Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Secrétariat général pour la modernisation de l'action publique

Identité(s) numérique(s)

Quelle stratégie pour l'Etat ?

Point de vue initial soumis à la consultation

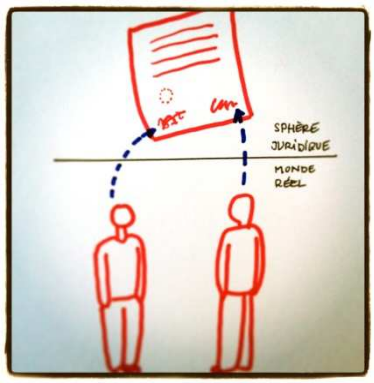
modernisation.gouv.fr

Ce document est le « point de vue initial » du SGMAP au moment du lancement de la concertation sur l'identité numérique. Il a été rédigé dans l'objectif de provoquer des réactions : compléments, questions, autres points de vue. Sur la base de ce document et des réactions qu'il aura suscitées sera élaboré le projet de stratégie de l'État en matière d'identités numériques.

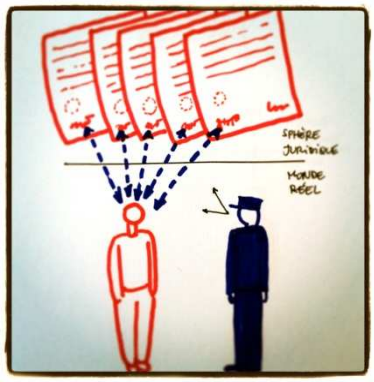
Le cœur du dispositif consiste en la mise en place d'une plateforme de service d'identité de confiance. En parallèle, des travaux conceptuels sont à mener sur les modèles de données et sur la rationalisation du nombre d'identifiants personnels gérés par le service public, ainsi que des travaux de transformation des systèmes d'information publics. Le document identifie les cas particuliers de l'identification des agents publics (dont les collectivités locales) et des personnes morales.

Pour devenir la feuille de route de l'Etat en matière d'identités numériques, cette étude nécessitera, après la concertation, approfondissement sur de nombreux points techniques, et financement des investissements que le document sous-tend.

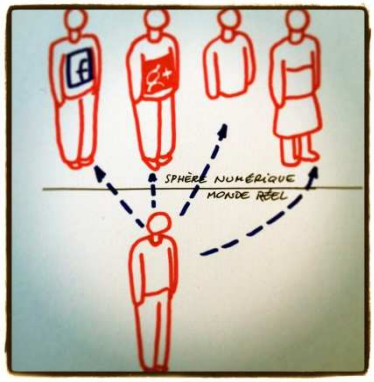
L’interaction réussie entre deux êtres humains requiert et produit de la confiance.



Lorsque l’interaction prend un caractère juridique, entre sujets de droit, la responsabilité devient centrale ; il faut en particulier identifier les sujets de droit pour qu’ils répondent de leurs engagements contractuels ou de leur respect de la loi.
La distinction entre l’être humain qui existe dans le monde réel et le sujet de droit qui le « représente » dans la sphère de l’abstraction juridique sous-tend depuis plus de deux mille ans le développement de notre civilisation du droit. En réduisant l’engagement du corps de l’être humain dans ses interactions, elle a permis de démultiplier les échanges dans les proportions que l’on connaît.

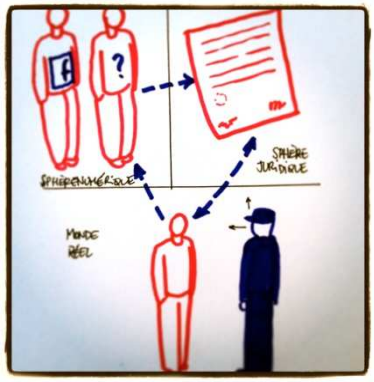


Elle a cependant fait naître le besoin de relier de manière univoque l'être humain et le sujet de droit qui le représente. La confiance dans les échanges juridiques abstraits repose notamment sur la capacité de retrouver l'être humain correspondant au sujet de droit. En effet, quand l'interaction se passe mal, l'abstraction finit par se dissiper et ce sont bien des êtres humains qu'on prive de liberté…
La qualité de la relation entre l'être humain et le sujet de droit qui le représente, qui est l'un des aspects de l'identité de l'être humain, est un des fondements de la cohésion de notre société.
La plupart des activités économiques et sociales des êtres humains ainsi que leurs relations à l'État et aux services publics, s'appuient sur cette relation d'identité, socle des actes juridiques dans notre société, qu'ils portent sur les personnes (filiation, citoyenneté, libertés publiques…), sur les choses (propriété) , sur les contrats (travail, services…).
Cette relation d'identité est ainsi une « infrastructure », largement outillée par l'État : l'état civil en est la plateforme ; la carte d'identité en est l'une des applications que l'État fournit aux sujets de droit de son ressort pour leur usage quotidien.
La transition numérique en cours a engendré une nouvelle sphère d'abstraction aussi puissante et créative que celle du droit. Ainsi l'être humain possède un ou plusieurs « représentants » dans la sphère numérique. Les relations d'un être humain à ses « avatars » sont aussi des relations d'identité.



Pouvoir acheter un bien en ligne est le signe que l'avatar numérique d'un être humain est aussi le support d'un sujet de droit. Les condamnations pénales pour diffamation dans l'espace numérique le montrent également : ce ne sont pas les avatars qui sont condamnés, mais, à travers les sujets de droit, les êtres humains qu'ils représentent.

La question des identités numériques s'intéresse aux relations croisées entre un être humain, les avatars qui le représentent dans la sphère numérique et le sujet de droit qui le représente dans la sphère juridique.



Les relations d'un être humain aux avatars qui le représentent dans la sphère numérique sont plus complexes que celle d'un être humain au sujet de droit qui le représente dans la sphère numérique. Premièrement, elles ne sont pas par principe univoques : un même être humain se fait représenter par autant d'avatars distincts qu'il le souhaite dans la sphère numérique.
Deuxièmement, alors que le sujet de droit agit en conscience, avec la conscience de l'être humain qu'il représente, les avatars divulguent beaucoup d'informations à des tiers à l'insu de l'être humain qu'ils représentent. Des avatars sont même créés par des tiers sans l'accord de l'être humain qu'ils représentent.
Troisièmement, beaucoup de relations marchandes peuvent fonctionner sans nécessiter de moyen formel d'identification : l'achat en ligne classique nécessite ainsi généralement uniquement la garantie de paiement. D'autres activités ne peuvent cependant pas s'en contenter : l'ouverture d'un compte en banque ou l'achat d'un abonnement téléphonique par exemple, nécessitent aujourd'hui des actions « non numériques », pour établir de manière univoque la relation entre avatar numérique (login et mot de passe), sujet de droit (signataire du contrat) et être humain (état civil). Certaines activités nécessitent seulement une vérification partielle de cette relation, par exemple la date de naissance de l'être humain représenté par son avatar numérique dans les systèmes de jeu en ligne.
L'absence d'infrastructure outillée par l'État pour ce qui concerne les relations d'identités numériques n'a pas empêché un développement massif de l'économie numérique, ni même la construction d'une relation numérique entre l'État et le citoyen. Pour autant, la situation actuelle appelle les États à l'action dans le domaine, pour plusieurs raisons :

- Aucun service public ou commercial agissant isolément n'a la dimension suffisante pour mettre en place à des coûts raisonnables, pour ses seuls usages, une infrastructure d'authentification sécurisée à destination du grand public. A défaut, chaque offreur de service met en place des solutions de plus ou moins bons niveaux de sécurité, avec pour conséquence une multiplicité de dispositifs peu ergonomiques pour l'utilisateur, un surcoût et une inefficacité globale.

- En réponse, les géants de l'Internet, tels Google ou Facebook, qui disposent d'une part de marché considérable, investissent la question des identités numériques. D'ores et déjà aujourd'hui, beaucoup de services en ligne s'appuient sur l' « identité Google » ou l'« identité Facebook » de leurs clients, qui, au lieu de créer un compte, utilisent leur compte Google ou Facebook pour accéder au service. Il est très vraisemblable que cette tendance s'amplifie, ce qui pose de nombreuses questions (dépendance de « l'identité » des internautes à un positionnement commercial et à des conditions d'utilisation du service d'une société privée, utilisation de données personnelles par

des sociétés dépendant de législations hors Union Européenne, maîtrise du niveau de confiance…).

- En parallèle, le développement des services publics en ligne, qu'ils soient destinés aux personnes ou aux citoyens, se heurte, pour un développement de services simplifiés de bout-en-bout, à une absence de vision transversale de l'identité entre les différentes administrations, agences, collectivités en charge d'un même dossier et d'une même procédure.

Ce n'est pas un sujet nouveau en France, mais une nouvelle approche est nécessaire pour tirer les leçons des écueils des précédentes réflexions qui, même si elles ont toutes fait avancer les concepts, n'ont pas abouti[1].
En particulier, du fait des enjeux démocratiques, sociétaux et économiques qu'il s'agit de traiter, pour « partir du bon pied », il est nécessaire de partager beaucoup plus largement les concepts et les besoins entre les utilisateurs, les administrations, les prestataires de service, les acteurs économiques du secteur, pour définir les objectifs à poursuivre, les solutions à déployer et les responsabilités de chacune des parties, bien au-delà de la sphère de l'identité « régalienne », ce que ce document propose.

[1] Projets « titre fondateur » (2001-2004), carte électronique du citoyen du plan ADELE (2004-2007), « identité nationale électronique sécurisée » (INES) en 2006-2008, loi « protection de l'identité » finalement largement censurée par le Conseil Constitutionnel en mars 2012.

I. De l'identité aux identités numériques : de quoi parle-t-on ?

a. Quelques éléments sur les origines de l'identité

Sans entrer dans un historique détaillé des dispositifs d'identification[2], il est utile, au moment de définir une stratégie sur « l'identité numérique », de rappeler quelques éléments de repère :

- L'identification des personnes est pendant longtemps essentiellement basée sur la reconnaissance entre individus, vivant pour l'essentiel dans des communautés fermées stables.
- Les premiers dispositifs de recensement de la population et d'Etat civil sont liés aux besoins des Etats en matière de mobilisation de troupes militaires, puis de fiscalité, de police et de justice.
- Les premiers papiers d'identité apparaissent avec l'évolution des sociétés : l'essor des transports, l'urbanisation croissante, la poussée de l'individualisme rendent nécessaire de disposer d'un moyen d'identifier les personnes sans s'appuyer sur une tierce personne.
- La première carte d'identité française, facultative, apparaît en 1921 dans un objectif (déjà à l'époque !) de simplification administrative (uniformisation des dispositifs d'identification délivrés par différents services et départements, suppression de l'exigence de témoins pour les principales démarches)
- Les usages de documents d'identité délivrés par l'Etat se sont développés progressivement au-delà des seules relations entre le détenteur et l'administration, lorsque le titulaire doit justifier de son identité dans la vie courante.

Ces éléments doivent attirer notre attention sur les points suivants :

- La vision de l'identité évolue en fonction de la société. Le déplacement de nombreuses relations entre individus, Etat, entreprises, vers le monde numérique constitue un bouleversement important rendant nécessaire de se pencher sur la transposition du « papier d'identité » dans un nouveau contexte numérique.
- Les besoins originels pour l'Etat de disposer d'une garantie de l'identité sont toujours présents : fiscalité, police, justice ; le recensement militaire est toujours d'usage.
- Les usages actuels des dispositifs d'identification n'étaient pas prévisibles d'avance. Leur diffusion actuelle tient à la simplicité du système et au niveau de confiance dans celui-ci.

Il est également intéressant de constater qu'à ce stade, il n'a pas été nécessaire de construire une définition légale en France de ce qu'est l'identité, des concepts qu'elle recouvre. Même la loi relative à la protection de l'identité[3], ne définit pas précisément ce qu'elle protège. L'élément le plus tangible dans la loi en matière d'identité numérique est l'article 226-4-1 du code pénal en ce qu'il dispose que "Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est puni d'un an d'emprisonnement et de 15 000 € d'amende" et que "Cette infraction est punie des mêmes peines lorsqu'elle est commise sur un réseau de communication au public en ligne".

[2] On lira utilement Pierre Piazza, *Histoire de la carte nationale d'identité*, Odile Jacob 2004

[3] Loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité

b. L'impact de la « révolution numérique »

Les relations économiques, humaines se sont transportées massivement sur les réseaux. Plus de 30 millions de Français font des achats en ligne (dont plus de 4 millions sur mobile), plus de 90% des 40 millions d'internautes français réguliers utilisent les réseaux sociaux[4]. Le changement est profond, il affecte la relation entre individus, il transforme l'économie.
Le concept d'identité, dans le monde numérique, vit également une évolution radicale[5]. L' « identité numérique » dépasse très largement le concept de mon « identité délivrée par l'Etat dans le monde numérique ». De nouvelles formes d'identité sont apparues. Elles sont liées à nos adresses e-mails, nos pseudonymes sur Internet, nos profils sur les réseaux sociaux, les traces que l'on laisse souvent à son insu lors de l'utilisation d'applications numériques, nos adresses IP, notre carte SIM de notre téléphone mobile, notre compte bancaire…
Les changements ayant les conséquences les plus importantes sont les suivantes :

- Les différentes formes d'identité peuvent n'être liées à notre identité traditionnelle que de façon indirecte, voire plus du tout ; il ne s'agit pas de l'anonymat, qui a toujours existé, mais du règne du pseudonymat ou de l'avatar, qui a l'immense avantage, pour celui qui en maîtrise les rouages, de compartimenter ses différentes activités, et de différencier ce qui l'identifie dans une communauté particulière par rapport ce qui l'identifie dans sa vie courante. L'usage de l'« identité réelle » ne va pas de soi dans le monde numérique, tout particulièrement pour les nouvelles générations (chats, jeux en ligne, blogs…). Dans certaines circonstances (blog, compte twitter), le pseudonymat peut être une identité très efficace et très investie.
- A contrario, la numérisation des activités multiplie de façon radicale les traces que chacun laisse dans les systèmes ; au-delà des informations qu'on fournit sciemment sur soi via les réseaux sociaux, le détail de nos dépenses, l'historique de nos recherches sur internet et de nos téléchargements, nos appels téléphoniques (voire la géolocalisation de notre téléphone), notre usage des transports publics, notre image dans le cadre de la vidéosurveillance, sont stockés dans des systèmes d'informations variés ; même en absence de tout dispositif commun d'identification, le recoupement de proche en proche des informations est (technologiquement) possible, pour reconstituer un profil très complet d'une personne. Dans un cadre défini par la loi, un magistrat peut obtenir auprès des fournisseurs d'accès à internet, des opérateurs téléphoniques, des banques, … les informations nécessaires aux actes de justice. L'identité administrative peut donc s'enrichir, plus ou moins volontairement, de nombreuses informations personnelles qui ne lui étaient auparavant pas corrélées.
- Le changement d'échelle est radical. Les activités en ligne sont mondiales, et la question ne peut pas faire abstraction des enjeux transfrontaliers, des questions de reconnaissance mutuelle des systèmes d'identification entre Etats, de la nécessaire convergence des contextes juridiques des différents Etats. Un registre existe déjà de facto pour les objets connectés avec la standardisation complète autour des normes de l'Internet6, et est planifié pour l'identification internationale des entreprises7. La relation au client ou à l'usager s'inscrit de plus en plus dans une vision globale, à des fins de performance du fournisseur de service et de qualité au profit.

[4] Source : FEVAD, chiffres clés 2012
[5] On pourra utilement se pencher sur les travaux du FIDIS (Future of Identity in the Information Society – www.fidis.net)
[6] IPv6 est le nouveau protocole en cours de déploiement dans le monde entier, dont les plages d'adresses permettront de connecter sans limite au réseau internet tous les objets intelligents.
[7] Le projet LEI, initiative du G20, prévoit la mise en place d'un identifiant permanent unique, invariable et universel attaché à toute personne morale, contrepartie à une transaction financière. Voir http://bloglei.com

De l'identité formelle et établie par l'Etat, le monde numérique nous transpose donc vers un faisceau d'identités beaucoup plus multiforme, liées aux profils que l'individu crée pour se représenter sur ses réseaux sociaux, liées à ses activités, à sa banque, à son opérateur téléphonique, à son fournisseur d'accès, … Dans cet ensemble d'identités, l'identité traditionnelle, régalienne, a perdu sa situation de quasi-monopole, mais continue à jouer néanmoins un rôle essentiel : c'est l'identité reconnue pour l'exercice de la force publique, de la justice.

c. Périmètre de la réflexion

Dans cet environnement élargi et complexe, nous proposons de centrer la réflexion sur une partie délimitée. Notamment, si le sujet de l' « e-reputation » est souvent associé au thème de l'identité numérique[8], on se concentrera sur la question originelle de « ce qui permet d'être reconnu, de façon non ambigüe, et avec un certain niveau de confiance, auprès d'un tiers ».
On prendra généralement des exemples dans la sphère de l'usager, être humain interagissant avec un service en ligne, réflexion qu'on pourra étendre ensuite à l'identité des personnes morales (entreprises, associations,…), ou à l'identité professionnelle.

[8] Lire par exemple : *Qu'est-ce que l'identité numérique ? Enjeux, outils, méthodologies*, Olivier Ertzscheid, OpenEdition Press.

II. Identités numériques : cas d'usage, et problèmes à résoudre

d. S'enregistrer sur un service en ligne (« créer son compte »)

Dans de nombreuses circonstances (achats en ligne, création d'une adresse de messagerie, abonnement à des services), lors de la première interaction, le service ne connaît pas l'utilisateur. La création d'un « compte utilisateur » est proposée. Il s'agit, en réalité, de créer, sur ce service, une « représentation » de l'utilisateur. En fonction de la nature du service en question, cette création de compte nécessitera la fourniture d'informations pouvant être liées à son « identité réelle » (nom, prénom, adresse postale, par exemple, pour les services d'achat en ligne).

Réflexion n°1 : Par défaut, les éléments de « création de compte » sont déclaratifs. Dans de nombreux cas, la délivrance d'un service commercial peut se contenter de ce caractère déclaratif des informations. Néanmoins, certaines obligations légales peuvent s'imposer à l'offreur de service, qui doit « s'assurer de l'identité de la personne ». Quels services délivrés par des entreprises nécessitent réellement un très haut niveau de garantie des éléments d'identité à la création de compte ? Entre l' « identité régalienne » établie de façon forte, et le caractère purement déclaratif, un « juste milieu » - à définir - a-t-il un sens ? Peut-on évaluer l'impact économique d'un tel dispositif ?

La très forte pénétration de certains services numériques (tels ceux mis en œuvre par Facebook ou Google) permet à ces acteurs de proposer une véritable plate-forme d'identité ouverte à de nombreux usages[9]. Par exemple, sur le site internet d'un journal, plutôt que l'auteur d'un commentaire soit contraint de créer un compte avant de pouvoir le mettre en ligne, il lui suffit de disposer d'un compte facebook sur lequel il s'identifiera et auprès duquel le site du journal récupérera les quelques informations pertinentes.
Les avantages (en dehors de l'intérêt pour la plateforme d'identité d'étendre ses cas d'usage et d'accroître potentiellement son audience) sont nombreux :

- Pour le fournisseur du service en ligne, cela simplifie largement la gestion des comptes utilisateurs, géré par la plateforme d'identité ;
- Pour l'utilisateur, il évite d'avoir à gérer un nouveau compte, associé à un nouveau mot de passe (qui aura toutes les chances d'être assez générique) ; il obtient le service souhaité sans obstacle ;

Réflexion n°2 : La situation de dépendance vis-à-vis d'un acteur commercial de l'internet, et le caractère essentiellement déclaratoire des informations dans les profils, créés avant tout pour l'usage d'un réseau social à des fins de loisirs, ne permet généralement pas d'utiliser ce type de dispositif dans les relations plus sensibles avec l'administration ou pour des services en ligne exigeant un lien avec l'identité réelle. Il paraîtrait pertinent que l'Etat organise ou pilote la mise en œuvre d'un dispositif de type plateforme d'identité[10], utilisables pour des usages y compris hors du service public.

[9] « Facebook connect » pour Facebook, OpenID pour Google.
[10] A noter : aujourd'hui, le portail « mon.service-public.fr » propose aux usagers un mécanisme d'agrégation de comptes détenus par des administrations, qui devrait évoluer pour répondre aux enjeux précités, notamment en matière de simplicité d'intégration dans les sites tiers, en matière d'évolutivité, et en matière de niveau de confiance dans les informations.

e. Se connecter auprès de son service en ligne

Une fois le compte créé, une fois l'utilisateur connu du service en ligne, il est nécessaire à chaque nouvelle occasion, de se connecter, de se faire reconnaître par le service, avec un dispositif d'authentification servant à s'assurer que la personne qui se connecte est bien celle qui est associée au compte.
Les dispositifs d'authentification disponibles dans les services en ligne sont variés. Les plus courants s'appuient sur des mots de passe, avec des exigences plus ou moins complexes (longueurs, caractères spéciaux, …) ; les dispositifs d'authentification plus avancés se développent et se répandent : cartes à puce associées à un code secret, envoi de code secret sur le téléphone mobile…

Réflexion 3 : La multiplicité des moyens d'authentification, notamment lorsqu'il s'agit de mots de passe, est pénalisante pour les utilisateurs des services, qui sont tentés de réutiliser de nombreuses fois les mêmes mots de passe, ce qui constitue un risque important de captation et d'utilisation frauduleuse. En parallèle, le fournisseur de service doit multiplier les dispositifs de vérification, qui peuvent finir par être coûteux. Un service de « porte-clés » d'authentification, indépendant ou non de l'identité régalienne en ligne, trouverait-il ses usages, et sous quelles conditions ?

f. Faire le lien entre mon moyen d'identification et mon dossier personnel

Dans de nombreux cas, la situation est plus complexe que celles décrites précédemment : l'usager qui réalise une démarche en ligne pour la première fois vis-à-vis de son administration est souvent déjà connu de celle-ci. Il ne s'agit pas de créer un compte, mais de faire le lien entre la personne qui se connecte et le « compte » dont dispose l'administration. Dans la situation et dans ce cadre, il est généralement nécessaire que l'administration et l'usager en question partagent une information qu'un tiers ne pourra pas connaître (un secret), que l'usager saisira pour prouver qu'il est bien celui qui correspond au dossier. Prenons plusieurs exemples :

- le service de consultation sur internet du solde des points du permis de conduire exige de l'internaute la production d'un code secret qu'il obtiendra auprès de la préfecture ;
- les services numériques de la CAF exigeront de l'allocataire la production d'un code secret qu'il aura obtenu par courrier de sa CAF ;
- les services numériques des impôts exigeront du représentant du foyer fiscal qu'il communique des informations qui figurent sur un avis d'imposition envoyé à domicile.

Ainsi, le « dossier personnel » peut être rattaché à l'individu, ou à un « rôle » qu'il détient (en tant que membre d'un foyer fiscal, en tant qu'assuré social, …).
Il est important de noter que la mise en place d'un dispositif mutualisé d'authentification forte, par exemple sous forme d'une carte d'identité numérique, ne permettrait pas à lui seul de résoudre simplement la difficulté pour un système donné de « faire le lien » entre l'individu qui décline son identité, et le « dossier individuel » lui correspondant. Ceci est

fondamentalement lié au fait que les différents systèmes d'information des administrations s'appuient sur des identifiants distincts[11]. Dans l'exemple ci-dessus :

- le système de gestion des permis de conduire est organisé autour du numéro de permis de conduire,
- le système d'information des caisses d'allocations familiales est organisé autour du numéro d'allocataire,
- le système d'information des impôts est organisé autour de l'identifiant fiscal, attaché au foyer fiscal.

La multiplicité des identifiants différents constitue, de façon évidente, un frein à la capacité de mutualiser les moyens d'identification et d'authentification des usagers et un frein à l'organisation de procédures transverses entre plusieurs administrations.
Pour autant, le sujet de « l'identifiant administratif unique » est, en France, un sujet quasiment tabou[12], ce qui n'est pas le cas dans d'autres pays[13]. Si les raisons, développées par la CNIL, qui amènent à vouloir distinguer les identifiants utilisés dans des secteurs administratifs distincts, sont nombreuses, cela conduit néanmoins à rendre complexe et peu performant le développement des services en ligne et de la transversalité entre administrations. Et paradoxalement, le recoupement des informations entre ensembles de données constituées d'un agrégat de traces, d'informations publiquement disponibles et de données stockées dans les systèmes d'information, n'a jamais été aussi simple avec les technologies de « big data » appliquées au « data mining »[14], peu importe l'existence ou non d'identifiants uniques.

Réflexion n°4 : Faut-il faire évoluer, au moins en partie, l'approche de l'Etat sur les identifiants personnels utilisés dans le secteur public, qui amène à rendre complexe et coûteuse la délivrance du service, mais ne présenterait pas une grande résistance à une organisation mal intentionnée qui s'emparerait des données ? Est-il envisageable de définir une cartographie rationalisée et un peu plus homogène de quelques identifiants sectoriels autour desquels organiser l'ensemble du système d'information du secteur public[15] ?

La situation actuelle, avec des identifiants distincts des individus, doit probablement être considérée comme durable (même si elle était amenée à devoir évoluer en fonction de la réflexion précédente), dans la mesure où l'alignement des systèmes existants sur un dispositif plus homogène d'identifiants nécessiterait de longs travaux.

---

[11] Un « identifiant » est une donnée qui, au sein d'un ensemble donné d'individus, n'existe que pour un unique individu. L'identifiant peut n'avoir de sens que dans cet ensemble donné (cas d'un pseudonyme dans un forum en ligne, par exemple).

[12] Le projet « SAFARI » (système automatisé pour les fichiers administratifs et le répertoire des individus), en 1974, avait envisagé l'utilisation du « numéro INSEE » (numéro de sécurité sociale), comme identifiant utilisé dans l'ensemble des fichiers administratifs. Le souvenir récent de la seconde guerre mondiale et craintes liées aux possibilités de recoupement d'information entre différents fichiers, notamment par le ministère de l'intérieur, avait conduit à abandonner le projet et à mettre en évidence l'importance de protéger les libertés individuelles dans le cadre de la centralisation de l'information grâce à l'informatique, ce qui a abouti à la loi du 6 janvier 1978, dite « loi informatique et libertés ».

[13] Cas par exemple de la Belgique, du Danemark, des Pays-Bas, de la Suède. Source : Sénat - *Étude de législation comparée n° 181 - décembre 2007 - Le numéro unique d'identification des personnes physiques*, disponible sur http://www.senat.fr/lc/lc181/lc181_mono.html

[14] Le « data mining », ou « l'exploration de données » désigne un ensemble de technologies et de procédés qui traitent une grande quantité de données pour en extraire des informations supplémentaires, par recoupement, corrélation, analyse statistique, analyse probabiliste…

[15] Cette démarche a déjà été menée avec la CNIL dans le cadre spécifique des services délivrés par les collectivités locales

Si on souhaite tout de même diffuser un moyen commun d'identification et authentification, il faut que le service recevant l'identifiant commun puisse faire le lien avec un identifiant qu'il connaît. Dans certains cas avec des enjeux faibles de confidentialité et de sécurité, on peut envisager qu'une simple déclaration de l'identifiant par l'usager soit acceptée. Dans d'autres cas, il s'agirait de pouvoir, au moment de l'identification et de l'authentification, envoyer également, sous contrôle de l'utilisateur connecté, des données liées à son identité, qui disposeraient d'un certain niveau de garantie. Ces données pourraient être comparées avec celles dont le service dispose, ce qui permettrait de confirmer que l'identifiant est le bon.
Pour assurer l'envoi, avec un certain niveau de garantie, de données liées à l'identité, on peut envisager que ces données soient issues d'une carte d'identité électronique ; les données sont alors certifiées par l'Etat (choix de l'Allemagne[16]).
Une alternative consiste à créer un espace en ligne de type « entrepôt personnel de données », sous le contrôle de l'usager. Les données pourraient alors disposer d'un degré de confiance lié à l'usage qui en a été fait, ou lié à une information de vérification par une administration dans le cadre d'une précédente démarche administrative. L'utilisation, par une administration, d'une donnée issue de cet entrepôt de données, serait soumise à accord de l'utilisateur, à l'instar de ce qui est fait dans les plateformes d'identité liées aux réseaux sociaux. Il s'agirait d'une évolution majeure de ce que permet aujourd'hui le portail mon.service-public.fr (évolution notamment pour étendre et structurer les données, pour organiser l'intégration d'information en retour, pour mettre en œuvre une interface plus claire pour les partenaires, pour inciter plus de partenaires à intégrer le portail, pour impacter réellement le processus de bout en bout dans un objectif de simplification pour l'usager et pour l'administration).
Dans cette alternative, il est également nécessaire de définir les moyens d'identification et authentification acceptables pour créer et utiliser ce compte ; ces moyens pourraient être multiples, et les droits sur le compte modulables en fonction de la confiance qui pourra être accordée au moyen d'authentification[17] (exemple : tableau de bord et démarches simples accessibles avec un simple identifiant/mot de passe ; démarches plus sensibles accessibles après authentification plus forte : téléphone, carte à puce, …). Il apparaît clairement que des niveaux différents d'authentification sont acceptables en fonction du niveau de sécurité souhaité.

Réflexion n°5 : La mise en œuvre d'un « entrepôt personnel de données » associé à un écosystème de moyens d'identification constitue-t-elle une alternative crédible au déploiement d'une carte d'identité numérique ? Un écosystème de moyens d'identifications pourrait-il s'appuyer sur un mécanisme de labellisation de systèmes tiers tel qu'envisagé avec la création d'IdeNUM[18] ?

g. Remplissage de formulaires en ligne

Beaucoup de procédures administratives ne sont que partiellement dématérialisées. La démarche de dématérialisation des formulaires (dématérialisation de la demande), qui ne

[16] Voir (texte en allemand) http://www.personalausweisportal.de/SharedDocs/Downloads/DE/Flyer-und-Broschueren/eID_Broschuere.html?nn=3043354
[17] Les banques permettent d'accéder à nos comptes par un dispositif d'identifiant / mot de passe, mais exigent une sécurité renforcée pour effectuer un virement (par exemple, envoi d'un code par SMS)
[18] IdeNUM est une société créée avec des capitaux publics et privés, ayant vocation à organiser l'interopérabilité d'offres de moyens d'identification déployés par des opérateurs téléphoniques, banques, …

concerne à ce stade déjà pas tous les formulaires[19], n'a généralement pas été corrélée à une révision des processus de relation à l'usager, ni même à une révision du système d'information recevant l'information (quand celui-ci existe). Ceci est vrai à tous les échelons du service public, administrations, établissements publics, collectivités.
Pour mettre réellement à profit un dispositif d'identité numérique, il n'est pas pertinent de se contenter d'une dématérialisation simple d'un formulaire, et continuer à exiger le remplissage de nombreuses données personnelles, voire même la production, à l'appui de la demande, d'une copie (scannée, ou postée) d'un document d'identité. Il faut envisager systématiquement la révision du processus de traitement des demandes pour le dématérialiser et l'automatiser plus complètement, et faire évoluer les éventuelles obligations réglementaires (rendant explicitement obligatoire la production, la vérification, voire l'archivage de pièces justificatives). L'idée est de supprimer les exigences inutiles, de mettre en place les dispositifs appropriés d'échanges de données auprès des sources fiables (principe des projets de type « dites-le nous une fois »), de remplacer l'archivage de pièces justificatives par la conservation des traces numériques des vérifications effectuées.
Réciproquement, la dématérialisation de certaines procédures s'est heurtée à la difficulté de pouvoir disposer d'un niveau de confiance supérieur à un simple niveau déclaratif ; un système d'identité numérique disposant d'un certain degré de fiabilité doit permettre de résoudre ces cas.

Réflexion n°6 : La mise en œuvre d'un système harmonisé de gestion d'identités ne donnera ses pleins effets qu'à la condition d'une dématérialisation sensiblement plus aboutie des procédures, bien au-delà de la seule dématérialisation des demandes et des formulaires. Elle appellera donc à une migration volontariste de l'ensemble de l'existant vers des dispositifs numériques permettant la prise en compte pertinente du dispositif d'identité numérique.

h. Interopérabilité des moyens d'authentification, de la gestion d'identité et de la gestion des rôles.

Le développement de procédures numériques transverses à plusieurs administrations demande un alignement de la gestion des identités dans ces procédures ; il ne s'agit pas seulement d'organiser l'interopérabilité des moyens d'authentification[20], mais véritablement d'organiser le transfert ou le partage de données entre administrations. Ceci exige un alignement des formats, des définitions, de l'organisation des données, voire des règles de gestion sur ces données, dans les systèmes d'information de l'Etat qui doivent s'appuyer sur les données d'identité, ou des données attachées à un individu (adresse par exemple).
Les données relatives aux moyens d'identification et authentification (système de mot de passe, de certificats, de carte, …), à l'identité de la personne telle qu'elle est connue dans le système, aux rôles et aux droits associés à cette personne, doivent nécessairement être distingués dans les systèmes d'information, à défaut de quoi l'interopérabilité ou l'évolutivité peuvent être difficiles.

[19] A titre d'illustration, le site www.service-public.fr/formulaires référence 115 téléservices, et 481 formulaires à télécharger.
[20] Les dispositions contenues dans le référentiel général de sécurité (RGS) ainsi que le dispositif de référencement associé organisent (notamment) la reconnaissance mutuelle des niveaux de sécurité et l'interopérabilité des seuls mécanismes d'authentification s'appuyant sur des certificats électroniques (voir http://references.modernisation.gouv.fr). L'interopérabilité des dispositifs de gestion d'identité, de gestion des rôles, et des droits n'est traitée ni dans le RGS, ni dans le RGI

Des modèles de données bien conçus devront permettre par exemple de faire en sorte qu'un individu puisse être considéré distinctement en tant qu'assuré social, pour accéder à l'information sur l'ensemble de ses remboursements ainsi que de ses ayant-droits, et en tant que patient, pour accéder uniquement à son propre dossier médical. De nombreux standards, plus ou moins convergents, existent, notamment au niveau de l'Union Européenne, et pourront servir de base au travail de conception.

Réflexion n°7 : Un modèle de données suffisamment riche autour de l'individu, la gestion des droits, la gestion des identifiants, partagé entre les différentes parties de l'administration, doit être défini, adopté dans les nouveaux systèmes et devra s'imposer progressivement dans les anciens systèmes.

i. Cas des « cartes professionnelles » (cartes agents)

Dans un cadre professionnel, pour protéger l'accès au système d'information, les entreprises, les organisations professionnelles et les administrations disposent, pour certaines (notamment lorsqu'il y a d'importants enjeux de confidentialité ou de traçabilité), de dispositifs d'identification appuyées sur des cartes à puce.
Les réflexions précédentes s'appliquent à ce cadre professionnel, avec néanmoins quelques différences :

- En interne de l'entité considérée, le système d'identification et le système de gestion de droits peut s'appuyer sur un annuaire exhaustif de l'ensemble des employés ; la question de l'identifiant commun n'est normalement pas un problème. A contrario, le système d'information interne est souvent très varié technologiquement : si le cadre d'emploi des téléprocédures s'appuie essentiellement sur des technologies de l'internet, fortement standardisées, les systèmes d'information internes sont souvent constitués d'un empilement historique de nombreuses technologies, qui disposent de gestions de droits variées et pas vraiment simples à faire converger.
- Les employés ou agents de l'entité considérée peuvent être amenés à devoir utiliser des systèmes tiers, sur lesquels il paraît pertinent de pouvoir utiliser le même moyen d'identification. Dans ce cadre, il est nécessaire :
    - D'une part que le moyen d'authentification soit reconnu en matière de sécurité ; le RGS en interne France, la « Trusted List » pour les entreprises à l'échelle européenne ont été conçus à cet effet ;
    - D'autre part que le système tiers puisse accorder des droits d'accès, après « enrôlement », à chacun des employés ou agents qui doivent en bénéficier. Les mécanismes à mettre en place peuvent à nouveau être de plusieurs natures, en fonction de la répartition des responsabilités :
        - Dans le cas idéal, le droit d'accès se déduit du « rôle » dont dispose l'employé ou l'agent, que son employeur a défini et enregistré dans un système accessible aux tiers ;
        - A défaut, un enrôlement « au cas par cas » est nécessaire.

S'agissant des administrations de l'Etat et ses agences (plus de 2 millions d'agents sont concernés), à ce jour, les systèmes d'identification internes des structures, des annuaires, des gestions de droits, … ne sont pas mutualisés, et faiblement interopérables. Ils sont uniquement alignés, s'agissant de l'authentification par carte à puce et certificats, sur le respect du RGS, et sur les couches technologiques les plus profondes (*de facto* communes, dans la mesure où elles sont fournies par un acteur unique : l'agence nationale des titres sécurisés). Les autorités

de certification sont disjointes (même si elles sont reliées à une même autorité racine), il n'y a pas d'annuaire de référence commun[21], la gestion des rôles n'est pas cadrée à l'échelle interministérielle.

Réflexion 8 : Au moment où les systèmes d'information transversaux et mutualisés de l'Etat se multiplient, et avec le partage d'infrastructures communes, il apparaît indispensable de mettre en place un socle commun de gestion des identités et des accès pour les agents au sein du système d'information de l'Etat, socle contenant a minima un référentiel commun des agents, un système harmonisé d'authentification, des schémas de partage et de reconnaissance de rôles (un cadre de sécurité et un cadre technique communs, des cadres d'usages liés aux besoins de l'entité).

j. Cas des agents des collectivités territoriales

S'agissant des collectivités territoriales et de leurs relations avec l'Etat (plus de 40000 structures concernées et près de 2 millions d'agents), le degré de complexité est supérieur. Chaque système que l'Etat a mis en œuvre et déployé pour les collectivités est arrivé avec son propre schéma d'authentification, de gestion d'identité, de gestion de rôle ; au-delà des relations avec l'Etat, la collectivité, pour ses besoins propres, peut avoir besoin de systèmes d'authentification et de gestion d'identité de ses agents.
Le déploiement de dispositifs référencés RGS permet d'assurer un alignement progressif vers des moyens d'authentification mutualisés, utilisables dans l'ensemble des systèmes. Néanmoins, la chaîne de certification ne garantit que la qualité de l'identification (le cas échéant de la signature électronique) de l'agent, mais n'est pas conçue pour gérer le rôle de la personne identifiée, et par voie de conséquence les droits associés à ce rôle.
Typiquement, dans le cadre des échanges de données d'Etat civil, ce n'est pas la carte délivrée qui porte le statut d'officier d'Etat civil, mais c'est le système d'information qui organise les échanges qui gère les droits d'accès, accordés aux seuls officiers d'Etat civils habilités.

Réflexion n°9 : De la même manière qu'en interne de l'Etat, un socle commun Etat-collectivités apparaît devoir être défini en matière d'identité numérique ; il s'agit :
- de renforcer la standardisation au-delà des préconisations du RGS, et mettre à disposition une offre mutualisée, tout en laissant la liberté aux collectivités de choisir le moyen qu'elles souhaitent ;
- de mettre en place un annuaire commun de référence des agents en relation avec l'Etat et des rôles associés, sur lequel s'appuierait l'ensemble des systèmes d'information de l'Etat. Cet annuaire serait mis à jour sous responsabilité des collectivités, soit par une interface de gestion (notamment pour les petites collectivités), soit par échanges automatisés (notamment pour les collectivités importantes disposant de leur propre annuaire) sous réserve de la définition d'un modèle commun de données. Il permettrait l'enrôlement quel que soit le moyen d'authentification.

[21] « Annuaire » est à prendre au sens de « référentiel des agents » sur lequel les systèmes d'authentification, de gestion des identités, des droits, peuvent s'appuyer.

k. Cas des personnes morales (entreprises, associations,…)

S'agissant des personnes morales (entreprises, associations, …), le sujet apparaît également complexe ; dans le cas, par exemple, du dépôt d'une offre dans le cadre d'un marché public, il s'agit :

- d'identifier l'entreprise en question,
- d'identifier la personne physique qui réalise la démarche,
- de s'assurer que cette personne physique a bien mandat pour prendre des engagements au profit de la personne morale.

Plusieurs pistes d'amélioration et simplification peuvent être envisagées :

- L'identification de l'entreprise est assurée au travers de son immatriculation « SIREN » gérée par l'INSEE[22]. Néanmoins, des évolutions en matière d'interface, de complétude sont considérées comme nécessaires pour les administrations en relation avec les entreprises pour pouvoir s'appuyer de façon plus forte et plus universelle sur la base SIREN. Un chantier autour des référentiels « entreprises », dans le cadre du projet « dites-le nous une fois », est en cours.
- Les dispositions législatives et réglementaires ne reconnaissent pas explicitement l'identification et la signature électronique des personnes morales. Le projet de règlement européen à l'étude sur le sujet[23] prévoit l'existence de ce type de disposition. Dans les cas d'usage compatibles, cela simplifierait sensiblement les mécanismes d'interaction entre les entreprises et l'Etat, puisqu'il n'y aurait plus à vérifier l'identité et les droits de la personne physique connectée (la protection et le bon usage du moyen d'identification de l'entreprise étant alors sous responsabilité de l'entreprise).

Réflexion n°10 : les pistes ouvertes par la reconnaissance de l'identité et de la signature des personnes morales dans le cadre du projet de règlement européen doivent être mises à profit, techniquement et juridiquement au maximum en France, du fait de la simplification qu'elle peut amener, tant du point de vue de l'entreprise que du point de vue de l'administration.

D'une manière générale, il serait judicieux de tirer parti des dispositions du règlement européen e-IDAS concernant les documents et les cachets électroniques pour examiner, au-delà du seul sujet de la signature électronique des personnes morales, les opportunités ouvertes par l'utilisation au sein de l'administration française de ces instruments largement répandus dans certains Etats membres ou dans les services de la Commission européenne. Cela pourrait concerner notamment les greffes électroniques, les échanges de documents électroniques entre les administrations ou entre les administrations et leurs partenaires extérieurs (collectivités territoriales, entreprises).

l. Interface homme-machine, ou dialogue entre systèmes ?

Si de nombreux services en ligne sont élaborés dans la perspective de la connexion d'une personne physique, qu'elle interagisse pour son propre compte ou pour celui d'une personne

[22] Avec, néanmoins, des évolutions à envisager ; un chantier autour des référentiels entreprises, dans le cadre du projet « dites-le nous une fois », est en cours.

[23] Projet de règlement e-IDAS, disponible sur http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0238:FIN:FR:PDF

morale, dans d'autres cas, les services peuvent être envisagés dans la perspective d'une interaction largement automatisée entre deux systèmes, sous forme d'envoi de fichiers (EDI) ou d'utilisation de web services. C'est par exemple le cas des transmissions de données entre les principaux constructeurs automobiles et le système d'immatriculation des véhicules, des transmissions de déclarations sociales issues de la paie des entreprises vers les organismes sociaux dans le cadre de la DSN[24].
Ce cas nécessite généralement la mise en place, entre les deux systèmes, d'un canal de communication disposant d'un certain niveau de sécurité ; par contre, le fournisseur du service n'a plus à se préoccuper de l'identification des personnes, dont la responsabilité revient au gestionnaire du système connecté.

Réflexion 11 : Dans bien des cas, la gestion de l'identité peut être simplifiée lorsqu'on envisage des échanges de systèmes à systèmes. Il devient alors indispensable d'éviter la multiplication des canaux sécurisés de communication, chacun ayant son coût de déploiement et son propre dispositif de sécurisation. Aussi, il est souhaitable que l'Etat mette en place des plateformes d'échange mutualisées, et privilégie chaque fois que possible l'échange de système à système.

L'échange de système à système est d'autant plus facile à mettre en œuvre lorsque l'émetteur s'appuie sur des logiciels libres largement diffusés ou sur des logiciels élaborés par des éditeurs ; il suffit alors de travailler avec les communautés et les éditeurs pour s'assurer que chacun de ces logiciels intègre la capacité d'interaction au format adapté, et ainsi de toucher l'essentiel des partenaires.

m. La signature électronique

Le sujet de la signature électronique est intimement lié au sujet de l'identité numérique, dans la mesure où la signature électronique est un acte qui, à la fois, garantit que le document signé n'a pas été modifié entre l'instant où le signataire l'a signé et où le lecteur le consulte, et identifier de façon non ambiguë son signataire[25].
La loi confère à la signature électronique la même valeur légale qu'une signature manuscrite, sous réserve de conditions de mise en œuvre définies dans des textes réglementaires. Ces conditions sont particulièrement exigeantes en matière de qualité du dispositif de signature, tant d'un point de vue technique (notamment cryptographique) qu'organisationnel, sans compter les exigences liées au stockage et à l'archivage des preuves sur la durée.
La validation (case à cocher), voire le scellement cryptographique d'un document au niveau d'un serveur, par un utilisateur authentifié sur un système auditable, apporte un niveau de confiance qui peut être suffisant dans bien des cas.
Aussi, la mise en œuvre de la signature électronique d'une personne physique paraît devoir être réservée aux cas les plus exigeants en matière de traçabilité et d'imputabilité des actions, après une étude approfondie des besoins de sécurité. Le simple fait de dématérialiser un document, un envoi, qui est, par usage, signé à la main, ne doit pas conduire de façon systématique à mettre en œuvre une signature électronique personnelle, d'autant plus si celle-ci constitue une rupture dans un flux d'information automatisé. Lorsque la signature est

[24] Déclaration sociale nominative, voir www.dsn-info.fr
[25] Cette page sur le site internet de l'ANSSI référence l'essentiel des informations utiles : http://www.ssi.gouv.fr/fr/reglementation-ssi/signature-electronique/

prévue par un texte réglementaire ou législatif, il convient même, au moment de la dématérialisation, d'en réétudier l'opportunité.
Il n'est donc pas envisagé d'associer de façon générale, au dispositif d'identité numérique, un déploiement de solutions de signature électronique à valeur probante forte ; les dispositifs ont, à ce stade, vocation à rester sectoriels, restreints à des usages spécifiques.

III. Scénario de mise en œuvre

n. Récapitulatif des réflexions.

Les réflexions du chapitre précédent nous amènent à proposer la mise en œuvre :

- **D'outils communs autour d'une plateforme d'identité** :
  - Fédération et partage d'identité (réflexion 2), permettant la réutilisation simple des identités au travers différents services,
  - Porte-clés d'authentification (réflexion 3), permettant de limiter les effets de la profusion des dispositifs d'authentification,
  - Entrepôt de données personnelles qualifiées (réflexion 5), donnant la possibilité à l'usager de diffuser auprès des services en ligne des données personnelles stockées par lui, le cas échéant disposant d'un certain niveau de confiance, associés à un écosystème de moyens d'authentification labellisés.
  - Socle agent public de l'Etat (réflexion 8), pour mutualiser les systèmes d'authentification, mettre en commun les annuaires et rendre effectivement interopérables les systèmes d'information
  - Socle collectivités locales (réflexion 9), pour limiter la profusion des solutions d'identification et de gestion d'accès à des systèmes d'informations de l'Etat
  - Socle entreprises (réflexion 10), pour simplifier les relations entre les entreprises et l'Etat, en s'appuyant notamment sur l'opportunité ouverte par le projet de règlement européen.
- De **travaux sur les systèmes d'information existants** :
  - Une dématérialisation plus complète et aboutie s'appuyant sur une simplification des processus rendue possible par le numérique (réflexion 6), et articulée avec les nouveaux outils commun de la plateforme d'identité
  - Une fédération des plateformes d'échange (réflexion 11) pour favoriser l'échange de système à système en substitution de formulaires dématérialisés
- De dispositifs techniques et réglementaires permettant le **développement des usages du système dans la sphère commerciale** (réflexion 1)
- De **travaux conceptuels transversaux de fondation** et indispensables à tous les autres chantiers :
  - Définition d'une cartographie d'identifiants en nombre restreint, utilisables dans les systèmes d'information de l'Etat (réflexion 4)
  - Définition de modèle de données, de schémas d'échanges et d'architectures types (réflexion 7), sur lesquels seront basés les éléments de la plateforme d'identité ; mise en œuvre progressive dans les systèmes d'information clients.

Les travaux de fondation auraient vocation à être menés au second semestre 2013, afin de permettre des premières mises en œuvre d'outils communs en 2014. Les travaux généraux sur les systèmes d'information existants seront de plus long terme ; néanmoins la cible et la trajectoire de convergence des plateformes d'échange devront être définies en 2014.

o. Quelques orientations clé proposées pour la mise en œuvre

Nous proposons que la mise en œuvre de la stratégie sur l'identité numérique respecte plusieurs principes.

i. Biométrie

Il n'apparaît pas nécessaire de lier de près ou de loin la biométrie, sous quelque forme que ce soit, aux usages de ce dispositif d'utilisation d'identité numérique dans la sphère administrative ou commerciale en ligne.
L'utilisation des technologies biométriques dans le cadre de la sécurisation de la procédure de délivrance des titres d'identité et du contrôle (tel le passage frontière) relève d'un autre débat.

ii. Protection des données personnelles et des libertés individuelles

Il apparaît opportun de mettre en œuvre, dans le cadre d'un tel dispositif d'identité, plusieurs principes de protection de la vie privée, inspirée du « privacy by design »[26] :

- Les fonctionnalités de gestion des droits sur les données sont mises sous le contrôle systématique de l'utilisateur, sont claires et transparentes, et sont paramétrées *ab initio* sur un niveau protecteur ;
- Le système, son architecture et ses modèles de données intègrent en leur cœur les fonctions de protection de la vie privée, qui doivent être appliquée sur l'ensemble du cycle de vie des données personnelles, y compris sur leur effacement (droit à l'oubli) ;
- La sécurité informatique est vérifiée en amont (démarche d'homologation), gérée et suivie au quotidien, et vérifiée régulièrement.

Cette approche se veut non contradictoire avec l'enjeu de simplicité pour l'utilisateur et de fluidité pour l'administration ; la transparence sur les données stockées par l'utilisateur, échangées sous son contrôle peut être mise en œuvre de façon ergonomique.
Le caractère optionnel de l'usage de ce type de dispositif paraît important à garantir. Si bien entendu l'intérêt de simplification a vocation à rendre attractif son usage, chacune des procédures administratives devra conserver la possibilité d'être mises en œuvre sans contraindre l'utilisateur à utiliser la plateforme d'identité commune.

iii. Ergonomie proche des usages courants du grand public

Bien qu'ils soient parfois critiqués au sujet en particulier de la protection des données et du manque de transparence sur l'utilisation faite des informations recueillis sur les usagers, les réseaux sociaux ont fait émerger la conscience des utilisateurs sur le besoin de protéger leurs données personnelles, et ont développé des dispositifs de paramétrages assez ergonomiques et compréhensibles.
Il sera important que les dispositifs proposés capitalisent sur l'expérience acquise par l'utilisateur et développent une ergonomie et un vocabulaire proches des systèmes courants.
Le mode « laboratoire », agile, impliquant des utilisateurs, apparaît assez incontournable pour le développement de l'interface homme-machine. Pendant la durée de vie de la plateforme, une veille attentive sur l'évolution des tendances et une analyse des comportements sur la plateforme en vue de l'améliorer sera indispensable. Une évolutivité forte sera à prévoir.

[26] http://www.privacybydesign.ca/index.php/about-pbd/

iv. Facilité d'intégration

Il est impératif que l'intégration des interfaces avec la plateforme d'identité et l'entrepôt de données personnelles dans les systèmes tiers (qu'il s'agisse de systèmes administratifs ou de systèmes tiers) soit raisonnablement simple, et soit la plus agnostique d'un point de vue technologique, en particulier, qu'elle n'impose pas au système tiers l'usage d'un langage de développement particulier ou une architecture très spécifique.
A cet effet, les spécifications d'interface devront être autant que possible appuyées sur des standards (typiquement : openID, SAML, Oauth) et être publiées.

v. Articulation avec les initiatives de l'Union Européenne

La proposition de règlement européen e-IDAS stipule notamment que les EM ont toute latitude pour définir les principes d'identification numérique des citoyens et des entreprises et pour organiser leur mise en œuvre. Néanmoins, cette liberté est assortie de l'obligation de notifier ces éléments à leurs partenaires de l'UE et de mettre à leur disposition les instruments appropriés leur permettant de vérifier de façon univoque l'identité de leurs ressortissants.
Aussi, l'architecture qui sera mise en place devra comprendre les éléments permettant de remplir pleinement cette obligation et permettre ainsi :

- D'accueillir les ressortissants des Etats Membres sur nos dispositifs, et en particulier de bénéficier des services numériques de l'Etat,
- D'assurer la pleine reconnaissance de nos ressortissants et de nos entreprises dans les autres Etats membres de l'Union Européenne.

p. Les technologies sont-elles prêtes et mûres ?

Les concepts proposés dans ce document s'appuient tous sur des technologies existantes et mûres, disposant en outre d'un environnement favorable en France. Les technologies et standards sous-jacents sont assez largement répandus et bénéficient de retours d'expérience dans d'autres pays ou d'autres usages.
En France, la filière de la sécurité numérique, qui sera concernée par la mise en œuvre d'un certain nombre de ces briques, représente un chiffre d'affaires de 10 milliards d'euros. Elle comprend près de 800 entreprises dont la plupart sont des TPE et PME, plus de 55 000 emplois sur le sol national, avec une activité de R&D et de production[27].

* *
*

[27] Source : Alliance pour la Confiance Numérique, *feuille de route nationale pour l'identité numérique,* sur http://confiance-numerique.fr

Secrétariat général pour la modernisation de l'action publique
Direction interministérielle des systèmes d'information et de communication

Mai 2013