQ) du 15 novembre 2001[14] rappelle à l'article 29 modifiant l'article L. 32-3 du Code des postes et télécommunications que : « les opérateurs de télécommunications (...) de la loi n° 86-1067 du 30 septembre 1986 (...), sont tenus d'effacer ou de rendre anonyme toute donnée relative à une communication dès que celle-ci est achevée... ». Mais d'un autre côté, la LSQ précise en ses points II, III et IV que : « pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire d'informations, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données technique (…) les données conservées et traitées... portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs et sur les caractéristiques

[13] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

[14] LOI no 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne JORF n°266 du 16 novembre 2001, NOR: INTX0100032L

techniques des communications assurées par ces derniers ». Une certaine doctrine en déduit que « La LSQ rappelle le principe général, mais que la réalité est bien différente. Pour des raisons de sécurité, le droit à l'anonymat cède plutôt le pas à une obligation d'identification contrôlée »[15].

#### 1.2.4.2 CONDITIONS DE LICEITE DES TRAITEMENTS DE DONNEES PERSONNELLES

Un traitement de données personnelles doit respecter les conditions suivantes :

##### 1.2.4.2.1 La collecte des données est loyale et licite

La finalité du traitement est au cœur du système de protection des données personnelles. C'est l'indicateur principal pour déterminer sa conformité avec la loi, depuis sa création, au cours de ses évolutions et jusqu'à sa destruction ou archivage. La CNIL a déjà eu l'occasion de déclarer qu'elle est pleinement favorable aux nouveaux services (a l'occasion du projet « Carte ville ») conçus pour simplifier les démarches administratives des usagers. La CNIL a néanmoins insisté sur le fait que ces nouveaux services, « parce qu'ils peuvent nécessiter de nouveaux traitements de données personnelles, le développement d'interconnexion voire la constitution de bases de données centralisées, appellent, sur le plan de la protection des données à caractère personnel, une vigilance particulière »[16]

##### 1.2.4.2.2 La finalité du traitement doit être légitime et déterminée

En vertu du principe de finalité, les données personnelles ne peuvent être traitées que pour un usage légitime et déterminé. A ce titre, il est très important que le responsable de traitement d'information se conforme à cette exigence et précise très clairement toutes les finalités du traitement.

##### 1.2.4.2.3 Les données personnelles sont adéquates, pertinentes et non excessives au regard de la finalité du traitement

Il s'agit d'un point crucial en ce qui concerne l'identification en ligne : l'exigence d'identification doit être strictement justifiée et son degré (faible/fort) proportionné au besoin.

La CNIL a déjà rappelé que la dématérialisation des procédures ne doit pas être l'occasion de recueillir plus de données à caractère personnel que nécessaire. Ex : ne pas imposer l'identification des usagers en ligne pour le simple téléchargement d'un formulaire ; ne pas recueillir des données qui ne seraient pas pertinentes - comme le numéro de carte d'identité - pour la délivrance d'un extrait d'acte d'état civil.

##### 1.2.4.2.4 La durée de conservation des données est limitée en fonction de la finalité du traitement

La durée de conservation des données personnelles doit être établie en fonction de la finalité du traitement. Attention, toutes les données peuvent ne pas avoir la même durée de conservation au sein d'un même traitement. Ex : un échange de courriels pour l'obtention d'information n'a pas lieu d'être conservés par l'administration. La durée de conservation de certaines données (ex : données relatives au paiement) peut être fixée à raison des exigences au titre de la preuve ou du contrôle exercé par les autorités habilitées, dans une limite raisonnable.

Au-delà de cette durée, les données doivent être archivées dans les conditions définies par l'ancienne loi du 3 janvier 1979 sur les archives, désormais codifiée aux articles L. 211-1 et suivants du Code du patrimoine[17].

---

[15] Thierry Piette-Coudol, L'identité des personnes, les certificats et la signature électronique, Communication Commerce électronique n° 1, Janvier 2005, Etude 2

[16] CNIL, 24ème rapport d'activité 2003, p. 76

[17] Ordonnance 2004-178 du 20 février 2004 relative à la partie législative du Code du patrimoine, JORF 24 février 2004



#### 1.2.4.2.5 Les destinataires doivent être précisément définis et limités

Les destinataires sont toutes les personnes habilitées à recevoir communication des données autres que les "sous-traitants" et les "tiers autorisés". Comme pour déterminer les données traitées et la durée de conservation, les destinataires sont définis au regard de la finalité du traitement. Il s'agit des seules personnes concernées par le traitement.

En matière d'administration électronique, la CNIL veille tout particulièrement à ce que les données des administrés ne puissent pas être diffusées trop largement. Dans le cadre de FC², les partenaires du cercle sont multiples mais leur nombre peut augmenter avec le temps .Le problème sera de savoir si l'acceptation de la personne de fédérer son identité dans le cercle est un engagement envers le cercle en tant qu'entité ou en tant que l'ensemble des partenaires (avec chacun de manière individuelle). La solution pourrait être la voie contractuelle, via les conditions d'acceptation du cercle de confiance. Cette question, liée à la gouvernance de la plate-forme, reste toutefois ouverte.

#### 1.2.4.2.6 Le traitement de données personnelles doit respecter le principe de proportionnalité concernant les interconnexions

La CNIL vise au respect du principe fondamental suivant : chaque destinataire des données personnelles n'a accès qu'aux données qui le concerne, et ce, afin d'éviter la constitution de bases de données centralisées. Il faudra alors examiner de façon approfondie les différentes options techniques envisagées et préférer celle qui maintient des identifiants sectoriels. Selon la CNIL, « les sphères d'intervention du secteur public et du secteur privé doivent être respectées avec pour chacune un identifiant différent »[18].

Un problème flagrant se pose dans le cadre de FC² puisque le même identifiant sert sur plusieurs sites publics et privés. « La CNIL rappelle son attachement à préserver la pluralité des identifiants -en général- en fonction des besoins sectoriels, plutôt qu'une identité numérique unique » [Rencontre avec la CNIL du 26 février 2008]

Par ailleurs, tout projet de mise en relation de fichiers ou de bases de données fait l'objet d'un contrôle spécifique de la CNIL qui apprécie la finalité même de l'interconnexion, notamment par la nécessité d'un intérêt public important, et la pertinence des données échangées. A cet égard, la CNIL a adopté une interprétation large de la notion d'interconnexion : il s'agit de « tout traitement automatisé mis en œuvre par un ou plusieurs responsables qui consiste à mettre en relation des données ayant une finalité avec d'autres données ayant une finalité identique ou différente. Cette mise en relation peut consister à transférer un fichier pour alimenter un autre fichier ou pour réaliser la fusion de ces fichiers, à mettre ponctuellement en relation plusieurs fichiers normalement gérés séparément, par exemple en constituant un fichier d'appel à partir de l'un de ces fichiers qui servira à interroger les autres fichiers et sera enrichi par les résultats de cette interrogation. Il peut également s'agir d'assembler des informations provenant de plusieurs fichiers au sein d'une même base de données (exemple des bases dénommées « entrepôts de données » alimentés par des informations provenant de différents fichiers) avec un éventuel recours à des techniques logicielles de mises en relations ponctuelles (outils dits de datamining) ou de créer un lien technique entre plusieurs bases de données nominatives qui permettra, par exemple, de les consulter simultanément (par exemple, des sites portails permettant par des « liens hypertextes » d'assurer une mise en relation avec d'autres bases) »[19].

La sanction du non-respect de ces principes au stade de l'étude de faisabilité du projet fait courir le risque de rencontrer des difficultés lors de l'instruction du dossier par la CNIL. En effet, toutes les caractéristiques du traitement, y compris techniques, doivent être énoncées dans le détail lors de l'accomplissement des formalités auprès de la CNIL.

[18] CNIL, 24ème rapport d'activité 2003, p. 115
[19] CNIL, 24ème rapport d'activité 2003, p. 119

Dans un stade plus avancé, les données pouvant être réparties entre un fournisseur d'identité et un fournisseur de service, le client devra alors faire deux demandes distinctes toutes les deux sur le fondement de la loi Informatique et Libertés. Les recours relatifs à la protection des données personnelles contre le fournisseur d'identité viseront plutôt les informations relatives à l'identité du client (nom, domicile) alors que ceux du fournisseur de service viseront plutôt les informations relatives aux données spéciales à sa relation avec le client et qu'il détient (numéro de compte bancaire si le fournisseur de services est une banque).

#### 1.2.4.3 RESPECT DES DROITS FONDAMENTAUX DES PERSONNES

##### 1.2.4.3.1 Les droits consacrés

Les droits fondamentaux des usagers sont le droit à l'information, des droits d'accès et de rectification et du droit d'opposition :

- **droit de communication** : il permet à toute personne d'obtenir la communication des données à caractère personnel la concernant en vertu de son droit d'accès. le responsable de traitement ne peut s'y opposer, sauf en cas de demandes manifestement abusives, notamment par leur nombre ou leur caractère répétitif ou systématique. la faculté de subordonner la délivrance de la copie des données personnelles au paiement d'une redevance dont le montant ne peut excéder le coût de reproduction lui est toutefois laissée.
- **droit d'accès et de rectification** : le législateur a incité les citoyens à participer directement à leur défense en mettant à leur disposition un moyen d'action qui est le droit individuel d'accès aux fichiers. c'est le *privacy act* américain de 1974 et un arrêt du conseil d'état[20] du 13 février 1976 ont inspire les rédacteurs de la loi n° 78-17 du 6 janvier 1978 cette dernière a consacré ce droit d'accès non seulement pour les fichiers automatisés, mais aussi pour les fichiers manuels. il résulte des termes mêmes des articles 34 et 45 de la loi du 6 janvier 1978 que cette dernière loi régit seule le droit d'accès aux fichiers de l'administration comportant des mentions nominatives, qu'ils soient automatisés, mécanographiques ou manuels, et en limite le bénéfice aux personnes physiques[21]. toute personne peut demander que soient rectifiées, complétées, mises à jour, verrouillées ou effacées, les données la concernant qui sont inexactes, périmées, incomplètes, équivoques ou dont le traitement est interdit. les héritiers d'une personne décédée ont également le droit de faire procéder aux mises à jour nécessaires pour tenir compte du décès intervenu. depuis la réforme de la loi informatique et libertés, le responsable de traitement doit justifier qu'il a procédé à ces opérations, sans aucun frais pour le demandeur. en outre, si la rectification ou suppression est obtenue par la personne concernée grâce a l'exercice de son droit d'accès, le responsable de traitement est tenu de lui rembourser la redevance éventuellement perçue pour la délivrance de la copie de ses données personnelles.
- **droit d'opposition** : toute personne a le droit de s'opposer au traitement des données personnelles la concernant à la condition de justifier d'un motif légitime. le motif légitime est présumé lorsqu'il s'agit des traitements ayant pour finalité la prospection commerciale ; la personne concernée n'a pas à se justifier et ne doit supporter aucun frais pour exercer son opposition. a l'évidence, nul ne peut s'opposer aux traitements obligatoires répondant aux exigences législatives, tels que la tenue du registre d'état civil, etc.

[20] 13 févr. 1976, Deberon : Rec. CE, p. 100 ; AJDA 1976, p. 217 et chron. Michel Boyon et Michèle Nauwelaers, p. 199. Arrêt ou a été admis le droit des intéressés à être informés des mentions portées sur les fichiers administratifs les concernant et à en obtenir, en cas d'inexactitude, la suppression lorsque ces mentions sont susceptibles d'être communiquées à des tiers.

[21] CE, 10e et 3e sous-sect, 15 févr. 1991, Eglise de scientologie de Paris, requête n° 68639, Dr. adm. 1991, comm. n° 158. – 22 mai 1995, Synd. Régional Sud PTT Midi-Pyrénées, req. n° 151288



#### 1.2.4.3.2 Les obligations du responsable de traitement

En pratique, la CNIL invite le responsable de traitement à communiquer spontanément aux personnes l'identité et les coordonnées de la personne ou du service à contacter afin qu'elles soient effectivement en mesure d'exercer leurs droits et vérifier l'exactitude de leur situation administrative.

En application de l'art. 226-18-1 du Code pénal, le fait de procéder à un traitement de données personnelles malgré l'opposition de la personne concernée lorsque ce traitement répond à des fins de prospection, notamment commerciales, ou lorsque l'opposition est fondée sur des motifs légitimes et refusée est passible d'une peine maximale de 5 ans d'emprisonnement et de 300.000 € d'amende, multiplié par cinq si la personne est morale.

Dans le cadre de FC$^2$, qui sera le responsable du traitement ? Le recours croissant à l'externalisation a brouillé la cartographie des responsabilités. Vers qui l'utilisateur du service se retournera t-il? La directive européenne sur la protection des données prévoit qu'il peut y avoir plusieurs responsables de traitement, ce n'est pas le cas en France, ou il y a comme on l'a déjà vu un seul responsable. Nous considérons le fournisseur d'identité la personne la plus apte à jouer ce rôle, vu sa maitrise et sa mise à disposition permanente des données personnelles.

Il faut que ce responsable informe la personne auprès de laquelle sont recueillies les informations de la finalité des traitements, la conséquence du défaut de réponse et de son droit d'accès, du transfert des données à l'extérieure de l'Union Européenne.
«Toute personne utilisatrice de réseau électronique doit être informée de l'accès à des infos stockées dans son terminal de connexion ou dans l'équipement, des moyens pour s'y opposer » art 32 allongé en 2004 (rajout dans grand 2). Egalement il est dit que les données recueillies par les prestataires de services de certification électronique (PSCE) pour les besoins de la délivrance et de la conservation des certificats doivent l'être directement auprès de la personne concernée. Le responsable de traitement doit prendre toutes les mesures nécessaires pour que les infos ne soient pas divulguées. Article 34 de la loi Informatique et Libertés modifiée : « Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »

Il s'agit ici d'une **obligation de moyens renforcée,** c'est-à-dire que le responsable de traitement est tenu d'évaluer lui-même et de mettre en œuvre des mesures de sécurité d'autant plus strictes et efficaces que les risques sont importants. Dans le contexte de l'administration électronique, la CNIL a indiqué que les échanges de données à caractère personnel entre le site Internet et les personnes publiques doivent être sécurisés (par des procédés de chiffrement des données par exemple). Pour autant, il ne faut pas en déduire que toute démarche administrative dématérialisée exige le recours systématique à de tels mécanismes de sécurisation (ex : une demande de formulaire en ligne).

Quant au cas de transfert des données hors du territoire national, il n'existe pas d'obligation spécifique en cas de transfert des données personnelles dans un Etat membre de l'Union Européenne. En effet, le régime de la protection des données personnelles a été harmonisé par la Directive européenne 95/46. En revanche, certains principes doivent être respectés dès lors que les données sont transférées hors de l'Union Européenne, vers un pays tiers. En règle générale, le transfert vers un pays tiers n'est autorisé que s'il assure un « niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes». En pratique, la Commission Européenne

s'attache à identifier les pays qui présentent un niveau de protection suffisante, avec l'aide du Groupe de protection des données (G29) de l'Union Européenne.
A ce jour, il s'agit de l'Ile de Man, Guernesey, la Suisse, le Canada, et l'Argentine. FC² étant un projet national sinon européen, le problème de transfert des données en dehors du territoire national ne se pose que dans la limite du cadre européen.

### 1.2.4.4 FORMALITES PREALABLES

#### 1.2.4.4.1 La déclaration à la CNIL et le « Correspondant Informatique et Libertés »

L'Art. 22 de la loi informatique et libertés parle de « déclaration » ; il s'agit d'un envoi du dossier à la CNIL qui renvoie un récépissé, avec possibilité de déclaration par voie électronique et le défaut de déclaration est sanctionné pénalement.

On note une absence de formalités préalables pour les activités purement personnelles et les copies temporaires (pas de formalités préalables pour le correspondant à la protection des données). Les traitements aux fins de journalisme et de manière générale dans l'activité de presse sont également dispensés vu leurs finalités. Les formalités durcies sont ceux concernant les traitements qui doivent faire l'objet d'une autorisation de la CNIL, qui peut faire un recours devant la CE.

L'art. 25 de la loi évoque les traitements sensibles de l'art 8 : pour les traitements concernant les données génétiques, traitement relatifs aux mesures de sûreté, aux traitements relatifs à l'interconnexion, les traitements sur les appréciations des difficultés sociales des personnes, les traitements comportant des données biométriques relatifs au contrôle des personnes. Certains traitements sont par ailleurs autorisés par arrêté des ministres compétents après avis motivé de la CNIL. Un avis de la CNIL sur décret et projet de loi seraient utile pour les traitements de police (ex : art 26 et 27 de la loi).
L'art. 22 de la loi informatique et libertés indique qu'un correspondant à la protection des données tient la liste des traitements de l'entreprise ou de l'administration et veille à la protection de la loi. Ce correspondant sera soit un agent de l'entreprise soit une personnalité ou un organisme extérieur à l'entreprise. Il est indiqué au représentant du personnel et notifié à la CNIL. « Le correspondant est une personne bénéficiant des qualifications requises pour exercer ses missions. Il tient une liste des traitements effectués immédiatement accessible à toute personne en faisant la demande et ne peut faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions. Il peut saisir la Commission nationale de l'informatique et des libertés des difficultés qu'il rencontre dans l'exercice de ses missions. » Un décret d'application de la loi précise le statut du correspondant.

#### 1.2.4.4.2 Rôle du « Correspondant Informatique et Libertés » (CIL)

En principe, les traitements automatisés de données à caractère personnel font l'objet d'une déclaration auprès de la CNIL (Art 23 et 24 de la loi du 6 janvier 1978). Cependant, les traitements pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel sont dispensés de ces formalités de déclaration[22]. La seule exception à ce principe est lorsqu'un transfert de données à caractère personnel à destination d'un Etat non membre de la Communauté européenne est envisagé (Art 22 de la loi du 6 janvier 1978). Le correspondant est chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la loi du 6 janvier 1978 (modifiée par la loi du 6 août 2004).

*La désignation du correspondant*
La désignation du correspondant est notifiée à la CNIL. Cette notification est adressée par lettre recommandée avec demande d'avis de réception, ou par remise au secrétariat

[22] hwww.cnil.fr/fileadmin/documents/approfondir/dossier/CIL/Guide_correspondants.pdf

de la commission contre reçu, ou par voie électronique avec accusé de réception qui peut être adressé par la même voie (Art 42 du décret du 20 octobre 2005).

Plusieurs mentions doivent figurer dans cette notification, dont :

- La nature des liens juridiques entre le correspondant et la personne, l'autorité publique, le service ou l'organisme auprès duquel il est appelé à exercer ses fonctions - Tout élément relatif aux qualifications ou références professionnelles du correspondant.
- Les mesures prises par le responsable des traitements en vue de l'accomplissement par le correspondant de ses missions en matière de protection des données (Art 43 du décret du 20 octobre 2005).

De plus, la désignation du correspondant est, préalablement à sa notification à la CNIL, portée à la connaissance de l'instance représentative du personnel compétente par le responsable des traitements, par lettre recommandée avec demande d'avis de réception (Art 45 du décret du 20 octobre 2005).

Le responsable des traitements ou son représentant légal ne peuvent être désigné comme correspondant (Art 46 du décret du 20 octobre 2005). L'externalisation est seulement réservée aux petites et moyennes entreprises car lorsque plus de cinquante personnes sont chargées de la mise en œuvre ou ont directement accès aux traitements ou catégories de traitements automatisés pour lesquels le responsable entend désigner un correspondant à la protection des données à caractère personnel, seul peut être désigné un correspondant exclusivement attaché au service de la personne, de l'autorité publique ou de l'organisme, ou appartenant au service, qui met en œuvre ces traitements (Art 44 du décret du 20 octobre 2005).

Cependant, plusieurs exceptions sont posées et vont à l'encontre de ce principe à l'exclusivité de l'attachement du correspondant :

- lorsque le responsable des traitements est une société qui contrôle ou qui est contrôlée (au sens de l'article l. 233-3 du code de commerce), le correspondant peut être désigné parmi les personnes au service de la société qui contrôle, ou de l'une des sociétés contrôlées par cette dernière.
- lorsque le responsable des traitements est membre d'un groupement d'intérêt économique - gie (au sens du titre v du livre deuxième du code de commerce), le correspondant peut être désigné parmi les personnes au service dudit groupement
- lorsque le responsable des traitements fait partie d'un organisme professionnel ou d'un organisme regroupant des responsables de traitements d'un même secteur d'activités, il peut désigner un correspondant mandaté à cette fin par cet organisme (art 44 du décret du 20 octobre 2005).

*Les modalités d'exercice de la mission du correspondant*
Le correspondant à la protection des données à caractère personnel exerce sa mission directement auprès du responsable des traitements et il ne reçoit aucune instruction pour l'exercice de celle-ci. De plus, les fonctions ou activités exercées concurremment par le correspondant ne doivent pas être susceptibles de provoquer un conflit d'intérêts avec l'exercice de sa mission (Art 45 du décret du 20 octobre 2005).

Cependant, il n'a pas au sein de l'entreprise le statut de salarié protégé (tel un délégué du personnel) et il est difficile de définir les limites de son indépendance ou des pressions qu'il serait susceptible de subir, en l'absence d'un tel cadre légal pour le protéger. Les textes semblent seulement permettre la possibilité d'éviter un conflit d'intérêt direct et manifeste entre la mission exercée par le correspondant et les intérêts du responsable des traitements ou les fonctions exercées en parallèle par ce salarié, et il appartiendra donc à la CNIL de préciser l'étendue de l'application de telles dispositions.

Enfin, c'est le responsable des traitements qui doit fournir au correspondant tous les éléments lui permettant d'établir et d'actualiser régulièrement une liste des traitements automatisés mis en oeuvre au sein de l'établissement, du service ou de l'organisme au sein duquel il a été désigné (Art 47 du décret du 20 octobre 2005).

*Les missions du correspondant*
Dans les trois mois de sa désignation, le correspondant dresse une liste où sont précisés, pour chacun des traitements automatisés :

- les nom et adresse du responsable du traitement et, le cas échéant, de son représentant.
- la ou les finalités de traitement.
- le ou les services chargés de le mettre en oeuvre.
- la fonction de la personne ou le service auprès duquel s'exerce le droit d'accès et de rectification ainsi que leurs coordonnées.
- une description des catégories de données traitées, ainsi que les catégories de personnes concernées par le traitement.
- les destinataires ou catégories de destinataires habilités à recevoir communication des données.
- la durée de conservation des données traitées (art 48 du décret du 20 octobre 2005).

Mais le correspondant doit également veiller au respect des obligations prévues par la loi Informatique et Libertés pour les traitements au titre desquels il a été désigné. Pour ce faire :

- il peut faire toute recommandation au responsable des traitements.
- il est consulté, préalablement à leur mise en œuvre, sur l'ensemble des nouveaux traitements appelés à figurer sur la liste qu'il est chargé de dresser.
- il reçoit les demandes et les réclamations des personnes intéressées relatives aux traitements figurant sur la liste qu'il est chargé de dresser. lorsqu'elles ne relèvent pas de sa responsabilité, il les transmet au responsable des traitements et en avise les intéressés.
- il informe le responsable des traitements des manquements constatés avant toute saisine de la cnil.
- il établit un bilan annuel de ses activités qu'il présente au responsable des traitements et qu'il tient à la disposition de la commission.

Pour finir, lorsque la CNIL constate, après avoir recueilli ses observations, que le correspondant manque aux devoirs de sa mission, elle demande au responsable des traitements de le décharger de ses fonctions (Art 52 du décret du 20 octobre 2005).

Le recours au CIL semble adapté aux structures complexes comme les fédérations de cercles de confiance. En effet dans un cercle de confiance il est difficile de désigner la personne qui sera chargée des déclarations auprès de la CNIL. Est ce le fournisseur d'identités, détenteur des données personnelles ? Est ce l'émetteur d'identité ? Le fournisseur de services / commerçant ? La nomination d'un CIL dont le mode de nomination reste à déterminer pour chaque cercle de confiance, semble plus adapté et aurait pour avantage de simplifier les procédures.

### 1.2.5 SIGNATURE ELECTRONIQUE

Le type d'architecture adopté par FC² repose sur l'établissement de liens de confiance entre fournisseurs de services, les fournisseurs d'identités, les fournisseurs d'attribut et autorités en charge des procédés administratifs. Les entités ainsi liées forment un cercle de confiance. Les fournisseurs de services acceptent les affirmations faites par les autorités administratives ou tout fournisseur d'identités, qui ont la charge de fournir la preuve des données personnelles auprès des fournisseurs de services. Cela se traduit

dans la pratique par le partage de confiance permettant la signature des affirmations, généralement, grâce à une infrastructure à clés publiques. Les problèmes complexes en termes de gestion des identités proviennent de l'interconnexion d'applications intra ou inter-systèmes d'informations, et la conception d'applications inter-systèmes d'informations. « Il est en effet nécessaire d'assurer la sécurité des échanges, mais aussi de gérer les identités de clients. Une architecture de fédération d'identités basée sur les technologies du Web est une architecture orientée services. Un conditionnement des échanges de messages, en ajoutant des informations de sécurité aux entêtes des messages échangés »[23] est tout a fait concevable.

La sécurité juridique des transactions passe nécessairement par l'authentification et l'identification des personnes, sous-entendu dans le respect de l'anonymat. La CNIL insiste sur le respect des règles de sécurité les plus simples comme la gestion des mots de passe rigoureuse, comme la fermeture des logiciels lors des pauses du personnel, la restriction des accès aux applications au seul personnel habilité en raison de la fonction des agents, et l'élaboration d'une *Charte de Sécurité*[24]. L'utilisation conjointe de divers moyens d'identification et de vérification d'identité apparaît, à l'heure actuelle, comme étant la solution la plus apte à assurer un équilibre entre les fiabilité et simplicité au niveau de l'utilisation.

Pour la mise en place des téléprocédures, le recours systématique à des procédés d'authentification ou de signature électronique ne constitue pas, pour la CNIL, une condition préalable. Généralement, les démarches administratives ne nécessitent pas une identification formelle. Pour des besoins d'information, il est possible de demander en ligne des formulaires, qui sont disponibles librement auprès de l'administration, ou de consulter un document administratif, sans avoir à « décliner son identité ». La CNIL a quand même, depuis 2000, recommandé une signature électronique pour la mise en œuvre des télédéclarations fiscales.

C'est l'**authentification** qui fournit la certitude attendue. L'entité détentrice des clés présente la clé publique au certificateur. Le certificateur, grâce au certificat électronique, atteste de la concordance entre l'identité de l'entité et une clé publique, cette dernière lui ayant été présentée par un porteur identifié.

La **certification** établit le lien indispensable entre la clé publique et son propriétaire, à la fois pour l'authentification et la signature électronique. Selon l'Organisation internationale de standardisation (ISO), le certificat électronique est « un objet informatique qui permet de lier de façon intangible une identité d'entité à certaines des caractéristiques de cette entité ».
La Commission Européenne affirme : « Une des tâches principales des certificateurs consiste à authentifier le propriétaire et les caractéristiques d'une clé publique de manière à créer la confiance. Dès qu' [un certificateur] a établi la propriété et les caractéristiques d'une clé publique de signature[25], un certificat contenant cette clé et d'autres détails est émis. Ce certificat est lui-même signé numériquement, c'est-à-dire que [le certificateur] signe le certificat avec sa clé privée afin d'établir une corrélation avec le propriétaire de la clé »[26]. Le certificat électronique est employé pour donner cette certitude : la concordance et l'adéquation entre l'identité du signataire ou de la personne qui s'authentifie et la clé publique.

[23] Architectures de fédération d'identités et interopérabilité, Mikael Ates, Christophe Gravier, Jeremy Lardon, Jacques Fayolle, Bruno Sauviac, Equipe SATIN – Laboratoire DIOM, Institut Supérieur des Techniques Avancées de Saint-Etienne
[24] CNIL, 24ème rapport d'activité 2003, p. 115-116 « Penser à la sécurité informatique »
[25] Peut être étendu à l'authentification
[26] COM 97/503 de la Commission Européenne

La **signature électronique**, elle, est au cœur de tout procédé de sécurisation d'échanges électroniques. Jusqu'à présent, elle est l'apanage de la personne physique sauf pour les factures des personnes morales[27]. Son importance dans la fluidité des actions en ligne fait que certaines voix[28] s'expriment en faveur de la signature électronique de la personne morale.

La future carte nationale d'identité électronique (CNIE) mettra à la disposition des citoyens un moyen de signature électronique, en plus d'un procédé d'authentification. La CNIE simplifiera l'accès à certains services en permettant à ses détenteurs de signer électroniquement. La signature électronique joue le rôle primordial de preuve entre le client et le fournisseur de services, par exemple lors d'un abonnement en ligne ou d'une ouverture de compte en ligne.

Transposant la directive 1999/93/CE du 13 décembre 1999 pour un cadre commun sur les signatures électroniques[29] du Parlement et du Conseil européens, la loi du 13 mars 2000 a posé le cadre juridique de la preuve et de la signature électronique. Elle a été complétée par les décrets n° 2001-272 du 30 mars 2001 et n° 2002-535 du 18 avril 2002 ainsi que l'arrêté du 31 mai 2002. Ce dernier arrêté a d'ailleurs été abrogé par un arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique (PSCE) et à l'accréditation des organismes qui procèdent à leur évaluation. Enfin, la loi n°2004-575 pour la confiance dans l'économie numérique du 21 juin 2004 (LCEN) a consacré la validité juridique des écrits sous forme électronique (article 1108-1 du code civil)[30].

La première définition légale de la signature électronique a été donnée par la loi du 13 mars 2000. Ce fut une définition plutôt fonctionnelle. Deux fonctions doivent être remplies par toute signature : l'identification de l'auteur de l'acte et l'expression du consentement du signataire au contenu de l'acte (art 1316-4 al 1 du code civil).

La définition générale de la signature électronique se trouve quant à elle à l'article 1316-4, al.2 code civil, qui dispose : « Lorsqu'elle est électronique, elle [la signature] consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat ».

On peut distinguer les signatures électroniques dites "**simples**", dont l'utilisateur doit démontrer qu'elles sont fiables, et les signatures électroniques **sécurisées** pour lesquelles la loi pose une présomption de fiabilité du procédé dès lors qu'elles répondent aux exigences juridiques et techniques découlant du décret d'application du 30 mars 2001.

Ainsi, la fiabilité « est présumée jusqu'à preuve contraire lorsque ce procédé met en œuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié » (art. 2) délivré par un prestataire de services de certification (PSCE). En pratique, pour qu'une signature soit sécurisée, le certificat ne suffit pas : il faut que tout l'environnement soit sûr (clef privée sous contrôle exclusif du signataire, dispositif de création de signature protégé contre les

[27] C'est un point de vue juridique (la loi ignore le concept de signature de personne morale), mais cela n'empêche pas en pratique de faire signer une personne morale (humainement ou via un serveur). D'ailleurs, la loi ignore aussi le concept d'authentification.
[28] Eric Caprioli, Caprioli et associés – Les nouvelles applications de la signature électronique , FNTC, 2007
[29] Directive 1999/93/CE du 13 décembre 1999, JOCE n° L. 13, 19 janvier 2000, p.12
[30] J.O. n° 143 du 22 juin 2004, p. 11182.

piratages) de manière à garantir que ce que le logiciel fait signer à l'utilisateur est bien ce qui est affiché à l'écran.

En tout état de cause, le marché français ne dispose pas, à ce jour, de signature électronique sécurisée ni de certificats qualifiés (hormis celui établi par la Banque de France dans ses relations avec les banques). Seuls certains modules sont accrédités par la D.C.S.S.I.

## 1.2.6 RESPONSABILITE

### 1.2.6.1 ROLE STRUCTURANT DU PSCE

L'activité des différents PSCE est directement ou indirectement liée à la collecte et à l'utilisation de données à caractère personnel. Il peut s'agir de prestataires techniques comme les fournisseurs d'accès ou d'hébergement ou de prestataires de services de confiance comme les fournisseurs d'identité par exemple. Dans un cercle de confiance, le principe de fédération positionne le fournisseur d'identité (ou IdP) comme structure pivot permettant la navigation d'un même principal entre des services qu'il a fédérés. Le fait de placer le fournisseur d'identité comme PSCE peut simplifier la structure déjà complexe d'un cercle de confiance. Ce n'est toutefois pas une obligation. Un fournisseur d'identité qui serait aussi PSCE pourrait donc authentifier l'utilisateur sur la base de son certificat électronique.

Les P.S.C.E. délivrent, à titre principal, des certificats électroniques permettant d'établir le lien entre les données de vérification d'authentification ou de signature électronique (clé publique) et l'individu concerné[31]. Ce processus de normalisation permet la régulation de l'activité de P.S.C.E. en tentant d'assurer une interopérabilité technique minimale entre les différents prestataires. Dans cette optique technique, les différents P.S.C.E. se situent au cœur d'une Infrastructure à clé publique (ICP ou PKI)[32].

Cette I.C.P. se compose de plusieurs organismes : autorité de certification, opérateur de certification et autorité d'enregistrement, services de publication (annuaire ou liste de révocation des certificats ou des autorités de certification reconnues). En règle générale, c'est l'autorité de certification qui sera le P.S.C.E. dans la mesure où c'est elle qui est responsable du certificat émis.
Du fait de leur rôle central dans les réseaux numériques, les P.S.C.E. ont un régime juridique différencié selon qu'ils délivrent ou non des certificats qualifiés.

*Cadre juridique des PSCE*
Le décret du 30 mars 2001 précise les obligations juridiques qui pèsent sur les P.S.C.E. Comme l'énonce l'article 6 de ce décret, «un certificat électronique ne peut être regardé comme qualifié que s'il comporte les éléments énumérés au I et que s'il est délivré par un prestataire de services de certification électronique satisfaisant aux exigences fixées au II. ». L'article 6-II du même décret prévoit à leur charge, l'obligation «de conserver, éventuellement sous forme électronique, toutes les informations relatives aux certificats électroniques qui pourraient s'avérer nécessaires pour faire la preuve en justice de la certification électronique ou d'utiliser des systèmes de conservation des certificats qui garantissent que l'introduction de la modification des données est réservée aux seules personnes autorisées à cet effet par le prestataire et que toute modification de nature à compromettre la sécurité du système puisse être détectée ».
Le certificat électronique doit comporter ainsi un certain nombre de mentions obligatoires : le nom du porteur, la clé publique du porteur, le nom de l'autorité de certification qui a délivré le certificat, la signature de cette autorité de certification au moyen de sa propre clé privée et la durée de validité du certificat (date de début et de fin de validité).

[31] Article 1. 11 du décret du 30 mars 2001.
[32] Ou encore appelée Infrastructure de Gestion de Clés (I.G.C.).

La libre circulation au sein de l'Union européenne des services de certification est assurée. Il est également prévu, hors de l'Union européenne, un mécanisme de reconnaissance des entreprises extérieures à l'Europe (dir. 13 déc.1993, art. 7).
Les arrêtés du 31 mai 2002 (art. 7) et du 26 juillet 2004 fixent les conditions dans lesquelles ces prestataires peuvent demander à être reconnus comme « qualifiés », après évaluation et selon une procédure d'accréditation des organismes de qualification décrite dans ce même arrêté. Ces organismes sont eux mêmes accrédités par le Comité français d'accréditation (Cofrac) et la Direction centrale de la sécurité des systèmes d'information (DCSSI) contrôle la délivrance des accréditations.

Le PSCE doit être en mesure de vérifier de manière certaine et non équivoque l'identité du demandeur ; la procédure d'enregistrement du certificat en dépend ainsi que toute la sécurité juridique en termes de preuve et de validité des processus contractuels qui en découlent. Afin d'établir un certificat, le PSCE est amené à collecter diverses informations directement liées à la personne de son titulaire.

#### 1.2.6.2 MISE EN ŒUVRE DE LA RESPONSABILITE

L'article 33 de la LCEN fait peser sur les PSCE une responsabilité de plein droit : « sauf à démontrer qu'ils n'ont commis aucune faute intentionnelle ou négligence, les prestataires de services de certification électronique sont responsables du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats présentés par eux comme qualifiés dans chacun des cas suivants :

- les informations contenues dans le certificat, à la date de sa délivrance, étaient inexactes ;
- les données prescrites pour que le certificat puisse être regardé comme qualifié étaient incomplètes ;
- la délivrance du certificat n'a pas donné lieu à la vérification que le signataire détient la convention privée correspondant à la convention publique de ce certificat ;
- les prestataires n'ont pas, le cas échéant, fait procéder à l'enregistrement de la révocation du certificat et tenu cette information à la disposition des tiers ».

La responsabilité du prestataire pourra cependant être écartée lorsqu'il sera établi que l'utilisateur aura fait du certificat un usage « dépassant les limites fixées à son utilisation ou à la valeur des transactions pour lesquelles il peut être utilisé, à condition que ces limites figurent dans le certificat et soient accessibles aux utilisateurs ».

Pour que toutes les parties intéressées aux services de certification (ex : les abonnés, les tierces parties au contrat d'abonnement qui se fient aux certificats) puissent être en mesure de les utiliser dans leurs opérations en ligne, il est nécessaire que le P.S.C.E. leur procure une information correcte sur les modalités d'utilisation du certificat, la demande de qualification ainsi que les modalités de contestation et de règlement des litiges (article 6-II).

Comme le souligne le rapport de l'AFNOR[33] : « Lorsque le P.S.C.E. fournit à son client des services de gestion de clés, il ne doit ni stocker, ni copier les données afférentes à la création de signature de celui-ci (article 6-II, i). Cette exigence découle directement d'un principe de sécurité en vertu duquel il faut disposer de deux paires de clés distinctes lorsque l'on entend signer et chiffrer des messages. L'usage d'une seule paire de clés à la fois pour la signature et pour le chiffrement des messages aurait pour conséquence de créer le risque de voir un tiers s'approprier ou reconstituer la clé privée de signature

[33] « La signature électronique et les infrastructures à clé publique dans le contexte de l'identité numérique : Quels usages pour les titres sécurisés émis par l'Etat dans le monde de l'économie numérique », novembre 2007.

d'une personne et qu'elle se fasse passer pour elle (usurpation d'identité) . Dans le cas de signature numérique, la clé privée doit rester secrète et sous le "contrôle exclusif" du signataire. Pour les clés de confidentialité, en revanche, le P.S.C.E. peut être amené à les conserver dans l'hypothèse où un client, suite à la perte de sa clé, lui demanderait de la reconstituer (service de recouvrement de clé de confidentialité) pour être en mesure d'accéder à l'ensemble des fichiers qu'il aurait antérieurement chiffrés.
Dans toute Infrastructure à clé publique, l'enregistrement des abonnés aux services de certification s'effectue par l'entremise d'autorités d'enregistrement.

Enfin l'enregistrement peut s'effectuer soit en ligne et les pièces justificatives de l'identité sont envoyées par voie postale (pièces d'identité, quittances attestant du domicile), soit du face-à-face aux bureaux ou aux agents prévus à cet effet (sur présentation des pièces justificatives).

Cette opération est très importante car elle permet de vérifier l'identité conformément aux exigences posées par le décret (article 6-II, m). Concernant l'exactitude des informations que le certificat doit contenir, il faut reconnaître qu'elles ne peuvent que résulter des pièces fournies lors de l'enregistrement (ex: pièce d'identité, quittance) » .
En cas de falsification, tant matérielle qu'intellectuelle, du ou des document(s), ou d'informations obsolètes, l'autorité d'enregistrement ne devrait pas être responsable des informations inscrites dans le certificat. En effet, actuellement les enregistrements s'effectuent le plus souvent en ligne et par l'envoi des pièces justificatives par courrier. Mais ce problème de faux documents serait le même dans le cadre des procédures d'enregistrement en face à face.

L'autorité d'enregistrement ne peut garantir que l'exactitude formelle des informations au vu des pièces transmises et non leur exactitude sur le fond.
Cette entité ne souscrit pas d'engagement juridique envers les clients, elle est uniquement en relation contractuelle avec l'autorité de certification. Cette dernière génère le certificat numérique d'identification sous sa seule responsabilité et à ce titre elle s'engage à remplir certaines obligations essentielles (art. 33 de la LCEN), c'est à dire établir et garantir le lien qui existe entre une personne et une paire de clés asymétriques dont elle est titulaire. En outre, le P.S.C.E. crée et assure, sous sa responsabilité, le fonctionnement d'un service d'annuaire (rapide et sûr) et d'un service de révocation (fiable et immédiat)[34].

Avant d'émettre un certificat, l'autorité de certification doit s'assurer de l'identité de la personne avec laquelle elle contracte. Pour ce faire, elle doit recueillir un certain nombre de renseignements personnels relatifs au statut de cette personne. La conservation de ces renseignements est indispensable au bon fonctionnement d'une autorité de certification. La plupart du temps, ceux-ci peuvent permettre l'identification de la clé privée. L'autorité a donc la responsabilité de prévoir des mécanismes qui protégeront la confidentialité des renseignements recueillis afin de limiter l'accès à ceux-ci à des personnes expressément autorisées et ainsi prévenir la commission de fraudes et les risques d'usurpation d'identités.

Concernant les données à caractère personnel contenues dans le certificat, la loi Informatique et Libertés précise dans son article 33 : « sauf consentement exprès de la personne concernée, les données à caractère personnel recueillies par le prestataire de services de certification électronique pour les besoins de la délivrance et de la conservation des certificats liés aux signatures électroniques doivent l'être directement auprès de la personne concernée et ne peuvent être traitées que pour les fins en vue desquelles elles ont été recueillies ».

[34] (article 6-II, c)

Par ailleurs, tout prestataire qui fournit un attribut est temporairement un fournisseur d'identités et chacun des acteurs du cercle est potentiellement un fournisseur d'identités.

**Quel régime de responsabilité sera-t-il appliqué à une fédération d'identité ?**

On pourrait imaginer plusieurs niveaux de responsabilité selon la quantité de données fournies, ou encore un impératif unique régissant la question avec la concentration de la responsabilité autour d'un responsable.

**Dans la seconde hypothèse**, c'est sans doute le PSCE qui concentrerait cette responsabilité. Dans ce cas, on peut supposer que la responsabilité des différentes parties sera inspirée de celle s'appliquant au PSCE, donc une responsabilité de plein droit. Cette dernière hypothèse semble toutefois exagérée.

**Dans l'hypothèse de gradation de responsabilités ou plutôt de partage de risque**,

il faudra nuancer entre la vérification d'identité et la déclaration d'identité. Exemple : l'opérateur de téléphonie mobile fournissant un attribut sera-t-il en train de déclarer simplement cet attribut ou devra t-il le vérifier et en répondre s'il s'avère inexact ? Sinon s'agit-il d'un partage de risques entre tous les acteurs en présence ?

#### 1.2.6.3 DIVERGENCES ENTRE DROIT PUBLIC ET DROIT PRIVE

L'ordonnance n° 2005-1516 du 8 décembre 2005 a vocation à encadrer les échanges électroniques entre les usagers et les autorités administratives. En effet, le texte s'écarte du régime instauré par la loi du 13 mars 2000 (C civil art. 1316-4) en décidant que « les actes des autorités administratives peuvent faire l'objet d'une signature électronique. Celle-ci n'est valablement apposée que par l'usage d'un procédé, conforme aux règles du référentiel général de sécurité mentionné au i° de l'article 9, qui permette l'identification du signature, garantisse le lien de la signature avec l'acte auquel elle s'attache et assure l'intégrité de cet acte ».

Comme le rappelle Christiane Feral Schuhl, « sauf pour les échanges électroniques avec les tribunaux ou en rapport avec la Défense nationale, il est ainsi possible de communiquer électroniquement avec les administrations, l'ordonnance ayant établi une équivalence juridique entre le courrier électronique et le courrier support papier ». Des référentiels de sécurité et d'interopérabilité élaborés par la Direction Générale pour la modernisation de l'Etat (DGME) définissent les exigences de sécurité. Ce dispositif devrait permettre la généralisation de l'administration électronique à courte échéance.

Pour les particuliers, les certificats de CNIE pourront servir dorénavant à signer leur déclaration de revenus et à se connecter à leur dossier fiscal, qui, pour des questions de confidentialité, requiert ce niveau de sécurité.

L'ordonnance 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre usagers et autorités administratives et entre autorités administratives précise que c'est l'autorité administrative elle même qui met en place son télé service pour déterminer les fonctions de sécurité de sa protection ainsi que le niveau de sécurité de ces fonctions. La CNIL n'a montré aucune objection quant à un usage étendu de la future CNIE, si la vie privée de l'internaute est préservée et si l'Etat ne procède pas à une surveillance poussée (« tracking ») de ses actions sur le web.

Dans un projet de gestion d'identités qui réunit sur une même plateforme des partenaires commerciaux et des personnes publiques, l'enchevêtrement des données de la sphère privée et des données de la sphère publique brouille la cartographie des responsabilités.

## 1.3 PROBLEMATIQUES JURIDIQUES IDENTIFIEES

### 1.3.1 REGIMES JURIDIQUES DIVERS ET OBJECTIFS CONTRADICTOIRES

- droit administratif et droit commercial ;
- statut des données publiques gérées pour l'intérêt général versus les données commerciales secrètes donnant des avantages comparatifs concurrentiels ;
- le droit de la consommation et le droit commercial, libertés publiques et propriétés privés (propriété intellectuelle) ;
- vie publique et vie privée ;
- liberté d'accès à l'information et droit à la vie privée ;
- transparence et droit de la concurrence où les informations commerciales sont secrètes, transparence et secrets, libre parcours et droit de propriété.
- régime juridique applicable aux transferts de données hors de france, notamment vers les usa et les principes de safe harbor (accord du 26 juillet 2002).

### 1.3.2 EXIGENCES DIFFERENTES EN MATIERE DE PREUVE ET DE TRAÇABILITE

Cette disparité apparaît dans différents domaines :

- L'absence de formalisme de la preuve en droit administratif, à opposer aux exigences posées par le droit de la consommation ou par toutes règles protégeant les utilisateurs ;
- La validité des conventions de preuve peut être très différente en terme de contraintes d'une branche de droit à l'autre ;
- Les exigences en matière de contrôle d'accès sont également fort diversifiées selon le statut secret, ou public, des données concernées

C'est surtout en **matière de preuve** que paraissent les divergences entre droit public et droit privé. Les exigences en matière de preuve et plus généralement de traçabilité sont différentes.

Ainsi, on remarque l'absence de formalisme de la preuve en droit administratif, fait que les administrations n'ont pas l'obligation d'établir les preuves de l'exactitude des titres et documents qu'elles fournissent, ce qui s'oppose aux exigences posées par le droit de la consommation et plus généralement par toutes les règles protégeant les utilisateurs.
D'un autre côté, la validité des conventions de preuve peut être très différente en termes de contraintes d'une branche de droit à l'autre ; la preuve des transactions effectuées avec un commerçant est libre. Si le cocontractant est un consommateur, la preuve est conforme à chaque type de transaction.

Quant aux exigences en matière de contrôle d'accès, elles sont également diversifiées selon le statut, secret ou public, des données concernées : il y aurait des niveaux d'authentification variables selon le degré de confidentialité. Cette technique a par ailleurs été adoptée par l'administration. Ainsi l'on trouve plusieurs niveaux de sécurité, sur le plan de l'authentification : anonymat, simple adresse e-mail de correspondance, authentification par mot de passe, authentification par l'usage d'un certificat électronique. Une gradation des mesures de sécurité en fonction de la nature des services proposés et du niveau de confidentialité ou de valeur juridique probante est exigée.

### 1.3.3 USURPATION D'IDENTITE SUR INTERNET : UN VIDE JURIDIQUE

Actuellement, l'usurpation d'identité sur Internet n'est pas punie par la loi, et ne fait ne peut pas faire l'objet de poursuites.
Dans le cadre de son plan « France Numérique 2012 » (octobre 2008), le gouvernement français a annoncé l'introduction, à l'occasion de la loi d'orientation et de programmation intérieure (LOPPSI), d'un **délit d'usurpation d'identité sur les réseaux de communications électroniques**.
Ce nouveau cadre juridique est indispensable et permettra de garantir la confiance et la sécurité des échanges de données personnelles certifiées en ligne, qui plus est pour des usages évolués tels que des inscriptions ou ouvertures de comptes. Il apportera également une légitimité aux systèmes de gestion des identités qui se proposeront de lutter contre les délits d'usurpation d'identité ou de vol ou détournement de données personnelles.

## 1.4 CONCLUSIONS

En conclusion, le groupe de travail relève les difficultés à réconcilier des objectifs divergents et contradictoires, tels qu'exprimés *supra*. Toutefois cette contrainte n'est pas insurmontable.
Le seul moyen valable consistera à se focaliser avant tout sur les besoins de l'administré / citoyen / consommateur / professionnel.
Il sera nécessaire de réfléchir en droit sur ce qui semble être une question majeure de l'interopérabilité des cercles de confiance et des solutions de gestion des identités numériques.

# 2. RESPONSABILITE DES ACTEURS ET PREUVE

Ce chapitre a pour objet d'analyser certains des cas d'utilisation retenus par le projet FC², dans une optique générique, afin d'apporter un éclairage sur deux problématiques fondamentales : la responsabilité des acteurs de la chaîne, et la gestion de la preuve dans le système de gestion des identités.

## 2.1 DROITS ET OBLIGATIONS DES ACTEURS

Cette analyse est réalisée sur la base de deux des cas d'utilisation définis. A noter que n'est pas étudié dans cette partie le cas « enquête judiciaire », qui est très spécifique et est fortement impacté par des textes que nous n'avons pas cités, tels que le code de procédure pénale, ou le code des communications électroniques pour les enquêtes côté opérateurs télécoms.

### 2.1.1 RAPPELS IMPORTANTS

- **responsabilité civile et pénale** en cas de collecte par moyen frauduleux, déloyal ou illicite et le détournement du fichier (art. 1382 cc et 226-18 code pénal) et la jurisprudence et les dénonciations de la cnil.
- **obligation de sécurité renforcée** (voir art. 17 de la directive protection des données) sur les mesures techniques appropriées pour protéger les données contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération ou l'accès non autorisés ou tout autre forme de traitement illicite. le responsable du traitement doit décrire les dispositions prises dans le formulaire de déclaration de traitement auprès de la cnil (art. 34 loi 6/01/1978 : sanctions : 5 ans de prison, 300 000 euros d'amendes. multiplié par 5 si personne morale (c.pén. art. 226-17).

- **archivage** : délibération de la cnil n°2005-213 du 11/10/2005 et ses recommandations sur la sécurité des archives et l'article 6-ii de la loi du 21 juin 2004 (len) sur l'obligation de conservation des données et éventuellement loi du 23/01/2006 contre la lutte du terrorisme (art. 34-1 ii cpce) sur la conversation des données pendant au moins un an, après expiration de la durée de conservation des données). nota : documentation intéressante sur l'archivage sur le site web de la dcssi.
- **responsabilité du sous-traitant** : l'obligation de sécurité renforcée s'applique également lorsqu'il est fait appel à un sous-traitant. ce dernier désigne « toute personne traitant des données à caractère personnel pour le compte du responsable du traitement » (art. 36, al.1 l.6/01/1978). le sous-traitant doit garantir la mise en œuvre de mesures de sécurité et de confidentialité. cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures. le sous-traitant ne peut agir que sur instruction du responsable du traitement (art. 35).

### 2.1.2 CAS « OUVERTURE DE COMPTE BANCAIRE »

Dans ce cas d'utilisation, Anne souhaite ouvrir un compte bancaire en ligne. Le site de la banque offre la possibilité d'ouvrir un compte « full on line », c'est à dire sans envoi de pièces justificatives par courrier ou nécessité de les scanner. Sur le même principe, Anne pourrait aussi souscrire à un contrat d'assurance, ou demander un crédit à la consommation (ouverture de compte de crédit), par exemple.

Toute personne, capable, majeure, qui peut justifier de son identité et de son domicile en France, a droit à un compte bancaire. Ce droit au compte a en effet été prévu par l'article L312-1 du Code Monétaire et Financier[35].
Toutefois, il existe des obligations propres au secteur financier en matière de justification de l'identité du client. Il est notamment nécessaire de mettre en application les dispositions de la loi du 12 juillet 1990 en matière d'identification lors de l'entrée en relation d'affaires avec un client qui n'est pas physiquement présent. En particulier, le client doit présenter une pièce d'identité et, normalement, la banque doit effectuer un contrôle de visu. Néanmoins, il est aujourd'hui toléré d'envoyer les copies des pièces justificatives par courrier, et même de les scanner puis les envoyer par e-mail ou les transférer sur le site de la banque.

Dans un livre blanc de la Banque de France[36], il est recommandé aux banques en ligne ce qui suit: « *le dossier d'ouverture de compte, comprenant notamment l'identifiant et le mot de passe du client (ou son équivalent) peut être envoyé par la poste, si possible avec accusé réception. On remarque souvent que le fonctionnement d'un compte - y compris la réception de fonds et d'instruments financiers – n'est autorisé qu'une fois que la procédure d'identification a été achevée* ». Sur le contrôle des opérations douteuses, le livre blanc remarque qu' « *il est difficile, voire impossible, de savoir si la personne faisant fonctionner le compte est réellement celle qui l'a ouvert.* »

[35] « Toute personne physique ou morale, domiciliée en France, dépourvue d'un compte de dépôt, a droit à l'ouverture d'un tel compte dans l'établissement de crédit de son choix. L'ouverture d'un tel compte intervient après remise auprès de l'établissement de crédit d'une déclaration sur l'honneur attestant le fait que le demandeur ne dispose d'aucun compte. En cas de refus de la part de l'établissement choisi, la personne peut saisir la Banque de France afin qu'elle lui désigne soit un établissement de crédit, soit les services financiers de La Poste ».
[36] Banque de France, « Internet : quelles conséquences prudentielles ? », 2001, disponible à l'adresse http://www.banque-france.fr/fr/supervi/telnomot/supervi_banc/Ibinet.pdf

En outre, l'article 3 de la directive « blanchiment » de 2001[37] pose le principe de l'identification obligatoire. Cette identification doit se faire au moyen d'un document probant. Il ne s'agit pas d'une obligation formelle. Il s'agit d'identifier l'opérateur réel au-delà de tout ayant droit. Dès lors qu'il existe un doute sur le point de savoir si les clients agissent pour leur propre compte, ou s'il est certain qu'ils n'agissent pas pour leur compte, il convient de prendre les mesures raisonnables en vue d'obtenir des informations sur l'identité réelle des personnes pour le compte desquelles ces clients agissent.

La directive impose une vigilance particulière dans le cadre des opérations dites « à distance ». L'identification doit se faire en ayant recours à des vérifications approfondies « *par exemple en demandant des pièces justificatives supplémentaires, des mesures additionnelles de vérification ou de certification des documents fournis ou des attestations de confirmation de la part d'un établissement relevant de la présente directive ou en exigeant que le premier paiement des opérations soit effectué par un compte ouvert au nom du client auprès d'un établissement de crédit* » relevant de la directive. L'identification du client doit intervenir dès lors que des relations d'affaires se nouent, notamment lorsqu'il y a ouverture de compte ou de livret ou prestation de services de garde des avoirs. Elle s'impose également à l'occasion de transactions avec des clients qui ne sont pas en relation d'affaires et dont le montant atteint ou excède 15 000 euros.

L'article L. 563-1 du Code monétaire et financier exprime la même inquiétude : « Les organismes financiers ou les personnes visées à l'article L. 562-1 doivent, avant de nouer une relation contractuelle ou d'assister leur client dans la préparation ou la réalisation d'une transaction, s'assurer de l'identité de leur cocontractant par la présentation de tout document écrit probant. Ils s'assurent dans les mêmes conditions de l'identité de leur client occasionnel qui leur demande de faire des opérations dont la nature et le montant sont fixés par décret en Conseil d'Etat. Les personnes visées au 8 de l'article L. 562-1 satisfont à cette obligation en appliquant les mesures prévues à l'article L. 565-1.
Pratiquement, lors d'une demande d'ouverture de compte auprès d'un fournisseur de service, la banque X, le client s'authentifiera auprès de divers fournisseurs d'identité ou d'attributs (agence gouvernementale, opérateur télécoms, autre banque) pour récupérer et transmettre tous les documents nécessaires à l'ouverture du compte (justificatif de domicile, données d'identité, etc.).

L'obligation de sécurité renforcée sur les mesures techniques appropriées pour protéger les données contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération ou l'accès non autorisés ou tout autre forme de traitement illicite. Cette obligation s'applique aussi lorsqu'il est fait appel à un sous-traitant. Ce dernier désigne « toute personne traitant des données à caractère personnel pour le compte du responsable du traitement » (art. 36, al.1 L.6/01/1978). Le sous-traitant doit garantir la mise en œuvre de mesures de sécurité et de confidentialité. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures. Le sous-traitant ne peut agir que sur instruction du responsable du traitement (art. 35).

Ainsi, la dématérialisation totale est possible même si, juridiquement, elle présente un risque. Dans le cas précis de l'ouverture d'un compte de dépôt, la condition incontournable consistera pour le client à pouvoir fournir les données d'identité demandées par la banque de manière dématérialisée et sécurisée, en s'affranchissant de leur support physique. Le fournisseur de service (banque) doit avoir la garantie que les données sont valides légalement, c'est-à-dire que son client est identifié de manière certaine, en cas de litige ou de contestation. Cette garantie doit être pérenne et être

[37] Directive 2001/97/CE du Parlement européen et du Conseil du 4 décembre 2001 modifiant la directive 91/308/CEE du Conseil relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux

valable pendant toute la durée de l'engagement des parties (convention de compte en l'occurrence).

Idéalement, le client pourrait utiliser sa CNIE pour fournir, par l'intermédiaire d'un lecteur de cartes sécurisé, les données personnelles nécessaires, signées à l'aide d'un certificat électronique. Le fournisseur du certificat, qu'il soit l'Etat directement – en tant que fournisseur d'identité – ou un tiers de confiance (PSCE) désigné par lui, devra engager sa responsabilité sur l'intégrité des données, c'est-à-dire garantir qu'elles auront été traitées dans le respect des règles légales énoncées plus haut.
En outre, le PSCE devra être en mesure d'assurer la conservation des données signées pour tout litige ultérieur, pendant toute la durée du contrat liant les parties, pour le compte du fournisseur d'identité.

En cas de litige sur l'identification du client, ce dernier pourra se retourner contre le fournisseur de services, qui engagera la responsabilité du fournisseur d'identité quant au traitement des données, dont il est responsable y compris s'il a fait appel à un sous-traitant pour remplir le rôle de PSCE. Le responsable du traitement a, rappelons-le, une obligation de sécurité renforcée telle que définie *supra*.
Toutefois, si les données de la CNIE en elles-mêmes avaient fait l'objet d'une fraude prouvée et que le PSCE les avaient indûment signées, sa responsabilité ne pourra pas être engagée.

De manière générale, ces considérations sont valables pour toutes les données signées qui pourraient être échangées dans un système de gestion d'identité : au delà de la CNIE, cela concernera les données de la carte bancaire, d'une carte professionnelle, d'une carte ville, etc.

### 2.1.3 CAS « LOCATION DE VOITURE »

Anne souhaite réserver un véhicule en ligne, en perdant un minimum de temps à la réservation puis à l'usage du véhicule, notamment le temps de passage à l'agence de location pour les formalités administratives. Anne a un compte bancaire et une carte bancaire. Anne a également un téléphone mobile et plusieurs cartes de fidélité dématérialisées qui peuvent lui apporter des avantages commerciaux.

La transmission des données du permis de conduire par le cercle régalien permet d'accélérer voire de supprimer le traitement en agence. Elle nécessite une dématérialisation du permis de conduire, ou bien un enregistrement préalable de son titulaire auprès d'un tiers de confiance qui pourra alors en garantir la validité et la date de délivrance. Dans ce cas d'usage, l'âge du client devra également être certifié, car il existe la plupart du temps un âge minimum pour accéder à ce service, en plus de l'ancienneté du permis de conduire.

Éventuellement, ce cas d'usage pourrait permettre de fournir également des attributs « conjoncturels », par exemple un numéro de vol lié à une carte de fidélité de compagnie aérienne, dans le cadre de la réservation consécutive d'un billet d'avion, d'un hébergement et d'une voiture de location.

Pour le loueur, la fourniture d'informations certifiées sur l'âge et surtout le permis de conduire de son client est très utile afin de lutter contre la fraude, qui est non négligeable dans ce domaine[38]. Toutefois, La vérification du nombre de points du permis de conduire pourrait poser problème car le cadre juridique actuel ne l'autorise pas, même pas pour l'employeur d'un chauffeur routier… En revanche, le service ne serait disponible dans un

[38] Il y aurait 42 millions de permis de conduire en circulation en France, dont 2,7 millions de faux, www.forumatena.org, newsletter n°3, juillet août 2007.

premier temps que pour des clients français ou dans un second temps européens, qui représentent il est vrai la grande majorité des clients des loueurs.

Si la signature du contrat de service est réalisée en ligne, alors la réalisation de la prestation peut intervenir sans passage du client en agence. Les clés du véhicule peuvent être délivrées de manière automatisée, et le suivi de la relation client passera par d'autres canaux, en particulier le téléphone mobile dont le numéro aura été fourni à la réservation. Au retour du véhicule à l'agence, le loueur pourra vérifier la bonne exécution du contrat et encaisser le restant dû avec la carte bancaire utilisée au moment de la réservation.

De la même manière que pour l'ouverture de compte, la signature du contrat est un élément fondamental de la chaîne dans l'optique d'une dématérialisation totale, à la différence près que l'on se situe ici dans un contrat de prestation qui sera exécuté à une période déterminée. Le formalisme n'est pas donc pas forcément aussi important que pour un contrat engageant à plus long terme, comme un abonnement de téléphonie mobile ou un compte bancaire. Il n'en reste pas moins que le PSCE est responsable de la bonne marche du traitement des données certifiées, pour le compte du fournisseur d'identité (Etat et banque). Là encore, il agit sous le régime du sous-traitant et a donc l'obligation, comme le responsable du traitement, de garantir la sécurité et la confidentialité des données dont il assure le traitement.

Concernant les données du cercle télécoms, elles ne sont pas certifiées et donc les responsables de traitement ne sont pas soumis aux mêmes obligations en matière de certificat. Ceci ne change en aucun cas la nature de la responsabilité des fournisseurs d'identité pour le traitement des données de manière générale.
Enfin, dans tous les cas, le fournisseur de services devra informer son client du service de gestion d'identité qu'il lui propose, et bien entendu des possibilités de recours à sa disposition en cas de dysfonctionnement.

## 2.2 GESTION DE LA PREUVE DANS LES CAS D'UTILISATION

L'un des bénéfices majeurs attendus par les fournisseurs de services de la gestion des identités numériques est le fait, dans le cadre de transactions entièrement dématérialisées, de pouvoir non seulement identifier de manière certaine les utilisateurs, mais aussi le prouver en cas de litige. L'inverse est également vrai : dans certains cas, l'utilisateur final pourrait disposer de la preuve qu'il a affaire au bon fournisseur de services.

Ainsi, une gestion de la preuve efficace est une condition à la dématérialisation de certaines transactions complexes comme une ouverture de compte, et peut apporter un service supplémentaire pour d'autres types d'usages. La preuve doit pouvoir être émise et conservée de manière valide pour différentes fonctions : la signature d'un contrat, mais aussi la signature de données personnelles (attributs « certifiés »), ou encore une authentification.

### 2.2.1 CONSIDERATIONS GENERALES

Les tiers de confiance sur des réseaux comme Internet sont aujourd'hui indispensables pour valider et prouver les échanges électroniques. Ils jouent le rôle d'autorité de certification. Les solutions qu'ils mettent en œuvre reposent sur l'utilisation de certificats électroniques émis par des autorités de certification, et de services tels que la signature électronique, l'horodatage et l'archivage. Elles garantissent également la traçabilité et la confidentialité des échanges.

Le cadre juridique afférant repose sur la loi portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (loi n°2000-230 du 13 mars 2000 art. 1 : *l'écrit électronique est probant à condition que son auteur puisse être dûment identifié et que le document soit conservé sous une forme garantissant son intégrité*).

Ces services nécessitent de respecter les normes et standards internationaux et de disposer d'infrastructures hautement redondantes liées à une expertise d'exploitation spécifique, compte tenu des fortes contraintes sécuritaires inhérentes.

Il est nécessaire, pour ce tiers de confiance, d'obtenir la qualification de prestataire de services de certification électronique (PSCE), conformément à la norme ETSI/TS 101456 (AFNOR Z 74-400) et à l'arrêté du 26 juillet 2004 qui vient la compléter. La loi pour la confiance dans l'économie numérique (LCEN) impose également des normes d'échanges pour le commerce électronique.

### 2.2.2 CAS « OUVERTURE DE COMPTE »

Comme détaillé dans le chapitre précédent, la banque a l'obligation légale de pouvoir prouver l'identité du demandeur de l'ouverture d'un compte. Il s'agit pour elle d'un élément fondamental pour assurer la confiance et dématérialiser ce service, alors que c'est aujourd'hui un élément freinant la dématérialisation complète. Ceci d'autant plus que la banque ne connaît pas le futur client (prospect), qui se présente pour la première fois. Le fournisseur de service doit donc être certain que les éléments de preuve dont il dispose, sous quelque forme que ce soit, pourront être acceptés au même titre qu'un titre d'identité en bonne et due forme par un juge.

Le cas d'usage se décompose en 4 étapes principales, au cours desquelles la gestion de la preuve interviendra de différentes manières :

a. **identification du prospect** : fourniture des données issues de la cnie. l'obligation légale impose l'utilisation de la cnie, dont les données signées à l'aide du certificat fourni par l'etat devront être conservées. la question de savoir sous quelle forme se présenteront ces données n'est pas encore tranchée, étant donné que la loi sur la carte d'identité électronique n'est pas encore votée à la date du présent document. ces éléments seront suivis au cours du projet. etant donné l'état de l'art dans le domaine, on peut toutefois considérer que les données issues de la cnie, signées électroniquement, constitueront une preuve tangible et opposable.
b. **données complémentaires** : fourniture des données issues du profil télécoms (coordonnées postales, téléphoniques, e-mail, etc.). pas de gestion de preuve puisque ces données ne sont pas certifiées.
c. **approvisionnement du compte** : fourniture des données de la carte bancaire, issues du profil bancaire. pour ce qui est du paiement par carte bancaire en vente à distance sécurisée (vads), il s'agit d'une pratique déjà largement répandue. la banque qui a émis la carte, c'est-à-dire le fournisseur d'identité étant responsable de toute fraude, c'est elle qui a la charge de la preuve également.
d. **signature électronique de la convention de compte** (contrat). de la même manière que pour son identification à l'aide de la cnie, le prospect pourra utiliser le certificat de sa carte d'identité pour signer la convention de compte. d'autres méthodes de signature sont possibles mais elles devront, pour être valides, utiliser un certificat électronique fourni par une autorité de certification reconnue.

Dans ce cas d'usage, c'est l'identification de l'utilisateur qui compte sur le plan juridique, alors que la certitude de l'identité du fournisseur de services peut être fournie à l'utilisateur par des moyens techniques.

### 2.2.3 CAS « ENQUETE JUDICIAIRE »

Le cas d'usage « enquête judiciaire » est particulièrement intéressant du point de vue de la gestion de la preuve. Il a ceci de particulier qu'il nécessite une identification de haut niveau, réciproque, de la part de l'utilisateur du service (l'officier de police judiciaire, ou OPJ) et du fournisseur du service (opérateur télécoms ou opérateur bancaire). Cette identification doit pouvoir être prouvée devant un juge et doit donc faire l'objet d'une procédure exempte de tout reproche, car la défense des suspects cherchera à exploiter le moindre vice de procédure.

De plus, la gestion de la preuve comporte deux niveaux de chaque côté :

a. **du côté de l'utilisateur**, il faudra prouver non seulement l'identité de l'opj (éventuellement par le biais d'une carte « agent » professionnelle), mais aussi qu'il dispose de l'habilitation suffisante pour effectuer une demande d'enquête. on devra également être capable de prouver que la commission rogatoire (dématérialisée) qu'il utilise pour mener cette enquête lui a bien été délivrée et que son objet correspond à l'usage qu'il en fait.
b. **du côté du fournisseur de service**, de la même manière, on devra pouvoir prouver l'identité de l'employé du service chargé des enquêtes, et aussi que l'agent en question est bien habilité à répondre à la sollicitation de l'officier de police ou de la justice.

La mécanique de ce cas est donc particulièrement complexe.

La traçabilité de tous les échanges de données devra être assurée, de même que l'identité de la personne qui a procédé à ces échanges, des deux côtés.

A partir de ce cas, plusieurs questions majeures se posent concernant la gestion de la preuve de manière générale :

- la gestion de certificats dans le cadre d'une igcp ne pose pas de problème et est déjà largement répandue. en revanche, la question de savoir quelle forme doivent prendre les données échangées électroniquement afin de constituer des preuves valides reste ouverte.
- les données certifiées sont fournies par les fournisseurs d'identités, qui doivent eux-mêmes s'assurer de l'identité de leur « client », qui demande l'envoi de données personnelles le concernant. quelles pourraient être les obligations pour les fournisseurs d'identité en matière d'authentification sur leurs serveurs, ou même pour accéder aux supports sécurisés qu'ils ont distribués à leurs clients ou administrés (carte bancaire, carte ville, cnie, etc.) ?
- quelles doivent être les obligations et les conditions de stockage et de conservation de ces éléments par le fournisseur d'identité ou son sous-traitant tiers de confiance ? dans un premier temps, il pourrait être recommandé que la durée de conservation soit calquée sur la durée et l'échéance de l'exécution du contrat liant les parties à l'issue du premier tour de table.

## 2.3 SYNTHESE ET RECOMMANDATIONS

Un système d'identité numérique global commande, selon nous, que les utilisateurs des réseaux délèguent la gestion de leur identité numérique à un tiers. Ce tiers, qui pourrait être de droit privé, à la différence du monde « réel », dans lequel l'État assume en partie ce rôle, devrait obéir à un statut garantissant sa pérennité et sa bonne moralité, ou du moins prendre des engagements en ce sens. Ce tiers, que nous appelons *fournisseur d'identité,* et qui ne devrait en aucun cas être unique, sera immanquablement amené à gérer un registre d'identité servant à identifier les utilisateurs et à garantir leur identité auprès de fournisseurs de service. À ce stade, plusieurs remarques sont nécessaires.

**En premier lieu,** les règles minimales de sécurité commandent que le registre ne soit pas centralisé afin de ne pas être l'objet d'attaques. Au sein d'un cercle de confiance par exemple, les différents fournisseurs d'identités ou d'attributs pourront conserver les mêmes données, ce qui garantira la sécurité des données et permettra de répartir les tâches entre eux.

**En deuxième lieu,** ce registre d'identité devra est géré selon des règles transparentes, clairement affirmées. En clair, le gestionnaire du registre devra prendre des engagements contractuels forts (voir Correspondant informatique et libertés). Enfin, ce registre devra comporter des règles de sécurité fortes, telles que la loi l'impose

Pour mémoire, l'article 29 de la loi du 6 janvier 1978 formalise cette obligation de sécurité renforcée vis-à-vis des données à caractère personnel, lequel est devenu article 34 et a été modifié comme suit par la loi n° 2004-801 du 6 août 2004 : « Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles ne soient déformées, endommagées ou que des tiers non autorisés y aient accès. » L'article 7 de la convention du Conseil de l'Europe du 28 janvier 1981 comporte, en son article 7, des principes voisins puisqu'il y est question de prendre des « mesures appropriées » pour protéger les données à caractère personnel contre la destruction, accidentelle ou non, ou la perte.

C'est donc bien une **obligation générale de sécurité et même une obligation de résultat qui pèsent sur le gestionnaire du registre**. Pour ceux qui en douteraient, rappelons que la loi française sanctionne le manquement à l'obligation de sécurité d'une peine d'emprisonnement de cinq ans et d'une amende de 300 000 euros[39].
Enfin, le fournisseur d'identité ou d'attributs aura la responsabilité, directement ou par le biais d'un sous-traitant tiers de confiance, de **générer, conserver et fournir en tant que de besoin la preuve électronique valable** des transactions réalisées et de l'identité des utilisateurs finaux ayant utilisé le service de gestion d'identité.

Un registre de référence avec à sa tête un ou plusieurs fournisseurs d'identité au sein du même cercle de confiance, dans lequel seraient recensées les identités numériques est possible, et même indispensable. Un système de gestion d'identité numérique global ne peut se passer d'un tel référentiel pour trancher les litiges sur l'identité et la protection des données personnelles.

# 3. CONTEXTE SOCIO-ECONOMIQUE ET SOCIETAL

## 3.1 INTRODUCTION

### 3.1.1 RAPPEL SUR LES EQUIPEMENTS ET USAGES

Si l'on considère les trois cercles envisagés par le projet - Télécoms, Administration et Finance – il est indispensable de prendre en compte les disparités importantes d'un pays à un autre en Europe, à la fois dans les usages et dans les perceptions.

**Mobiles : Un taux d'équipement uniformément élevé avec un usage homogène**
La pénétration du téléphone mobile reste assez homogène en Europe. Selon les statistiques fournies par Eurostat : le taux d'abonnements mobiles (cartes prépayées incluses) par personne y est en moyenne de 96% dans l'Europe des 27. Si certains pays

[39] Art. 226-17 du Code pénal : « Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. »

comme l'Italie, le Luxembourg ou les pays scandinaves ont des taux d'équipements parfois supérieurs à 120% (plusieurs mobiles par personne), d'autres à l'inverse comme la Pologne ou la Roumanie sont plus proches de 65%.

En revanche, aucun différentiel d'usage notable n'apparaît. La consommation de services mobiles reste majoritairement centrée sur la téléphonie et dans une moindre mesure l'utilisation de messages courts (SMS). La consommation de services mobiles (Data) reste encore le fait d'une fraction très minoritaire (évaluée à moins de 10% des utilisateurs). Le m-commerce reste pour le moment très embryonnaire.

### Internet : Un européen sur deux seulement accède à internet

En matière d'équipement Internet, si 54% des ménages sont désormais équipés d'Internet (*source Eurostat 2007*), l'équipement des foyers est variable selon les pays avec des taux d'équipement qui dépassent largement 80% dans les pays de l'Europe du nord, là où ils sont plus proches de 25 à 30% dans les pays ayant rejoint l'Europe plus récemment.
Dés lors, on constate, sans surprise, un différentiel important dans les usages avec une segmentation en trois groupes :

- la Grande Bretagne, l'Allemagne, la France, le Benelux et les pays Scandinaves qui possèdent une pratique assez courante de l'e-commerce (En moyenne plus de 65% des internautes ont acheté en ligne au cours des trois derniers mois),
- les pays de l'Europe du Sud où l'e-commerce moins répandu, prend son essor
- l'Europe de l'Est où l'e-commerce reste encore une pratique très marginale.

### E-administration : un usage intensif dans les pays du nord de l'Europe

Dans la sphère administrative, la dernière étude statistique[40] menée par l'union européenne en 2004 soulignait que la disponibilité des informations et services fournis par les pouvoirs publics et les administrations était forte dans tous les pays d'Europe. Toutefois ce sont les pays du Nord de l'Europe qui ont poussé le plus loin le traitement électronique des dossiers.

L'étude relevait qu'une entreprise sur deux utilisait les sites Web des pouvoirs publics pour obtenir des informations, télécharger des formulaires ou interagir avec ceux-ci, avec en revanche des variations importantes selon les secteurs (le secteur des services est le plus enclin) et la taille des entreprises (les petites entreprises utilisent moins les sites Web des pouvoirs publics que les grandes).

Les usages relevés sont les plus intensifs dans les pays scandinaves et les pays baltes, pays où la dématérialisation des procédures est la plus développée, et l'utilisation de certificats par les entreprises plus courante.

De la même façon, si près d'un particulier sur deux n'hésite pas à recourir au site des pouvoirs publics, moins d'un sur 5 en revanche utilise une procédure de téléchargement ou d'e-administration. Les personnes ayant un emploi, les diplômés de l'enseignement supérieur et la classe d'âge des 25-34 ans sont les groupes socio-démographiques qui font l'usage le plus réguliers des sites des pouvoirs publics.

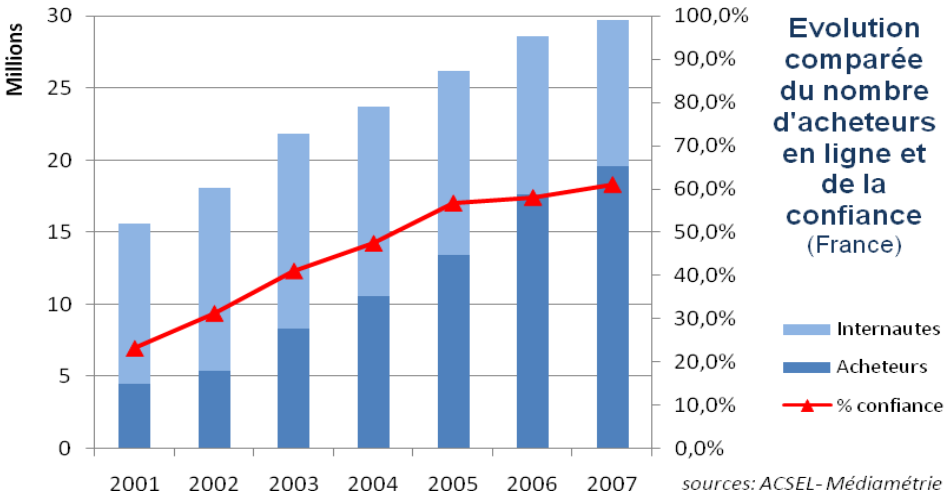
### E-commerce : Une Europe encore fractionnée

Le développement du commerce électronique est lié à trois facteurs principaux : au développement des infrastructures de haut débit tout d'abord, à la pratique de la vente à distance (forte en Grande Bretagne et dans les pays scandinaves) et enfin et surtout il est très dépendant de la confiance que peut avoir le consommateur dans l'acte d'achat.

[40] Eurostat – Statistiques en Bref – N° 35 - 2005

A ce titre le graphe ci-dessous est éloquent : Il montre l'évolution du nombre d'internautes en France (en millions) comparativement avec la part des internautes qui achète en ligne (histogramme en bleu foncé).

Le graphe met en évidence la corrélation presque parfaite entre ce nombre et la confiance exprimée en pourcentage par les internautes (courbe en rouge) dans l'acte d'achat en ligne.

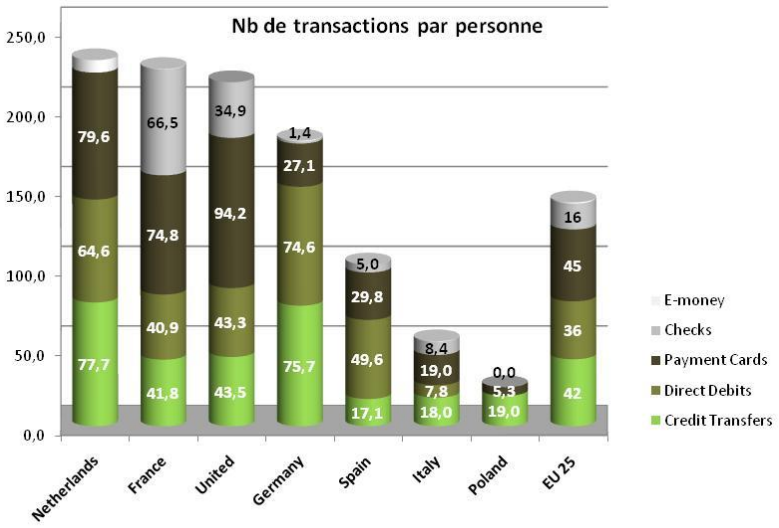



## Des usages très disparates en matière de paiement

Pour ce qui relève de la sphère financière, les usages en termes de moyens de paiement sont assez disparates en Europe.

Très schématiquement, l'Europe s'articule en deux grands groupes de pays : ceux pour lesquels l'usage du « cash » reste encore la pratique courante (Italie, Espagne, Pologne parmi les pays les plus peuplés), et ceux qui ont une pratique plus soutenue des moyens de paiement scripturaux.

Parmi ceux-ci, la carte bancaire reste le moyen de paiement le plus pratiqué en Europe puisqu'elle représente en volume 32% des opérations de paiement des particuliers.




*Source ECB Bluebook - 2007*

Mais dès lors qu'il s'agit de payer en ligne, les usages varient selon les pays : la France, l'Angleterre, l'Italie et l'Espagne utilisent majoritairement la carte bancaire. L'Allemagne, les Pays-Bas font un usage intensif des virements en ligne. Enfin l'on assiste à la montée en puissance des systèmes de paiement alternatifs (Paypal, etc.) comme solution de paiement complémentaire.

### 3.1.2 ZOOM SUR LES ASPECTS LIES A LA SECURITE

#### Sécurité : une prise de conscience de la nécessité d'une protection accrue

L'installation et l'utilisation d'outils de protection contre les virus, les pourriels (*'spams'*), etc. sur les ordinateurs personnels se sont largement répandues dans tous les pays européens au cours des dernières années : selon Eurostat (*Statistiques en Bref – N° 25 – 2005*), plus d'un quart des particuliers utilisateurs d'Internet ont installé des pare-feux au Danemark, en Allemagne, en Hongrie, au Royaume-Uni et en Islande. De même, les programmes de détection de virus informatiques sont couramment utilisés eux aussi: le pourcentage d'internautes qui ont installé ce dispositif au cours des 3 mois précédant l'enquête va de 18% en Lituanie à près de 60% au Luxembourg.

| | % ayant déjà utilisé l'authentification |
|---|---|
| DK | 64,2 |
| **DE** | **29,1** |
| EE | 0,5 |
| **EL** | **18,8** |
| IE | 68,7 |
| **CY** | **38,5** |
| LT | 19,8 |
| **LU** | **41,3** |
| HU | 28,0 |
| **AT** | **28,0** |
| PT | 29,5 |
| **SI** | **81,0** |
| FI | 66,4 |
| **SE** | **51,0** |
| UK | 31,6 |
| **IS** | **64,3** |
| NO | 72,1 |

*Source Eurostat 2005*

Les mécanismes d'authentification en ligne, tels que l'emploi de codes confidentiels ou de mots de passe, sont aussi de plus en plus utilisés. La proportion d'internautes ayant eu recours à ces mécanismes récemment est particulièrement élevée en Slovénie, en Norvège, en Irlande, en Finlande et au Danemark.

Plus particulièrement, le pourcentage d'internautes qui ont récemment installé ou mis à jour leur logiciel antivirus (y compris la mise à jour automatique) ou un pare-feu matériel ou logiciel a dépassé 50% dans 12 des 15 pays pour lesquels des données sont disponibles, ce qui est le signe d'une sensibilisation accrue dans ce domaine.

Le *spam* (courrier électronique non sollicité) représente un autre problème majeur: dans de nombreux pays, la plupart des utilisateurs d'Internet en ont fait l'expérience: 81% des internautes islandais ont déclaré qu'ils ont été victimes du *spamming*, et le pourcentage est nettement supérieur à 40% dans la majorité des pays pour lesquels des données sont disponibles.

#### La fraude reste limitée, mais son impact commence à peser dans les usages

Quoique le problème du spamming puisse être considéré comme gênant, il n'a cependant pas les mêmes effets que les utilisations frauduleuses de cartes de paiement ou la perte d'informations.

L'usage frauduleux de cartes de paiement et l'utilisation abusive d'informations personnelles transmises par Internet sont potentiellement plus perturbateurs, car ils touchent à la sécurité et à la vie privée des personnes.

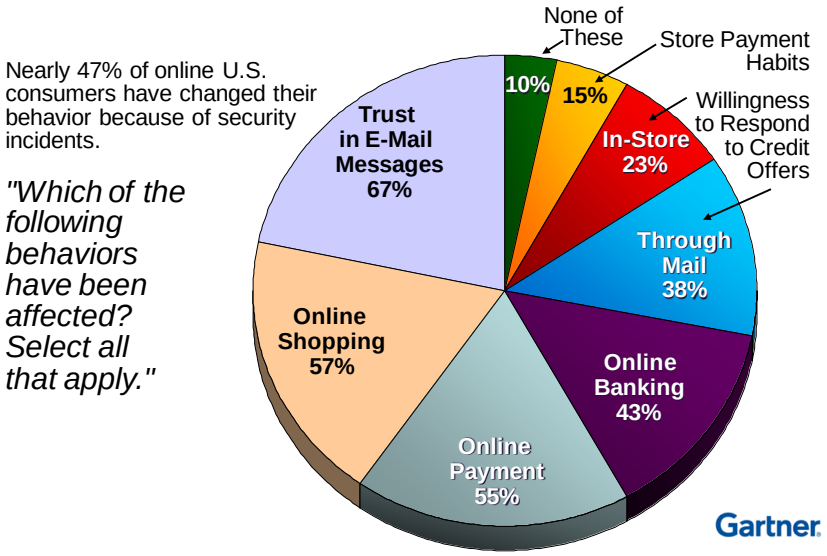
Dans la plupart des cas, la part des utilisateurs d'Internet ayant été confrontés à un usage frauduleux de leur carte de paiement reste bien en deçà de 2%, sauf en Islande (2,8%) et au Royaume-Uni (2,4%). Il convient néanmoins de noter que ce pourcentage se rapporte à tous les utilisateurs individuels, et pas seulement à ceux qui ont effectivement acheté ou commandé des biens ou des services.

De même l'utilisation abusive d'informations personnelles transmises par Internet concerne relativement peu d'internautes: dans la plupart des pays, ce problème a été

cité par moins de 4% des utilisateurs, à l'exception de la Suède où ils étaient plus de 7% à s'en plaindre.

Toutefois, la prise de conscience du risque de fraude a un impact direct sur les usages consommateurs comme le souligne l'étude menée par Gartner aux Etats unis.
Près de 47% des 155 millions d'internautes ont radicalement changé leur mode de fonctionnement dans bien des usages.

L'étude avance même une perte potentielle de l'ordre de 2 Milliards de dollars, par manque de confiance du consommateur dans la sécurité des systèmes de commerce électronique




## 3.2 PERCEPTION DES METHODES D'AUTHENTIFICATION ET DE SIGNATURE

### 3.2.1 DEMANDE POUR UNE GESTION SIMPLE DE L'AUTHENTIFICATION

Les études préliminaires menées autour de la CNIE en France en liaison avec le Forum des droits sur l'Internet ont mis en évidence le besoin exprimé par les internautes d'un système de gestion d'identité avec plusieurs niveaux d'authentification :

- une identification éventuellement anonyme avec authentification faible, pour répondre à des besoins simples de personnalisation de services.
- une identification avec authentification forte pour répondre à des besoins bien identifiés de paiement ou d'identification auprès de services publics.

Sur ce dernier point, une récente étude lancée par la Commission européenne en décembre 2007[41] fait un point complet sur les perceptions des principaux modes d'identification des utilisateurs des cartes de paiements, des paiements par téléphone portable et des paiements électroniques.

Des quatre facteurs d'authentification répertoriés dans le document FC²_SP1-Lot1-GT4_Authentification (« Etat de l'art sur l'authentification des utilisateurs ») – pour mémoire, ce que l'on est, ce que l'on possède, ce que l'on sait, ce que l'on sait faire – c'est le troisième facteur qui est le plus couramment utilisé en matière de paiement scriptural, généralement sous la forme d'un mot de passe (ou d'un code PIN).

[41] EEC – Study on user identification methods in card payments, e-payment and mobile payments – Nov 2007

### 3.2.2 AUTHENTIFICATION FAIBLE OU FORTE : UNE EUROPE PARTAGEE

Dans beaucoup de pays, la signature manuscrite a longtemps été (jusque récemment) le moyen d'identification le plus usité pour les moyens de paiement. Il est jugé particulièrement convivial (81%) dans l'utilisation d'une carte de paiement de manière assez homogène dans tous les pays. Il faut noter quand même la prise de conscience que le degré de confiance dans ce moyen reste faible (47%) sauf s'il est accompagné d'un deuxième facteur d'identification, généralement la production d'une pièce d'identité (74%).

Les efforts déployés par les établissements bancaires pour renforcer la sécurité des moyens de paiement, et en particulier l'introduction d'un code PIN ont considérablement fait évoluer les mentalités. L'authentification (ou la signature) à l'aide d'un code est unanimement jugée conviviale (90%), plus encore que la signature manuscrite et avec une fiabilité très supérieure (76%). Si l'on compare la dernière étude faite par sur ce sujet par la Commission Européenne en 2003, on constate l'évolution des mentalités en Europe. Le renforcement de la sécurité dans les moyens de paiement, et plus particulièrement autour de la carte bancaire, considérée comme une fonctionnalité 'nice to have' en 2003, est désormais jugée indispensable.

#### 3.2.2.1 AUTHENTIFICATION FAIBLE : LA NORME

En matière d'application bancaire (online banking), c'est l'utilisation d'un login et d'un mot de passe qui semble la méthode la plus fréquemment pratiquée. 71% des européens *utilisateurs de la banque en ligne* l'utilisent au moins sur une base mensuelle ou hebdomadaire. 7% seulement n'y ont jamais recours.

Elle est très appréciée pour sa convivialité (à 92%) avec une perception relative de la confiance (74%).

Si la facilité d'utilisation est assez homogène d'un pays à un autre (de 92% à 86%), la confiance en revanche est très fluctuante : sans surprise, les pays les moins confiants dans ce type d'authentification (Hongrie, Pays bas, Belgique, Suède) sont ceux qui l'utilisent le moins.

Q: How often do you use a static password as authentication method for e-banking? (base=users of e-banking)

| | Static pasword | Trust | User friendlines |
|---|---|---|---|
| Denmark | 94% | 87% | 92% |
| Austria | 93% | 67% | 92% |
| France | 93% | 81% | 96% |
| UK | 91% | 86% | 96% |
| Germany | 91% | 65% | 91% |
| Portugal | 88% | 72% | 88% |
| Spain | 87% | 79% | 89% |
| Finland | 85% | 76% | 94% |
| Italy | 81% | 77% | 94% |
| Poland | 77% | 75% | 92% |
| Hungary | 75% | 64% | 86% |
| Netherlands | 71% | 64% | 90% |
| Belgium | 67% | 70% | 88% |
| Sweden | 63% | 63% | 90% |
| **Europe** | **86%** | **74%** | 92% |

*Source : CEE - 2007*

#### 3.2.2.2 AUTHENTIFICATION FORTE : ENCORE MINORITAIRE

Comparativement, l'authentification avec mot de passe dynamique est beaucoup moins pratiquée : 31% des internautes *utilisateurs de la banque en ligne* n'y ont jamais eu recours en moyenne, et ils sont 56% seulement à l'utiliser au moins une fois par mois (avec des divergences assez fortes en fonction des pays : certains pays d'Europe du Nord ont des taux de pénétration très élevés). L'une des raisons principales en est la perception de la convivialité par ses utilisateurs jugée nettement inférieure, tout particulièrement dans les pays qui la pratiquent peu.

En revanche, la confiance des consommateurs à l'égard de ce type de solution est forte et assez homogène en Europe, preuve que la médiatisation des tentatives de fraude et les efforts de pédagogie des banques ont été payants.

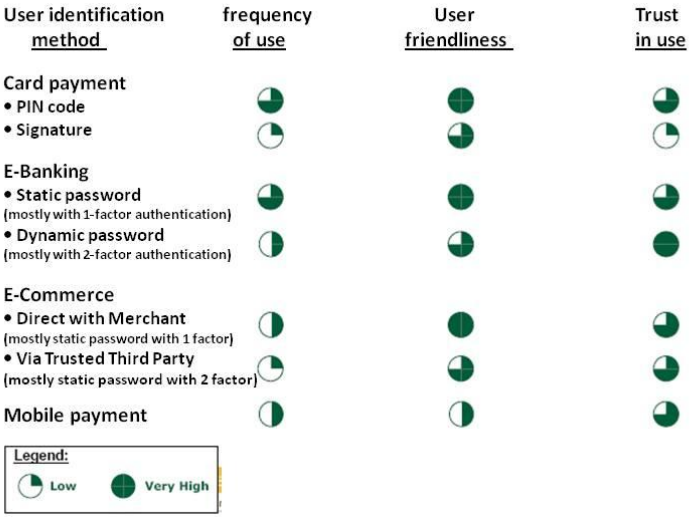
Q: How often do you use a dynamic password as authentication method for e-banking? (base=users of e-banking)

| | Dynamic pasword | Trust | User friendliness |
|---|---|---|---|
| Finland | 81% | 91% | 84% |
| Belgium | 79% | 91% | 76% |
| Sweden | 78% | 83% | 74% |
| Netherlands | 66% | 88% | 81% |
| Spain | 65% | 85% | 76% |
| Portugal | 64% | 78% | 75% |
| Poland | 62% | 87% | 65% |
| Germany | 59% | 81% | 73% |
| Italy | 57% | 81% | 84% |
| Hungary | 53% | 87% | 71% |
| Austria | 50% | 84% | 74% |
| UK | 38% | 86% | 75% |
| France | 35% | 80% | 80% |
| Denmark | 28% | 85% | 77% |
| **Europe** | **56%** | **85%** | **77%** |

En matière de paiement en ligne par carte, l'ergonomie de l'authentification du paiement est fortement appréciée (90%). Dans un peu moins d'un cas sur deux (43%), l'authentification s'effectue après un routage auprès du site de la banque ou d'un prestataire de paiement (PSP – Payment Service provider). Ce routage semble avoir un impact sur la convivialité de la solution (appréciée a 80% soit 10 points de moins) mais pas d'influence notable sur la confiance mise dans la solution (78% de confiance en payant directement chez le commerçant versus 76% chez un tiers).

Sur les mobiles, le paiement est encore très embryonnaire. Toutefois, sur le faible taux de répondants, la perception du consommateur sur les mobiles est tout à fait équivalente à celle sur Internet : l'authentification utilisée dans 80% des cas est basée sur un code PIN à quatre chiffres. Elle est jugée fiable (76%).

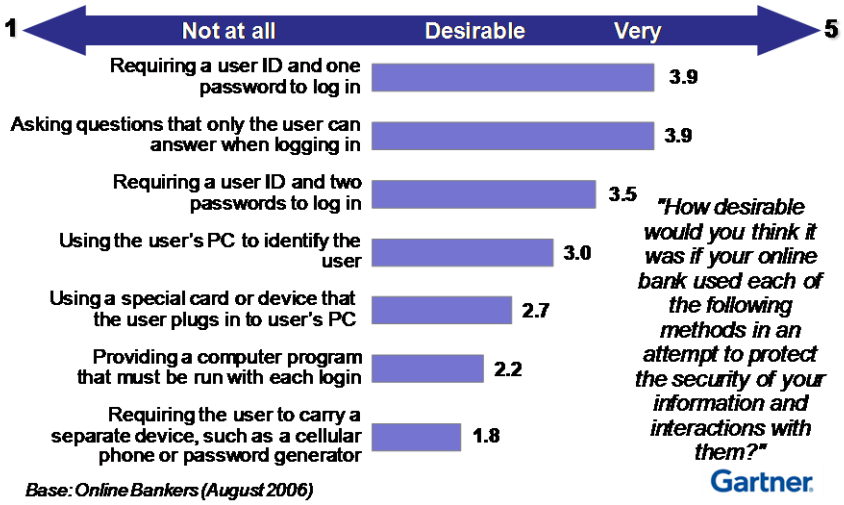
En synthèse, les usages et les perceptions des différentes méthodes d'authentification peuvent être synthétisés comme suit.




## 3.2.3 PERIPHERIQUES D'AUTHENTIFICATION : APPRECIES MAIS POSENT PROBLEME EN PRATIQUE

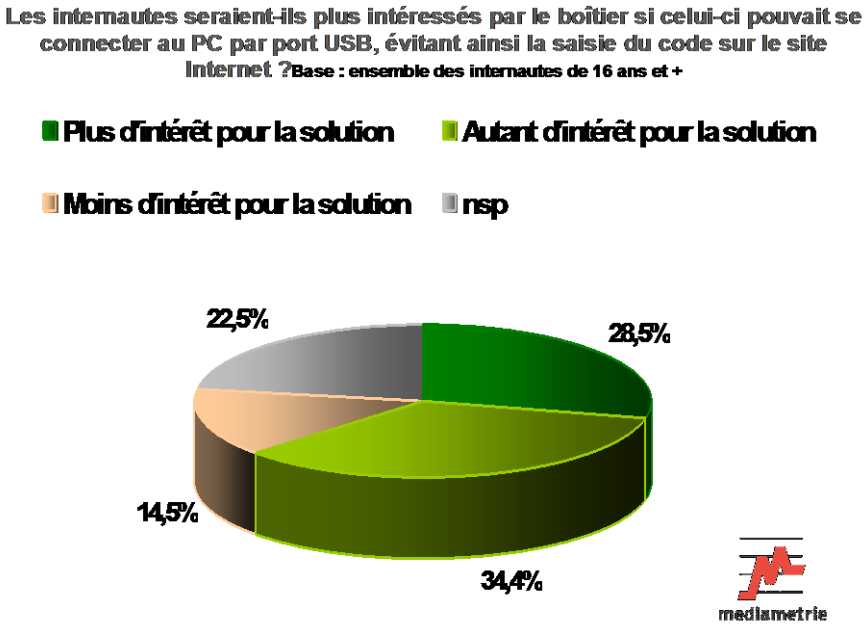
### 3.2.3.1 ERGONOMIE VS SECURITE : UN DEBAT OUVERT

Une étude de Gartner souligne la préférence affichée par les utilisateurs pour les systèmes d'authentification faisant appel à un ou deux mots de passe, plutôt qu'une authentification nécessitant l'adjonction d'un système matériel ou logiciel pour renforcer la sécurité. Le degré d'acceptabilité de ce type de solution chute assez rapidement. Même s'ils ont conscience que ces systèmes renforcent la sécurité, les consommateurs ne semblent pas prêts à sacrifier la facilité d'utilisation de l'authentification, ceci aux dépens de la sécurité.




**L'expérimentation MSP** (mon.service-public.fr), menée par la DGME, confirme les difficultés rencontrées par les utilisateurs pour installer le lecteur de carte à puce fourni sur leur ordinateur, ou pour déclarer l'accès carte à puce dans le service. Il s'agit là d'une problématique à prendre en compte et à traiter dans le cadre de l'utilisation de tels systèmes. Néanmoins, cela ne semble pas poser de problème pour des déploiements à grande échelle dans d'autres pays européens.

Selon une **étude Groupement des Cartes bancaires** sur l'authentification[42], 65 % des internautes sont favorables à l'utilisation d'un boîtier (lecteur de carte à puce avec clavier) connecté à leur PC.




Afin de favoriser une meilleure acceptation, ce périphérique devrait de préférence être simple (d'installation et d'utilisation) et gratuit, ou même intégré au matériel de l'utilisateur.

### 3.2.3.2 SOLUTIONS BIOMETRIQUES : PERCEPTION FAVORABLE

Pour le choix d'une méthode d'authentification renforcée, les consommateurs semblent séduits par les systèmes biométriques (reconnaissance vocale, empreinte digitale, réseau veineux, reconnaissance d'iris, etc.). Ils sont sans doute rassurés par le fait de toujours porter leur sésame sur eux, à condition bien entendu que les techniques d'identification considérées soient fiables.

C'est ce que souligne une étude menée par Unisys[43] en mai 2006 dans 14 pays. Elle confirme la préférence exprimée par des utilisateurs pour des techniques d'identification biométriques (66%), devant les technologies de type lecteur de cartes à puce (46%), jeton de sécurité (42%), ou le rajout d'un mot de passe supplémentaire (15%).

Would the following methods be a good idea ?

| | Total monde |
|---|---|
| Biometrics | 66% |
| Smart card reader | 46% |
| Security tokens | 42% |
| More passwords or PIN numbers | 15% |
| Other | 8% |

Les répondants qui utiliseraient volontiers la biométrie le feraient essentiellement pour la facilité qu'elle leur procure, en évitant de mémoriser un identifiant d'accès et un mot de passe et en accélérant le processus de vérification.

[42] Etude GIE CB / Mediamétrie sur l'authentification porteur (Mars 2007) - Base : Internautes 16 ans et + : 21 027 000 individus

[43] "Unisys- Global Study on the public perception about Identity Management" - Mai 2006. L'ANTS exprime ses réserves concernant cette étude.

Toutefois, l'étude met également en valeur les réticences fortes rencontrées de manière très homogène à travers tous les pays, chez près d'un tiers des personnes interrogées : suspicions sur la fiabilité des technologies biométriques où refus de livrer des informations intimes.

**Why would you not consider using biometrics ?**

| | Total monde |
|---|---|
| Suspicious about technolgy | 74% |
| Don't want to provide biometric information | 62% |
| Do not believe biometrics accurately idetntify | 36% |
| Fearful of biometric infortaion being accessed | 32% |

De manière générale, **la perception favorable des solutions biométriques est à relativiser en raison du manque de connaissance du grand public de la nature et des modalités d'utilisation des solutions biométriques, qui sont encore très peu diffusées.**

## 3.3 SENSIBILITE LIEE AU PARTAGE ET A L'UTILISATION DE DONNEES PERSONNELLES

A l'heure du succès des « réseaux sociaux » sur le net, la question de la protection des données personnelles est cruciale. La CNIL juge ainsi la situation « angoissante » à bien des égards. Paradoxalement, si les utilisateurs se disent inquiets des dérives possibles, ils ne prennent dans le même temps que peu de précautions quant à la divulgation de leurs données (au moins pour un certain nombre d'entre elles) et de leur vie privée, en particulier les jeunes. Les données personnelles les moins sensibles sont devenues, en quelque sorte, un instrument de mise en relation ou de négociation, et le phénomène a commencé à s'étendre aux données sensibles.

A noter que ne seront pas traités ici les comportements d'utilisation de fausses identités, de pseudos ou d'avatars, qui n'entrent que très marginalement dans le cadre des usages de FC² (en dehors de l'usage éventuel de pseudos pour l'authentification).

D'après l'enquête en ligne réalisée par Caroline Lancelot-Miltgen en 2004-2005 sous l'égide de la FING, intitulée « Vous et votre identité numérique », les risques liés à la fourniture de données sur internet sont jugés élevés et très élevés par 89 % des répondants[44]. Les résultats de cette étude sont bien entendu à relativiser car ils ne prennent pas en compte les évolutions récentes des usages (ex. réseaux sociaux), de même qu'une éventuelle prise de conscience des dangers par les utilisateurs.

Selon une étude de Forrester Research, 84 % des internautes estimaient en 2006 que les sites n'étaient pas suffisamment protégés, et 24 % n'effectuaient aucun achat en ligne, en partie pour cette raison. Selon une enquête Verisign récente, 70 % des internautes français se déclarent inquiets des risques de vol de leurs informations personnelles.

[44] L'échantillon était composé de 1364 internautes français, majoritairement de sexe masculin et fréquents utilisateurs d'internet.

**Consommateurs inquiets sur Internet (%)**

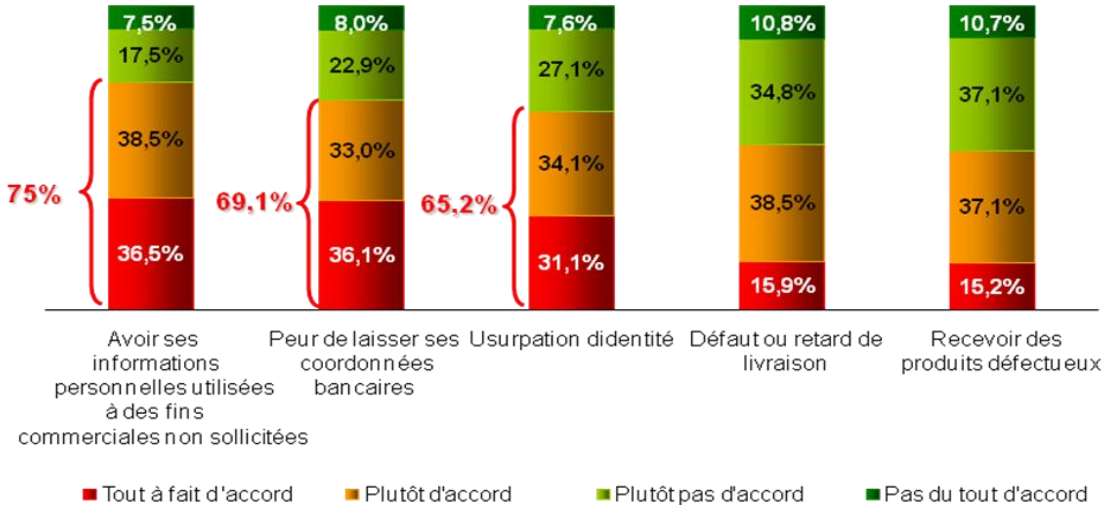
| | |
|---|---|
| Allemagne | 79% |
| Royaume Uni | 78% |
| *France* | *70%* |
| Suède | 55% |
| Danemark | 41% |

*Source : Etude YouGov pour Verisign, 2008*

La bonne gestion du partage et du transfert de données personnelles apparaît comme l'une des conditions majeures de l'acceptabilité et de l'utilisation effective du service fourni par la future plate-forme FC².

Une étude récente menée en France par Médiamétrie[45] pour le Compte du Groupement des Cartes Bancaires met en évidence cette extrême sensibilité vis-à-vis des données personnelles.
Elle souligne que les craintes exprimées sont essentiellement liées au fait de laisser ses données personnelles sur le site qu'il s'agisse d'identité personnelle ou de coordonnées bancaires *(cf graphe ci-dessous*).

**Raisons pour lesquelles les internautes n'effectuent pas d'achat sur Internet**




Base : internautes **n'ayant jamais acheté** sur Internet ou l'ayant fait il y a plus d'1 an

### 3.3.1 DETERMINANTS DE LA PERCEPTION DE L'UTILISATEUR VIS-A-VIS DE SES DONNEES

De nombreux facteurs entrent en jeu dans la perception des utilisateurs, parfois irrationnels, et influencent les arbitrages qu'ils opèrent en matière de divulgation des données personnelles sur Internet :

- il existe tout d'abord des **variations de perception et de comportement entre les différentes zones géographiques**, dont les causes sont liées à la fois aux spécificités **culturelles** (approches divergentes de la notion de vie privée, culture de la transparence) et **institutionnelles** (par exemple, le numéro de sécurité sociale est l'identifiant unique aux usa ou dans les pays nordiques, alors qu'il n'a pas la même fonction en france). une étude mondiale sur la perception du public

[45] Etude GIE CB sur l'authentification porteur (Mars 2007) - Base : Internautes 16 ans et + : 21 027 000 individus

en matière de gestion d'identité » (2006) met en valeur le caractère plus prudent des européens en la matière, comparé en particulier aux nord-américains et aux asiatiques (voir graphiques ci-dessous)[46].

- l'importance du **contexte de sollicitation** : la décision de divulguer les données personnelle est en grande partie « situationnelle », et répond à 4 critères selon caroline lancelot-miltgen :

| | |
|---|---|
| **CONFIDENTIALITE PERÇUE** | confiance dans la capacité du récipiendaire à garder les informations confidentielles – lien avec la sécurité perçue |
| **SENSIBILITE PERÇUE** | degré de « sensibilité » de l'information (voir ci-dessous) |
| **PERTINENCE PERÇUE** | légitimité, proportionnalité de la demande d'information par rapport au type de transaction |
| **EQUITE PERÇUE** | rapport coût / bénéfice perçus |

Le niveau de confiance est évidemment à relier avec le type de site internet utilisé : administration, entreprise familière, association, entreprise réputée, ou entreprise non familière (par ordre décroissant de confiance).

Le graphique ci-dessous illustre les différences de comportement entre un fournisseur de service commercial / entreprise et une administration, en Europe :

- l'utilisateur est logiquement plus enclin à confier ses informations d'état civil à l'administration : identifiant national, permis de conduire, date de naissance, nationalité.
- il fournit plus volontiers une adresse e-mail, un moyen de signature électronique, et dans une moindre mesure son numéro de carte bancaire, à une entreprise privée.
- Le **profil de l'utilisateur** a bien entendu un impact majeur. Sur la base de l'enquête réalisée auprès d'internautes français, Caroline Lancelot-Miltgen définit 4 profils d'utilisateurs (classés du moins méfiant au plus méfiant). Ces résultats sont cohérents avec la typologie établie aux Etats-Unis par Alan Westin, en 1995.

| TYPE D'UTILISATEUR | PROPORTION | CARACTERISTIQUES |
|---|---|---|
| **DESINTERESSES** | 31 % | prêts à fournir des données sans contrepartie / opposés à la marchandisation |
| **BIENVEILLANTS** | 20 % | fournissent des données uniquement si garantie de sécurité et confidentialité |
| **NEGOCIATEURS** | 25 % | négocient leurs données personnelles, souhaitent en tirer un bénéfice tangible : prix, service |
| **RETICENTS** | 24 % | position de principe de ne pas fournir de données personnelles |

[46] Echantillon composé de 1661 répondants issus de 14 pays, répartis de manière relativement homogène sur les 4 régions. L'échantillon européen était composé de 150 Britanniques, 140 Allemands, 103 Français et 34 Danois.

On note ainsi que 24 % des utilisateurs français sont totalement « réticents » à fournir des données personnelles sur internet, dans l'état actuel des solutions disponibles. Il s'agit d'une proportion très importante, mais certainement exagérée en raison des spécificités de l'échantillon étudié. Il s'agissait en effet d'une population avertie, consciente des problèmes de sécurité et qui serait donc aisément sensibilisée à l'intérêt d'une plate-forme telle que FC².

Il existe également une tendance à négocier la fourniture de données personnelles en échange d'avantages en termes de prix ou de service (25 % de « négociateurs »). Il s'agit là d'une approche commerciale qui pourrait éventuellement trouver sa place dans un modèle économique.

**Le type de données fournies, classées par degré de sensibilité :**

| | |
|---|---|
| **DONNEES TRES SENSIBLES** | Numéro de téléphone, numéro de carte bancaire, [détection de présence sur le réseau, infos agenda, appartenance à un groupe, contenus] |
| **DONNEES SENSIBLES** | Situation familiale, professionnelle, adresse, [adresse professionnelle, centres d'intérêt, liste de contacts, localisation] |
| **DONNEES PEU SENSIBLES** | Nom, prénom, sexe, âge, adresse e-mail |

*Sources : Caroline Lancelot-Miltgen, Trusting Orange – projet R&D Confucius*

Plus la donnée est « sensible », moins l'utilisateur sera enclin à la partager sur le net et à déléguer sa gestion à un tiers de confiance.

**L'ergonomie** : la manière dont le site est présenté joue un rôle majeur dans la création de la confiance. En particulier, la bonne mise en valeur du consentement de l'utilisateur pour le partage des données personnelles, et l'homogénéité des visuels (notamment logo de la marque de confiance) d'un site à l'autre dans les différents cercles de confiance.

### 3.3.2 EXIGENCES DES UTILISATEURS ET DECLENCHEURS DE PERTE DE CONFIANCE

De manière générale, le consommateur réalise des arbitrages en termes de partage de données personnelles, selon l'intérêt qu'il peut avoir à partager ses données (coût d'opportunité). Son comportement prend en compte l'ensemble des facteurs de perception énumérés ci-dessus.

Toutefois, ce phénomène d'arbitrage ne peut pas expliquer tous les comportements de l'utilisateur. En fonction des différents facteurs de perception, les utilisateurs ont des **exigences incontournables**, dont le non respect peut déclencher la perte de confiance, et donc l'interruption d'une transaction (abandon en cours de procédure) :

- **L'utilisateur doit avoir le sentiment de garder la maîtrise** : il doit pouvoir s'assurer avec certitude des données qu'il partage, de leur provenance, de son droit de modification. Son autorisation doit être explicite. Les phases de connexion et déconnexion au service doivent être clairement identifiées.
- **L'utilisateur doit se sentir responsabilisé** : on ne manie pas des informations personnelles sans précautions, il doit avoir le sentiment qu'il donne son autorisation en connaissance de cause (comme s'il confiait une pièce d'identité à un tiers pour que celui-ci puisse s'en servir pour l'accès à un service).
- **L'utilisateur doit être rassuré sur la sécurité du système** (accès de tiers, possibilités de fraude), éventuellement grâce à une marque de confiance et / ou à un dispositif de contrôle et d'audit. Sur ce dernier point, le service FIA-Net pourrait servir de benchmark.

Les **déclencheurs** de la perte de confiance :

- **Le manque d'information et de transparence** : l'utilisateur a besoin de se sentir informé à chaque étape de la transaction. Un équilibre doit être trouvé entre la quantité d'information transmise et la simplicité d'utilisation du site, qui est également un critère important.
- **L'hétérogénéité de la présentation visuelle** entre des sites appartenant à un cercle de confiance : besoin d'une interface utilisateur familière, qui ne déroutera pas l'utilisateur, et éventuellement d'un logo clairement identifiable.
- **Les utilisateurs se méfient de tout stockage de données**, même volontaire, sur un espace dédié en ligne de type porte-documents ou coffre-fort[47]. Dans le cas du pilote MSP (mon.service-public.fr), cette fonctionnalité avait été peu utilisée, notamment par crainte que tous les sites fédérés puissent avoir accès aux données y étant archivées (ex. la CAF qui pourrait avoir accès à ma déclaration d'impôt sur le revenu).

## 3.4 PERCEPTION DES FOURNISSEURS DE SERVICES

Une étude d'impact mandatée par l'AFNOR[48] fait une évaluation de l'impact potentiel de la signature électronique dans le contexte de l'identité numérique.
Bien que cette étude limite son périmètre à la France et ne peut donc en tant que telle être extrapolée, elle souligne quand même un certain nombre d'attentes et de freins de la part des fournisseurs de services.
D'une manière générale, l'étude révèle le déficit de perception de la part des fournisseurs de services, qui n'ont pas intégré le potentiel considérable offert par les certificats pouvant générer des signatures juridiquement équivalentes à une signature manuscrite.

### 3.4.1 VENTE EN LIGNE

La croissance du chiffre d'affaires du e-commerce reste soutenue (+35%) et s'établit aux alentours de 16 Milliards d'Euros en France (19 si l'on comptabilise également les services).

La fraude sur les cartes de paiement, principal moyen de paiement utilisé en France, reste faible. Comme **près d'un acheteur sur deux en moyenne abandonne la transaction d'achat entre la validation de la commande et le paiement**, les e-commerçants sont à priori réticents à renforcer la sécurité du paiement au risque de complexifier la transaction et d'augmenter encore le taux d'abandon. Mais confrontés à cette évolution, de grands fournisseurs de services (Air France, Accor) n'ont pas constaté de diminution de commandes.

Ce comportement pourrait se modifier en cas d'augmentation du taux de fraude, ou de diminution de la confiance des acheteurs dans le paiement (qui reste élevée actuellement).

### 3.4.2 CREDIT A LA CONSOMMATION

Dans un contexte très concurrentiel, puisque les demandes de crédit en ligne peuvent atteindre jusqu'à 30% des nouveaux encours, les établissements de crédit semblent intéressés à poursuivre leur conquête de parts de marché agressivement sans pour autant négliger les fondamentaux juridiques.

[47] Ceci exclut le stockage de données sur un support sécurisé de type carte à puce ou clé usb.
[48] « La signature électronique et les infrastructures à clé publique dans le contexte de l'identité numérique : Quels usages pour les titres sécurisés émis par l'Etat dans le monde de l'économie numérique », novembre 2007.

Même si elles sont soumises au contraintes des lois Scrivener, à savoir le respect du délai de rétractation et la rédaction d'un contrat de prêt, elles cherchent à fluidifier au maximum les relations clients en amont, notamment à travers la communication en ligne de justificatifs numérisés, pour sécuriser l'ouverture d'un compte au nouveaux demandeurs, en réduisant au minimum la procédure de constitution du dossier solide sur le plan juridique.

### 3.4.3 BANQUE EN LIGNE

Si les acteurs bancaires sont par l'expérience du métier plus matures dans l'appréhension des enjeux liés à l'identité numérique que les acteurs du monde du e-commerce, il convient de distinguer les types d'opération pour lesquels ils semblent être les plus demandeurs.

#### Ouverture de compte

Compte tenu des contraintes de la réglementation bancaire relatives au blanchiment des fonds, qui les obligent à demander à leurs clients la justification de l'origine des fonds, et à l'évaluation du risque potentiel à accepter tout nouveau client, les banques traditionnelles ont pour le moment plutôt privilégié l'entretien en face à face pour l'ouverture d'un compte plutôt qu'une procédure en ligne.
Les déboires passés des acteurs de banque en ligne « pure player » et leur repli ne semblent pas pousser les banques à faire évoluer sensiblement leur point de vue à court terme.

#### Opérations courantes de banque en ligne

En revanche, l'évolution forte de la banque en ligne et son ambition de dématérialiser la gestion de compte constitue un champ privilégié pour l'authentification forte et la traçabilité des transactions, et donc l'un des secteurs les plus favorables a l'utilisation des solutions développées par les acteurs de FC².

### 3.4.4 SERVICES PUBLICS

La volonté des services publics d'améliorer le niveau de service fourni tant aux citoyens qu'aux entreprises, les exigences de rationalisation des dépenses et de modernisation du secteur public alliés à la montée progressive en puissance de cartes d'identité électroniques ont créé les conditions propices d'adoption de systèmes d'identité numérique.

Dès lors que les systèmes proposés sont conformes aux réglementations européenne et locales relatives aux données personnelles, les attentes sont fortes et les cas d'utilisation nombreux.

## 3.5 COMPREHENSION DU CONCEPT DE FEDERATION

Certaines études reflètent les attentes des utilisateurs pour un système de gestion d'identité interopérable[49]. La fédération d'identité paraît tout à fait adaptée pour répondre à ce besoin, dans le respect de la protection de la vie privée, sous réserve de prendre en compte un certain nombre d'éléments de présentation et de pédagogie.

### 3.5.1 LE TERME « FEDERATION »

Le terme de « fédération d'identités » est encore nouveau pour bon nombre d'utilisateurs. Derrière ce **terme relativement imperméable**, se cache un concept que les utilisateurs doivent bien comprendre afin d'en cerner l'objectif et les implications. Il

[49] En Europe, les répondants à l'une d'elles citent d'ailleurs spontanément trois types d'institutions les plus aptes à émettre et gérer un système d'identité unique : une agence gouvernementale (à 56 %), un établissement bancaire (44 %) et la police (39 %). Les autres acteurs arrivent loin derrière.

sera donc nécessaire de bien définir ce dont il s'agit, de manière simple, afin de lever tout malentendu (par exemple, il ne s'agit pas de stocker tous les éléments de son identité au même endroit…). L'utilisation d'un sélecteur d'identité de type *Infocard* faciliterait considérablement cet effort de pédagogie, grâce à la correspondance naturelle avec le monde physique.

Au niveau terminologique, l'expérimentation de l'administration française MSP (mon.service-public.fr)[50], qui sera ici notre principale référence, utilise le terme de « liaison de compte » plutôt que celui de « fédération », afin de faciliter la compréhension de ce concept. Néanmoins, ce terme n'est peut-être pas totalement adapté et il est souhaitable d'étudier d'autres termes (ex. « trousseau de clés » dans le transport aérien).

### 3.5.2 CAPACITE DE L'UTILISATEUR A CERNER L'OBJECTIF ET LES AVANTAGES DU SERVICE

Les principaux retours d'expérience du pilote MSP sont les suivants :

- « La fédération d'identité a été comprise, jugée utile et simple par 76 % des usagers ».
- Néanmoins, on relève une difficulté à cerner l'objectif de la fédération dans le cadre du pilote, qui ne comprenait que 2 partenaires pour la fonctionnalité de fédération d'identité (ANPE et CAF). Rendre le maximum de services compatibles avec la fédération permettrait d'apprécier au mieux tous les avantages qu'elle procure. Il apparaît nécessaire de créer de vrais bouquets de service complets et cohérents.
- La visite guidée du site et de ses fonctionnalités a été jugée utile par 70 % des utilisateurs (sans oublier la présentation générale du service).
- Un moteur de recherche transversal doit permettre d'effectuer une recherche sur l'ensemble des sites fédérés.

L'avantage déterminant procuré par le service de fédération est bien perçu par l'utilisateur : naviguer d'un site à l'autre sans avoir à se ré-identifier. Cet avantage est bien entendu corrélé au nombre de sites fédérés.

### 3.5.3 SIMPLICITE / COMPLEXITE PERÇUE

De manière générale, le site MSP est jugé simple ou très simple d'utilisation à 80 %.
La fonctionnalité de « liaison de comptes » est jugée facile d'utilisation par 90 % des utilisateurs l'ayant utilisé (50 % d'entre eux ont lié au moins une fois leur compte ANPE ou CAF à MSP).

D'après les retours d'expérience, le service de fédération ne doit pas être trop compliqué à mettre en œuvre, au risque de décourager les utilisateurs.

#### Remarque importante

Comme évoqué plus haut, le comportement et la confiance du consommateur varient en fonction de la situation dans laquelle il se trouve (type de site internet notamment). Ainsi, il faut relativiser les retours d'expérience de la DGME sur MSP, car la confiance est créée beaucoup plus facilement dans le cas d'un site de service public. Par ailleurs, l'utilisateur perçoit alors immédiatement tous les avantages qu'il peut tirer d'un service fédérant un grand nombre de sites publics, au niveau national et local, alors que les usages commerciaux sont dans la plupart des cas d'ampleur beaucoup plus restreinte.

[50] Le pilote, basé sur une architecture de type « Liberty », concernait 418 utilisateurs, en 2 phases, de mai à juillet 2006. Un service d'assistance par e-mail ou téléphone était disponible. Source : DGME - *Expérimentation mon.service-public.fr – synthèse des résultats (sept. 2006).*

## 3.6 CONDITIONS DE FAISABILITE ET D'ACCEPTABILITE DE SERVICES BASES SUR LA PLATE-FORME FC² : RECOMMANDATIONS

Afin de favoriser l'adoption et l'utilisation des services offerts par la plate-forme FC², en prenant en compte l'ensemble des considérations mentionnées ci-dessus, il est primordial de se poser les questions suivantes :

- quels sont les facteurs clefs de succès, du point de vue des consommateurs et des fournisseurs de services ?
- quels facteurs de « réassurance » vis à vis des problèmes de protection de vie privée et de sécurité ?
- quels risques de fraude[51]?
- quels sont les critères de faisabilité et d'appropriation propres à favoriser l'acceptation du service par la plus large population possible d'utilisateurs (y compris ceux peu familiers avec la technologie, ou peu équipés)
- quelle présentation des concepts de fédération et de sso/slo aux acteurs de manière à leur en faire saisir immédiatement les avantages ?

### 3.6.1 DU POINT DE VUE DES CONSOMMATEURS / UTILISATEURS

En synthèse, l'analyse de l'ensemble des études fait ressortir **3 exigences** incontournables pour l'utilisateur :

- **garder la maîtrise des données à partager**
- **se sentir responsabilisé, tout particulièrement sur les données sensibles**
- **être rassuré sur la sécurité du système**

Elle permet également d'identifier **3 freins**, déclencheurs de la perte de confiance :

- **le manque d'information et de transparence**
- **l'hétérogénéité des la présentation visuelle d'un site à l'autre**
- **la centralisation des données en un espace de stockage unique**

Ainsi, le groupe de travail a formulé les recommandations suivantes.

**L'utilisateur doit disposer d'une information précise sur la gestion de ses données personnelles**

- identification claire de l'entité qui collecte les données personnelles
- information précise sur les données collectées (type, stockage, période de stockage etc.)
- explication de la procédure de collecte des données personnelles
- transmission des données personnelles aux fournisseurs de service avec accord circonstancié du consommateur
- il est capital de pouvoir donner accès à la bonne information au consommateur, pas à pas au cours des parcours utilisateur, quand il le souhaite, et aussi quand il en a besoin (afin de fluidifier le parcours).
- il faut distinguer les éléments d'information qu'il faut absolument pousser vers l'utilisateur (« obligatoires »), et ceux qu'il peut consulter de manière optionnelle tout au long du parcours utilisateur pour une information plus complète (par exemple via des info-bulles déroulées en positionnant le pointeur).
- par ailleurs, l'utilisateur doit être informé qu'il existe un slo (single logout) qui lui permet de se déconnecter de la plate-forme. il y a un effort à produire en matière d'ergonomie pour bien mettre en valeur cette fonctionnalité.

[51] En matière de lutte contre la fraude, par usurpation d'identité et/ou répudiation du paiement, il est possible de regrouper dans un même ensemble les approches fondées d'une part sur les bases d'information et d'autre part sur les technologies décisionnelles (scoring, datamining, réseaux de neurones) dans la mesure où elles sont souvent mises en oeuvre par les mêmes sociétés. Ce sont des outils probabilistes, ce qui tend à les rapprocher des solutions biométriques.

**Garantir la maîtrise des données**

- Un choix explicite doit être offert par le fournisseur de service au consommateur en termes de sélection des données à envoyer, en matérialisant distinctement les données obligatoires de celles optionnelles qui peuvent être modifiées ou effacées.
- Un accès direct aux données personnelles et aux consentements déjà fournis doit être proposé, avec la possibilité de les modifier.

**Rassurer le consommateur**

- Il est important de rappeler au consommateur ses droits à défendre la protection des données pour le rassurer.
- Lui assurer de la conformité du système aux réglementations en vigueur (notamment CNIL).
- L'informer de manière simple sur la sécurité des données.
- Proposer un recours en cas de litige : le mécanisme de recours doit être calqué sur ce qui existe aujourd'hui en matière de litiges commerciaux. Le rôle du (des) Correspondant informatique liberté devra être précisé dans ce cadre.

### 3.6.2 DU POINT DE VUE DES FOURNISSEURS DE SERVICE ET PRESTATAIRES TECHNIQUES

Le groupe de travail a formulé les recommandations suivantes, à l'égard des fournisseurs de services et prestataires techniques.

**Information client**

- offrir une transparence des traitements : information claire à chaque étape.

**Faciliter l'adoption par les consommateurs par la simplicité d'utilisation**

- respect des consignes d'harmonisation des processus (respect de la charte, utilisation d'une bibliothèque de services paramétrables)
- suivre les préconisations ergonomiques (fluidité du parcours et information à chaque étape). notamment, l'authentification et la validation du paiement 3dsecure devront, autant que faire se peut, être intégrés dans les pages du site du fournisseur de service, et bénéficier d'une propagation d'authentification, sans introduire de rupture dans l'expérience utilisateur.

**Confiance**

- sécurité: se conformer aux contraintes sécuritaires (respect des cahiers des charges, acceptation du principe d'audits).
- se conformer impérativement aux contraintes relatives aux durées de conservation des données.
- proposer un mécanisme de recours.

## 3.7 MISE EN ŒUVRE DES RECOMMANDATIONS DANS LE CADRE DE LA PLATE-FORME

La matérialisation de ces recommandations implique que soient définis préalablement un certain nombre de points.

### 3.7.1 MARKETING

*Marque, logo*

- intérêt d'une marque/label[52] pour matérialiser la confiance : il y a consensus du groupe de travail sur le besoin d'une marque correspondant à la plate-forme fc² (qui ne sera pas « fc² » mais une marque commerciale à déterminer).

[52] Les « marques de confiance » ou « sceaux électroniques » sont des mécanismes qui ne font pratiquement pas appel à la technologie. Des initiatives américaines comme TRUSTe ou BBBOnline (http://www.truste.org, http://www.bbbonline.org) ont connu une large diffusion aux Etats-Unis dans le domaine du commerce électronique, principalement pour leur dimension « privacy » dans un pays qui ne dispose pas, au niveau fédéral, d'une loi informatique et libertés de portée générale. En France, de telles initiatives existent également

- rôle de cette marque : à définir plus précisément dans le cadre du travail sur la chaîne de valeur et le modèle économique (l1 gt2).
- 2 rôles sont possibles :
- rôle de label : affichage d'un logo à côté des différentes marques des fournisseurs d'identité ;
- marque matérialisant « l'entrée » dans la fédération des cercles de confiance et donnant accès aux différents fournisseurs d'identité.
- place de la marque et du logo dans les parcours clients à définir et à harmoniser (*cf. story boards des cas d'utilisation*).

Afin de donner une reconnaissance encore plus forte au service, l'opportunité d'un label officiel est à envisager. A ce titre, la Charte pour la promotion de l'authentification sur internet[53], signée en 2008 par les pouvoirs publics et les professionnels de l'internet, vise particulièrement le sujet de FC².

### 3.7.2 RENFORCER LA PEDAGOGIE SUR LE SUJET

**Expliquer simplement le concept de fédération d'identité**

Le groupe de travail s'accorde sur la nécessité de définir une manière simple et pédagogique le concept de « fédération d'identité ». Plusieurs pistes sont envisagées :

- sélecteur d'identité ? (de manière générique, c'est-à-dire sans réduire ce terme à son acception dans le monde de la gestion d'identité)
- trousseau de clés ? (cf. air france)
- portefeuille, sac à main ? (métaphore de la vie de tous les jours : le portefeuille est traditionnellement l'endroit qui réunit tous nos supports d'identité, qu'ils soient des pièces d'identité « régaliennes », cartes bancaires ou de fidélité, ou autres documents auto-déclarés)

Il faut trouver une solution simple et compréhensible pour proposer à l'utilisateur de « fédérer » ses comptes en fin de transaction.

**Expliquer le concept de sso (single sign-on) et de slo (single logout) :** ces fonctionnalités doivent être compréhensibles par le plus grand nombre des internautes, utilisateurs réguliers d'internet ou non. Cela suppose de :

- développer les argumentaires d'information pédagogiques réutilisés par les fournisseurs de service.
- élaborer une charte de service.

Au-delà la pédagogie portera sur les points clés suivants :

- **Ergonomie, simplicité**
  - élaboration de principes ergonomiques et d'harmonisation des processus.
  - le service doit être multi canaux / multi plateformes, c'est-à-dire accessible sur tous types de terminaux et de navigateurs web.
  - mettre en œuvre les principes d'information consommateur tout au long du parcours utilisateur (voir plus haut)
  - comment élaborer ceux-ci avec les fournisseurs de services concernés ?

---

à l'instar de Labelsite dans le domaine de commerce électronique BtoC ou de ChamberTrust pour le BtoB. La diffusion de ces « labels » reste cependant modeste.
Bien souvent ces marques de confiance vont se trouver confrontées à la concurrence des « marques de confiance de fait », comme les logo « Visa », « MasterCard » ou « CB » ou la référence aux autorités de certification Verisign ou Thawte, qui contribuent à rassurer le public sans formalités ou engagements particuliers de la part du site marchand.
L'assurance peut aussi être rattachée à cet univers. Le fait que l'assureur accepte de couvrir une technologie devient un label de confiance dont il est fait un usage marketing. Le marché est incité à faire confiance à celui qui, par nature, fera le moins confiance : l'assureur. La démarche d'assurance peut se situer à la frontière de la marque de confiance et du système de détection des fraudes.

[53] http://ddm.gouv.fr/surfezintelligent/spip.php?article22

- **Sécurité**
  - authentification, outils et matériels utilisés : les solutions retenues par le sp2 pour les méthodes d'authentification devront prendre en compte la politique de sécurité propre à chaque cas d'usage.
  - standardisation d'un processus de recours.
  - supervision des litiges.

Enfin la question des **périphériques connectés** (lecteur de carte à puce ou périphérique externe, type) nécessite un traitement particulier en termes de recommandations. En effet, il ressort d'un certain nombre d'études et de retours d'expérience que les consommateurs sont plutôt réticents à les utiliser, qui plus est quand ceux-ci nécessitent une installation logicielle.

Leur mise en œuvre pose parfois des difficultés techniques et pratiques, et nécessite un support utilisateur important (cf. retour pilote MSP, même si les retours d'expérience en taille réelle à l'étranger incitent à être beaucoup plus optimiste).
Il est donc indispensable de se demander sous quelles conditions ces périphériques seraient acceptables par l'utilisateur.

Les lecteurs de cartes intégrés dans les ordinateurs portables se développent progressivement, mais le pourcentage de PC équipés reste encore trop faible pour représenter une solution sur laquelle s'appuyer.

Sans doute serait-il opportun que l'application web puisse installer et gérer automatiquement le périphérique, avec une intervention minimale de l'utilisateur.


**CONTACT**

**Jean-Pierre Tual** - Gemalto
+33 (0)1 55 01 61 60
jean-pierre.tual@gemalto.com

www.fc2consortium.org

