N° 3190

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 8 juillet 2020

RAPPORT D'INFORMATION

DÉPOSÉ

en application de l'article 145 du Règlement

PAR LA MISSION D'INFORMATION COMMUNE [1],

*sur l'**identité numérique***

ET PRÉSENTÉ PAR

Mme MARIETTA KARAMANLI,
Présidente,

MME CHRISTINE HENNION ET M. JEAN-MICHEL MIS,
Rapporteurs,

Députés

(1) La composition de cette mission figure au verso de la présente page.

La mission d'information sur l'identité numérique est composée de Mme Marietta Karamanli, présidente, et de Mme Christine Hennion et M. Jean-Michel Mis, rapporteurs.

SOMMAIRE

___

Pages

INTRODUCTION

L'identité numérique, c'est-à-dire **la capacité à utiliser de façon sécurisée les attributs de son identité pour accéder à un ensemble de ressources, est un projet décisif pour la France et les Français.** Dans notre ère résolument numérique, **les citoyens utilisent en effet de plus en plus l'internet pour réaliser les tâches de leur vie quotidienne**, qu'il s'agisse d'inscrire leurs enfants à l'école, d'acheter des biens et des services, ou encore d'accéder à des services publics de plus en plus dématérialisés. Ils ont donc besoin **d'un moyen simple et sécurisé de prouver leur identité en ligne**, tout comme, dans l'espace physique, ils peuvent recourir à leur titre d'identité physique (carte nationale d'identité, passeport) afin de prouver leur identité dans les situations où cela s'avère nécessaire.

Le projet d'identité numérique porté par le programme France Identité Numérique, dirigé par Mme Valérie Peneau, vise à répondre à ce besoin. Après la mise en place de FranceConnect, en 2016, fédérateur d'identité, et l'expérimentation d'Alicem en 2019, **le déploiement de la carte nationale d'identité électronique (CNIe), à partir de 2021, devrait permettre de proposer une solution d'identité numérique régalienne à l'ensemble des Français**. Dérivée de ce titre d'identité, **l'activation de cette identité numérique serait proposée à l'utilisateur au moment du retrait de la CNIe**. Cette identité numérique fonctionnerait en lien avec **le fédérateur d'identité FranceConnect** et constituerait **un moyen d'atteindre un niveau de sécurité élevé pour ses utilisateurs**, conformément aux exigences du droit européen en la matière.

Dans le cadre de ses travaux, la mission d'information a souhaité approfondir les avantages de ce projet pour les citoyens et les gardes-fous à mettre en œuvre le cas échéant. Trois axes de constat se dégagent des travaux menés.

D'abord, la France possède incontestablement une histoire singulière avec l'identité numérique. Chacun se souvient, par exemple, du projet SAFARI et de la polémique qu'il avait déclenchée, qui est en partie à l'origine de la création de la commission nationale de l'informatique et des libertés (CNIL). À sa suite, plusieurs autres initiatives de modernisation numérique ont échoué dans notre pays, pour des raisons diverses tenant principalement à **une défiance des citoyens vis-à-vis de leurs conséquences supposées sur la protection de la vie privée**. La protection des données des utilisateurs, en particulier lorsqu'il est fait usage de la technologie de reconnaissance faciale est donc un sujet essentiel, que la mission s'est attelée à traiter en profondeur, consciente de la sensibilité de nos concitoyens sur ce point. L'avis rendu en 2019 par la CNIL sur l'expérimentation Alicem, qui

estime que l'absence d'alternative à la reconnaissance faciale constitue une violation du principe de consentement de l'utilisateur, en a confirmé toute la pertinence sur un plan juridique.

Des questions importantes se posent également sur le modèle économique de l'identité numérique, et donc sur la place laissée à l'initiative privée dans ce domaine. Le positionnement de l'État comme fournisseur d'identité et la possibilité pour les acteurs privés d'utiliser les solutions qu'il élabore auront en effet un impact important sur le développement de ce marché. Il en va de même de l'éventuelle gratuité de la solution régalienne, qui pourrait décourager l'investissement des fournisseurs d'identité privés sur ce segment d'activité, réduisant en conséquence, *de facto*, la faculté pour l'utilisateur de choisir son fournisseur d'identité. La question de la valorisation économique des données échangées a elle aussi été étudiée dans le cadre de la présente mission.

Enfin, la mission d'information s'est concentrée sur un dernier sujet très concret : les conditions de succès du déploiement rapide de l'identité numérique en France. Les membres de la mission ont, à cette fin, interrogé les différents acteurs sur leurs attentes. Trois éléments importants ressortent des échanges conduits : la capacité de faire connaître l'identité numérique, l'explication pédagogique de son fonctionnnement et des protections offertes à l'utilisateur, et enfin la nécessaire mobilisation des collectivités locales, partenaires de terrain dans la délivrance puis l'utilisation de l'identité numérique. Les acteurs économiques insistent, de leur côté, sur leur besoin de visibilité vis-à-vis du modèle économique choisi et sur la possibilité d'utiliser cette solution à titre expérimental pour mieux l'appréhender. Enfin, la dimension inclusive de la solution technologique ne saurait être ignorée, à l'heure où près de 13 millions de personnes continuent de souffrir d'illectronisme dans notre pays.

Face à ces éléments de constat, les rapporteurs de la mission formulent 43 recommandations visant à permettre le déploiement rapide d'une identité numérique régalienne en France. Celles-ci s'articulent autour d'un fil rouge unique : **le citoyen**. La prise en compte de ses attentes, de ses besoins et de ses craintes conditionnera en effet le succès ou l'échec du développement en France d'une identité numérique massivement utilisée.

I. L'IDENTITÉ NUMÉRIQUE : DE QUOI PARLE-T-ON ?

L'identité numérique est une notion à la fois sociologique et technique qu'il n'est pas simple de définir. De l'utilisateur final au fournisseur de services, son fonctionnement mobilise plusieurs acteurs et soulève de nombreuses interrogations relatives à la fois à la confiance et à la transparence des dispositifs, à leur simplicité d'usage, à leur modèle économique, à la sécurité des utilisateurs et à la souveraineté des États.

A. QU'EST-CE QUE L'IDENTITÉ NUMÉRIQUE ?

1. L'identité : une pluralité de définitions

a. Une définition « subjective » centrée sur l'utilisateur et l'ensemble des traces laissées dans le monde numérique

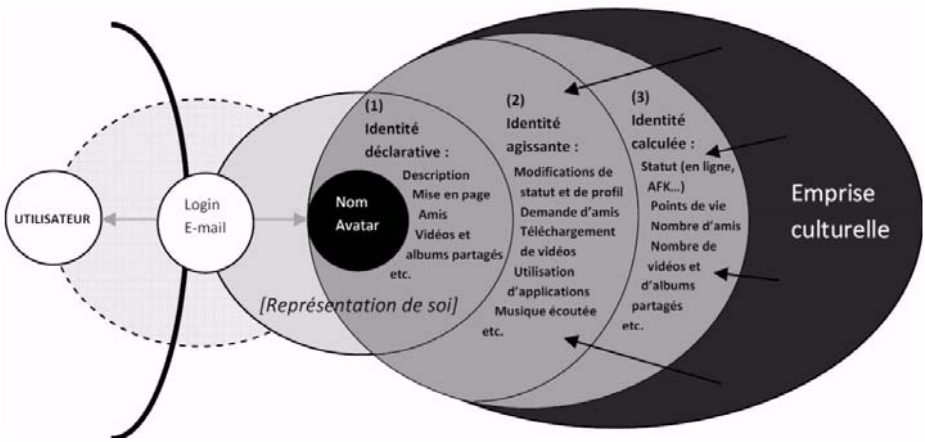
L'identité numérique peut être perçue comme une identité « comportementale », se rapprochant de la notion philosophique de **l'identité-*ipse*** du philosophe Paul Ricœur (1), qui renvoie à l'individu tel qu'il se rapporte à lui-même, dans ses interactions sociales aux autres. Toutefois, cette identité numérique « comportementale » sur internet peut aussi être **construite à l'insu de l'individu**, et donc en pleine « inconscience ».

Pour la chercheuse Fanny Georges (2), l'identité numérique regroupe l'ensemble des données qui se rattachent à une personne lors d'une requête dans le moteur de recherche, c'est-à-dire à la fois ses identifiants, les traces de navigation qu'elle laisse derrière elle et les documents qu'elle partage sur internet. L'identité numérique ne comprend donc pas seulement des informations descriptives mais se réfère aussi aux **activités en ligne**. L'ensemble de ces informations sont saisies par le sujet lui-même (**l'identité déclarative**), sont des informations renseignées par ses proches et le système informatique (**l'identité agissante**) ou peuvent être des informations valorisées par le web 2.0 (**l'identité calculée**).

---

*(1) Il distingue deux aspects, l'identité-*idem *et l'identité-*ipse*, qui permettent tous deux d'approcher la notion d'identité numérique sous un angle différent. L'identité-*idem *d'un individu est celle reposant sur son caractère, c'est-à-dire l'ensemble des marques distinctives qui permettent de ré-identifier un individu humain comme étant le même. Elle réduit l'individu à un ensemble d'attributs objectifs. À l'inverse, l'identité-*ipse *se renouvelle en fonction des contextes sociaux et de l'individu lui-même.*

(2) Audition par la mission d'information du mardi 10 décembre 2019.



Source : Fanny Georges, Réseaux*, 2009*

En somme, pour la chercheuse Danièle Bourcier [(1)], **l'identité numérique est constituée de l'ensemble des traces numériques qui se rapportent à un individu**, qu'il s'agisse des traces profilaires (ce que je dis de moi), des traces navigationnelles (ce que je consulte) et des traces inscriptives ou déclaratives (ce que je pense et partage sur les réseaux).

Cette identité n'est pas finalisée, mais elle est au contraire **en constante construction**. La chercheuse Valérie Schafer [(2)] constate que la sauvegarde de ces traces rend l'identité numérique de plus en plus volumineuse dans le temps, alors qu'elle évolue sous l'effet des nouveaux réseaux sociaux et des nouvelles formes d'interactions et d'engagements.

Cette identité n'est pas davantage monolithique puisqu'elle diffère en fonction des contextes sociaux. Selon M. François Pellegrini, qui préfère parler d'« *apparences numériques* » plutôt que d'identité numérique, « *chacun d'entre nous se montre aux autres sous différentes apparences, qui dépendent de son environnement : on n'agit pas de la même manière dans son cercle familial, ses cercles d'amis et professionnels, associatifs,* etc. *L'identité est ce qui relie de façon unique une personne à ses différentes apparences. Elle est ce qui nous distingue les uns des autres.* » [(3)]

L'emploi du pluriel pour qualifier « les identités numériques » a également été utilisé par plusieurs contributeurs de la consultation en ligne de l'Assemblée nationale sur le sujet de la mission d'information [(4)], qui considèrent que chaque individu en possède plusieurs.

---

(1) Audition par la mission d'information du mercredi 27 novembre 2019 – voir la vidéo de l'audition sur le site de l'Assemblée nationale.

(2) Contribution écrite aux travaux de la mission d'information de M. François Pellegrini.

(3) Audition par la mission d'information du mercredi 11 décembre 2019.

(4) L'Assemblée nationale a ouvert une consultation en ligne sur son site internet du 9 mars au 31 mai 2020 afin d'associer pleinement les internautes aux réflexions de la mission d'information sur l'identité numérique. Près de 200 contributeurs y ont participé.

b. Une définition « objective » : l'ensemble des identifiants pour prouver son identité

L'identité numérique peut également être perçue comme **un ensemble d'attributs stables et finis**.

i. Une identité numérique « objective » publique

L'identité numérique peut se confondre avec **l'identité civile**, définie comme l'« *ensemble des éléments qui, aux termes de la loi, concourent à l'identification d'une personne physique (dans la société, au regard de l'état civil) : nom, prénom, date de naissance, filiation,* etc. » (1).

Pour le chercheur Michaël Bardin (2), l'identité numérique est **un prolongement de l'identité légale** et le droit français n'établit pas de distinction entre les deux notions. Cette identité est composée d'« *éléments fixes* » – à l'instar du nom, prénom, âge et lieu de naissance de la personne –, c'est-à-dire de données qui ne peuvent *a priori* pas faire l'objet de modification et qui ne relèvent pas du comportement, mais aussi d' « *éléments fluctuants* » tels que l'activité professionnelle.

Le développement de l'administration en ligne a conduit les services de l'État à recourir à cette définition pratique de l'identité numérique pour permettre aux internautes de prouver leur « identité pivot », c'est-à-dire leur identité au sens de l'état civil. Cette « identité pivot » est constituée d'un nombre restreint de données tels que les nom, prénom, date, lieu de naissance et sexe de l'individu. **L'identité numérique comme déclinaison de l'identité physique est une approche récente, retenue dans le cadre du projet d'identité numérique régalien.**

Comme l'a indiqué **Mme Valérie Peneau, directrice du programme interministériel sur l'identité numérique**, dans sa contribution écrite aux travaux de la mission d'information, l'identité numérique « *constitue le prolongement dans le monde numérique de l'un des plus anciens services publics fournis par la puissance publique dans le monde physique à ses citoyens : assurer leur droit à l'identité par l'inscription et la tenue de l'état civil et le certifier par la délivrance de titres d'identité* ». Les données d' « identité pivot » collectées dans ce cadre « *sont au demeurant les seules données à la disposition de l'État qui, à la différence des grands acteurs privés du Net, ne trace ni ne recoupe les comportements, habitudes ou préférences numériques des usagers* ».

---

(1) Gérard Cornu. « identité » in Vocabulaire juridique*, 10e édition, Ed Quadridge/Presses universitaires de France., janvier 2014.*

(2) Audition par la mission d'information du mardi 3 décembre 2019 – voir la vidéo de l'audition sur le site de l'Assemblée nationale.

ii. Une identité numérique « objective » privée

L'identité numérique « objective » se compose également de **l'ensemble des identifiants détenus par les utilisateurs**. Il peut par exemple s'agir des identifiants d'accès à ses comptes Google et Facebook ou aux services en ligne d'une banque ou d'un office notarial. Dans sa contribution écrite aux travaux de la mission d'information, la direction générale des réseaux de communication, du contenu et des technologies (DG CONNECT) observe d'ailleurs que « *l'identité numérique demeure parcellaire et dispersée entre de nombreux comptes et identifiants* ».

Ces différents identifiants ne se ressemblent pas. Le chercheur François Perea (1) distingue les identifiants transparents – par exemple, le couple « prenom.nom » – des identifiants complexes – comme une adresse email « pseudonymisée ». Selon les représentants de l'entreprise CISCO auditionnés par la mission d'information (2), l**es identifiants sont d'ailleurs souvent liés à la technologie d'accès**, qu'il s'agisse du *login* pour les mails, de la carte SIM pour les téléphones ou de la prise « box » pour recevoir internet à domicile.

Pour la chercheure Primavera De Filippi (3), l'identifiant doit remplir deux conditions :

- il doit être **unique** : deux personnes ne doivent pas avoir le même ;
- il doit être **singulier** : il ne doit exister qu'un seul identifiant par personne au sein d'un même domaine, par exemple un seul numéro de passeport dans un pays donné.

Le recours à **une autorité centralisée** est souvent nécessaire pour vérifier ces deux caractéristiques. Cette autorité peut être l'État ou une entreprise privée comme un réseau social ou une banque.

iii. Les attributs

L'identité numérique « objective » est **constituée de nombreux attributs** sur lesquels reposent les identifiants. Ces attributs servent à décrire une facette de cette identité, sans être propre à un individu – genre, hauteur, âge – et peuvent changer au cours du temps – profession, nationalité. L'Alliance pour la confiance numérique, qui propose également de les distinguer selon qu'ils sont **biométriques** – photo, empreinte digitale, oculaire, *etc.* – ou **alphanumériques** – nom, adresse,

---

(1) Table ronde de professeurs réunissant Mme Primavera de Filippi et MM. Jean-Gabriel Ganascia et François Perea, organisée par la mission d'information le mardi 21 janvier 2020 – voir la vidéo de la table ronde sur le site de l'Assemblée nationale.

(2) Audition de MM. Guillaume Sauvage de Saint Marc et Bruno Bernard par la mission d'information le jeudi 13 février 2020.

(3) Table ronde de professeurs réunissant Mme Primavera de Filippi et MM. Jean-Gabriel Ganascia et François Perea, organisée par la mission d'information le mardi 21 janvier 2020 – voir la vidéo de la table ronde sur le site de l'Assemblée nationale.

etc. – les distingue du support qui les exploite, qui peut par exemple être une carte d'identité, un *token* physique ou un support logiciel. Pour l'Alliance, c'est « *la combinaison des attributs requis et du support utilisé* [qui] *définit une solution unique d'identification* » (1).

Ainsi qu'en conclut la Fondation internet nouvelle génération dans sa contribution écrite aux travaux de la mission, « *l'identité est donc mouvante, plurielle, en construction permanente, et marie des objets subjectifs et objectifs* » nombreux.

2. La construction de l'identification

La façon dont les individus s'identifient et sont identifiés par les autres a beaucoup varié dans l'histoire de l'humanité. Prenant pour cadre l'Europe depuis l'an mil, les historiens Ilsen About et Vincent Denis identifient **cinq grandes périodes** :

– du XI^{ème} au milieu du XV^{ème} siècle, l'identification est « *caractérisée par la place importante du* ***face-à-face****, la mise en place de multiples signes d'identité* (2)*, les débuts de l'identification à distance sous la tutelle des formes d'autorité publique qui s'imposent alors* » ;

– à partir du XV^{ème} siècle et pendant l'époque moderne, « *le rôle de* ***l'identification écrite*** *se renforce considérablement alors que se multiplient registres et documents d'identité, qui coexistent avec des manières d'identifier liées au face-à-face et à l'interconnaissance* » ;

– à la fin du XVIII^{ème} et le début du XIX^{ème} siècles sont marqués par « *l'avènement d'une nouvelle structure politique en Europe, l'État-nation, qui a pour conséquences* ***l'étatisation et la nationalisation de l'identification****,* [tandis que] *les grandes mutations de l'âge industriel (migrations, urbanisation, démocratisation, révolutions des transports) obligent à un investissement administratif et technologique en la matière* » ;

– à l'issue de la première guerre mondiale, « ***l'attribution à tous les individus d'une identité certaine*** » devient un enjeu pour les États européens, tandis qu'une « *définition exclusive des identités et des mesures coercitives d'identification caractérise en outre les régimes totalitaires* » ;

– enfin, les auteurs considèrent la période contemporaine comme marquée par « *l'avènement d'une* ***"identification de masse"*** » et par « *la question d'un nouveau "seuil" représenté par l'informatisation des données et la diffusion des techniques de surveillance à la fin du XX^{ème} siècle* » (3).

---

(1) Contribution écrite de l'Alliance pour la confiance numérique aux travaux de la mission d'information.

(2) Comme des armoiries et des signes vestimentaires.

(3) About Ilsen, Denis Vincent, Histoire de l'identification des personnes*. Paris, La Découverte, 2010, p. 7.*

L'histoire de l'identification est donc celle du passage **d'une identité interpersonnelle à une identité délivrée par l'État**, consignée dans les registres de l'état civil, et dont les modalités de vérification ont évolué dans le temps.

3. La délivrance de l'identité va de pair avec le risque d'usurpation

Au Moyen Âge, **l'identification était donc un processus faillible** reposant essentiellement sur le face-à-face, la mémoire du groupe et le port de signes et d'insignes. L'usurpation d'identité, c'est-à-dire **le fait d'utiliser, sans l'accord d'une personne, des informations permettant de l'identifier**, était donc particulièrement facile, ainsi qu'en témoigne l'affaire Martin Guerre à Toulouse, en 1560, du nom d'un paysan du comté de Foix qui avait quitté sa famille pendant une décennie, avant qu'un individu se faisant passer pour lui ne la rejoigne ensuite, jusqu'à ce qu'un ancien compagnon d'arme de Martin Guerre ne dénonce l'imposteur (1).

Les progrès de la période contemporaine auraient dû mettre un terme au phénomène d'usurpation d'identité. Comme le relève Mme Marine Monteuil, « *l'anthropométrie, la biométrie et par la suite la biologie, avec l'ADN, permettent d'identifier les individus avec une quasi-certitude,* [tandis que] *les puces, insérées aux documents d'identité, contiennent des empreintes digitales de plusieurs doigts, infalsifiables et numérisées* » (2). Toutefois, **le développement de l'espace internet a renouvelé le phénomène de l'usurpation d'identité**, renforcé par le recours à ce qu'elle appelle une « *identité d'emprunt* ».

Alors qu'en 2018, la France a enregistré plus de 1,5 milliard de transactions en ligne (3) et que 65 % des Français utilisaient internet pour réaliser des démarches en ligne (4), **40 % de la population considérait la protection des données personnelles comme le principal frein à l'utilisation d'internet** (5).

À défaut de l'existence de statistiques consolidées en la matière (6), un sondage du CSA réalisé en 2012 indiquait que **8 % des Français ont été victimes, dans la décennie qui précédait, d'une usurpation d'identité en ligne** (7). Bien que la détention et l'usage de faux documents délivrés par une administration soit un délit (8), la fraude identitaire et la revente de documents d'identité sur le

---

(1) Voir l'ouvrage de Nathalie Zemon-Davis, Le retour de Martin Guerre, publié en 2008 aux éditions Tallandier.

(2) Marine Monteuil, L'usurpation d'identité à l'épreuve du numérique*, Recueil Dalloz 2020 p.101.*

(3) Fédération e-*commerce et vente à distance (Fevad),* Les chiffres clés 2019.

(4) Baromètre du numérique, édition 2018.

(5) Ibid.

(6) Guy de Felcourt, Usurpation d'identité. Fraudes, menaces et parades où l'art de la fraude sur les données personnelles*, CNRS, 2011. L'auteur y déplore notamment l'archaïsme des systèmes de traitement statistique du recueil des plaintes.*

(7) CSA, Les Français et la criminalité identitaire*, sondage, Fellowes, oct. 2012, p. 4.*

(8) Articles 441-2 et 441-3 du code pénal.

darkweb (1) se développent. Ces faits concernent tant les **vrais documents d'identité volés** – par exemple, en réutilisant des photocopies de documents d'identité ou en dérobant des documents d'identité – que les **faux papiers fabriqués**, qui représentent une activité lucrative. **Environ 25 000 faux documents sont saisis chaque année en France** (2).

B. LE FONCTIONNEMENT DE L'IDENTITÉ NUMÉRIQUE

L'identité numérique peut donc recouvrir des définitions différentes, ce qui peut induire des incompréhensions et des appréhensions légitimes, d'autant plus que **son fonctionnement concret n'est pas, à première vue, évident**. Dans une perspective pédagogique, la mission d'information a souhaité revenir de façon simplifiée sur celui-ci, afin de **dissiper tout malentendu et de donner à voir l'ensemble des opportunités que l'identité numérique peut offrir à ses utilisateurs**, au premier rang desquelles **une gestion frugale des données**, particulièrement respectueuse de la vie privée de ces derniers.

1. Le trinôme « utilisateur – fournisseur de services – tiers de confiance »

L'identité numérique, comprend une phase d'identification puis d'authentification faisant intervenir trois figures clefs : **l'utilisateur, le fournisseur de services et enfin le tiers de confiance**, ce dernier étant amené à jouer plusieurs rôles. Il convient de toujours bien distinguer **l'identification**, qui consiste à établir l'identité de l'utilisateur (*via* un *identifiant* unique) de **l'authentification**, qui permet à l'utilisateur d'apporter la preuve de son identité, selon différentes modalités en fonction du niveau de sécurité exigé. **Une solution d'identité numérique permet donc à un utilisateur identifié de prouver son identité numérique, avec la solution d'authentification de son choix, qu'elle soit publique ou privée**.

a. L'utilisateur

L'utilisateur est la personne physique souhaitant accéder à un ensemble de services aussi bien publics (effectuer une déclaration de revenus en ligne, par exemple), que privés (achats de biens et services). Il recherche en général **la facilité d'accès au service** et **la protection de ses données personnelles**, afin de se prémunir de toute tentative d'usurpation d'identité.

b. Le fournisseur de services

Le fournisseur de services est l'opérateur public ou privé qui met à la disposition de l'utilisateur un ensemble de services en ligne. L'accès à ces derniers est en général conditionné à une **authentification** de l'utilisateur. Cette

---

(1) Le darkweb *est un ensemble de sites internet non indexés aux moteurs de recherche, et dont l'accès nécessite le recours à des logiciels spécifiques.*

(2) « Faux papiers : un marché juteux en plein essor », La Dépêche du Midi*, 17 février 2019.*

phase passe, le plus souvent, par la création d'un compte utilisateur unique, propre à ce service et à ce fournisseur, ce qui a pour conséquence de multiplier les identités numériques des utilisateurs (1).

Cette authentification voit son niveau de sécurité varier en fonction de la nature du service proposé. **Elle reste néanmoins, à l'heure actuelle, une authentification faiblement sécurisée pour la plupart des sites internet des fournisseurs de services**. Le fournisseur de services dispose assez rarement des moyens de vérifier la véracité des attributs présentés par l'utilisateur dans sa phase de création d'accès et de connexion à distance au service proposé (2).

c. Le fournisseur d'identité - tiers de confiance

Le fournisseur d'identité, qui est un tiers de confiance, va permettre de faire le lien entre le fournisseur de services et l'utilisateur. Sa fonction est de s'assurer de la correspondance entre les attributs présentés par l'utilisateur et leur véracité.

Il existe en France des acteurs économiques spécialisés dans le domaine de la vérification de l'identité électronique. Ces derniers appartiennent au secteur économique dit « de la confiance numérique », et sont représentés au sein de l'Alliance pour la confiance numérique.

Le tiers de confiance peut assurer les trois fonctions différentes, distinctes ou cumulées suivantes :

– autorité de délivrance (ou fournisseur d'identité *originelle*) : le tiers de confiance fait alors le lien initial entre la personne physique ou morale et son identité numérique. Il attribue l'identité numérique originelle. À titre d'exemple, l'autorité de délivrance de la carte nationale d'identité électronique (CNIe) est l'État, et plus spécifiquement l'Agence nationale des titres sécurisés (ANTS), placée sous la tutelle du ministère de l'intérieur. La délivrance en mairie, qui intervient après la validation du dossier au niveau de la préfecture (centre d'expertise et de ressources titres) permet ainsi de faire le lien initial entre l'identité physique de la personne et son identité numérique ;

– fournisseur d'identité *authentifiée* : le tiers de confiance assure alors la gestion au quotidien de cette identité et procède à sa confirmation auprès du fournisseur de services. Le fournisseur d'identité confirme donc auprès du fournisseur de services, les attributs « de base » que prétend détenir l'utilisateur du service. L'identité donnée au fournisseur de services dérive nécessairement d'une identité originelle ;

---

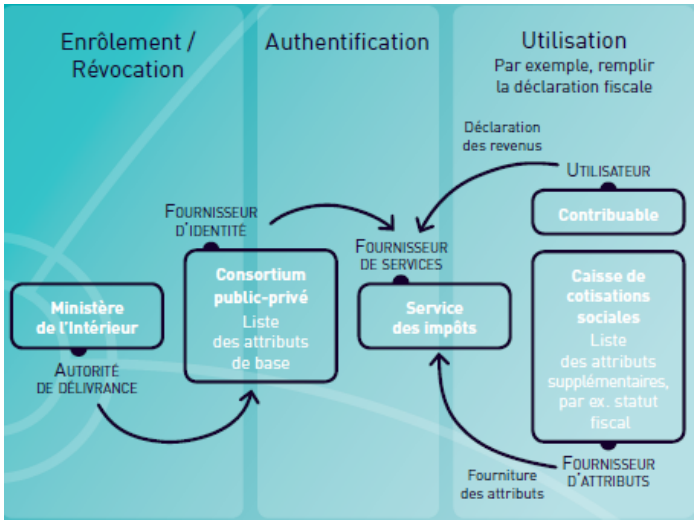
(1) Les internautes gèrent en moyenne une centaine de comptes en ligne. Ils réutilisent donc de facto les mêmes mots de passe, ce qui constitue une source de fragilité pour la sécurité de leurs données.

(2) Ce n'est en effet pas sa spécialité, et la prise en charge du coût de cette éventuelle vérification constituerait un non-sens économique pour cet acteur.

– fournisseur(s) d'attributs : le tiers de confiance fournit alors des attributs supplémentaires concernant l'utilisateur, afin de garantir un niveau d'authentification plus fortement sécurisé. Ce peut être, par exemple, l'exercice d'une profession, ou la valeur d'un revenu fiscal.

Le schéma suivant, proposé par Armen Kahtchatourof et Claire Levallois-Barth décrit **le processus de mise en oeuvre de la carte nationale d'identité électronique, en reprenant ces différents concepts.**

LES ÉTAPES DE L'USAGE DE LA CARTE NATIONALE D'IDENTITÉ ÉLECTRONIQUE : DE L'ENRÔLEMENT À L'UTILISATION



Source : Chaire Valeurs et Politiques des Information Personnelles, Cahier n° 1, Identités numériques, *coordonné par Claire Levallois-Barth, mars 2016.*

2. Les trois phases de la vie d'une identité numérique : enrôlement – authentification – utilisation

a. L'enrôlement

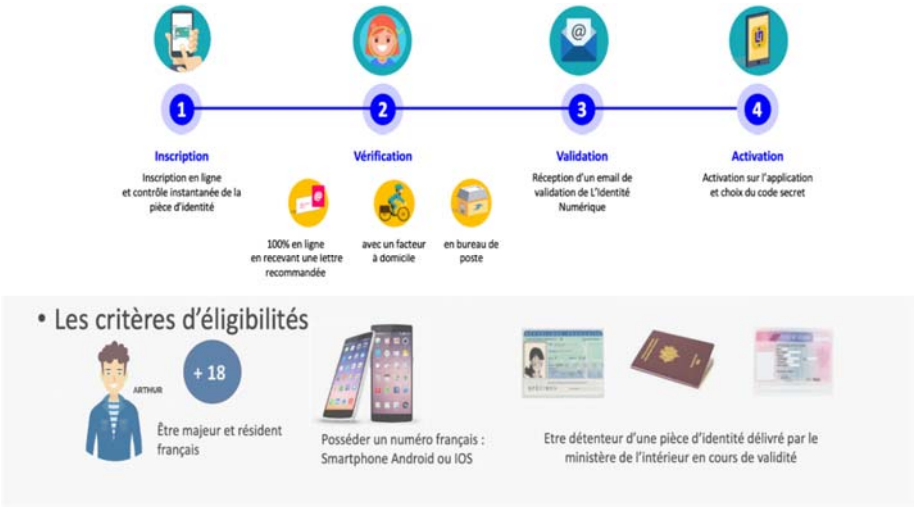
L'utilisation d'une solution d'identité numérique passe par une première phase dite d'enrôlement (de l'anglicisme *enrolment*) qui correspond *de facto* à l'inscription. C'est le moment où **l'autorité de délivrance**, qui peut également être le fournisseur d'identité, **établit de façon certaine le lien entre l'utilisateur et son identité numérique (c'est-à-dire la somme de ses attributs)**.

Le niveau de sécurité requis fait logiquement varier les conditions encadrant cette phase d'inscription (*voir infra*). L'enrôlement peut ainsi simplement comprendre la fourniture d'un identifiant, d'un mot de passe, d'un numéro de téléphone et d'une adresse mail (Facebook), ou comporter des éléments

plus complets pour assurer un niveau de sécurité plus élevé, tels que l'usage d'un titre d'identité, certifié par exemple (Alicem [1]).

La phase d'enrôlement est donc une étape essentielle pour garantir la sécurité de l'identité numérique délivrée [2], mais aussi son déploiement à grande échelle. Le processus d'enregistrement doit en effet être **suffisamment fluide et robuste** pour que l'utilisateur souhaite aller jusqu'à son terme. Cela implique notamment un nombre limité d'étapes. Au-delà de 4 à 5 étapes, les courbes d'abandon deviennent importantes et une partie conséquente des utilisateurs potentiels abandonnent le processus .

LA PROCÉDURE D'ENRÔLEMENT AU SEIN DE L'IDENTITÉ NUMÉRIQUE DE LA POSTE



Source : La Poste

b. L'authentification

Une fois enregistrée, la personne est en capacité de s'authentifier et donc d'accéder aux services *via* **l'usage de son identité numérique**. L'authentification désigne le fait de produire la preuve de l'identité présentée *a priori*, en vue d'accéder à un service. Elle est donc un processus qui permet de confirmer l'identité d'une personne, qui ne doit pas être confondu avec

---

(1) Alicem est une solution d'identité numérique de niveau substantiel à élevé au sens du règlement eIDAS, développée par le ministère de l'intérieur et l'Agence nationale des titres sécurisés (ANTS). Cette application expérimentale dérive en effet l'identité numérique de l'utilisateur du titre de séjour ou passeport de ce dernier, la vérification de leur authenticité s'effectuant grâce à la lecture sans contact NFC par le smartphone *de la puce contenue dans le titre d'identité. Un processus de comparaison faciale permet enfin de s'assurer que la personne réalisant la démarche d'enrôlement est bien celle qui correspond au passeport utilisé.*

(2) Il convient d'observer, par ailleurs, qu'il existe plusieurs niveaux de sécurité à prendre en compte dans ce cadre. On peut citer le niveau de sécurité de l'identification elle-même (en fonction des attributs), de l'opération d'enrôlement et enfin celui de l'authentification employée en fonction de l'usage.

l'identification, qui permet de déterminer l'identité de quelqu'un à partir d'un ensemble d'attributs.

Cette phase d'authentification, moins lourde que celle d'enrôlement, varie elle aussi en fonction de la nature du service demandé et donc de l'utilisation de l'identité numérique. Dans le cadre envisagé de la dérivation d'une identité numérique à partir de la carte nationale d'identité électronique (CNIe), **l'utilisation de ce titre d'identité serait par exemple nécessaire uniquement pour des usages d'un niveau de sécurité élevé**. Pour les usages d'un niveau faible ou subtantiel, le smartphone seul suffirait.

c. L'utilisation

L'utilisation de l'identité numérique consiste à s'appuyer sur son identité numérique pour accéder à un ensemble de services, une fois l'authentification réussie. L'avantage d'une identité régalienne réside dans la robustesse des données utilisées pour créer l'identité numérique (l'État faisant office en l'espèce d'autorité de délivrance et de fournisseur d'identité) et dans la confiance que peuvent lui accorder les citoyens au regard de son rôle de garant de l'intérêt général.

L'utilisation d'une identité numérique régalienne passerait par l'utilisation du fédérateur d'identité FranceConnect (*infra*). On désigne, par le terme de **fédérateur d'identité,** un environnement organisé utilisant des systèmes d'identités numériques, sous forme de plateforme, permettant de gérer un ou plusieurs schémas d'identités.

Très concrètement, utiliser son identité numérique régalienne nécessitera, dans le cadre d'une dérivation de la CNIe, de recourir soit au smartphone et à ce titre d'identité (authentification de niveau élevé), soit au seul terminal de l'utilisateur, pour des usages ne requérant qu'un niveau de sécurité simple ou subtantiel (*voir infra*).

Il peut être mis fin à cette utilisation par simple déconnexion du service concerné. **En cas de perte ou de vol du *smartphone*, l'utilisateur** doit se créer une nouvelle identité numérique afin de faire expirer son identité numérique précédente.

3. L'interopérabilité de l'identité numérique : une exigence importante dans le cadre de l'Union européenne (UE)

a. L'interopérabilité dans le cadre de l'UE

L'interopérabilité désigne la possibilité, pour l'utilisateur de l'identité numérique, d'utiliser sa solution d'identité numérique quel que soit son support d'usage (1). Concrètement, cela signifie que l'accès à des services en ligne

(1) Le règlement général sur la protection des données (Règlement UE 2016/679), notamment par son article 20, avait déjà renforcé l'interopérabilité des données, même si, en pratique, il n'est pas suffisamment appliqué.

via une authentification fournie par l'identité numérique ne doit être limité pour l'utilisateur **ni en raison du modèle de téléphone qu'il possède, ni en raison du pays dans lequel il se trouve**.

Le règlement eIDAS du 23 juillet 2014 (1), fixe ce **cadre d'interopérabilité**. Il prévoit ainsi que les États membres reconnaissent, pour s'identifier sur leurs propres services en ligne, **les moyens d'authentification qui leur ont été notifiés ainsi que ceux qui auront été notifiés aux autres États membres**. Ce règlement contient en conséquence **un ensemble de spécifications techniques**. Il prévoit également **un ensemble de règles visant à faciliter le recours à la signature électronique au sein des États membres**.

b. L'interopérabilité en fonction du système d'exploitation des smartphones

L'interopérabilité renvoie également, d'une façon plus prosaïque, à la compatibilité de la solution d'identité numérique avec les caractéristiques techniques des smartphones des utilisateurs.

Cette question s'est d'ailleurs posée, de façon récente, dans le cadre du débat autour de l'application Stop Covid, l'efficacité de la technologie *Bluetooth* pouvant varier en fonction notamment du système d'exploitation utilisé (IOS ou Android) et de la version de la technologie *Bluetooth* employée.

En matière d'identité numérique, certains fournisseurs d'identité vont recourir, par exemple, à la technologie NFC. Il apparaît *de facto* que la majorité du parc de smartphones (90 %) est déjà équipée de cette technologie. L'impératif d'interopérabilité a par ailleurs été intégré par ces différents acteurs économiques dans le cadre du développement de leurs solutions d'identité numérique.

4. L'authentification biométrique : une garantie de sécurité au service de l'utilisateur

a. L'authentification n'est pas une identification

L'authentification s'effectue selon la combinaison de plusieurs facteurs qui déterminent le niveau de sécurité concerné. Ces différents facteurs sont les suivants : « **qui je suis** » (identifiant) ; **« ce que je sais** » (mot de passe), **« ce que je possède »** (élément physique, un téléphone par exemple), « **ce que je suis** » (élément biométrique).

L'identité numérique, dans son processus d'enrôlement, peut nécessiter de recourir à **l'authentification biométrique**, c'est-à-dire au fait de comparer l'image de la personne avec l'image du titre d'identité utilisé, pour s'assurer de la

(1) Règlement européen du 23 juillet 2014 relatif à l'identification électronique et aux services de confiance pour les transactions électroniques au sein du marché intérieur.

correspondance. Pour rappel, l'authentification biométrique est d'ores et déjà utilisée lors de la réalisation de titres d'identité, par exemple lorsqu'il s'agit de récupérer les empreintes digitales d'un citoyen dans le cadre de la production de son passeport.

Comme le rappelle la note publiée par l'Office parlementaire d'évaluation des choix scientifiques et technologiques en juillet 2019 (1), **il est important de distinguer cette authentification biométrique,** forme de comparaison faciale**, de l'identification biométrique**. **La procédure d'enrôlement de l'identité numérique n'a en effet pas vocation à procéder à l'identification de la personne**, c'est-à-dire à comparer son image à une banque d'images dans le but de la singulariser. Si ces deux techniques procèdent bien d'une forme de reconnaissance faciale, **leur objectif est différent, et les risques de la première, bien plus faibles, selon la CNIL** (2).

b. Un outil au service de la simplicité d'usage et de la sécurité de l'utilisateur

Le recours à l'authentification biométrique, qui constitue un moyen parmi d'autres d'atteindre un niveau de sécurité élevé, s'explique par **la commodité de cette technique pour l'utilisateur**, d'une part, et **le haut niveau de sécurité qu'elle lui assure**, d'autre part.

Il convient d'observer, d'abord, que **l'authentification biométrique est d'ores et déjà proposée par la plupart des constructeurs d'équipements mobiles pour protéger son terminal** (verrouillage/déverouillage par reconnaissance faciale ou empreinte digitale, par exemple). Il ne s'agit donc pas, *stricto sensu*, d'une pratique nouvelle.

En outre, cette pratique, qui offre une réelle sécurité pour l'identité numérique de l'utilisateur, n'intervient que ponctuellement, lors de la phase d'enrôlement. Les données recueillies à cet égard **ne font pas l'objet d'une conservation**. Il s'agit en effet uniquement de disposer d'une preuve de vivant (3), et de vérifier la correspondance entre la personne en train de créer son identité numérique et le titre d'identité utilisé à cette fin.

L'authentification biométrique offre incontestablement une rapidité d'exécution particulièrement appréciable pour l'utilisateur. Elle lui permet en effet de créer son identité numérique sans se déplacer, en quelques minutes seulement. Elle renforce donc le caractère inclusif de l'identité numérique.

---

(1) OPECST, La reconnaissance faciale*, note n°14, juillet 2019.*

(2) Audition de la CNIL par la mission d'information le mercredi 4 mars 2020 - voir la vidéo de l'audition sur le site de l'Assemblée nationale.

(3) C'est-à-dire que l'utilisateur n'est pas un robot. Cette preuve de vivant passe par la réalisation de plusieurs mouvements.

Enfin, il convient de rappeler que le recours à cette technique ne s'imposera pas, *de facto*, aux utilisateurs. En effet, la création d'une identité numérique régalienne viendra compléter les offres privées déjà disponibles, et qui proposent des alternatives, pour un niveau de sécurité substantiel par exemple [(1)]. **En outre, le projet d'identité numérique régalienne proposera une alternative à *l'authentification biométrique*, afin de tirer les leçons des recommandations de la CNIL sur Alicem [(2)], en capitalisant sur le moment de la délivrance du titre [(3)]**.

L'authentification biométrique n'a vocation, au fond, qu'à proposer à l'utilisateur un parcours d'enrôlement plus simple, qui ne nécessite pas de se déplacer pour réaliser le face à face de contrôle en phase d'enrôlement, prévu dans le cadre du référentiel eIDAS pour permettre la création d'une identité numérique, en écartant tout risque d'usurpation d'identité.

Elle fera par ailleurs l'objet d'un travail attentif de veille juridique et technologique. En effet, comme l'indique Mme Valérie Peneau dans sa contribution écrite [(4)], il convient d'être attentif, « *outre le sujet de protection des données personnelles* […] *au fait que cette technologie de reconnaissance repose sur une probabilité, et non une certitude absolue [(5)], de correspondance, qu'elle est très évolutive, et que nous ne pouvons dépendre en l'état des seuls algorithmes développés par des acteurs étrangers, paramétrés au regard de bases de populations de référence plus ou moins éloignées de la population française. Cette technologie emporte des enjeux de souveraineté et de risques cyber auxquels il faut prêter une attention particulière et qui suppose une capacité d'évolution constante dans le temps pour pouvoir offrir un service de qualité et sécurisé* ».

C. LES ACTEURS DE L'IDENTITÉ NUMÉRIQUE

L'identité numérique est une solution technique qui mobilise plusieurs acteurs publics et privés chargés d'en assurer le fonctionnement et la régulation.

---

(1) L'identité numérique proposée par La Poste, qui est de niveau substantiel c'est-à-dire qu'elle correspond à l'immense majorité des usages quotidiens, en donne un exemple. Lors du processus d'enrôlement, il est ainsi possible soit de recourir à la solution vidéo en ligne, plus rapide, soit de procéder à la vérification de l'identité lors du passage du facteur.

(2) Dans son avis rendu sur l'application Alicem, la CNIL avait en effet noté qu'en plus du fait que le consentement de l'utilisateur doit être réel, c'est-à-dire qu'il doit y avoir une alternative pour accéder au service concerné, ni la nécessité de recourir à un dispositif biométrique pour vérifier l'identité d'une personne dans le but d'atteindre le niveau de garantie « élevé » de l'identité numérique, au sens du règlement e-IDAS, ni le développement d'une solution alternative au traitement de données biométriques, n'ont été caractérisés par le ministère de l'intérieur.

(3) Contribution écrite de Mme Valérie Peneau aux travaux de la mission d'information.

(4) Ibidem.

(5) Ce qui est au demeurant également le cas dans l'hypothèse d'une vérification physique dans le cas d'un face à face.

1. Les acteurs publics

a. L'État

L'État est **un acteur central en matière d'identité numérique**, à plusieurs titres.

Il dispose d'abord d'une **légitimité historique** liée à son rôle clef dans **la tenue des registres d'état civil**, qui constitue l'une de ses fonctions essentielles. Comme une identité numérique de niveau élevé nécessite de recourir à la dérivation de titres d'identité physiques, dont il est le seul à assurer la délivrance, l'État constitue un fournisseur d'identité et une autorité de délivrance naturels pour déployer des projets de ce type.

L'État dispose ensuite **d'une relation de confiance avec les citoyens, en tant que puissance publique en charge de l'intérêt général**. En matière numérique, les citoyens font ainsi davantage confiance à l'État pour gérer leurs données qu'aux acteurs privés (1).

En matière d'identité numérique, l'État s'appuie sur les acteurs suivants :

– la direction interministérielle du numérique (DINUM), qui accompagne, sous la responsabilité du Premier ministre, les ministères dans leur transformation numérique, conseille le Gouvernement et développe des services et ressources partagées (réseau interministériel de l'État, **FranceConnect**, data.gouv.fr, *etc*) ;

– le ministère de l'intérieur, autorité de tutelle de l'**Agence nationale des titres sécurisés** (ANTS) ;

– **l'Agence nationale de la sécurité des systèmes d'information** (ANSSI), placée sous la tutelle du secrétariat général de la défense et de la sécurité nationale (SGDSN).

C'est **le programme interministériel France identité numérique,** dirigé par Mme Valérie Peneau, et placé sous l'autorité des ministères de l'intérieur et de la justice, et du secrétariat d'État chargé du numérique, qui a pour mission de développer une identité numérique régalienne.

b. Les agences techniques

Deux agences techniques interviennent principalement sur le sujet de l'identité numérique en France : l'Agence nationale des titres sécurisés et l'Agence nationale de la sécurité des systèmes d'information. Au niveau européen, l'Agence

(1) Les enquêtes utilisateurs réalisées à la demande de la direction interministérielle de la transformation publique (DITP) par IPSOS en mars 2018 et mai 2019 donnent d'ailleurs à voir un niveau important de confiance des usagers dans le rôle de l'État comme architecte de l'identité numérique.

européenne chargée de la sécurité des réseaux et de l'information (ENISA) devrait également être amenée à jouer un rôle croissant.

- **L'Agence nationale des titres sécurisés**

L'Agence nationale des titres sécurisés (ANTS) est un établissement public administratif créé en 2007. Elle compte près de 130 personnes collaborateurs, pour un budget annuel de 240 millions d'euros.

Cette agence remplit principalement trois missions suivantes :

– la conception des démarches en ligne (CNI, passeports, cartes grises, permis de conduire) en tant que maître d'œuvre des systèmes d'information ;

– l'accompagnement des usagers et partenaires institutionnels dans le cadre de la réalisation de leurs démarches en ligne ;

– la production et l'acheminement des titres sécurisés demandés.

Cette agence apporte également **une expertise technique dans le cadre des innovations en matière de titres sécurisés**, qu'il s'agisse d'expérimentations portées par le Gouvernement (maîtrise d'œuvre du projet Alicem) ou qui s'inscrivent, d'une façon plus générale, dans le cadre de l'Union européenne (carte nationale d'identité électronique).

- **L'Agence nationale de la sécurité des systèmes d'information**

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est un service à compétence nationale rattaché au secrétariat général de la défense et de la sécurité nationale, qui fournit une expertise au Gouvernement sur les questions relatives à la sécurité des systèmes d'information. Elle comprenait environ 610 agents au 31 décembre 2019.

Cette agence remplit principalement les trois missions suivantes :

– **la défense des systèmes d'information face aux cyberattaques** : elle intervient comme « pompier informatique » auprès des victimes de ce type d'attaques, pour arrêter ces dernières le plus rapidement possible et reconstruire ensuite le système d'information de façon sécurisée. Cette mission peut prendre la forme d'une assistance à distance ou de l'envoi d'experts sur place ;

– **une action de prévention des cyberattaques**, en travaillant à élever le niveau de cybersécurité des infrastructures informatiques en France et à améliorer l'efficacité de leur détection. Cette mission se traduit, par exemple, par la qualification et la certification de prestataires de confiance, la protection des systèmes des bénéficiaires et enfin une activité de cyber-recherche ;

– **une action d'information et de sensibilisation auprès de différents publics vis-à-vis des risques numériques** (production de guides, formations en ligne *etc*).

Dans le domaine de l'identité numérique, **l'ANSSI accompagne le programme interministériel France identité numérique et garantit la sécurité des moyens d'identification électronique prévus par le règlement européen n° 910/2014 dit « eIDAS ».** À ce titre, elle établit **le référentiel des exigences de sécurité applicables à chaque niveau de garantie des moyens d'identification électronique** et elle évalue le bon respect de ces exigences par les organismes fournissant les moyens d'identification électronique. Elle est également **chargée de l'évaluation d'Alicem** et participe, d'une façon plus générale, aux instances de coopération européenne sur le sujet de l'identité numérique.

Sur les projets Alicem et CNIe, l'ANSSI apporte donc une double expertise à l'ANTS, à la fois en phase de réalisation de projet et lors de l'évaluation, en aval, de leur conformité aux exigences de sécurité définies par le règlement eIDAS.

- **L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)**

Enfin, au niveau européen, **l'Agence européenne chargée de la sécurité des réseaux et de l'information,** joue un rôle secondaire en matière d'identité numérique, qui pourrait être amené néanmoins à se renforcer, comme l'ont indiqué plusieurs acteurs auditionnés par la mission. Le règlement (UE)2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA et à la certification de cybersécurité des technologies de l'information et des communications prévoit actuellement qu'elle peut contribuer à l'élaboration et à la mise en œuvre de la politique et du droit de l'Union en ce qui concerne « *l'identification électronique et [l]es services de confiance, en particulier en fournissant des conseils et en délivrant des lignes directrices techniques, ainsi qu'en facilitant l'échange de meilleures pratiques entre les autorités compétentes* ».

2. Les régulateurs de l'identité numérique

Plusieurs institutions jouent un rôle important de régulation de l'identité numérique, en posant le cas échéant les garde-fous nécessaires au respect strict des libertés publiques et des droits individuels des citoyens.

a. La Commission nationale de l'informatique et des libertés (CNIL)

La CNIL, autorité administrative indépendante instaurée en 1978 par la loi « Informatique et libertés », constitue, dans l'écosystème de l'identité numérique, l'un des principaux régulateurs d'une solution d'identité numérique régalienne. Elle rend en effet des avis sur des projets de loi ou de décret

concernant la protection des données personnelles et procède à des contrôles pour vérifier la bonne application du cadre juridique afférent (1).

Dans le cadre de sa mission de conseil, la CNIL a ainsi rendu un avis sur l'arrêté du 24 juillet 2015, qui crée FranceConnect, fédérateur d'identité permettant à tout utilisateur d'utiliser les identifiants de son choix pour accéder à un certain nombre de services publics et privés. Les échanges avec cette autorité ont eu un impact sur la forme de cette plateforme. Le recours à un identifiant unique a ainsi été écarté, et le principe de minimisation des données transmises renforcé.

La CNIL a également rendu un avis le 18 octobre 2018 sur le projet de décret autorisant la création d'un traitement automatisé permettant de délivrer une identité numérique dénommée « Application de lecture de l'identité d'un citoyen en mobilité » (Alicem). Dans ce cadre, elle a ainsi notamment rappelé que **le consentement de l'individu au traitement de ses données biométriques n'est valable que dans l'hypothèse où la personne concernée dispose d'un contrôle et d'un choix réel concernant l'acceptation ou le refus des conditions proposées ou encore de la possibilité de les refuser sans subir de préjudice**.

Dans ces deux cas, la CNIL a fait preuve d'une grande vigilance vis-à-vis du respect du règlement général sur la protection des données RGPD (2).

b. Le comité européen de la protection des données (CEPD)

Au niveau européen, *le comité européen de la protection des données* (CEPD), créé par l'article 68 du RGPD, assure la cohérence de la mise en œuvre du RGPD entre les différents États membres, et pourrait donc être amené à se saisir de sujets relatifs à l'identité numérique.

c. Le Conseil d'État

La juridiction administrative joue également **un rôle de régulation sur le sujet de l'identité numérique, à la fois *ex-ante* et *ex-post***.

Le Conseil d'État s'assure d'abord, en amont, dans son rôle de conseiller du Gouvernement, que **les projets de texte réglementaire envisagés par le Gouvernement respectent bien le cadre juridique national et européen**. Pour prendre l'exemple du projet de décret Alicem, le Conseil avait ainsi estimé, après analyse, que le décret respecte le principe de consentement de l'utilisateur, tel que prévu par le RGPD, au regard, notamment, de la possibilité de désinstaller l'application à tout moment, de la suppression des données biométriques dès l'enrôlement terminé ou encore de l'information délivrée à l'usager par l'ANTS au moment de la demande d'ouverture du compte. Cet avis avait donc certes pris le contrepied de l'analyse de la CNIL, mais constituait surtout un deuxième regard critique sur le dispositif proposé.

---

(1) Article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(2) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité.

Le Conseil d'État constitue également la voie de recours naturelle contre les textes réglementaires, en référé et au fond. En matière d'identité numérique, la Quadrature du Net a par exemple déposé devant lui, pendant l'été 2019, un recours en illégalité contre le décret du 13 mai 2019 de création d'Alicem, au motif que le maintien du dispositif de reconnaissance faciale comme unique moyen d'activation du compte Alicem, qui est contraire à l'avis de la CNIL, entâcherait le décret d'illégalité.

d. Le Parlement

Le Parlement, enfin, assure un contrôle vigilant vis-à-vis du déploiement d'une identité numérique régalienne, conformément à sa mission de contrôle de l'action du Gouvernement (article 24 de la Constitution). La définition des règles concernant « *les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* » appartient en outre au domaine de la loi (article 34 de la Constitution).

e. La société civile

La société civile a enfin pleinement un rôle à jouer dans la régulation de l'identité numérique. Les associations dont l'objet vise la protection des utilisateurs sur internet assurent un suivi vigilant et utile des solutions mises à la disposition des citoyens/consommateurs. Les citoyens doivent également faire preuve de vigilance dans ce domaine.

3. Les acteurs privés

a. Les acteurs industriels et fournisseurs de briques de solution

L'identité numérique est un secteur d'activité rassemblant un ensemble d'entreprises spécialisées dans le domaine de la confiance numérique. **En France, ce secteur, pris dans sa globalité, comprend environ 500 entreprises, pour un chiffre d'affaires de 1,4 milliard d'euros en 2018**. La France est très bien dotée dans ce domaine et dispose d'un certain nombre de champions industriels, parmi lesquels **Thales, IN Groupe, IDEMIA** ou encore **Atos**.

La brochure capacitaire produite par l'Alliance pour la confiance numérique en 2019, distingue quatre grands types d'offres au sein du processus d'identité numérique, qui sont assurées ou non par ces mêmes acteurs économiques :

– les offres relatives à la création de l'identité numérique et à la souscription à un service de confiance. Elles correspondent aux activités d'interfaçage de l'identité numérique, d'enrôlement, de dérivation et de certification de cette identité ;

– les offres relatives aux supports de l'identité numérique, qu'il s'agisse de supports physiques (puces, cartes, jetons) ou dématérialisés (logiciels, *etc.*) ;

– les offres portant sur l'utilisation, en propre, de l'identité numérique et des services de confiance. Elles sont proposées par des acteurs à la pointe de la gestion de logiciels d'authentification numérique et de signature électronique. On y retrouve également des services de validation d'identité et des fournisseurs d'attributs ;

– enfin, des offres relatives à l'administration du système d'identité numérique, qui renvoient à des solutions et services *Public Key Infrastructure* (PKI) et à des activités de fournisseurs d'identité ou de service de confiance.

Au total, on compte plus de **15 entreprises spécialisées dans le secteur de l'identification électronique en France**. Un contrat de filière signé le 29 janvier 2020 unit par ailleurs les entreprises membres du comité de filière Industries de sécurité, et encadre le déploiement de l'identité numérique en France.

b. Les fournisseurs d'identité numérique

À l'heure actuelle, plusieurs acteurs économiques français se positionnent comme fournisseurs d'identité numérique. C'est le cas notamment du **groupe La Poste**, *via* sa branche numérique Docaposte, qui propose une solution d'identité numérique de niveau substantiel certifiée par l'ANSSI, ou du **groupe Imprimerie Nationale**, qui propose lui aussi une solution d'identité numérique (IN Wallet).

Un exemple d'identité numérique de niveau substantiel : La Poste

La Poste a lancé, le 26 mai dernier, la première identité numérique certifiée de niveau substantiel par l'ANSSI. Cette solution permet, en 4 étapes, de créer son identité numérique en ligne, grâce à l'utilisation d'un titre d'identité (carte d'identité ou passeport) et d'un smartphone. Elle offre un accès à près de 700 sites de services publics ou privés *via* FranceConnect. Le modèle économique de l'identité numérique de La Poste repose sur une stratégie d'acquisition adossée aux usages publics – justifiant sa gratuité – et une monétisation auprès du secteur privé. Le service est et restera gratuit pour les utilisateurs finaux.

c. Les acteurs « non spécialistes »

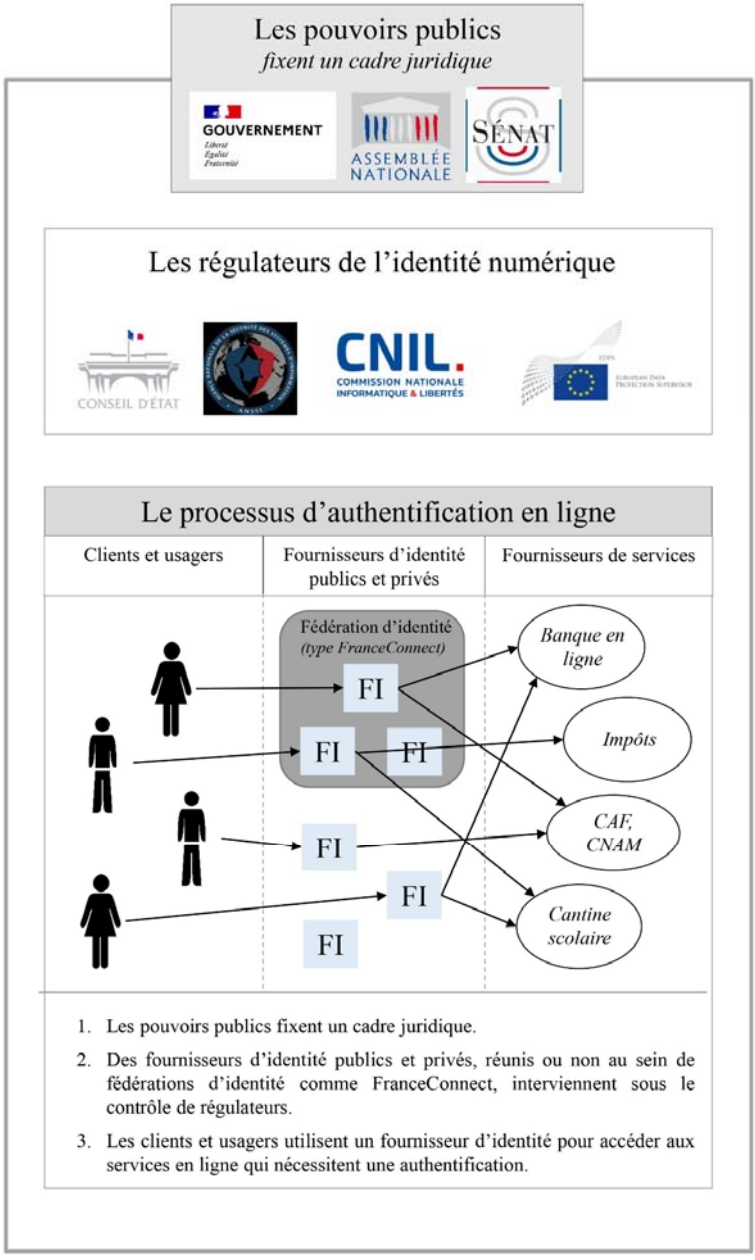
Aujourd'hui, la fourniture d'identité numérique est réalisée par **des acteurs non spécialistes**, qui dérivent cette identité à partir des données qu'ils recueillent et valorisent (Google, Facebook, *etc.*) ou proposent tout simplement la création d'une identité numérique « basique » composée d'un identifiant et d'un mot de passe, pour l'usage de leur service **(*e*-commerce).**

Google et Facebook proposent en effet, outre une identité numérique subjective, une identité numérique dérivée à partir du compte Gmail ou Facebook de l'utilisateur. Il s'agit des solutions *Facebook Connect* et *Google sign-in*. Très concrètement, cela consiste, pour l'utilisateur du réseau social Facebook, à réutiliser ses identifiants pour se connecter à un fournisseur de services partenaire. Il peut ainsi procéder à des transactions facilement, sans avoir besoin de

se créer un compte. Ce service, gratuit repose néanmoins sur la valorisation des données personnelles.

En dehors de Google et Facebook, de nombreux autres acteurs existent sur ce marché en forte croissance, qu'il s'agisse, par exemple, de *Digits* (Twitter), *d'Apple Pay* ou encore de l'identification par *Paypal*. La souveraineté des données constitue évidemment une problématique importante lorsqu'il s'agit de solutions non européennes (pas d'obligation de stockage des données en Europe notamment).

SCHÉMA D'ENSEMBLE DE L'IDENTITÉ NUMÉRIQUE



Source : Assemblée nationale

D. LES ENJEUX DE L'IDENTITÉ NUMÉRIQUE

L'identité numérique soulève un nombre important d'interrogations. La confiance dans les dispositifs mis en place, leur accessibilité au plus grand nombre, l'association du monde économique, ainsi que des problématiques liées à la sécurisation des données et à la souveraineté numérique des États ont été abordés dans les nombreuses auditions que la mission d'information a menées.

1. Un prérequis : créer la confiance

a. Une nécessaire transparence sur la gestion des données personnelles collectées

Actuellement, le dispositif d'identité numérique mis en place par FranceConnect nécessite la collecte d'**un socle minimal de données, dites « données pivot »** : le sexe, les prénoms, le nom de naissance, la date, le lieu et le pays de naissance. Il s'agit actuellement de seules données collectées par FranceConnect. D'autres données pourraient néanmoins être collectées et valorisées par les fournisseurs d'identité, avec le consentement de l'utilisateur.

D'une manière générale, il existe **trois traitements distincts des données personnelles** relatives à l'identité numérique :

– l'identification, qui « *relève du traitement de toutes les données relatives à l'identité d'un individu* » ;

– le consentement, c'est-à-dire le « *mécanisme par lequel l'individu va consentir à l'accès à ses données et ses attributs d'identité à un fournisseur de service qui les lui réclamera* » ;

– le flux des données personnelles, c'est-à-dire la « *manière dont ces données, ainsi que les données d'usages, vont circuler, être utilisées et associées* [(1)] ».

Pour chacun de ces opérations et traitements, **des règles claires et compréhensibles** de tous sont en effet un prérequis indispensable à la création de la confiance. Comme le constate la Fondation internet nouvelle génération dans sa contribution écrite, « *amener du sens, de la transparence et du contrôle en matière d'exploitation des données personnelles n'est plus une option, c'est aujourd'hui une nécessité* ».

Ainsi que le résume **Mme Valérie Peneau** dans sa contribution écrite, « *l'identité numérique sécurisée doit contribuer à la confiance de l'écosystème numérique et précisément contribuer à lutter contre les mésusages qui affectent sa crédibilité. Elle ne doit pas être un facteur de doute ou d'inquiétude injustifiée* ».

---

(1) Renaissance numérique, rapport Identité numérique : passer à une logique citoyenne*, janvier 2019, p. 38.*

b. Une définition claire des rôles de l'État et du secteur privé

Le rôle de l'État et celui des entreprises privées associées au développement des solutions d'identité numérique doivent être clairement définis et transparents.

L'établissement et la garantie de l'identité sont une prérogative régalienne depuis l'état civil et il est essentiel qu'ils le demeurent à l'avenir. Pour M. Cédric O, secrétaire chargé du Numérique (1), « *l'enjeu pour l'État est de faire en sorte que, demain, il continue de garantir l'identité et que, lorsque le citoyen a une démarche en ligne à effectuer, c'est l'identité certifiée par l'État* ». Dans le cadre de la consultation en ligne de l'Assemblée nationale sur l'identité numérique, de nombreux internautes ont également insisté sur le caractère régalien que doit, selon eux, revêtir l'identité numérique.

Toutefois, l'État ne devrait pas assumer seul la mise en place de ces solutions, sauf à susciter la méfiance et l'inquiétude des utilisateurs, qui pourraient se détourner des solutions mises en place. Selon le *think tank* Renaissance numérique, il doit plutôt « *pleinement jouer sa fonction d'État plateforme, c'est-à-dire non pas un État qui centralise, mais qui structure, fédère, ouvre, sécurise les dispositifs d'identité numérique. Il en va d'un enjeu d'acceptabilité pour les citoyens* (2) ».

Comme le relève Mme Valérie Peneau dans sa contribution écrite, « *l'écosystème numérique national a pleinement intérêt au déploiement large de solutions d'identité numérique sécurisées, qui en conditionne largement la confiance d'ensemble, sous réserve que les données d'identité soient garanties par l'État* ».

L'association de partenaires privés à la construction et au fonctionnement de l'architecture des solutions d'identité numérique régalienne devrait donc être possible, sous réserve qu'elle soit strictement encadrée, par exemple en la conditionnant à **l'obtention d'une certification** exigeante de la part de l'Agence nationale de la sécurité des systèmes d'information.

Le législateur pourrait s'inspirer **du partage des tâches prévu en Suisse** depuis l'adoption de la loi fédérale sur les services d'identification électronique à l'automne 2019 (3). Ce projet est néanmoins contesté par une partie de la population, qui redoute une exploitation illégale des données personnelles collectées par les

---

(1) Audition par la mission d'information du mardi 18 février 2020 – voir la vidéo de l'audition sur le site de l'Assemblée nationale, ainsi que le compte rendu en annexe au présent rapport.

(2) Renaissance numérique, rapport Identité numérique : passer à une logique citoyenne*, janvier 2019.*

(3) La loi prévoit que l'État soit chargé, en amont, du contrôle de l'identité et de la confirmation de l'existence de la personne ainsi que des caractéristiques permettant de l'identifier (nom, sexe, date de naissance). En revanche, les supports matériels nécessaires pour utiliser cette identité électronique contrôlée et confirmée par l'État, à l'instar des téléphones mobiles, des cartes bancaires ou des abonnements de transports publics, ne seront ni développés, ni délivrés par la Confédération, mais par des prestataires chargés de fournir une identité numérique à l'utilisateur. L'État devra néanmoins soumettre les prestataires et les solutions que ceux-ci proposent à des procédures de reconnaissance très strictes et à des contrôles réguliers.

entreprises privées associées au dispositif [1], et qui s'est mobilisée pour obtenir l'organisation d'un référendum à l'occasion duquel les Suisses se prononceront sur ce projet dans les prochains mois.

Cette situation souligne avec acuité la nécessité absolue de faire preuve, en matière d'identité numérique, et plus largement, d'innovations numériques, de pédagogie et de transparence. Cette démarche suppose aussi d'associer l'ensemble des acteurs, y compris en mobilisant l'expertise citoyenne et associative.

c. Faire preuve de pédagogie

L'identité numérique est **un sujet mal compris et parfois sources d'inquiétudes** que vos rapporteurs ont perçues au cours de leurs auditions et dans certains commentaires de la consultation citoyenne organisée par l'Assemblée nationale dans le cadre de la mission d'information.

Comme le relève le Conseil national du numérique, ces inquiétudes sont nourries par une « *appréhension de l'identité numérique* [par les citoyens] *difficile, en raison de la technicité du sujet. Celui-ci est également perçu comme très anxiogène, ce qui implique d'initier une démarche volontaire visant à créer les conditions de la confiance de la part des citoyens* » [2].

Faire preuve de pédagogie semble indispensable pour dissiper les inquiétudes et instaurer un débat apaisé sur ce sujet.

d. Le maintien de l'anonymat sur internet

La confiance dans les dispositifs en cours de développement impose que **l'anonymat demeure la solution par défaut**.

La mise en place d'une solution d'identité numérique régalienne est **un service proposé à la population**. Elle doit lui permettre de simplifier l'accès sécurisé à l'ouverture d'un droit ou à une prestation qui nécessite de prouver son identité, comme cela est actuellement le cas en présentiel. **En aucun cas, l'identité numérique ne doit conduire à une authentification obligatoire des internautes**.

Comme le relèvent les chercheurs Armen Khatchatourov, Pierre-Antoine Chardel et Claire Levallois-Barth, « *l'absence d'identification immédiate peut dans certains cas être perçue comme une difficulté, par exemple lorsque l'identification s'avère nécessaire pour réaliser une transaction bancaire ou pour lutter contre des contenus illicites* », mais « *elle constitue* [également] ***un formidable gage de liberté****, à la fois en termes de liberté d'information, d'action et d'expression dans*

---

(1) « Les Suisses favorables à une identité numérique gérée par l'État », RTS.ch, 28 mai 2019. Cet article présente les résultats d'un sondage selon lequel 87 % des sondés souhaitent que l'État administre le schéma d'identification numérique, tandis que seuls 2 % des sondés font confiance au secteur privé pour y parvenir. La crainte principale des sondés est que les entreprises privées utilisent les données personnelles des utilisateurs à des fins commerciales.

(2) Conseil national du numérique, rapport Identités numériques : clés de voûte de la citoyenneté numérique*, juin 2020, p. 52.*

le cadre des débats favorisés techniquement par ce nouvel espace public qu'est le web » (1) à laquelle vos rapporteurs sont attachés.

La mission d'information relève que cette préoccupation est partagée par le Gouvernement. Durant son audition, M. Cédric O a affirmé qu'il n'est « *pas imaginable que l'on mette fin, par la contrainte, à l'anonymat en ligne* » et qu'il s'agit d'un « *combat non seulement vain mais dangereux* » (2).

2. Faciliter l'accès à un ensemble de services pour les citoyens

a. Améliorer l'accès aux services en ligne déjà existant

La mise en place d'une identité numérique sécurisée doit permettre de **garantir l'accès à des services en ligne de manière sécurisée**, qu'il s'agisse de services publics tels que l'assurance maladie et les impôts, ou des services privés tels que les assurances ou les services bancaires dématérialisés.

Comme l'a souligné M. Sauvage de Saint Marc, directeur de l'innovation de l'entreprise Cisco (3), l'accès à ces services nécessite **un degré de sécurisation du processus d'authentification de plus en plus élevé**. Cette tendance croissante au renforcement du niveau de sécurité exigé pour bénéficier de ces services amène au développement de solutions qui vont au-delà du simple couple « login-mot de passe », qui caractérise les modèles d'authentification les moins sécurisés.

Cette exigence de sécurisation se constate également à l'étranger. Comme l'a relevé Mme Valérie Peneau dans sa contribution écrite, « *sur la plateforme publique belge, la quasi-totalité des connexions aux 700 services en ligne (impôts, assurance maladie…) se font déjà au moins au niveau substantiel, ce qui semble montrer qu'une grande partie des services publics devront à court ou moyen terme passer à un niveau sécurisé (au moins substantiel) et encourage* [l'action de la mission interministérielle sur l'identité numérique] *en ce sens* ».

b. Engager une réflexion sur de nouveaux usages

Alors que certaines opérations nécessitant une authentification sûre ne sont actuellement pas accessibles par la voie dématérialisée, le développement de solutions d'identité numérique sécurisée doit permettre, selon M. Cédric O, « *d'ouvrir en ligne des services qui nécessitent l'identification élevée des personnes sans contact physique, en les protégeant contre les risques croissants d'usurpation d'identité en ligne et en conservant la maîtrise des données d'identité* » (4).

---

(1) Chaire Valeurs et Politiques des Information Personnelles, Cahier n° 1, Identités numériques, *coordonné par Claire Levallois-Barth, mars 2016, page 3.*

(2) Audition par la mission d'information le mardi 18 février 2020 – voir la vidéo de l'audition sur le site de l'Assemblée nationale, ainsi que le compte rendu en annexe au présent rapport.

(3) Audition par la mission d'information le jeudi 13 février 2020.

(4) Audition par la mission d'information le mardi 18 février 2020 – voir la vidéo de l'audition sur le site de l'Assemblée nationale, ainsi que le compte rendu en annexe au présent rapport.

Cette ouverture pourrait concerner des **services publics délivrés par l'État ou par les collectivités territoriales**, à l'exemple des demandes de procuration de vote, d'aides sociales, d'inscription sur les listes électorales, de dépôt de plainte, la téléconsultation médicale, de demande de passeport, *etc*. Mais ces nouveaux usages pourraient également s'étendre aux **services privés**, comme les services bancaires (ouverture d'un compte bancaire, demande de crédit, virement d'un montant élevé, *etc*.) ou assurantiels, lorsque ces services nécessitent une authentification préalable de leurs clients.

La mission souhaite relever le potentiel fort de l'identité numérique dans le domaine de la santé. Le rapport « Usages de l'identité numérique sécurisée » de la DITP de juillet 2019 en fait l'un des quatre secteurs les plus porteurs (fort potentiel en termes de volumétrie, de niveau de pénibilité, et niveau de sécurité important requis), avec ceux des prestations sociales, de la fiscalité et des services bancaires.

Une solution d'identité numérique régalienne serait très utile, par exemple, dans le cadre du déploiement du dossier médical partagé (DMP). Elle offrirait en effet à son utilisateur **un outil souple et sûr pour accéder à ses informations personnelles**. Les acteurs auditionnés par la mission en attendent notamment une plus grande fiabilité et un recours accru des Français aux outils du numérique en santé.

Cet intérêt est d'ailleurs confirmé par l'expérience d'autres pays comme l'Australie. Dans ce dernier, la solution Digital ID, lancée en 2016, service d'identification développée par Australia Post, permis déjà aux Australiens de gérer leur dossier de santé et leurs remboursements de frais de santé. MyGovID, service d'identification en cours de développement par l'Etat australien, leur permettra à l'avenir d'accéder également à un résumé en ligne de leurs données de santé (*My Health Record*).

Au-delà de ces usages, le *think tank* Renaissance numérique considère que l'identité numérique sécurisée permettrait également de **redynamiser la vie publique**. Ainsi, « *son périmètre a également vocation à s'élargir aux pratiques citoyennes, à l'instar du champ de la concertation. En assurant l'identité des participants, et donc l'intégrité du vote, à l'échelle locale ou nationale, elle pourrait permettre de garantir et de généraliser le recours aux dispositifs participatifs en ligne* » (1).

La mission d'information considère néanmoins que **le vote en ligne ne peut pas être réalisé pour toutes les élections**. Il peut par exemple l'être pour les élections professionnelles ou associatives, et peut être expérimenté pour les élections consulaires, les Français de l'étranger rencontrant davantage de difficultés à se déplacer dans les bureaux de vote. Il importe néanmoins d'écarter un tel recours pour les autres élections.

---

(1) Renaissance numérique, rapport Identité numérique : passer à une logique citoyenne*, janvier 2019.*

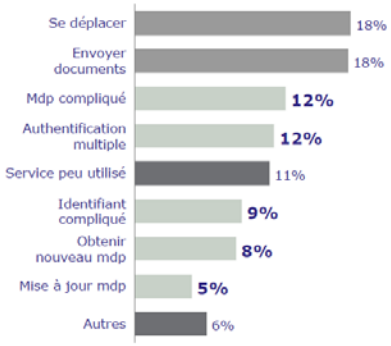
c. Proposer une solution pratique et facile d'accès

Les solutions d'identité numérique doivent **faire preuve d'ergonomie et de simplicité en développant l'expérience utilisateur**. Comme l'ont relevé les représentants d'IN Group auditionnés par la mission d'information (1), une solution nécessitant des procédures d'enrôlement trop compliquées ou trop nombreuses découragerait les utilisateurs.

Afin de séduire les entreprises privées et leurs clients, et de ne pas cantonner les solutions développées aux seules relations entre les administrés et les services publics, ces solutions doivent garantir la **fluidité des usages.** Dans le cas contraire, les utilisateurs se détourneront des solutions étatiques au bénéfice de solutions d'authentification privées moins vertueuses en termes de protection de la vie privée. L'Association des départements de France (ADF) relève à cet égard que « *l'expérience utilisateur, l'ergonomie et la simplicité d'usage sont, dans un marché globalisé, largement mieux illustrés par les services* [proposés par les] *GAFAM* (2)*, et partant engendrent une forte appétence pour les formes d'identité numérique que ces derniers développent* ».

Pourtant, les attentes des Français en la matière sont très fortes. Selon deux enquêtes qualitatives publiées dans un récent rapport de la direction interministérielle de la transformation publique (DITP) (3), 46 % des Français considèrent les difficultés qu'ils rencontrent pour s'identifier ou s'authentifier comme des facteurs dissuasifs à la réalisation de telles opérations.

LES FACTEURS DISSUASIFS DANS LA MANIÈRE DE S'IDENTIFIER



Source : Direction interministérielle de la transformation publique, Usages de l'identité numérique sécurisée*, juillet 2019, p. 79.*

(1) Audition par la mission d'information le lundi 8 juin 2020.

(2) Acronyme désignant les entreprises Google, Amazon, Facebook, Apple et Microsoft.

(3) DITP, Usages de l'identité numérique sécurisée*, juillet 2019.*

3. Une opportunité économique pour un grand nombre d'acteurs privés

a. Un attrait fort des acteurs privés pour une identité numérique régalienne

Le marché de l'identité numérique devrait représenter 250 millions d'euros d'ici 2024 et plus d'1 milliard d'euros d'ici 2029.

Les nombreuses auditions conduites par la mission d'information font apparaître, comme l'envisageait l'étude EY réalisée à la demande de la direction générale des entreprises (DGE) sur le « modèle économique de l'identité numérique » [(1)], qu'un très grand nombre d'acteurs économiques sont intéressés par le développement d'une solution d'identité numérique régalienne.

Ces acteurs privés appartiennent aussi bien au secteur de la **banque, que des jeux en ligne, des assurances, de la mobilité, de la santé, des plateformes en ligne, sans évoquer les usages transverses pouvant intéresser la plupart des acteurs économiques, quel que soit leur secteur d'activité** (pour recruter à distance, par exemple, en s'assurant de l'identité de la personne).

Les entreprises françaises technologiques, spécialistes du secteur, y sont également bien positionnées (Idemia, IN Groupe, Atos). Il faut donc saisir cette opportunité de développer l'écosystème industriel français dans ce domaine afin d'éviter la préemption de ce marché par des grands groupes internationaux étrangers.

Enfin, un certain nombre de professions réglementées soutiennent également le déploiement d'une solution régalienne. Elles ont parfois d'ailleurs déjà mis en œuvre leurs propres solutions dans un cadre professionnel (greffiers des tribunaux de commerce, notaires).

(1) EY, Modèle économique de l'identité numérique des particuliers et des entreprises*, 2019.*

L'identité numérique des personnes morales

Dans les textes européens, l'identité numérique concerne les personnes physiques, mais également les personnes physiques représentant des personnes morales.

Le traitement de cette question spécifique a néanmoins , pour des raisons d'efficacité et d'expertise, été pris en charge par le secrétariat général du ministère de l'économie et non par la mission dirigée par Mme Valérie Peneau. Cette dernière a toutefois indiqué à la mission que des « *travaux conjoints [étaient] conduits en étroite articulation, l'identité numérique des personnes physiques représentant la personne morale étant indispensable à la plupart des procédures concernant les personnes morales en ligne* ».

Dans le cadre de ses travaux**, la mission d'information a pu observer que certains acteurs s'étaient d'ores et déjà saisis de la question de l'identité numérique « professionnelle », en développant leur propre solution**.

C'est le cas des notaires et de leur solution d'identité numérique ID.not, lancée en 2015. Cette identité numérique certifiée, massivement adoptée (83 % des études ont un compte actif), leur permet d'accéder à un ensemble de services propres à la profession de façon sécurisée. Cet outil se distingue de la clé réal mise à leur disposition par le Conseil supérieur du notariat (CSN) afin de leur permettre de signer de façon sécurisée un ensemble de documents en ligne.

C'est le cas également du Conseil national des greffiers des tribunaux de commerce et d'Infogreffe, qui ont lancé en 2019 MonIdenum, solution d'identité numérique à destination des chefs d'entreprises. Le service « Tribunal digital », qui s'appuie sur MonIdenum leur permet désormais d'ester en justice à raison de leur qualité de représentant d'une personne morale donnée. **On compte actuellement près de 64 000 comptes MonIdenum actifs**. Cette identité numérique « professionnelle » se fonde sur les données enregistrées au sein du registre du commerce et des sociétés (RCS). À terme, MonIdenum a vocation à permettre aux chefs d'entreprise et à leurs représentants légaux de s'identifier sur des plateformes tierces, et d'accéder ainsi à panel élargi de services en ligne.

Source : auditions conduites par la mission d'information

b. Un moyen de réduire les coûts de vérification d'identité pour les fournisseurs de services

Cette appétence des acteurs privés pour une identité numérique s'explique d'abord par le surcroît de sécurité qu'elle leur offrirait en étant largement déployée. Cette solution, même payante, leur permettrait de réduire leur coût de vérification d'identité de leurs clients qui est assez élevé. Chaque fournisseur doit en effet collecter un certain nombre d'informations, les stocker, les gérer et assurer leur protection. L'externalisation de cette activité réduirait donc leurs investissements dans les processus KYC (*Know Your Customer*).

En outre, la valeur croissante des données au sein de notre économie, en particulier dans certains secteurs d'activités, renforce l'intérêt d'une solution de cette nature. C'est le cas par exemple pour les acteurs de l'assurance,

dont les services s'appuient de plus en plus sur des concepts de *selfdata*, nécessitant de s'assurer de l'identité de la personne utilisatrice.

c. Une simplicité d'usage qui fluidifie la relation client

La fluidité de l'identité numérique offre également des perspectives de croissance pour ces acteurs. La relation client à distance est en effet très fortement dépendante de la facilité d'enrôlement et d'achat sur internet. Au-delà du secteur du *e*-commerce, celui des jeux en ligne, fortement réglementé, en tirerait un profit intéressant. À titre d'illustration, chez un acteur comme Betclic, près de 50 % des tentatives de création de compte utilisateur sont abandonnées avant leur terme, en raison des contraintes spécifiques qu'elles comportent. **La fluidité du processus d'enrôlement, puis d'usage de l'identité numérique pourrait être bénéfique pour ce type d'acteurs économiques.**

L'identité numérique offre, au surplus, un second atout en termes de confiance pour l'utilisateur et le fournisseur de données : elle promeut une gestion frugale de ces dernières, à la main de l'utilisateur. Lors de la phase d'authentification, l'interrogation par le fournisseur de services du tiers de confiance conduit à produire une réponse à la question qui est protectrice de la vie privée (réponse binaire oui-non, absence de transmission d'information non nécessaire). Très concrètement, à terme, un utilisateur X souhaitant accéder à un service pour lequel il est nécessaire d'être majeur ou de disposer d'un attribut particulier (absence de surdenttement par exemple), pourra transmettre cette information de façon binaire (absence ou non de majorité, d'endettement), sans avoir à dévoiler l'ensemble de ses informations personnelles (âge de l'utilisateur ou détail de ses comptes bancaires). Le fédérateur d'identité apporte ici une vraie plus-value en centralisant l'information, de manière à ce que ni le fournisseur de services, ni le fournisseur d'identité n'aient connaissance respectivement du service utilisé et du contenu précis de l'information demandée.

d. Un vecteur de concurrence et d'innovation pour le marché

Enfin, ce projet permettrait également **de valoriser en France le secteur de l'identité numérique, en lui donnant une visibilité nouvelle, au-delà des usages professionnels de cette technologique qui existaient jusqu'alors**. L'usage d'une solution d'identité numérique régalienne par les particuliers et les professionnels aurait pour conséquence de renforcer l'utilisation de ce type de solutions, et serait donc également bénéfique pour les fournisseurs d'identité privés présents sur le marché. **Cette démocratisation s'appuierait sur le niveau de confiance plus élevé que suscite une solution régalienne**, par rapport en particulier aux solutions moins sécurisées et axées sur la valorisation des données que proposent *Google* ou *Facebook* [1]. **De surcroît, l'arrivée d'une solution régalienne sur le marché de l'identité numérique pourrait stimuler la**

(1) Le baromètre de l'ACSEL montre ainsi que les Français ont confiance en FranceConnect pour 65 % d'entre eux, quand 33 % ont confiance en Facebookconnect ou Google-signin.

concurrence et l'innovation, au profit des acteurs français, particulièrement performants dans ce domaine.

Il apparaît nécessaire, en revanche, d'encourager **les utilisations à titre expérimental pour permettre aux acteurs privés de s'approprier cette nouvelle solution**. Il s'agit là d'une demande forte des acteurs économiques intéressés.

Recommandation n° 1 : Encourager les utilisations à titre expérimental de l'identité numérique régalienne par les acteurs privés, afin de leur permettre de s'approprier cette nouvelle solution.

4. Garantir un niveau de sécurité élevé et protéger la souveraineté européenne

À l'heure actuelle, la majorité des solutions d'identité numérique utilisées par les particuliers possèdent un niveau de sécurité relativement faible. Les fournisseurs de service proposent en effet la plupart du temps à l'utilisateur de **créer un compte avec un simple login et un mot de passe**. Seule la phase de paiement fait l'objet d'une sécurisation renforcée, grâce aux technologies proposées par les principaux acteurs du paiement en ligne.

Le développement d'une solution d'identité numérique régalienne, dans le cadre d'eIDAS, permettrait donc de rehausser le niveau de sécurité dans les usages quotidiens par les citoyens de services publics et privés. Le règlement eIDAS définit en ce sens trois niveaux de sécurité pour les solutions d'identification électronique : le niveau faible, le niveau substantiel et enfin le niveau élevé (*voir infra*). Les choix technologiques effectués conditionnent le niveau de sécurité d'une identité numérique régalienne.

Il s'agit enfin également **d'un enjeu de souveraineté technologique**. Le positionnement très favorable des entreprises françaises dans ce domaine à l'international doit être soutenu par un marché intérieur dynamique.

Le stockage des données comme enjeu de souveraineté : le projet GAIA-X

Le projet GAIA-X a été créé à l'initiative des gouvernements allemand et français. L'idée a d'abord vu le jour en Allemagne, intégrée à la « stratégie industrielle nationale pour 2030 », puis dans un manifeste franco-allemand pour une politique industrielle européenne début 2019. L'objectif est d'instaurer un écosystème européen souverain de données, reposant sur la promotion de la souveraineté digitale et de l'innovation.

Le développement de cet écosystème numérique a été annoncé en mai 2020 par les ministres de l'économie français et allemand, MM. Bruno Le Maire et Peter Altmaier. En janvier 2020, la Présidente de la Commission européenne, Mme Ursula von der Leyen, avait déclaré que « *pour être un acteur géopolitique, il faut pouvoir être garant de sa souveraineté technologique* ».

GAIA-X a été décrit par M. Bruno Le Maire comme une « *place de marché avec différents services et offres interopérables* ». Le projet sera développé par 22 entreprises, dont la moitié sont allemandes et l'autre moitié françaises. Parmi les entreprises françaises, on trouve Orange, EDF ou Dassault Systèmes. Du côté allemand, ce sont par exemple Deutsche Telekom, Siemens et Bosch qui ont rejoint le projet.

Ce réseau de partage de données devrait rassembler, à travers l'Europe, des entreprises, des administrations publiques, des acteurs de la santé, des institutions scientifiques et des citoyens. Les premiers services hébergés par le *cloud* devraient voir le jour début 2021. Une réflexion sur le rôle que ce *cloud* pourrait jouer en matière d'identité numérique devrait être engagée.

II. L'IDENTITÉ NUMÉRIQUE EN FRANCE : TIRER LES LEÇONS DU PASSÉ, S'INSPIRER DES SUCCÈS PRÉSENTS

D'abord en avance sur ses voisins, la France a désormais un retard conséquent que les dernières solutions mises en service ou en cours de développement visent à rattraper. Le cadre juridique européen facilite aujourd'hui le développement d'une identité numérique régalienne sécurisée, tandis que les expériences des États européens précurseurs peuvent servir de guide à l'action des pouvoirs publics en la matière.

A. DES EXPÉRIENCES NATIONALES PASSÉES AU SUCCÈS VARIABLE, POUR DES RAISONS TECHNIQUES ET POLITIQUES

1. La France, pionnière en matière d'identité numérique, a été confrontée à plusieurs échecs

a. Le projet SAFARI et la création de la CNIL

Plusieurs projets français plus ou moins liés à l'identité numérique ont été menés au cours des quarante dernières années.

En 1974, le **projet de système automatisé pour les fichiers administratifs et le répertoire des individus** (SAFARI) prévoit d'identifier chaque Français par un numéro unique – le numéro INSEE de sécurité sociale – et d'interconnecter sur la base de cet identifiant tous les fichiers administratifs afin de favoriser les échanges avec les administrations. Cette initiative fait néanmoins l'objet de nombreuses interrogations et remises en cause, illustrées par la Une du journal *Le Monde* du 21 mars 1974, intitulée « ¨Safari˝ ou la chasse aux Français ».

L'opposition à ce projet, considéré comme liberticide, contraint le Premier ministre de l'époque, M. Pierre Messmer, à le retirer et à créer une commission spécialisée, la **Commission nationale de l'informatique et des libertés** (CNIL) dont l'existence est consacrée par la loi « informatique et libertés » du 6 janvier 1978 [(1)].

Cette loi, dont l'article 1er dispose que « *l'informatique doit être au service de chaque citoyen* », pose les bases juridiques du traitement des données à caractère personnel tels que les droits d'information, d'opposition, d'accès et de rectification. Elle interdit notamment tout numéro d'identification unique en France, à la différence d'autres pays européens. La Commission qu'elle met en place est « *chargée de veiller au respect des dispositions de la présente loi, notamment en informant toutes les personnes concernées de leurs droits et obligations, en se concertant avec elles et en contrôlant les applications de l'informatique aux*

(1) Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

traitements des informations nominatives ». Elle dispose « *à cet effet d'un pouvoir réglementaire, dans les cas prévus par la présente loi* » (1).

Cette loi a eu **un effet durable sur la conception des politiques liées à l'identité numérique**. Pour Mme Valérie Peneau, « *la situation française actuelle en matière d'administration électronique est très largement l'héritage de ce projet et de son abandon : pas d'identifiant unique, mais de multiples identifiants sectoriels (fiscal, santé...), pas de registre unique de population, pas d'interconnexion de fichiers* » (2).

b. Le programme public INES

Au début des années 2000, une réflexion s'engage au sujet des difficultés rencontrées par l'administration pour certifier l'identité d'une personne, cette certification ayant lieu par l'intermédiaire d'un acte de naissance aisément falsifiable, pouvant donc permettre à un individu d'obtenir des documents d'identité à partir d'une fraude à l'état civil. En 2003, le Gouvernement développe le **programme public Identité Nationale Electronique Sécurisée** (INES) qui prévoit notamment, outre la mise en place du passeport biométrique, la mise en circulation de **cartes d'identité électroniques offrant un accès à des services en ligne**, et contenant les données biométriques du porteur ainsi que des certificats d'authentification et de signature.

Ce deuxième volet fait l'objet **de vives réticences** à la fois liées à la crainte encore vive d'un fichage généralisé, au caractère obligatoire et payant de ce nouveau titre, ainsi qu'au refus d'usages commerciaux envisagés, notamment de paiement (3). Les pouvoirs publics renoncent au projet en juin 2005.

Malgré ces échecs, **les premières cartes nationales d'identité électroniques sont distribuées dès la fin des années 1990**, mais elles concernent uniquement certains professionnels dans le cadre de leur emploi. C'est notamment le cas des cartes de professionnels de santé (CPS), qui contiennent les données d'identificateur du porteur et permettent à leur titulaire de s'authentifier, bénéficier de certificats d'authentification, signer électroniquement et fluidifier ses relations avec l'Assurance maladie.

c. Une nouvelle tentative de généralisation des cartes nationales d'identité électroniques en 2010

Les travaux relatifs à la mise en place d'une identité numérique régalienne sont relancés en 2010, à l'occasion de l'examen de la **proposition de loi relative à la protection de l'identité** (4), qui prévoit l'introduction dans la carte nationale d'identité de deux puces électroniques. La première, la « puce régalienne »

---

(1) Article 6.

(2) Contribution écrite de Mme Valérie Peneau.

(3) Le forum des droits sur internet, Le projet de carte nationale d'identité électronique, 16 juin 2005.

(4) Devenue la loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité.

obligatoire, permet d'y stocker des données d'identité et biométriques (1). Facultative, la seconde puce ouvre l'accès à certains services en ligne, en permettant aux utilisateurs de certains services publics ou privés de s'authentifier et d'apposer leur signature électronique.

La loi issue de cette proposition est adoptée par le Parlement, mais elle est ensuite **censurée partiellement par le Conseil constitutionnel en 2012**, notamment les dispositions concernant la seconde puce facultative, le Conseil estimant que **le législateur n'a pas défini avec suffisamment de précision le régime juridique de cette puce ainsi que la nature et le traitement des données collectées** (2).

d. L'ancienne société Idénum

Au début des années 2010, le **projet pilote Idénum**, pensé sur le modèle du groupement d'intérêt économique (3), doit permettre la mise en place d'**un titre électronique support d'une identité numérique sécurisée**, pouvant être utilisé à distance. En 2013, la société Idénum est créée, rassemblant le Crédit Mutuel, le CIC, Pages Jaunes, SFR et le Groupe La Poste, ainsi que l'État par l'entremise de la Caisse des dépôts et consignations. Il est alors prévu d'habiliter cette société à mettre en place des standards s'appliquant à tous les fournisseurs d'identité, rémunérés par les fournisseurs de services.

Toutefois, **en 2014, ce projet d'une identité unique, corrélée à un titre électronique, est abandonné par le Gouvernement**, qui préfère laisser à l'utilisateur le choix entre plusieurs fournisseurs d'identité en fonction des services auxquels il souhaite accéder. C'est cette nouvelle approche qui conduit, en 2015, à la création du **fédérateur d'identité FranceConnect**, qui permet à l'usager d'utiliser l'identité numérique d'un fournisseur d'identité partenaire (4) pour s'authentifier directement auprès des fournisseurs de services.

2. Les conditions semblent néanmoins réunies pour mener à bien ce projet aujourd'hui

Les échecs des projets passés ont fait perdre un temps important à la France dans la mise en œuvre d'une identité numérique sécurisée, mais ils permettent néanmoins aux travaux actuels d'éviter certains écueils.

Ainsi, le projet d'identité numérique régalienne sur lequel travaille le programme France identité numérique **ne cherche pas à créer un identifiant unique**, mais au contraire à poursuivre le développement d'un écosystème

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

(2) Décision n° 2012-652 DC du 22 mars 2012.

(3) À l'instar du GIE CB qui a permis, en rassemblant de nombreuses entreprises, de développer massivement les technologies de carte à puce dans le secteur bancaire.

(4) Il en existe six aujourd'hui : le compte impots.gouv.fr, ameli.fr, l'Identité Numérique La Poste, MobileConnect et moi, msa.fr et Alicem.

comprenant de nombreux fournisseurs d'identité différents, en fonction des usages souhaités par l'utilisateur. **Il ne s'accompagne pas de la création d'un fichier central**, mais permet à l'inverse à chaque individu de maîtriser le processus de création de son identité numérique, et de lui proposer une solution gratuite et facultative.

Le cadre juridique national et européen a évolué depuis une dizaine d'années, devenant plus protecteur et rassurant. À la suite de l'adoption du règlement général sur la protection des données du 27 avril 2016 et de la directive Police-Justice (1), le législateur français a adopté la loi du 20 juin 2018 relative à la protection des données personnelles (2) modifiant la loi Informatique et libertés afin de mettre en conformité le droit français avec le cadre européen.

En outre, **la société française semble aujourd'hui plus mature et prête à adopter ces nouvelles solutions**. Selon un sondage IPSOS d'avril 2018, cité par Mme Valérie Peneau dans sa contribution écrite, 74 % des français interrogés sont favorables au principe d'une carte d'identité numérique, 70 % estimant qu'elle serait source de simplification. L'étude de mai 2019 de la direction interministérielle de la transformation publique concernant les usages de l'identité numérique (3) montre de résultats similaires : deux usagers sur trois estiment la gestion de l'identité numérique par l'État pertinente car elle constitue une garantie contre le risque de commercialisation des données et assure aux citoyens la gratuité des dispositifs mis en place ainsi que la protection de leurs données personnelles.

Cette préoccupation a également été largement partagée par les contributeurs de la consultation en ligne de l'Assemblée nationale sur l'identité numérique, pour lesquels l'État doit s'engager à ce que les données personnelles liées à l'identité numérique ne soient ni exploitées à d'autres fins que l'authentification, ni revendues.

La mise en place d'un écosystème déjà fonctionnel, depuis le développement de FranceConnect en 2016, permet également d'encourager ces usages.

---

(1) Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

(2) Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

(3) Direction interministérielle de la transformation publique, Usages de l'identité numérique sécurisée, *juillet 2019.*

B. UN POINT D'APPUI SOLIDE : LE DISPOSITIF FRANCECONNECT, QUI A FACILITÉ L'ACCÈS DES CITOYENS À UN CERTAIN NOMBRE DE SERVICES PUBLICS ET PRIVÉS

1. Un projet de fédérateur d'identité qui a permis d'offrir un accès simplifié aux services publics

FranceConnect est un **système d'identification et d'authentification développé par l'État** et permettant aux citoyens d'utiliser un compte, un identifiant et un mot de passe uniques pour accéder de façon sécurisée à un ensemble de services publics et privés.

Le développement de FranceConnect a débuté au sein de la direction interministérielle à la transformation publique (DITP) en 2014. Ce dispositif a d'abord fait l'objet d'une phase d'expérimentation en 2015, avant d'être déployé auprès de toutes les autorités administratives à partir de juin 2016. Il a enfin été ouvert au secteur privé à partir de 2018 dans certaines conditions (*voir infra*).

L'utilisation de ce service public d'authentification numérique aux services en ligne est gratuite pour les fournisseurs de services, les fournisseurs d'identité et les utilisateurs. Son budget de fonctionnement, qui correspond à 4 millions d'euros par an depuis 2019, est pris en charge par la DINUM.

Le recours à ce service a connu un véritable engouement. Le nombre d'utilisateurs uniques de FranceConnect est ainsi passé de 1 million en 2017 à près de 15 millions à la fin du mois de mars 2020, avec un rythme de croissance actuel important (+ 485 000 utilisateurs par mois en moyenne en 2019). Cette forte croissance est alimentée par l'augmentation du nombre de services en ligne disponibles *via* cet outil, qui est de 700 environ aujourd'hui.

PRINCIPAUX FOURNISSEURS DE SERVICES *VIA* FRANCECONNECT

– Agence nationale des titres sécurisées. – Assurance Retraite. – MSA – Info Retraite. – Impôts.gouv.fr – Ameli. – Démarches liées au permis de conduire	– Retraites et Solidarités (Caisse des dépôts) – Le compter personnel d'activité – Mesdroitssociaux.gouv.fr – ministère de l'éducation nationale. – Agirc-Arrco. – Service-public.fr

Source : DINUM

2. Un fonctionnement simple d'interfaçage entre fournisseur d'identité et fournisseur de services.

FranceConnect est un **fédérateur d'identité**, c'est-à-dire un dispositif qui s'appuie sur les informations communiquées par le fournisseur d'identité de l'utilisateur, pour garantir un accès sécurisé à tous les services des fournisseurs connectés à l'interface.

Le fonctionnement de ce dispositif peut être décomposé **en cinq étapes** :

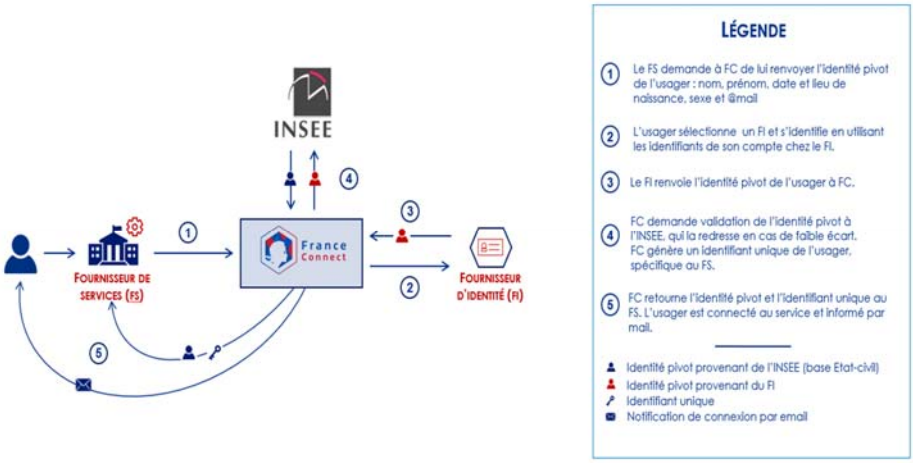
– le fournisseur de services demande à FranceConnect de lui renvoyer l'identité pivot de l'usager ;

– l'usager sélectionne le fournisseur d'identité de son choix et s'identifie en utilisant les identifiants de son compte chez le fournisseur d'identité ;

– le fournisseur d'identité renvoie l'identité pivot de l'usager à FranceConnect ;

– FranceConnect demande validation de l'identité auprès de l'INSEE [(1)], et génère un identifiant unique de l'usager, spécifique au fournisseur de services ;

– FranceConnect retourne l'identité pivot et l'identifiant unique au fournisseur de services. L'usager est connecté au service et informé par mail.



Source : DINUM

3. Un dispositif protecteur pour les données personnelles

a. *FranceConnect : une paroi étanche entre fournisseurs d'identité et fournisseurs de services*

Le positionnement de FranceConnect par rapport aux fournisseurs d'identité et de services constitue une première garantie de protection des données personnelles. FranceConnect assure en effet une couche d'étanchéité en se positionnant entre le fournisseur d'identité et le fournisseur de services. Ceux-ci ne peuvent donc en aucune façon dialoguer entre eux. Cela signifie que le fournisseur

(1) Cette vérification supplémentaire, effectuée au niveau du registre RNIPP de l'INSEE, est réalisée à chaque connexion de l'utilisateur via *FranceConnect afin de s'assurer qu'il s'agit bien d'une personne existante, non décédée, et sans risque d'homonymie.*

d'identité ne sait pas pour quel service il est sollicité et inversement, le fournisseur de services ne connaît pas le fournisseur d'identité utilisé. Il s'agit d'une garantie importante pour s'assurer de la protection de la vie privée des utilisateurs.

b. Des engagements stricts pris par les fournisseurs de services et d'identité

Les fournisseurs de services doivent également s'engager à ne pas commercialiser les données recueillies pour intégrer FranceConnect. Cet engagement figure explicitement dans les conditions générales d'utilisation (1) de ce dispositif. Selon les éléments fournis à la mission par la DINUM, aucun cas de commercialisation de données d'identité fournies par FranceConnect n'a été signalé à ce jour.

Les fournisseurs d'identité doivent pour leur part **remplir les conditions générales d'utilisation de la plateforme FranceConnect (2) et respecter les critères suivants :**

- être responsables des traitements qu'ils opèrent et respecter le RGPD ;
- **ne pas commercialiser les données et ne pas les communiquer à des tiers ;**
- pouvoir retracer l'ensemble des transactions en rapport avec le service et l'utilisateur ;
- être en capacité de collecter les données d'identité de leurs utilisateurs, de les vérifier et de les stocker.

c. Un fonctionnement protecteur des données personnelles

Le fonctionnement même de FranceConnect apporte des garanties complémentaires dans ce domaine. En effet, **FranceConnect ne stocke aucune donnée signifiante** : il assure simplement l'échange des données entre fournisseurs d'identité et de services uniquement pendant la durée de session technique. En conséquence, dès la fin de session, soit par une déconnexion volontaire de l'utilisateur, soit après un délai de 30 minutes sans activité de l'utilisateur, toutes les données d'identité sont supprimées.

FranceConnect s'est construit en outre sur un besoin primordial d'**identifier formellement un utilisateur avec la contrainte forte de ne pas gérer un identifiant unique pour tous ses usages**. Pour un fournisseur de services donné, FranceConnect définit donc par algorithme un identifiant unique non signifiant avec les six données pivots et le transmet au fournisseur de services. L'utilisateur sera

---

(1) Le cahier des charges à respecter par les fournisseurs de services est accessible sur le site partenaire FranceConnect sur le lien https://partenaires.franceconnect.gouv.fr/fcp/fournisseur-service. Il comprend l'ensemble des prérequis techniques, ergonomiques, de sécurité et fonctionnels à respecter. Toute demande de mise en production du dispositif FranceConnect fait l'objet d'une vérification du parcours de connexion par l'équipe FranceConnect qui contrôle également le respect des exigences précisées dans le cahier des charges.

(2) https://partenaires.franceconnect.gouv.fr/files/CGU_FI_v3.3.pdf

identifié de manière distincte pour chaque service en ligne auquel il accède. Cette précaution évite qu'un fraudeur puisse reconstituer l'ensemble des parcours de l'utilisateur.

En outre, depuis décembre 2019, un contrôle de cohérence entre les données demandées par le fournisseur de services et celles réellement consommées par la requête du service en ligne est systématiquement réalisé. L'accès à FranceConnect est bloqué en cas d'incohérence constatée.

Enfin, **l'utilisateur est informé, lors de l'utilisation du service FranceConnect, de la nature des données utilisées dans le cadre du processus d'identification et d'authentification**. Son consentement devrait d'ailleurs être explicitement sollicité *via* une nouvelle fonctionnalité, à la demande de la CNIL et du fonctionnaire de sécurité des systèmes d'information des services du Premier ministre (FSSI), pour le transfert des données nécessaires à l'utilisation des services en ligne pour les fournisseurs de services privés (1).

d. Une conservation des traces techniques à des fins d'audit ou en cas de saisine judiciaire

Néanmoins, il convient de noter qu'un certain nombre d'informations, dites « traces techniques » sont conservées pendant sept ans par FranceConnect à des fins d'audit ou pour répondre à un besoin de saisine judiciaire (2). Celles-ci comprennent des identifiants techniques non signifiants, ainsi que les actions réalisées avec les date et heure. Un accès frauduleux à ces traces ne permet pas de reconstituer les données de l'identité des utilisateurs.

C. ALICEM : UNE EXPÉRIMENTATION UTILE MAIS CONTESTÉE, QUI A PERMIS DE POURSUIVRE LES TRAVAUX SUR L'IDENTITÉ NUMÉRIQUE.

Le développement d'Alicem s'est accompagné de vives inquiétudes portant essentiellement sur le recours à la technologie de la reconnaissance faciale. Même si **la généralisation de cette application encore en phase d'expérimentation**, prévue initialement avant la fin de l'année 2020, **ne semblerait pas confirmée**, Alicem aura permis de développer des technologies innovantes – également appelées « briques technologiques » – qui pourront à l'avenir être réutilisées dans les futures solutions d'identité numérique régalienne, pourvu que les pouvoirs publics tirent pleinement les leçons de cette expérimentation.

---

(1) Elle permettra un affichage dynamique des données transmises au fournisseur de services avec un consentement par l'utilisateur à chaque transaction.

(2) Dans ce dernier cas, seule l'équipe FranceConnect est habilitée à reconstituer l'historique de connexion. En outre, toutes les actions de consultation au système FranceConnect effectuées par l'équipe « interne » sont contrôlées, font l'objet de droit (administrateur) et d'audits.

1. Identité numérique et reconnaissance faciale : les craintes soulevées par Alicem

La technologie de la reconnaissance faciale utilisée par Alicem est contestée sur plusieurs points.

a. Une technologie qui manque encore de maturité

La reconnaissance faciale serait encore insuffisamment mûre. Selon le député Didier Baichère, auteur d'une note de l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST) sur la reconnaissance faciale (1), *« malgré les progrès réalisés au cours des dernières années, les dispositifs de reconnaissance faciale ne sont pas encore parfaitement efficaces. Les conditions d'utilisation ont un véritable impact sur le taux de succès de ces dispositifs. Dans des conditions contrôlées (éclairage, angle de prise de vue, immobilité), comme cela est le cas par exemple pour le dispositif Parafe, le taux de fiabilité peut atteindre des valeurs supérieures à 99,5 %. La situation est toute autre dans des environnements non contrôlés* ».

Lors de son audition par la mission d'information, Mme Sophie Kwasny, directrice de l'unité de protection des données du Conseil de l'Europe (2), a insisté sur **le caractère probabiliste par nature de cette technologie**. Des associations comme la Quadrature du Net et GenerationLibre ont elles aussi fait part des mêmes craintes durant leur audition (3), soulignant que le développement des *deepfakes* (4) pourrait à l'avenir accroître les possibilités de tromper cette technologie.

---

(1) OPECST, La reconnaissance faciale*, note n°14, juillet 2019. Certains facteurs ont en effet des conséquences négatives sur la technologie de la reconnaissance faciale, comme le vieillissement des individus ou la qualité des images collectées.*

(2) Audition par la mission d'information le mercredi 4 mars 2020 – voir la vidéo de l'audition sur le site de l'Assemblée nationale.

(3) Audition par la mission d'information le mardi 4 février 2020 – voir la vidéo de l'audition sur le site de l'Assemblée nationale.

(4) Le deepfake*, ou hypertrucage, est une technique de synthèse d'images fonctionnant grâce à l'intelligence artificielle qui permet par exemple de générer un enregistrement audio ou vidéo altéré, mais néanmoins crédible.*

Authentification et identification faciales

La technologie de la reconnaissance faciale repose sur la vision par ordinateur, qui est un domaine de l'intelligence artificielle consistant à analyser des images de façon automatique. Elle repose sur des techniques dites d'apprentissage profond (*deep learning*).

À partir de la photographie d'un individu, un algorithme en extrait un gabarit, c'est-à-dire une signature propre à chaque visage, et donc à chaque individu, comparée ensuite à partir d'une base de données comprenant plusieurs gabarits.

Lors d'une authentification faciale, on cherche à vérifier si le gabarit en question correspond bien à celui de la personne que l'individu prétend être. Ce gabarit sera donc comparé à celui de cette personne. Il s'agit d'une comparaison dite « 1/1 ».

Lors d'une identification faciale, c'est-à-dire d'une comparaison « 1/n », le gabarit est comparé à l'ensemble de ceux enregistrés dans la base de données afin de déterminer l'identité à laquelle il correspond.

Dans les deux cas, les résultats sont ensuite exprimés en **un pourcentage de correspondance**, les résultats n'étant jamais complètement sûrs.

Alicem n'a pas recours à l'identification faciale, mais uniquement à l'authentification faciale : l'utilisateur doit uniquement démontrer qu'il est bien celui qu'il prétend être.

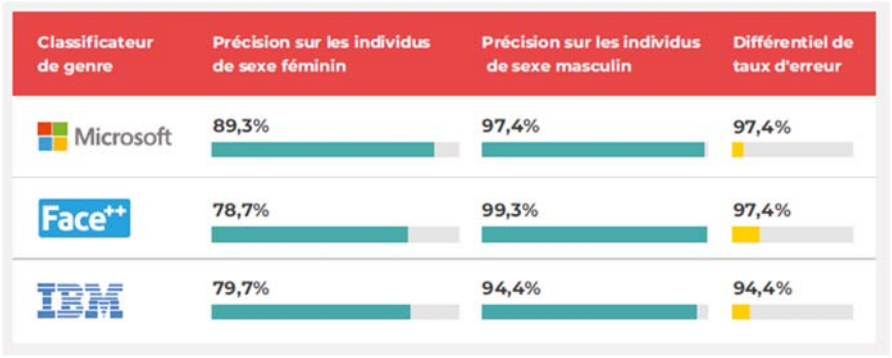
b. L'existence de potentiels biais discriminatoires

La reconnaissance faciale peut également être confrontée à **l'existence de biais discriminatoires, qui entraînent des résultats paradoxaux**. Selon le *think tank* Renaissance numérique, auditionné par la mission d'information (1), « *certaines technologies peuvent induire des biais pouvant provoquer des discriminations racistes, sexistes ou âgistes* » (2). Les bases de données utilisées peuvent en effet sous-représenter certains groupes, par exemple lorsqu'elles contiennent plus d'hommes que de femmes ou plus d'individus à la peau claire. L'étude du projet *Gender shades* de la chercheuse Joy Buolamwini du Massachusetts Institute of Technology, cité par Renaissance numérique, démontre que, pour les trois systèmes de reconnaissance faciale d'IBM, Face++ et Microsoft, le taux d'erreur est de moins de 1 % pour les hommes à peau claire, mais de plus de 20 % pour les femmes à peau sombre (3).

(1) Audition par la mission d'information le mardi 28 janvier 2020 – voir la vidéo de l'audition sur le site de l'Assemblée nationale.

(2) Renaissance numérique, Reconnaissance faciale : porter les valeurs de l'Europe*, juin 2020, p. 5-6.*

(3) L'ensemble des résultats de l'étude sont consultables en ligne sur le site http://gendershades.org/overview.html.



Source : Renaissance numérique, à partir des données consolidées du projet Gender shades

c. Deux inquiétudes limitées pour ce qui concerne Alicem

Les auditions de MM. Cédric O et Jérôme Letier, directeur de l'Agence nationale des titres sécurisés (1), ainsi que celle de Mme Valérie Peneau, ont permis à la mission de constater que **l'emploi de la reconnaissance faciale est restreint à une étape du processus d'enrôlement**. Comme l'a souligné M. Jérôme Letier, seule la photographie du titre d'identité est comparée aux vidéos « challenge » tournées par l'utilisateur, avant qu'elles ne soient immédiatement supprimées.

Par ailleurs, Alicem n'a pas recours à l'identification faciale, or cette opération est plus « à risque » que l'authentification faciale. Comme l'observe la CNIL, « *d'un point de vue strictement mathématique,* ***les dispositifs reposant sur l'authentification des personnes sont nécessairement plus fiables que ceux visant à identifier les personnes*** *: une comparaison 1/1 est toujours plus aisée et fiable qu'une comparaison 1/n* » (2).

La mission d'information considère que la technologie de la reconnaissance faciale, utilisée dans un cadre d'authentification biométrique, ne pose pas de difficulté particulière. Elle rappelle en outre que le RGPD pose un principe d'interdiction du traitement des données biométriques, sauf exceptions strictes (3). **Ces exceptions doivent être strictement contrôlées par la CNIL dans le cadre d'expérimentations**.

---

(1) Audition par la mission d'information le mercredi 19 février 2020 – voir la vidéo de l'audition sur le site de l'Assemblée nationale.

(2) Contribution écrite de la CNIL. Mme Marie-Laure Denis, présidente de la CNIL, a également été auditionnée par la mission d'information le mercredi 4 mars 2020 – voir la vidéo de l'audition sur le site de l'Assemblée nationale.

(3) Article 9.

2. Les inquiétudes liées au traitement des données personnelles collectées ne semblent pas fondées à ce stade

Au fil de ses auditions, la mission d'information a constaté, auprès de plusieurs personnes et structures auditionnées, **une inquiétude vis-à-vis de la protection des données personnelles collectées**.

Pourtant, **un nombre très restreint de données sont envoyées sur le serveur sécurisé du ministère de l'intérieur lors du processus d'enrôlement**. Ces données concernent, dans l'ordre d'envoi :

– un numéro de téléphone communiqué par l'utilisateur afin de servir d'identifiant lors la connexion à un service *via* FranceConnect ;

– une adresse électronique également transmise par l'utilisateur, afin d'y recevoir une confirmation après chaque demande d'accès auprès de FranceConnect, ainsi qu'un lien pour la suppression de son compte si l'utilisateur en fait la demande *via* le portail internet ;

– le numéro du titre – passeport ou titre de séjour – afin de vérifier dans la base DOCVERIF (1) l'authenticité et la validité du titre ;

– la photographie de l'utilisateur, extraite de la puce du titre lors de la lecture NFC ;

– la vidéo des « challenges » réalisée par l'utilisateur.

Ces deux derniers éléments sont comparés entre eux pour vérifier que l'utilisateur est bien le détenteur du titre, puis effacés quel que soit le résultat de la vérification.

Les autres données extraites de la puce du titre lors de la lecture NFC (2) restent stockées uniquement sur le *smartphone* de l'utilisateur, sous son contrôle exclusif et protégées par chiffrement. Elles ne sont pas transmises au serveur central sécurisé du ministère de l'intérieur, conformément aux bonnes pratiques de minimisation des données stockées sur des serveurs centraux.

D'autres inquiétudes portent sur **la collecte de données par les entreprises privées pouvant être associées au service d'authentification en ligne**. C'est notamment le cas de l'association *None of your business*, dont les représentants craignent que ces entreprises puissent exploiter les données personnelles récoltées dans le cadre de l'utilisation d'Alicem, occasionnant une confusion sur les finalités de traitement de ces données.

---

(1) DOCVERIF est un système de traitement automatisé des données à caractère personnel dont le fonctionnement est régi par l'arrêté du 10 août 2016 autorisant la création d'un traitement automatisé de données à caractère personnel dénommé « DOCVERIF », et dont l'objectif est « de faciliter le contrôle de la validité des documents émis par les autorités françaises et de lutter contre l'utilisation indue de tels documents, leur falsification ou leur contrefaçon » (article 1er).

(2) C'est-à-dire les nom, prénoms, date et lieu de naissance, nationalité, sexe, adresse postale, du porteur, ainsi que la date de délivrance du titre.

La mission d'information relève que **le décret du 13 mai 2019 autorisant la création d'Alicem encadre strictement les modalités d'association des entreprises privées à ce dispositif**. Ainsi, les données à caractère personnel et les informations susceptibles d'être enregistrées dans le cadre de son utilisation sont strictement limitées (1). Seul un nombre restreint de données peut être transmis à des entreprises privées, sous réserve qu'elles soient fournisseurs de téléservices liés par convention à FranceConnect ou à l'ANTS (2). En outre, les entreprises ne peuvent pas commercialiser les données collectées.

3. Le risque d'exclusion d'une partie de la population

À l'occasion d'une table ronde organisée par la mission d'information (3), l'association Emmaüs Connect, la Croix-Rouge française et la Fondation Petits frères des pauvres ont souligné que les solutions d'identité numérique, si elles sont pratiques et faciles d'accès, peuvent **contribuer à faciliter l'accès aux droits des citoyens**, et donc être **un véritable facteur d'inclusion sociale**.

Toutefois, dans le cadre d'échanges spécifiques concernant l'application Alicem, elles ont également soulevé les risques d'exclusion d'une partie significative de la population, encore coupée du numérique.

Selon la Mission Société Numérique, dont le directeur, M. Pierre-Louis Rolle, a été auditionné par la mission d'information (4), **13 millions de personnes demeurent éloignées du numérique**, c'est-à-dire n'utilisent jamais internet – 6,7 millions de personnes sont dans ce cas – ou l'utilisent peu, ou rencontrent des difficultés dans leur navigation. Cette statistique mériterait néanmoins d'être affinée : un adolescent qui consulte une vidéo sur une plateforme de *streaming*, mais qui ne sait pas rédiger ou envoyer un e-mail, serait par exemple considéré comme une personne éloignée du numérique, ce qui conduit la mission d'information à s'interroger sur la pertinence des critères utilisés.

a. La détention d'un smartphone

L'un des obstacles que pourraient rencontrer les publics les plus précaires dans l'utilisation quotidienne d'Alicem concerne **le recours à un *smartphone***. La moitié du public pris en charge par Emmaüs Connect gagne moins de 500 euros par

---

(1) L'article 7 dresse une liste de données et d'informations susceptibles d'être relevées qui permettent l'identification de l'usager, l'identification du titre détenu par l'usager et les données relatives à l'historique des transactions associées au compte.

(2) L'article 9 dispose que seules les données ci-après peuvent être transmises dans ca cadre : le nom de famille, le cas échéant, le nom d'usage, le(s) prénom(s), la date de naissance, le lieu de naissance, le sexe, l'adresse postale, l'adresse électronique et le numéro d'appel de l'équipement terminal de communications électroniques.

(3) Audition de représentants de l'association Emmaüs Connect, La Croix-Rouge française et la Fondation Petits frères des pauvres par la mission d'information le mercredi 15 janvier 2020.

(4) Audition par la mission d'information le mercredi 19 février 2020 – voir la vidéo de l'audition sur le site de l'Assemblée nationale.

mois, selon Mme Charlotte Bougenaux et M. Tom-Louis Teboul, qui représentaient l'association durant son audition par la mission d'information.

Le coût d'acquisition d'un *smartphone*, mais aussi celui d'un **forfait téléphonique** et de **l'électricité nécessaire à son fonctionnement** peuvent constituer un frein à l'utilisation du dispositif en l'état.

La mission d'information observe néanmoins que **le nombre de Français détenteurs d'un téléphone portable continue de croître**. Près de 42 millions d'entre eux disposaient d'un terminal mobile en 2018 – contre 38,5 millions en 2017 – et 88 % d'entre eux utilisent internet tous les jours sur leur téléphone [(1)].

b. La détention d'un passeport biométrique

Une autre difficulté spécifique a trait à **la nécessité de détenir un passeport biométrique** afin d'utiliser Alicem. À la différence de la carte nationale d'identité, ce titre d'identité est payant et son coût est assez élevé [(2)], ce qui explique le fait qu'une partie de la population n'en soit pas dotée.

À cet égard, vos rapporteurs relèvent que **la future carte nationale d'identité numérique, qui devrait être déployée à partir de l'été 2021, permettra aux utilisateurs d'Alicem de s'enrôler par le biais de ce titre, dont l'obtention sera gratuite**.

c. La formation au numérique

Des interrogations portant sur **l'accompagnement des personnes les plus éloignées du numérique** se sont également posées, les associations redoutant que ces publics ne bénéficient pas de telles solutions et soient, *in fine*, **victimes de la dématérialisation des services publics**.

Comme l'a résumé Mme Elsa Hajman, responsable du pôle « inclusion et accès aux droits fondamentaux » de la Croix-Rouge française, **ces publics sont donc confrontés à la fois à un frein à l'accès à ces technologies et à un frein à leur utilisation**.

Même si ces préoccupations sont légitimes, la mission d'information tient à rappeler que l'application Alicem a été conçue pour être un fournisseur d'identité parmi d'autres à la disposition des utilisateurs de FranceConnect, et ne représente qu'une modalité d'accès au service public. **Le recours à cette solution n'est donc nullement obligatoire**.

(1) Baromètre annuel 2018 du Marketing Mobile de la Mobile Marketing Association France.

(2) Qu'il s'agisse d'une première demande ou d'un renouvellement, un passeport coûte 86 euros pour une personne majeure, 42 euros pour un mineur de plus de 15 ans et 17 euros pour un mineur de moins de 15 ans.

4. Une suspicion de faillibilité technique

La mission d'information a constaté l'existence de débats relatifs à la sécurisation de l'application. Alors qu'Alicem était encore en phase de préproduction, l'informaticien Baptiste Robert a affirmé, lors de son audition par la mission d'information (1), être parvenu à y accéder à partir des traces publiques laissées par l'expérimentation de l'application, par le biais d'un lien hypertexte accessible par erreur sur un site public. Le site test contenait également une vidéo tutoriel, anonymisée de façon incomplète, ainsi qu'un ensemble d'informations sur Alicem. Il se serait également introduit dans l'application et y aurait découvert l'existence de failles techniques, parmi lesquelles le fait qu'Android, seul système permettant l'exploitation d'Alicem à ce jour, permette de *rooter* un téléphone (2).

Ces éléments ont toutefois été contredits par M. Jérôme Letier, qui a assuré à la mission d'information que rien, ni dans les traces systèmes ou applicatifs, ni dans les publications de M. Baptiste Robert sur son site**,** n'indique que ce dernier aurait réussi à tromper l'application.

Pour mettre un terme à ces interrogations, le ministère de l'Intérieur et l'ANTS prévoient de **recourir à des *hackers* éthiques**, c'est-à-dire à des informaticiens rémunérés pour rechercher les failles de sécurités éventuelles de l'application, afin de vérifier la sécurité de son dispositif. Dans l'hypothèse d'une généralisation, Alicem devrait également faire l'objet d'**une certification par l'ANSSI** afin d'évaluer la conformité de la solution aux exigences réglementaires applicables. **Ces garanties de sécurité doivent être mises en œuvre pour toutes les solutions d'identité numérique qui seront développées.**

5. Le recours à la biométrie pourrait poser une difficulté à l'avenir si la solution ambitionne d'atteindre un niveau de sécurité élevé

Deux avis récents du réseau de coopération eIDAS ont examiné le recours aux technologies biométriques lors de la phase d'authentification des systèmes letton (eParaksts) et belge (Itsme) (3).

Dans les deux cas, **ces avis excluent explicitement les applications d'identité numérique ayant recours à la biométrie pour une authentification de niveau élevé.** Dans sa contribution écrite, la Commission européenne relève ainsi que ces deux pays se sont engagés, « *afin de répondre aux exigences du niveau d'assurance eIDAS élevé, à désactiver l'utilisation de l'authentification biométrique* ».

---

(1) Audition de M. Baptiste Robert par la mission d'information le mercredi 29 janvier 2020.

(2) Le root*, du mot « racine » en anglais, consiste à permettre à l'utilisateur du téléphone d'avoir tous les droits d'accès sur le terminal mobile, et donc d'accéder également aux fichiers situés à la racine du mobile qui lui sont normalement inaccessibles.*

(3) Avis du réseau de coopération eIDAS du 3 octobre 2019, n° 7/201921 et n° 8/201922.

Alors qu'Alicem ou la solution qui la remplacera ambitionne précisément d'offrir un niveau de sécurité substantiel et élevé à l'avenir, cette difficulté supplémentaire devrait être prise en compte par le Gouvernement.

6. Des difficultés relatives au consentement et à l'utilisation de données biométriques selon la CNIL

Dans son avis du 18 octobre 2018 sur le projet de décret autorisant la création d'Alicem [(1)], la CNIL a soulevé deux difficultés liées au traitement des données biométriques et au consentement des utilisateurs d'Alicem, que les pouvoirs publics doivent prendre en compte.

a. Le consentement au traitement des données personnelles ne serait pas libre

La CNIL observe que le ministère de l'intérieur ne propose aujourd'hui **aucune alternative à l'utilisation de la reconnaissance faciale** lors de l'enrôlement.

Après avoir rappelé que l'article 9.1 du RGPD pose **un principe d'interdiction du traitement de certaines données sensibles**, dont les données biométriques, elle précise que cette interdiction peut être écartée au titre de l'article 9.2, notamment lorsque :

– la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques ;

– le traitement est nécessaire pour des motifs d'intérêt public importants.

La CNIL relève que l**e consentement au traitement de ses données personnelles, pour être valable, doit être « *libre, spécifique, éclairé et univoque*, *conformément à l'article 4-11 du RGPD* »**, ce qui implique que l'utilisateur dispose « *d'un contrôle et d'un choix réel concernant l'acceptation ou le refus des conditions proposées ou encore de la possibilité de les refuser sans subir de préjudice* ».

Se référant aux **lignes directrices sur le consentement du Comité européen de la protection des données** [(2)], la Commission rappelle que « *ce consentement n'est libre que si le traitement de ces données est strictement nécessaire à la fourniture du service demandé par la personne, ou si une alternative est effectivement offerte par le responsable de traitement à la personne concernée* ».

---

(1) Délibération n° 2018-342 du 18 octobre 2018 portant avis sur un projet de décret autorisant la création d'un traitement automatisé permettant d'authentifier une identité numérique par voie électronique dénommé « Application de lecture de l'identité d'un citoyen en mobilité » (ALICEM) et modifiant le code de l'entrée et du séjour des étrangers et du droit d'asile (demande d'avis n° 18008244).

(2) Lignes directrices sur le consentement au sens du règlement 2016/679 du groupe de travail « Article 29 » adoptées le 28 novembre 2017, version révisée et adoptée le 10 avril 2018.

En l'espèce, la CNIL estime que « ***le refus du traitement des données biométriques*** **[lors de l'étape de l'enrôlement à Alicem]** ***fait obstacle à l'activation du compte****, et prive de portée le consentement initial à la création du compte. Or, la nécessité de recourir à un dispositif biométrique pour vérifier l'identité d'une personne dans le but d'atteindre le niveau de garantie élevé de l'identité numérique, au sens du règlement e-IDAS, n'a pas été établie, compte tenu notamment de* ***la possibilité de recourir à des dispositifs alternatifs de vérification*** ».

b. Un enjeu particulier en matière de traitement de données biométriques

En plus de l'examen des conditions liées à la validité du consentement, la CNIL rappelle également que le traitement de données biométriques doit en tout état de cause reposer sur « *des motifs d'intérêt public important* [..] », que le ministère de l'intérieur n'aurait ni invoqués, ni démontrés. La commission estime en effet que « *la caractérisation d'un tel motif, tout comme l'appréciation de la nécessité mentionnée au (g) de l'article 9.2. supposeraient en tout état de cause de la part du ministère des éléments de démonstration complémentaires* ».

7. Alors qu'Alicem fait actuellement l'objet d'un recours auprès du Conseil d'État, plusieurs améliorations sont à l'étude pour faire de la solution d'identité numérique de demain une réussite

Alors que l'association la Quadrature du Net a déposé, à l'été 2019, un recours auprès du Conseil d'État contre le décret autorisant la création d'Alicem [(1)], la généralisation d'Alicem pourrait ne pas avoir lieu. Les « briques technologiques » qui auront fait l'objet d'une certification par l'ANSSI, pourraient alors être réutilisées dans un nouveau dispositif, notamment dans le cadre de la mise en service de la carte nationale d'identité électronique à l'été 2021.

La mise en place de nouvelles modalités d'enrôlement pour une solution plus inclusive à terme doit également demeurer au cœur des réflexions des pouvoirs publics.

a. De nouvelles modalités d'enrôlement sont possibles

Dans son avis sur le projet de décret autorisant la création d'Alicem, la CNIL cite plusieurs alternatives à l'enrôlement par reconnaissance faciale, estimant qu'elles « *pourraient notamment prendre la forme d'****un face à face*** *(tel qu'un déplacement en préfecture, en mairie, ou auprès d'un autre service public accueillant directement le public), d'****une vérification manuelle de la vidéo et de la photographie sur le titre*** *(telle qu'un envoi de la vidéo au serveur de l'ANTS et vérification de l'identité opérée par un agent) ou d'****un appel vidéo en direct avec un agent de l'ANTS*** ».

(1) La Quadrature du Net considère, à l'instar de la CNIL, que le consentement des utilisateurs d'Alicem n'est pas libre. Dans un communiqué de presse publié le 17 juillet 2019 sur son site internet, elle estime qu'en « conditionnant la création d'une identité numérique à un traitement de reconnaissance faciale obligatoire, le Gouvernement participe à la banalisation de cette technologie *».*

Qu'il s'agisse d'Alicem ou d'une autre solution déployée ultérieurement, le futur dispositif comporterait, selon Mme Valérie Peneau, plusieurs modalités d'enrôlement. **La reconnaissance faciale demeurerait possible** puisqu'elle constitue un gage de simplicité et de rapidité strictement encadré par les droits européen et français. Toutefois, **une modalité alternative d'enrôlement devrait être proposée aux usagers lors de la récupération de leur future carte nationale d'identité électronique** en mairie, voire *a posteriori*, auprès des maisons France-Services dont le réseau est en cours de déploiement.

b. Une solution plus inclusive à terme

La future solution d'identité numérique devrait également être plus inclusive que ne l'est Alicem à ce stade. Selon Mme Valérie Peneau, elle serait :

– « **multititre** » : elle fonctionnerait tant avec un passeport biométrique qu'avec un titre de séjour, comme c'est déjà le cas d'Alicem, mais serait également compatible avec la future carte nationale d'identité électronique ;

– « **multisupport** » : il serait possible d'utiliser cette solution à la fois sur *smartphone* puis, à terme, sur ordinateur ;

– « **multisystème d'exploitation** » : alors qu'Alicem n'est aujourd'hui compatible qu'avec le système d'exploitation Android, des négociations sont en cours avec Apple pour que la future solution d'identité numérique puisse également être compatible avec le système iOS.

c. Un bilan public d'Alicem est souhaitable

Face aux inquiétudes, il est nécessaire de réaliser un bilan public d'Alicem, pour en tirer toutes les leçons. Les citoyens et les parlementaires doivent disposer du maximum d'information pour garantir la confiance dans le développement de la solution d'identité numérique portée par le Gouvernement.

Recommandation n° 2 : Réaliser un bilan public d'Alicem afin de garantir la confiance dans les solutions d'identité numérique développées par le Gouvernement.

D. UN CADRE EUROPÉEN QUI A FAVORISÉ LE DÉPLOIEMENT D'IDENTITÉS NUMÉRIQUES INTEROPÉRABLES AU SEIN DES ÉTATS MEMBRES, SUIVANT DES MODÈLES DIFFÉRENTS

1. Le droit européen

a. Le règlement eIDAS a permis de donner « un coup d'accélérateur » au déploiement dans l'Union européenne de systèmes interopérables d'identité numérique

i. Un effort d'harmonisation important dans un contexte de développement du marché de l'identité numérique

Comme le relève la direction générale des réseaux de communication, du contenu et des technologies (DG Connect) dans sa contribution écrite adressée à la mission, l'identité numérique devient, dans une économie hyper connectée, de plus en plus « ***un catalyseur essentiel des transactions numériques*** » car « *la nécessité de pouvoir établir des identités individuelles de manière unique, précise, rapide et sécurisée s'étend désormais aux personnes, aux entités juridiques, aux machines et aux appareils connectés. Dans le même temps, la fourniture d'une identité numérique subit des changements fondamentaux, puisque des entités telles que les banques, les fournisseurs de services de communications électroniques ou les principales plateformes en ligne agissent de plus en plus comme fournisseurs d'identité* ».

Face à ce constat, l'Europe a innové en 2014 en adoptant le règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, qui abroge la directive 1999/93/CE. Ce règlement, entré en vigueur le 17 septembre 2014, est applicable depuis le 1er juillet 2016 pour la majeure partie de ses dispositions. La **reconnaissance mutuelle** par les États membres des moyens d'identification électronique est obligatoire depuis le 29 septembre 2018.

Le règlement eIDAS a trois objectifs principaux :

– assurer l'interopérabilité de l'identité numérique sur le marché unique ;

– renforcer le niveau de sécurité des transactions numériques ;

– garantir la fourniture d'une identité numérique à l'ensemble des citoyens européens.

ii. Des définitions et un cadre d'interopérabilité communs aux pays de l'UE

Le règlement eIDAS s'applique à l'identification électronique, aux services de confiance et aux documents électroniques.

En l'absence d'une définition unique de l'identité numérique en Europe, il vise à proposer un cadre commun, notamment *via* **des définitions communes relatives à l'identification et l'authentification électroniques**. Il établit également **un cadre d'interopérabilité** pour les différents systèmes mis en place au sein des États membres (on parle de « nœud eIDAS »), afin de promouvoir le développement d'un marché de la confiance numérique.

Enfin, ce règlement a également pour objectif d'**instaurer un cadre juridique pour l'utilisation des services de confiance**. Il prévoit des exigences pour les services de confiance relatifs à la signature électronique, au cachet électronique, à l'horodatage électronique, à l'envoi recommandé électronique et à l'authentification de sites internet.

i. Les trois niveaux d'assurance eIDAS

L'article 8 du règlement eIDAS introduit ainsi plusieurs niveaux d'assurance (faible, substantiel, élevé), qui sont précisés dans l'acte d'exécution correspondant, à savoir le règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 définissant les spécifications et procédures techniques minimales pour les trois niveaux d'assurance considérés à l'art. 8 du règlement eIDAS (« faible », « substantiel », « élevé »). Ces niveaux d'assurance déterminent les spécifications techniques, normes et procédures minimales pour garantir l'interopérabilité, la fiabilité et la qualité des éléments composant un système d'identité numérique.

Ces trois niveaux d'assurance sont les suivants :

– le niveau « faible » nécessite que le schéma d'identification électronique utilise **au moins un facteur d'authentification**, par exemple le nom d'utilisateur et le mot de passe ;

– le niveau « substantiel » exige que le système d'identification électronique utilise **au moins deux facteurs d'authentification**. Pour rappel, il existe au total trois facteurs différents pour l'authentification, à savoir « quelque chose que vous êtes », « quelque chose que vous avez » et « quelque chose que vous savez ». L'authentification à deux facteurs nécessite donc deux facteurs d'authentification distincts tels que « quelque chose que vous avez » (par exemple, un appareil mobile) et « quelque chose que vous savez » (par exemple, un code PIN). Un exemple de mécanisme d'authentification fournissant un niveau d'assurance substantiel est un mot de passe à usage unique ;

– le niveau « élevé », enfin, nécessite des moyens pour protéger le schéma d'identification électronique contre la duplication et la falsification, soit une authentification multi-facteurs, le stockage des données ou des clés privées sur des jetons matériels inviolables et une protection cryptographique des informations d'identification personnelle. Un exemple de mécanisme de

niveau d'assurance élevé est un schéma d'authentification basé sur PKI (infrastructure à clé publique) avec une carte à puce et un code PIN.

Lorsque les moyens d'identification électronique délivrés dans le cadre d'un schéma d'identification électronique notifié répondent à une exigence énoncée pour un niveau de garantie plus élevé, ils sont réputés respecter l'exigence équivalente d'un niveau de garantie inférieur.

LES DIFFÉRENTS NIVEAUX DE GARANTIE DU RÈGLEMENT eIDAS

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

Source : Chaire Valeurs et Politiques des Information Personnelles, Cahier n° 1 Identités numériques *coordonné par Claire Levallois-Barth, mars 2016.*

ii. Un principe fondamental : la neutralité technologique

Le règlement eIDAS est technologiquement neutre, c'est-à-dire qu'il ne prend pas position sur les choix technologiques opérés par les États pour mettre en place un parcours d'identité numérique.

Historiquement, les États membres ont principalement choisi des systèmes d'identité électronique basés sur des cartes exigeant des lecteurs de cartes afin de donner accès aux services publics à leurs citoyens. Cependant, soucieux d'améliorer le confort d'utilisation et de sécuriser davantage l'identification, **les États membres et les fournisseurs d'identité ont plutôt tendance désormais à se tourner vers des solutions basées sur le mobile pour refléter la pénétration croissante du mobile et l'augmentation des transactions mobiles en Europe** (1)**.** Ces moyens d'identification peuvent s'appuyer sur des applications logicielles mais également sur des composants matériels intégrés tels que les cartes SIM, les éléments sécurisés (*Secure Element*) et sur l'environnement d'exécution fiable (*Trusted Execution Environment*) afin d'accroître la protection assurée à l'utilisateur.

(1) Ce changement se reflète clairement dans les derniers systèmes notifiés pour lesquels davantage de moyens eID incluent l'utilisation de smartphones *reposant sur diverses technologies - le système letton eParaksts, le système portugais* Chave Móvel Digital*, le belge FAS / itsme eID, le danois NemID et certains moyens délivrés sous le SPID italien ou le eHerkenning néerlandais pour les personnes morales.*

b. Le règlement du 20 juin 2019 relatif à la sécurité des cartes nationales d'identité des citoyens de l'UE a accru l'exigence de robustesse des titres d'identité dans l'UE

Ce règlement a pour objectif de re**nforcer les normes de sécurité applicables aux cartes d'identité** délivrées par les États membres à leurs ressortissants et aux documents de séjour délivrés par les États membres aux citoyens de l'Union et aux membres de leur famille lorsqu'ils exercent leur droit à la libre circulation (article 1er du règlement).

Il prévoit que **les États membres de l'UE ont jusqu'au 2 août 2021 pour intégrer une puce conforme à la norme ICAO dans leur carte d'identité**. À cette occasion, en France, un volet « identité numérique » répondant aux mêmes exigences sera intégré dans la CNIe. Tout citoyen pourra alors, à sa demande, utiliser sa carte d'identité électronique en tant que moyen d'authentification électronique fiable et sécurisé.

Ce règlement indique enfin que « *les cartes d'identité intègrent un support de stockage hautement sécurisé qui contient une image faciale du titulaire de la carte et deux empreintes digitales dans des formats numériques interopérables* » (article 3 du règlement). Il intègre néanmoins fortement la question de la protection des données personnelles, dans ses articles 10 (Recueil d'éléments d'identification biométriques) et 11 (Protection des données personnelles). Au surplus, le considérant 40 du règlement rappelle que le RGPD (*voir infra*) s'applique dans le cadre du présent règlement.

Il ressort donc des articles cités ci-dessus que le règlement 2019/1157 prévoit de solides garanties de protection des données, à savoir :

– le stockage des données biométriques sur le support de stockage de la carte d'identité. Le règlement ne sert donc pas de base juridique pour l'introduction et l'exploitation des bases de données biométriques ;

– l'application du RGPD au traitement des données personnelles aux fins du présent règlement ;

– des règles strictes concernant la collecte d'identifiants biométriques ;

– une protection forte des données biométriques sur le support de stockage selon les dernières normes techniques, similaires à la protection des passeports biométriques.

c. La révision envisagée d'eIDAS devrait conduire à compléter le cadre juridique européen relatif à l'identité numérique et promouvoir peut-être un modèle d'identité numérique publique universelle (eID).

i. Une opportunité pour intégrer les grandes évolutions récentes en matière d'identité numérique et combler les lacunes du texte

Dans sa communication sur l'avenir numérique de l'Europe en date du 19 février dernier, la Commission a annoncé **la révision du règlement eIDAS** en vue d'en améliorer l'efficacité, d'étendre ses avantages au secteur privé et de promouvoir une identité numérique fiable pour tous les Européens.

Cette révision est portée par le constat selon lequel, malgré les avancées incontestables consécutives à eIDAS, **l'identité numérique reste encore parcellaire et dispersée entre de nombreux comptes et identifiants**. La DG Connect estime, en outre, que « *les lacunes réglementaires dans cet espace compliquent la protection des données personnelles et rendent les menaces de fraude et de cyber-sécurité difficiles à atténuer* ». Elle souhaite également qu'eIDAS joue à l'avenir un rôle essentiel dans la fourniture de services publics numériques focalisés sur l'utilisateur, en particulier à la lumière de la mise en œuvre imminente du règlement sur le portail numérique unique [(1)] et de l'application du principe « dites-le nous une seule fois » [(2)] dans les administrations nationales. **Une reconnaissance transfrontalière accrue et la notification plus rapide des eID publiques par les autres États membres apparaissent donc nécessaires**.

ii. Des axes de réflexion en faveur, notamment, d'un système universel d'identité numérique au profit de tous les citoyens de l'Union européenne.

La DG Connect propose donc de fonder les évolutions réglementaires à venir dans le domaine de l'identité numérique européenne sur les principes directeurs suivants :

– habiliter les citoyens européens à **utiliser les identités numériques de confiance de leur choix** dans toutes les transactions en ligne et à contrôler la divulgation de leurs données d'identité;

---

(1) Règlement (UE) 2018/1724 du Parlement Européen et du Conseil du 2 octobre 2018 établissant un portail numérique unique pour donner accès à des informations, à des procédures et à des services d'assistance et de résolution de problèmes, et modifiant le règlement (UE) n° 1024/2012, https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32018R1724&from=EN.

(2) Décret n° 2019-31 du 18 janvier 2019 relatif aux échanges d'informations et de données entre administrations dans le cadre des démarches administratives et à l'expérimentation prévue par l'article 40 de la loi n° 2018-727 du 10 août 2018 pour un État au service d'une société de confiance. Ce mécanisme vise à développer les échanges de données entre les administrations en permettant à un usager - particulier ou entreprise - entreprenant une démarche administrative de ne pas avoir à fournir certaines informations ou pièces justificatives (revenu fiscal de référence, justificatif d'identité, attestation de droit délivrées par les organismes de sécurité sociale) déjà détenues par l'administration.

– **faciliter la conformité au RGPD** en permettant la limitation de l'objectif, la minimisation de la collecte et de la divulgation des données et l'expression du consentement;

– **étendre la surveillance réglementaire** à la fourniture d'identité par les acteurs du secteur privé, tels que les plateformes en ligne;

– a**ssurer des conditions équitables pour les fournisseurs d'identité numérique** en créant des incitations réglementaires et en mettant en place des exigences de reconnaissance des moyens privés de l'identité numérique;

– **étendre la fourniture d'identités numériques fiables à de nouveaux acteurs** tels que les appareils de l'Internet des objets (IdO) et des agents d'intelligence artificielle ;

– évaluer les possibilités d'**introduire un système universel d'identité numérique** au profit de tous les citoyens de l'Union européenne ;

– mettre en place **un projet d'identité électronique publique universelle acceptée** (eID).

En outre, la Commission a également annoncé dans sa communication sur la stratégie pour une Europe numérique qu'elle envisage d'étendre le cadre eIDAS afin d'introduire de nouveaux services d'identification numérique et de soutenir une identité électronique publique (eID) universellement acceptée, protégeant les données personnelles et applicable à toutes les interactions numériques [(1)]. Elle estime en effet que « *les citoyens devraient aussi avoir la maîtrise de leur identité en ligne, lorsque l'accès à certains services en ligne nécessite une authentification. Une identité électronique publique (eID) universellement reconnue est indispensable pour que les consommateurs puissent accéder à leurs données et utiliser en toute sécurité les produits et services qu'ils recherchent sans devoir recourir pour ce faire à des plateformes tierces et partager inutilement des données personnelles avec celles-ci* ».

d. Un cadre européen de protection des données personnelles qui s'applique à l'identité numérique

La mise en place d'identités numériques régaliennes en Europe **est soumise au respect du droit européen, particulièrement protecteur pour les données personnelles des citoyens**.

Les règles de l'UE en matière de protection des données établissent un cadre de protection élevé des données à caractère personnel, y compris pour le traitement des données biométriques. Ces règles sont édictées respectivement **dans le règlement général sur la protection des données 2016/679 (RGPD), la directive (UE) 2016/680, et le Règlement (UE) 2018/1725.**

---

(1) https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_fr.pdf

i. RGPD et e-*Privacy*: le cadre global de la protection des données personnelles

Le règlement général sur la protection des données (RGDP), entré en vigueur le 25 mai 2018, établit un cadre de protection renforcé des données à caractère personnel directement applicable dans l'ensemble des États membres de l'Union européenne. Son article 9 interdit, en principe, le traitement de données biométriques aux fins d'identifier une personne physique de manière unique, sauf dans des conditions très strictes. En vertu du RGPD, un tel traitement ne peut ainsi avoir lieu **qu'au titre d'un nombre limité de motifs, et notamment lorsqu'il est nécessaire pour des raisons d'intérêt public important**. Dans ce cas, il doit avoir lieu sur la base du droit de l'Union ou du droit d'un État membre, sous réserve des exigences en matière de proportionnalité, de respect du contenu essentiel du droit à la protection des données et de garanties adéquates.

La **directive e-*Privacy*** (1) relative au « traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques » complète ce cadre juridique. **Une proposition de règlement « e-*Privacy* »**, qui vise à renforcer la protection de la vie privée en ligne des citoyens en détaillant le RGPD (***lex specialis***) est par ailleurs en cours de discussion depuis avril 2016.

ii. La directive Police-Justice : un cadre pour les fichiers de police et de justice

En ce qui concerne **le traitement des données à caractère personnel dans les fichiers de police et de justice**, le régime applicable à ces fichiers est fixé par la directive (UE) 2016/680. De manière similaire au RGPD, cette directive prévoit, en son article 10, une interdiction de principe des traitements portant sur des catégories particulières de données à caractère personnel, dont les traitements de données biométriques aux fins d'identifier une personne de manière unique. Ces traitements ne sont **autorisés qu'en cas de nécessité absolue**, sous réserve de garanties appropriées pour les droits et libertés de la personne concernée, lorsqu'ils sont autorisés par le droit de l'Union ou le droit d'un État membre, pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique, ou encore lorsque le traitement porte sur des données manifestement rendues publiques par la personne concernée.

(1) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. Elle a été actualisée en 2009 par la directive 009/136/CE, également appelée « Directive Cookie ».

iii. La charte des droits fondamentaux et un règlement spécifique pour le traitement des données personnelles des personnes physiques complètent ce cadre juridique

Les articles 7 et 8 de la charte des droits fondamentaux de l'UE font du respect de la vie privée et de la protection des données à caractère personnel des droits fondamentaux. En outre, les institutions, organes et organismes de l'Union sont soumis à des règles similaires au RGPD pour le traitement de données biométriques, édictées à l'article 10 du règlement (UE) 2018/1725.

2. Plusieurs exemples étrangers pourraient inspirer les pouvoirs publics français

La mission d'information a souhaité solliciter les pays les plus avancés sur la question de l'identité numérique en Europe. Elle a donc adressé un questionnaire à une dizaine de pays européens, par l'intermédiaire du centre européen de recherche documentaire parlementaire (CERDP), réseau documentaire cogéré par l'Union européenne et le Conseil de l'Europe, qui permet un partage d'informations entre les Parlements.

Les éléments ci-après s'inspirent des réponses communiquées par les Parlements étrangers, ainsi que du *benchmark* de l'étude de mai 2019 de la direction interministérielle de la transformation publique concernant les usages de l'identité numérique (1) et des propos tenus lors de la table ronde de représentants d'ambassades étrangères en France organisée en mars 2020 par la mission d'information (2).

a. Des dispositifs d'identité numérique ont été mis en place dans plusieurs États européens

En Allemagne, **il est possible de s'authentifier en ligne à partir d'une carte d'identité électronique,** déployée depuis 2010. Si l'utilisation de cette carte est obligatoire, la fonction e-ID qu'elle offre aux ressortissants allemands était facultative et activée seulement à la demande du citoyen jusqu'en 2017. Elle est désormais systématique, sauf pour les mineurs de moins de seize ans qui peuvent bénéficier d'un titre ne disposant pas de cette fonctionnalité. La solution a fait l'objet d'une notification dans le cadre du règlement eIDAS en 2017, pour un niveau de sécurité élevé.

---

(1) Direction interministérielle de la transformation publique, Usages de l'identité numérique sécurisée*, juillet 2019.*

(2) Audition par la mission d'information de Mme Kristel-Amelie Aimre, conseillère chargée des affaires économiques à l'ambassade d'Estonie en France, de M. Tore Keller, conseiller chargé des affaires politiques et économiques à l'ambassade du Danemark en France, et de MM. Thierry de Grunne, conseiller au cabinet du ministre de la sécurité et de l'intérieur de Belgique, et Bart Vrancken, chef de service de la transformation digitale et innovation du service public fédéral belge de l'intérieur le mercredi 4 mars 2020 – voir la vidéo de l'audition sur le site de l'Assemblée nationale.

La Belgique a également choisi d'asseoir sa solution d'identité numérique sur un support physique régalien. Dès 2004, une carte d'identité électronique obligatoire a été délivrée à chaque citoyen. En cinq ans, la Belgique est parvenue à doter 100 % de sa population de ce nouvel outil, qui contient une puce intégrant deux certificats : l'un permettant l'authentification en ligne, l'autre permettant l'apposition de la signature électronique de son détenteur. Ce dispositif a lui aussi été notifié dans le cadre du règlement eIDAS l'an dernier pour un niveau de sécurité élevé.

Le Danemark a développé un système différent, reposant depuis 2010 sur un dispositif, NemID, fruit d'une coopération entre l'*IT-og Telestyrelsen* (l'agence nationale des technologies de l'information et des télécoms) et le secteur bancaire, qui consiste en une carte contenant une série de codes à usage unique. Un nouveau dispositif, MitID, va remplacer NemID à partir de 2021 afin de faciliter les usages privés – qui sont aujourd'hui distincts des usages publics dans l'infrastructure de NemID. À l'instar d'Alicem en France, cette solution serait accessible uniquement par l'intermédiaire d'un *smartphone* – ce qui est déjà une modalité d'utilisation de NemID. NemID a fait l'objet d'une notification dans le cadre du règlement eIDAS en avril 2020, pour un niveau de sécurité modéré.

Le Royaume-Uni a développé un système semblable à celui de FranceConnect, qui n'est pas assis sur un support physique, mais repose depuis 2016 sur l'inscription de l'utilisateur sur la *e*-plateforme Gov.UK Verify, développée par les services du Gouvernement. Pour s'authentifier en ligne, l'utilisateur inscrit sur la plateforme a le choix entre cinq fournisseurs d'identité privés. En fonction du fournisseur qu'il choisit, il devra donner des éléments différents – numéro de permis de conduire, de passeport, facture téléphonique… Gov.UK Verify a été notifié dans le cadre du règlement eIDAS et permet de s'authentifier avec un niveau de sécurité similaire à celui de la solution allemande.

En Suisse, il existait déjà, en 2019, une pluralité d'offres privées d'identité numérique aux modalités d'enrôlement et d'utilisation différentes – *via* un ordinateur ou sur mobile, par le biais d'une offre gratuite ou payante. Depuis l'adoption de la **loi fédérale sur les services d'identification électronique**, l'État est chargé de la mise en place et du respect du cadre légal de l'identité numérique, tandis que les acteurs privés sont responsables de la mise à disposition des solutions techniques d'authentification. Le **dispositif Swiss ID**, principale solution d'identité numérique à ce jour avec 500 000 utilisateurs en 2019 – mais 4 millions anticipés en fin d'année – ambitionne de proposer à terme une identité numérique certifiée par l'État.

En Estonie, une identité numérique certifiée existe également depuis 2002 et la mise en service de la carte nationale d'identité électronique estonienne, qui est un document d'identité obligatoire. Comme en Belgique, cette carte contient une puce sécurisée au sein de laquelle sont insérés deux certificats, l'un pour l'authentification en ligne, l'autre pour la signature électronique. À partir de 2007, une solution sur mobile a également été développée par l'État avec les opérateurs

de télécom. Ces deux solutions réalisées en partenariat avec les pouvoirs publics et les acteurs privés, ont fait l'objet d'une notification dans le cadre du règlement eIDAS et permettent une authentification de niveaux substantiel à élevé.

b. Des processus d'enrôlement différents, qui expliquent pour partie les succès ou les échecs des solutions étrangères

La procédure d'enrôlement allemande est particulièrement longue, mais elle garantit ainsi une sécurité élevée lors de l'authentification. L'utilisateur doit d'abord faire une demande de carte d'identité électronique. Sa réception s'accompagne de l'envoi d'un courrier contenant un code PIN à cinq chiffres. Si le téléphone de l'utilisateur n'est pas équipé de la technologie NFC, l'installation d'un lecteur de carte fonctionnant avec son ordinateur est nécessaire. Un programme spécifique doit également être installé sur l'ordinateur ou sur le *smartphone* de l'utilisateur. Lors de l'authentification en ligne, l'utilisateur doit ouvrir ce programme et insérer son code PIN à cinq chiffres, qui est alors converti en un code PIN à six chiffres. Il sélectionne ensuite le fournisseur de services auprès duquel il souhaite s'authentifier – lequel a été en amont approuvé par le programme – et renseigne à cette fin son code PIN à six chiffres. C'est uniquement après cette étape que l'utilisateur peut s'authentifier par le biais de sa carte d'identité.

À l'inverse, **l'enrôlement et l'utilisation du dispositif danois NemID sont plus simples**. Le compte NemID consiste en un nom d'utilisateur et un mot de passe définis par l'utilisateur lors de sa première connexion, ainsi qu'une carte contenant des codes à usage unique – ou, depuis récemment, une application mobile générant des codes aléatoires. Lorsque l'utilisateur se connecte sur le portail de NemID – ou, depuis 2018, lorsqu'il utilise l'application en ligne –, il entre d'abord son nom d'utilisateur puis son mot de passe, et inscrit ensuite un code. **Cette simplicité traduit toutefois une sécurité moindre de l'authentification**.

Au Royaume-Uni, l'enrôlement pour utiliser la plateforme Gov.UK Verify se singularise par sa pluralité, l'utilisateur disposant de cinq fournisseurs d'identité différents proposant chacun des modalités d'enrôlement distinctes. Pour s'inscrire, il doit d'abord répondre à plusieurs questions censées l'orienter vers l'un des fournisseurs d'identité – a-t-il plus de 20 ans ? A-t-il vécu au Royaume-Uni durant les 12 derniers mois ? Dispose-t-il d'un permis de conduire ou d'un passeport britannique ? Peut-il installer Verify sur son téléphone ? En fonction de ses réponses, un ou plusieurs fournisseurs d'identité lui sont proposés.

La solution suisse Swiss ID propose un enrôlement très simple. Le dispositif prend la forme d'une clé numérique personnelle, par le biais d'un *login* unique permettant une authentification univoque lors de transactions en ligne. L'utilisateur doit se créer un compte SwissID – une procédure qui ne prend que quelques minutes – par le biais d'un e-mail, voire d'un numéro de téléphone portable s'il souhaite bénéficier d'une authentification à double facteur.

Une fois son compte créé, l'utilisateur peut renseigner davantage de données personnelles le concernant – comme son adresse et sa langue de correspondance et décider de créer ou non son identité certifiée (1). Les utilisateurs choisissent à quels services en ligne ils donnent l'accès à leurs données et peuvent révoquer cet accès à tout moment *via* leur espace personnel SwissID. Les données personnelles recueillies pour procéder à l'authentification en ligne sont cryptées, hébergées en Suisse et ne sont pas utilisées à des fins commerciales.

c. Le recours à la reconnaissance faciale : une exception à la règle

Dans le cadre des réponses des parlements européens au questionnaire de la mission d'information, **aucun pays n'a fait part du recours à la technologie de la reconnaissance faciale** pour permettre l'authentification en ligne, dans le cadre du règlement eIDAS.

Dans sa contribution écrite aux travaux de la mission d'information, la Commission européenne relève d'ailleurs qu'« *aucun dispositif notifié à ce jour dans le cadre du règlement eIDAS ne fait recours à la reconnaissance faciale automatique lors de la phase de l'enrôlement* ». Toutefois, « *le recours à la reconnaissance faciale automatique était envisagé au Royaume-Uni où un des fournisseurs d'identité, SecureIdentity, déploie cette technologie pour d'autres applications. Ce système n'a pourtant pas été notifié* ».

La solution estonienne Smart-ID, alternative à la carte d'identité électronique estonienne et à Mobile-ID créée en 2017 par le secteur privé, peut néanmoins être comparée à Alicem puisqu'elle a également recours à l'authentification faciale lors du processus d'enrôlement. Smart-ID compare ainsi le visage de l'utilisateur depuis son *smartphone* ou sa tablette avec la photographie de son passeport, seul titre d'identité pouvant à ce jour fonctionner avec cette solution. Smart-ID n'a néanmoins pas fait l'objet d'une certification dans le cadre du règlement eIDAS à ce jour.

d. Le coût de ces solutions

La solution allemande a un coût tant pour les particuliers que pour les fournisseurs de services. Les premiers doivent s'acquitter des frais d'acquisition de la carte d'identité, qu'ils utilisent ou non la fonction *e*-ID permise par ce support (2).

---

(1) Il est possible d'obtenir une identité certifiée via *l'application SwissID App. Une fois téléchargée, l'application invite à scanner un document d'identité valide (passeports ou CNI suisse, allemande et portugaise) et à enregistrer une vidéo du visage de l'utilisateur. Les données sont ensuite vérifiées par le service et l'utilisateur est averti par e-mail lorsque la vérification a abouti. Une expérimentation est également en cours dans plusieurs cantons afin de permettre aux utilisateurs d'obtenir une vérification d'identité auprès d'une administration communale ou municipale. L'utilisateur doit d'abord imprimer un formulaire* via *son compte personnel SwissID, puis faire établir une photocopie certifiée authentique d'un document d'identité auprès d'une administration. Le formulaire complété et la copie certifiée sont transmis à SwissSign Group pour une vérification. À l'issue de cette vérification, l'identité vérifiée est ajoutée au compte SwissID.*

(2) Ces frais s'élèvent à 52,80 euros pour les ressortissants âgés entre 18 et 24 ans et à 58,80 euros pour les autres.

L'utilisateur doit en outre supporter des coûts d'acquisition d'un lecteur de carte à puce, même si les derniers *smartphone*s équipés d'une puce NFC permettent désormais de se passer de ce dispositif. Les fournisseurs de services doivent s'acquitter d'un certificat d'autorisation pour utiliser la fonction d'authentification en ligne, dont les coûts s'élèvent entre 80 et 115 euros.

Le coût de la CNIe en Belgique est plus raisonnable puisqu'il s'élève à une vingtaine d'euros pour les adultes, voire à 10 euros pour les cartes à destination des enfants de moins de douze ans.

En Suisse, alors que la solution SwissID est gratuite, SuisseID était un dispositif payant, ce qui a sûrement contribué à en réduire l'usage. Il ne comptait que 30 000 utilisateurs fin 2019, date à laquelle le dispositif a été mis à l'arrêt. La même année, l'alternative gratuite SwissID comptait 500 000 utilisateurs, ce qui reste néanmoins assez peu pour un pays de 8,4 millions d'habitants.

e. Les services accessibles

i. En Allemagne, en Belgique et en Suisse, des solutions qui peinent à attirer les usages

La procédure d'enrôlement allemande, ainsi que le coût de la solution, n'encouragent pas à un usage massif du service d'authentification en ligne. Les fournisseurs privés et publics de services peuvent utiliser l'identité numérique fournie par l'État, mais elle est principalement sollicitée par les usagers dans leurs relations avec l'administration. En 2017, 2**20 services étaient fournis par 110 fournisseurs**, dont 40 % de fournisseurs publics et 60 % de fournisseurs privés. Seulement 17 millions de cartes disposaient d'une fonction e-ID active, contre 51 millions de titres d'identité en circulation la même année.

Toutefois, la procédure par laquelle les prestataires de services – entreprises et autorités publiques – sont autorisés à lire les données de l'e-ID a été simplifiée récemment et **depuis 2017, les pouvoirs publics ambitionnent de dématérialiser l'ensemble des services administratifs en 2022**, ce qui devrait inciter davantage les citoyens allemands à utiliser ce dispositif.

En Belgique, la solution d'identité numérique régalienne permet d'utiliser **22 services en ligne**, dont trois sont particulièrement plébiscités :

– le service d'impôt en ligne, *Tax-on-web*, qui comptabilisait 6 millions d'utilisateurs en 2018 (pour 11,4 millions d'habitants) ;

– le portail de suivi des dossiers de pension, *Mypension* ;

– *E-Birth*, qui permet à un prestataire de soin de notifier électroniquement une naissance à l'état civil de la commune concernée.

Certains services en ligne s'adressent aux personnes morales, à l'instar de E-greffe qui permet de déposer un dossier de création d'entreprise ou d'association en ligne, et Finprof qui permet de transmettre à l'administration concernée les déclarations du précompte professionnel.

Au Danemark, où la solution NemID est très utilisée, il est possible d'accéder à la quasi-totalité des services de l'administration, mais également à des services privés tels que les banques et les assurances. Au total, **plus de 700 services sont accessibles par cette solution**, utilisée par plus de 5 millions de Danois – pour une population de 5,75 millions d'habitants.

En Suisse, dans le cadre du développement d'une identité numérique certifiée par l'État d'ici la fin de l'année 2020, plusieurs usages à fort potentiel ont été identifiés. Ils concernent la cyberdémocratie, l'accès aux services publics dématérialisés et aux ressources scolaires, ainsi que les usages privés – *e*-commerce, accès sécurisé au *cloud* – et la signature électronique certifiée.

ii. Au Royaume-Uni, un usage insatisfaisant du dispositif conduit à sa refondation

Au Royaume-Uni, Gov.UK Verify ne compte que **5,4 millions d'utilisateurs pour une population de plus de 66 millions d'habitants**. Seuls 19 services publics sont accessibles par l'intermédiaire de ce dispositif, alors que le Gouvernement en annonçait 46 en 2018. Parmi ces 19 services, **huit peuvent être sollicités uniquement par l'intermédiaire de la plateforme**, dont l'obtention d'une pension d'État ou d'un crédit universel, ou la signature d'une dette hypothécaire.

Cet échec relatif a contraint le Gouvernement britannique à lancer **un appel à contributions sur le sujet de l'identité numérique en juillet 2019**. Cet appel à contributions, rédigé par le département en charge du numérique, de la culture, des médias et des sports du Bureau du Cabinet, précise notamment que le Gouvernement « *s'engage à mettre en place un système d'identité numérique qui corresponde aux besoins de l'économie digitale du pays* ***sans avoir besoin de recourir aux cartes d'identité****, en travaillant en partenariat avec les services privés et les secteurs associatif, académique et la société civile* ».

À l'issue de cette consultation, le Gouvernement a choisi de **laisser la gestion de ce dispositif aux partenaires privés** à partir de mars 2020.

iii. Dans plusieurs pays européens, des dispositifs privés, plus ergonomiques, font concurrence aux solutions régaliennes

L'une des raisons pouvant expliquer les difficultés rencontrées par la solution régalienne allemande, outre le lancement tardif de son dispositif, est **la concurrence qu'elle rencontre de la part d'autres fournisseurs d'identité publics et privés qui ont développé leur propre solution**. C'est notamment le cas, depuis 2017, de Verimi, une solution alternative privée développée par un

consortium d'entreprises exclusivement pour une utilisation sur mobile, plébiscitée pour son ergonomie et sa simplicité – mais qui n'a pas été notifiée dans le cadre du règlement eIDAS.

En Belgique, le dispositif régalien est concurrencé par une alternative privée, Itsme, développée par un consortium composé de banques et d'opérateurs télécoms et offerte au public depuis 2017. Cette solution fonctionne uniquement par par le biais d'une application mobile en permettant de lier l'identité de son utilisateur à son *smartphone*. Entre mai 2018 et février 2019, elle a enregistré une augmentation du nombre de ses utilisateurs de 114 %. **Itsme peut être utilisé pour accéder aux services publics en ligne ainsi qu'à certains services privés, comme les services bancaires ou les services notariaux**. La solution bénéficie d'une certification dans le cadre du règlement européen eIDAS, pour un niveau de sécurité élevé.

Depuis 2018, **le Danemark** a également choisi de rendre accessible sa solution NemID sur mobile.

En Suisse, la solution MobileID, très populaire, fonctionne également grâce à un *smartphone*. Initiée par les trois plus grands opérateurs télécoms suisses (Swisscom, Sunrise et Salt), elle offre une alternative gratuite adoptée par de nombreuses grandes entreprises et services. Elle est également compatible avec SwissID depuis 2019. Elle peut être utilisée tant pour signer électroniquement un document que pour transmettre de manière sécurisée des données sensibles. Elle permet également à ses utilisateurs de bénéficier d'une identité numérique certifiée.

Disponible directement auprès des opérateurs téléphoniques, **la solution estonienne Mobile-ID**, également accessible en Lituanie et en Azerbaidjan, **permet à l'utilisateur d'accéder à des services du secteur public comme du secteur privé**, de manière sécurisée, simple et rapide, **en utilisant un identifiant personnel et deux codes PIN**. Cette solution certifiée de niveau élevé permet, comme la carte d'identité électronique estonienne, d'accéder à des services bancaires en ligne, de voter électroniquement, de réaliser des démarches administratives numérisées, de naviguer de façon sécurisée sur différents portails numériques, et de signer des documents numériquement et directement depuis un téléphone portable.

Dans sa contribution écrite aux travaux de la mission d'information, la Commission européenne constate d'ailleurs que **les derniers systèmes qui lui ont été notifiés dans le cadre du règlement eIDAS concernent essentiellement des solutions fonctionnant sur mobile**, ce qui reflète la pénétration croissante de l'utilisation des *smartphone*s et des transactions en ligne utilisant ce type de terminal dans l'Union européenne. Selon la Commission, « *les témoignages des acteurs du marché (fournisseurs de services, usagers) ainsi que l'expérience des différents États membres indiquent que l'on s'attend à l'avenir à ce qu'il y ait davantage de systèmes d'identification basés sur les technologies mobiles* » (1).

(1) Contribution écrite de la DG Connect aux travaux de la mission d'information.

C'est d'ailleurs ce constat qui explique que la mission interministérielle française sur l'identité numérique fait du développement d'une solution fonctionnant sur mobile sa priorité.

f. Des conclusions à tirer pour la France : le besoin de solutions ergonomiques, simples et pratiques, utilisables pour de nombreux services

L'étude de ces différents pays souligne tout d'abord que **les utilisateurs plébiscitent les solutions d'identité numérique les plus ergonomiques et les plus simples d'usage**. L'enrôlement et l'utilisation quotidienne de ces solutions doivent demeurer les plus rapides possibles, tout en assurant leur sécurité.

L'association de services publics et privés paraît également une condition de la réussite des dispositifs. À l'inverse, un nombre trop limité de services accessibles par l'identité numérique, surtout lorsque ces services sont uniquement du domaine administratif, n'encourage pas le recours massif à ces solutions.

En outre, **adjoindre une fonction de signature électronique certifiée** semble être un gage de succès. Il convient donc d'ajouter cette possibilité dans le cadre du projet d'identité numérique actuellement en cours de développement.

Recommandation n° 3 : Adjoindre une fonction de signature électronique certifiée au dispositif d'identité numérique en cours de développement.

III. LA FRANCE À L'HEURE DES CHOIX : CONSTRUIRE ENSEMBLE UNE IDENTITÉ NUMÉRIQUE INCLUSIVE

L'identité numérique des Français devra être à la fois moderne, ergonomique, sécurisée, responsabilisante, transparente et rassurante. Pour être acceptée, elle devra s'accompagner d'un effort éducatif important, d'une offre de solutions alternatives pour tous ceux qui ne peuvent ou ne souhaitent pas l'utiliser, et devra s'inscrire dans un modèle économique pertinent qui définisse précisément les rôles de l'État et des acteurs privés.

A. MODERNISER ET SÉCURISER L'IDENTITÉ NUMÉRIQUE DES FRANÇAIS

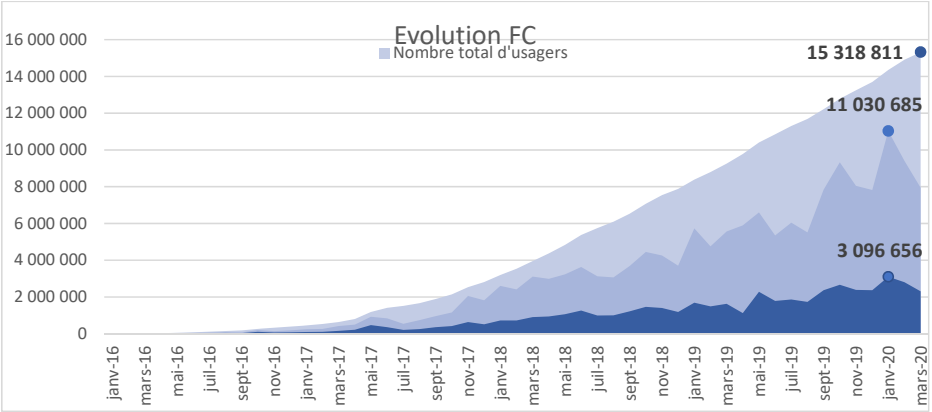
1. Exploiter pleinement les potentialités du programme FranceConnect, tout en maintenant un haut niveau de sécurité et de transparence

a. FranceConnect doit continuer à intégrer de nouveaux services pour faire croître son nombre d'utilisateurs et faciliter le déploiement d'une identité numérique régalienne

FranceConnect s'est construit sur la fédération d'identité permettant d'accéder à un nombre croissant de services publics mais aussi privés. Dans cette logique, le premier comité interministériel de la transformation publique (1er février 2018) avait prévu que, dans un premier temps, FranceConnect intégrerait l'ensemble des services publics lancés en ligne (au 1er avril 2018) avant de s'étendre à l'ensemble des services publics disponibles en ligne (au 31 décembre 2020). En outre, depuis novembre 2018, FranceConnect permet d'accéder à une trentaine de services privés parmi lesquels des banques (BNP Paribas, Boursorama, LCL), des assurances (Generali), des mutuelles (Humanis, Harmonie mutuelle), et des grands facturiers (Enedis, Engie). Enfin, depuis 2019, les ministères sont également encouragés à intégrer FranceConnect sur l'ensemble des démarches les plus utilisées en ligne par les Français (1).

Cette stratégie de déploiement a porté ses fruits, au regard du nombre croissant d'utilisateurs de FranceConnect. On dénombre ainsi désormais plus de 15 millions d'utilisateurs uniques, selon un rythme de croissance très élevé, comme le donne à voir le graphique ci-dessous, fourni par la DINUM.

(1) Le déploiement se poursuit et peut être suivi grâce à un tableau de bord en ligne : https://observatoire.numerique.gouv.fr/.



Évolution du nombre total d'usagers de FranceConnect entre 2016 et 2020

La mission d'information soutient les objectifs fixés pour les prochaines années, qui sont ambitieux, avec une cible à 20 millions d'utilisateurs à la fin de l'année 2020, 25 millions fin 2021 et 30 millions à la fin de 2022. Ce nombre devrait continuer de croître, avec le lancement d'AgentConnect, le déploiement d'AidantsConnect (consécutif à son expérimentation) et enfin l'intégration, au 4ème trimestre 2020, des services de Pôle Emploi, des caisses d'allocation familiales (CAF) et de l'agence centrale des organismes de sécurité sociale (ACOSS).

Le déploiement massif de FranceConnect est un préalable indispensable au succès de la création d'une identité numérique régalienne, qui s'interfacera nécessairement avec ce fédérateur d'identité. Il est d'ailleurs incontestable que le lancement de FranceConnect, en 2016, a d'ores et déjà permis de faire grandir l'écosystème de l'identité numérique, en simplifiant les processus d'identification et d'authentification, en fédérant les premiers fournisseurs d'identité privés existant et en sensibilisant les citoyens à l'utilité de recourir de façon croissante au numérique pour accéder aux services publics.

b. Un haut niveau d'exigence et de sécurité doit néanmoins être maintenu

Il semble néanmoins important de conserver un niveau d'exigence élevé vis-à-vis des fournisseurs d'identité, quant à la protection des données des utilisateurs de FranceConnect. La vérification du respect des conditions strictes de participation des partenaires de FranceConnect (1) doit être poursuivie en toute transparence, pour garantir la confiance que peuvent placer les citoyens au sein de FranceConnect.

(1) Ces derniers doivent s'engager, pour les Fournisseurs d'identité, à respecter le RGPD, à être responsable des traitements qu'ils opèrent, à ne pas commercialiser les données et à ne pas les communiquer à des tiers en dehors des cas prévus par la loi. Ils doivent également pouvoir retracer l'ensemble des transactions en rapport avec le service et l'utilisateur et être en capacité de collecter, vérifier et stocker les données d'identité de leurs utilisateurs.

Recommandation n° 4: Poursuivre l'ouverture de FranceConnect à un nombre croissant de services publics et privés, en continuant de contrôler de façon transparente le respect des conditions générales d'utilisation de la plateforme par ses différents partenaires.

En outre, FranceConnect doit désormais « monter en sécurité » en passant d'un niveau d'assurance faible au sens d'eIDAS, à une certification aux niveaux substantiel et élevé, pour anticiper la montée en charge des exigences de sécurisation des transactions en ligne. La mission d'information observe que le choix stratégique opéré dès le lancement de ce fédérateur d'identité, à savoir ne pas attendre la disponibilité des niveaux substantiel et élevé pour proposer ce service d'interfaçage, a été bénéfique, puisqu'il a permis de constituer une base d'utilisateurs solides, sans laquelle les efforts actuels de déploiement d'une identité numérique régalienne partiraient de zéro. De ce point de vue, la stratégie d'expérimentation et de construction « pas à pas » d'une identité numérique régalienne a porté ses fruits.

Cette montée en sécurisation de FranceConnect est en cours. Les équipes de FranceConnect disposent actuellement d'un échéancier pour acquérir la reconnaissance eIDAS et ciblent une qualification du dispositif FranceConnect auprès de l'ANSSI sur les niveaux de garantie substantiel et élevé au 4ème trimestre 2020, ainsi qu'une certification ISO 27001 du téléservice et du nœud eIDAS français d'ici fin 2020. La notification des schémas d'identification auprès de la Commission européenne devrait ensuite intervenir au 1er trimestre 2021, avec une étape intermédiaire en septembre 2020.

Dans le cadre du déploiement d'une identité numérique régalienne, FranceConnect constitue un point d'appui solide et de confiance pour les utilisateurs. La solution d'identité numérique proposée par l'Etat devra donc être proposée en son sein.

Recommandation n° 5 : Intégrer la solution d'identité numérique régalienne au sein du fédérateur d'identité FranceConnect.

c. Une identité numérique qui doit bénéficier aux publics les plus en difficulté

Dans le cadre du plan national pour un numérique inclusif, présenté en 2018, un outil d'accompagnement des aidants, AidantsConnect, a été mis en place, en lien avec le fédérateur d'identité FranceConnect. Cet outil a été expérimenté au cours de l'année 2019.

Sa conception est née du constat selon lequel certains Français ne sont pas autonomes pour réaliser leurs démarches administratives en ligne, et font appel à des aidants (des travailleurs sociaux ou des agents en mairie) pour bénéficier d'une assistance, voire pour que ces derniers réalisent ces démarches à leur place. Cette pratique pose toutes sortes de difficultés juridiques pour l'aidant

puisqu'elle le conduit à stocker des identifiants et des mots de passe dans des carnets papiers.

AidantsConnect, permet d'offrir **une solution d'accompagnement pour les personnes non autonomes dans leurs démarches numériques**, tout en assurant un cadre juridique sécurisé pour les aidants professionnels qui agissent en ce sens.

Son fonctionnement, relativement simple, comprend les étapes suivantes :

– l'usager se rend dans un lieu d'accompagnement où il rencontre l'aidant ;

– ces deux acteurs définissent ensemble **le périmètre du mandat** donné par la personne aidée (mandant) à l'aidant (mandataire) (1) ;

– l'usager valide son identité *via* FranceConnect et signe le mandat ;

– l'aidant se rend ensuite sur le site de la démarche à effectuer et choisit FranceConnect pour s'identifier. Il choisit ensuite AidantsConnect ;

– il réalise pour le compte de son mandataire les démarches nécessaires, dans les limites du mandat numérique dont il dispose.

Après sa phase d'expérimentation dans une dizaine de territoires, le dispositif AidantsConnect devait être généralisé à compter de juin 2020, notamment au sein des maisons France Services et des lieux de médiation numérique (2).

La crise du coronavirus a pu retarder ce déploiement pour des raisons évidentes. La mission souhaite insister sur **la nécessité de déployer rapidement cette solution indispensable pour de nombreuses personnes, qui continuent de rencontrer des difficultés pour réaliser leurs démarches en ligne et doivent être en conséquence accompagnées** d'une façon souple et sécurisée.

Recommandation n° 6 : Valoriser les retours d'expérience issus des expérimentations d'AidantsConnect et déployer ce service avant la fin de l'année 2020 sur l'ensemble du territoire national. Garantir pour la personne aidée la transparence des décisions prises en son nom par l'aidant.

(1) L'aidant est ainsi connecté sur son compte d'aidant professionnel rattaché à sa structure, et il sélectionne avec l'usager, présent physiquement, un ou plusieurs périmètres de démarches ainsi qu'une durée d'accompagnement. Révocables à tout moment, les mandats peuvent durer d'un jour à un an.

(2) Le ministère de la justice est intéressé par ce dispositif. Néanmoins, pour l'heure, seuls les publics en manque d'équipements ou de compétences, et qui ne sont pas autonomes dans leurs démarches administratives, sont concernés. Un élargissement est toutefois envisagé à destination des détenus et des personnes malades.

d. Maintenir l'interdiction d'utilisation des données personnelles traitées à des fins commerciales, publicitaires ou sécuritaires

Le décret autorisant la création d'Alicem [(1)] instaure **un régime particulièrement strict en matière de collecte et de traitement des données personnelles** [(2)].

Développé pour devenir un fournisseur d'identité dans le cadre de FranceConnect, **Alicem n'a pas connaissance de la nature des services consultés par l'utilisateur qui cherche à s'authentifier**. En outre, **les fournisseurs de service sollicitent uniquement les données dont ils ont besoin pour authentifier l'utilisateur**. FranceConnect assure ainsi, auprès d'Alicem et des autres fournisseurs d'identité fonctionnant avec la plateforme, une divulgation sélective des données personnelles.

Malgré ces précautions, la mission d'information a constaté avec étonnement **la persistance d'une inquiétude** parmi certains acteurs sollicités dans le cadre de ses travaux.

Réaffirmer le principe d'une interdiction de l'utilisation des données personnelles nécessaires à l'authentification en ligne à des fins commerciales, publicitaires ou sécuritaires, paraît donc indispensable.

Recommandation n° 7 : Réaffirmer le principe de l'interdiction de l'utilisation des données personnelles traitées par les solutions d'identité numérique régaliennes à des fins commerciales, publicitaires et sécuritaires posant problème quant à la protection des droits des citoyens, et l'indiquer clairement aux utilisateurs.

2. Proposer une solution souple, sécurisée et de confiance, dérivant de la CNIe

a. La CNIe sera le support de l'identité numérique régalienne des citoyens français

La carte nationale d'identité électronique constituera le vecteur du déploiement d'une solution d'identité numérique régalienne. Conformément au règlement européen du 20 juin 2019 relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des documents de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation, ce titre électronique devra être délivré en France à partir de l'été 2021. **Un déploiement pilote des premières CNIe aura lieu à partir du mois d'avril 2021, avec un premier parcours d'activation et de gestion d'une identité numérique sur mobile**. Cette offre d'identité numérique, disponible d'abord sur

(1) Décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile ».

(2) La combinaison des articles 7 à 11 du décret écarte toute utilisation en dehors du motif pour lequel elles ont été collectées. Comme l'a expliqué M. Jérôme Letier durant son audition, l'essentiel de ces données est conservé dans le téléphone de l'utilisateur. Elles ne sont reliées à aucune base publique ou privée.

Android, sera ensuite **étendue à iOS à la fin de l'année 2021**, **avant qu'un parcours de gestion PC soit mis à la disposition des utilisateurs en 2022.**

Le choix de la CNIe comme support de l'identité numérique régalienne s'explique, selon les responsables du programme France identité numérique, par le souhait de tirer profit du déploiement prochain de ce titre nouveau pour mutualiser les coûts de délivrance. Cette fenêtre d'opportunité apparaît pertinente pour **déployer l'identité numérique de façon attractive et lisible pour les citoyens français**, en associant identité physique et identité numérique. En outre, les caractéristiques matérielles de la future carte (composition en polycarbonate) et l'utilisation de procédés technologiques spécifiques rendent ce titre quasi infalsifiable. Enfin, il apparaît que **l'association d'une carte à puce** (facteur 1 : « ce que je possède »**), et d'un code** (facteur 2 : « ce que je sais ») est un mécanisme familier pour leur futur utilisateur, car **identique à celui des cartes bancaires classiques**.

D'après les informations fournies à la mission, **le coût du système de gestion de l'identité numérique (SGIN), en cours de conception et dont l'appel d'offres n'a pas encore été publié, serait de l'ordre de 35 millions d'euros sur quatre ans, dont 13 millions d'euros sur les deux premières années**. L'essentiel du financement serait supporté par l'agence nationale des titres sécurisés (ANTS). D'autres dépenses s'y ajouteront à partir de 2021, en matière de communication et d'accompagnement au changement, qui pourraient être prises en charge par le fonds de transformation de l'action publique (FTAP).

b. Un fonctionnement simple et intuitif pour l'usager

Cette carte inclura dans une même puce mais au sein de **deux compartiments séparés** deux applications complémentaires mais indépendantes :

– une application « Voyage » stockant les données d'identité alphanumériques mentionnées sur la carte, et les données biométriques (photo et empreintes digitales), ces dernières faisant l'objet d'une protection renforcée, aux termes du règlement européen du 20 juin 2019. Cette partie de la puce ne sera accessible qu'au personnel dûment autorisé des autorités nationales et européennes ;

– une application « Identité numérique » ne stockant que les seules données alphanumériques, qui ne sera accessible que sur présentation d'un code PIN connu du seul usager et ce, si et seulement si, ce dernier a, après avoir téléchargé l'application correspondante (1)**, volontairement finalisé la procédure de création de son identité numérique** (ce qui suppose la vérification de son identité, soit en face à face au moment de la délivrance du titre, soit par reconnaissance faciale).

(1) Dans un premier temps, la solution ne sera proposée que sur mobile, avec une lecture de la puce sans contact. Dans un deuxième temps, pour un public plus large, elle sera accessible sur PC, avec une lecture sans contact, ou en contact avec un lecteur spécifique ou son smartphone.

Une fois cette identité numérique créée, l'usager aura la capacité de s'authentifier en ligne pour accéder de façon sécurisée à un service *via* FranceConnect. En fonction de la sensibilité de l'usage, il devra se servir :

– soit uniquement de son *smartphone* *via* la saisine de son code de sécurité, pour un **niveau dit substantiel**. Ce sera incontestablement l'usage le plus courant pour réaliser la plupart des tâches et/ou accéder à la grande majorité des services ;

– soit de son *smartphone* et de sa carte nationale d'identité électronique, lorsque la sensibilité de la démarche nécessite une **authentification de niveau élevé**. Une lecture sans contact du titre d'identité, *via* la technologie NFC, permettra de vérifier le lien entre le détenteur du *smartphone* et le titre d'identité, *via* l'accès aux données d'identité pivôt présentes au sein de la CNIe.

c. Trois conditions de succès de la CNIe : confiance – simplicité d'usage – déploiement rapide

L'ensemble des auditions réalisées conduit la mission à insister sur trois conditions indispensables pour réussir le déploiement rapide à grande échelle d'une solution d'identité numérique utilisée par les citoyens et les acteurs économiques : la confiance, la simplicité d'usage et des objectifs ambitieux de délivrance de la CNIe.

i. La confiance

La première condition de succès d'une identité numérique régalienne est la confiance. Cette confiance possède un double aspect : il s'agit à la fois d'une garantie de protection des données personnelles, sujet particulièrement sensible dans notre pays, comme l'ont rappelé les débats sur StopCovid pendant le confinement, et d'une lisibilité sur l'intérêt pour le citoyen d'utiliser une identité numérique régalienne. Le citoyen doit avoir confiance tant dans les modalités techniques que dans l'utilité directe, pour lui, de l'identité numérique. Cette confiance ne peut évidemment se construire qu'avec une transparence accrue de la part des acteurs de l'identité numérique et des pouvoirs publics.

Cette confiance nécessite donc, d'abord, un niveau de sécurité élevé en matière de protection des données personnelles contre leur utilisation non désirée qu'il s'agisse d'un usage commercial intempestif ou de pratiques d'usurpation d'identité.

Sur le premier point, les conditions d'usage de FranceConnect, déjà évoquées, apparaissent satisfaisantes, à condition que les pouvoirs publics restent vigilants dans le contrôle strict de leur respect par les fournisseurs d'identité numérique. Une évaluation régulière du respect de ces engagements doit être réalisée et ses résultats publiés en toute transparence. Le risque d'un usage commercial non souhaité des données de l'utilisateur semble donc écarté pour l'heure.

Recommandation n° 8 : Mettre en place des contrôles réguliers du respect des engagements pris par les partenaires de FranceConnect et assurer la publicité de leurs résultats selon une périodicité déterminée.

Sur le second point, c'est-à-dire le risque d'usurpation d'identité, la mission souhaite insister sur le caractère profondément évolutif de la menace cyber, que l'édition 2020 de la revue annuelle de l'ANSSI a d'ailleurs rappelé (1). Comme l'ont ainsi fait valoir les experts auditionnés dans ce domaine, notamment ceux de l'ANSSI et du comité de filière « Industries de sécurité », le maintien de la robustesse cryptographique et applicative est absolument décisif pour garantir la sécurité de l'identité numérique. Il existe actuellement un consensus pour affirmer qu'en l'absence de tests de sécurité réguliers sur la puce de la CNIe, et des mises à jour afférentes, sa qualification renforcée deviendrait nulle au bout d'environ 5 ans. L'impératif d'assurer une protection constante dans la puce, dans un contexte où la durée de validité des titres est importante, doit donc être traité par les pouvoirs publics, avec l'appui des acteurs spécialisés dans ce domaine.

Recommandation n° 9 : Assurer un travail de veille sécuritaire constant sur la carte nationale d'identité électronique, en lien avec les acteurs experts de ce domaine.

Cette confiance, enfin, implique que le Parlement joue pleinement son rôle en matière d'identité numérique (*voir infra*).

ii. La simplicité d'usage

La seconde condition de succès du déploiement d'une identité numérique régalienne réside dans sa simplicité d'usage, c'est-à-dire dans une ergonomie centrée autour de l'expérience de l'utilisateur. Cette simplicité d'usage est plébiscitée par les Français, selon l'étude conduite par la direction interministérielle de la transformation publique sur ce sujet en 2019 (2). Les acteurs estiment, de façon constante, qu'un nombre d'étapes trop important pour l'enrôlement, par exemple (supérieur à 5), est associé avec des courbes d'abandon élevé du processus par l'utilisateur.

La mission note que cette préoccupation a été prise en compte dès le début de la conception des programmes FranceConnect et Alicem, autour de la notion de parcours utilisateur :

– en ce qui concerne FranceConnect, **les partenaires de la plateforme doivent en effet respecter les règles de qualité d'intégration UX (*User Experience* (3))**. Cette vigilance est d'autant plus importante que **la solution d'identité numérique régalienne s'interfaçera nécessairement avec ces fédérateur d'identité**. Il a été indiqué à la mission qu'un UX Designer avait rejoint

(1) Papiers numériques*, revue annuelle de l'ANSSI, 2020.*

(2) DITP, Usages de l'identité numérique sécurisée*, juillet 2019.*

(3) Un guide UX a d'ailleurs été élaboré par les équipes de FranceConnect à cette fin.

l'équipe FranceConnect mi-2019 pour retravailler le parcours utilisateur et que des ateliers avec des utilisateurs et non-utilisateurs avaient eu lieu en 2019. La refonte du parcours utilisateur FranceConnect est en cours pour le simplifier et réduire le nombre d'abandons des parcours des utilisateurs qui se connectent pour la première fois ;

– en ce qui concerne **la solution expérimentale Alicem**, qui n'est pas encore mise à la disposition du public, des tests dit « *friends and family* » ont été conduits pendant l'été 2019, permettant d'intégrer des suggestions d'amélioration de l'ergonomie du parcours utilisateur. Cette dynamique doit être poursuivie.

Pour la solution d'identité numérique régalienne dérivée de la carte nationale d'identité numérique, les responsables du programme France identité numérique ont indiqué à la mission que cet enjeu était au cœur de leurs réflexions. Deux UX designers ont été intégrés au sein de l'équipe de développement dès les premiers mois du projet. Ces derniers ont ainsi « *d'ores et déjà participé à la réflexion sur les parcours d'enrôlement* [(1)]*, sur les usages et les différents publics d'usagers, [et] capitalisé sur le premier retour d'expérience d'Alicem pour améliorer le parcours de cette première solution* » [(2)]. Un nombre restreint d'étapes lors de l'enrôlement reste un objectif prioritaire dans cette optique.

Sur ce sujet, la mission souhaite insister sur la nécessité de garantir une fluidité des « parcours utilisateurs », y compris lorsque ces derniers pourraient être amenés à utiliser différents niveaux d'authentification au sein même de leur parcours. Ce sera le cas, par exemple, lorsqu'un utilisateur, qui s'est authentifié en utilisant FranceConnect et son identité numérique, voudra procéder, sur le site d'un fournisseur de services donné, à une tâche suffisamment sensible pour nécessiter un niveau d'authentification supplémentaire, c'est-à-dire élevé. L'intégration fluide de cette seconde authentification est un enjeu qui doit faire l'objet d'une analyse spécifique pour conserver une dimension ergonomique, en dépit de contraintes de sécurité évidentes.

Recommandation n° 10 : Travailler à l'élaboration de parcours d'identité numérique fluides, à partir de FranceConnect, en particulier dans le cas où un niveau d'authentification supplémentaire est nécessaire pour réaliser, sur le site d'un même fournisseur de services par exemple, une tâche nécessitant un niveau de sécurité plus élevé.

Enfin, il a été indiqué à la mission que **l'appel d'offres relatif à la carte nationale d'identité numérique prévoyait le recours à une méthodologie agile**, intégrant la dimension UX à toutes les étapes de développement (fluidification des parcours et de leurs étapes, meilleure intelligibilité des libellés et textes…). **Le contenu de cet appel d'offres pourrait être examiné par la commission supérieure du numérique et des postes (CSNP).**

(1) L'organisation initialement prévue mi-mars de groupes utilisateurs pour tester la compréhension du parcours en face à face a dû être reportée mais sera reprise dès que possible à la sortie du confinement.

(2) Contribution écrite de Mme Valérie Peneau aux travaux de la mission d'information.

iii. Un déploiement rapide de la CNIe

La rapidité du déploiement du support de l'identité numérique, c'est-à-dire la CNIe, est un élément clef pour s'assurer que la France rattrape son retard dans ce domaine, et stimuler le marché de l'identité numérique.

Le règlement européen laisse à la France dix ans, à compter d'août 2021, pour substituer ce nouveau titre à l'ensemble des cartes d'identité existantes. Les objectifs de déploiement fixés doivent tenir compte de la capacité de production des CNIe, qui sera comprise entre 200 000 et 500 000/mois en phase pilote (mars/avril 2021), pour une volumétrie moyenne de 6,5 millions de cartes par an ensuite. Les acteurs du secteur estiment qu'en rythme maximum, la production pourrait atteindre 9,5 millions de CNIe par an [(1)].

Un déploiement accéléré de la CNIe sur une période de 5 ans apparaît souhaitable afin de favoriser le développement croissant des usages. La mission souhaite insister sur la nécessité de se fixer des objectifs ambitieux dans ce domaine.

Recommandation n° 11 : Fixer des objectifs ambitieux de déploiement de la CNIe, en privilégiant une cible inférieure à 10 ans (4 à 5 ans au maximum) afin de combler le retard français en matière d'identité numérique.

Ce déploiement doit évidemment s'accompagner **d'un effort de communication sur l'identité numérique,** afin de renforcer la visibilité et la compréhension du fonctionnement de FranceConnect, d'abord, et de la future solution d'identité numérique dérivée de la CNIe ensuite.

Recommandation n° 12 : Renforcer la communication au sujet de FranceConnect et de la future solution d'identité numérique régalienne, pour en expliciter l'intérêt pour le citoyen, les garanties et l'ensemble des usages offerts à court et moyen termes.

3. Associer pleinement les collectivités locales à l'identité numérique

Le déploiement d'une identité numérique régalienne en France, qui s'appuiera sur FranceConnect, ne peut être réalisé qu'en lien étroit avec les collectivités territoriales. Ces dernières auront en effet un rôle clef dans la délivrance des CNIe à partir de 2021, et par conséquent de l'identité numérique qui y est associée. Elles auront donc, dans ce cadre, un rôle à jouer dans la pédagogie de proximité auprès des citoyens.

a. Des avantages importants pour les collectivités

La mise en place d'une identité numérique présentera pour elles, par ailleurs, un certain nombre d'avantages. Cette solution devrait leur permettre de réduire leur volume **de courriers papiers et électroniques envoyés, ainsi que les déplacements réalisés par les usagers**. Un impact positif est également envisagé

(1) Audition d'IN Group par la mission d'information le 6 mars 2020.

sur **les tâches de vérification d'identité et de contrôle dont elles peuvent avoir la charge**. Enfin, une identité numérique régalienne permettrait d'envisager la dématérialisation de certaines démarches, de faciliter l'organisation de consultations citoyennes, ou encore de **lutter contre le non-recours aux prestations sociales.**

b. Une meilleure association indispensable pour le succès de l'identité numérique

Les collectivités assurent chacune, dans leur domaine de compétences, des services en ligne de proximité au plus près des usagers. Elles sont ainsi les mieux placées pour obtenir des retours d'expérience et permettre la conception d'outils adaptés aux demandes des citoyens. Elles sont, de plus, fortement impliquées dans le processus de dématérialisation des procédures administratives, avec le programme de développement concerté de l'administration numérique (DCANT), et parties prenantes de la stratégie nationale pour l'inclusion mise en place en 2018.

Les auditions menées par la mission ont néanmoins fait apparaître une certaine déception des collectivités territoriales, qui estiment avoir été insuffisamment associées au projet d'identité numérique régalienne, en dépit de leur souhait fort de participer à des expérimentations. Les acteurs des collectivités ont indiqué regretter, par ailleurs, que le projet d'identité numérique régalienne « *ne soit pensé que sous l'angle des missions tenant aux ministères de l'interieur et de la justice, et non élargi de manière transversale aux domaines de l'éducation, santé et affaires sociales, etc pour élargir l'approche et en faire un véritable outil de l'inclusion* » [(1)]. Ils relèvent également, **qu'au-delà du *smartphone*, les outils supports publics nécessaires pour accéder à cette identité numérique, comme les bornes interactives, doivent être disponibles « *dans l'hyper-proximité* *(la mairie et/ou le buraliste) plutôt que dans des entités plus lointaines comme les maisons France Services, qui ont plus une place de compléments spécialisés* ».** Enfin, les collectivités souhaiteraient être davantage considérées, en particulier les départements, au sujet du déploiement de l'identité numérique dans les collèges (EduConnect) et de la santé (dossier médical partagé, passeport santé).

Recommandation n° 13 : Renforcer l'association des collectivités au projet d'une identité numérique régalienne en leur garantissant un niveau d'information élevé et en les incluant dans la mise en place de la délivrance de cette identité.

La définition précise du rôle de chaque échelon de collectivité par rapport à l'identité numérique est également souhaitable pour créer des synergies. La mise en place d'équipes-projets chargées de favoriser le déploiement de la CNIe et donc de l'identité numérique au sein des territoires apparaît nécessaire.

(1) Contribution écrite de l'Association des départements de France adressée à la mission d'information.

Recommandation n° 14 : Définir précisément, en concertation avec les collectivités, une « feuille de route » pour le déploiement de la CNIe en leur sein, afin de favoriser la création de synergies. Créer un comité de pilotage chargé de coordonner son déploiement, en lien avec les collectivités.

Recommandation n° 15 : Créer des équipes-projets, en lien avec l'équipe centrale, travaillant spécifiquement au déploiement de la CNIe sur le terrain.

Enfin, la mission estime qu'il est important de prendre en compte le besoin de formation à destination des personnes en difficulté avec le numérique. Il doit donc être possible de déployer, en cas de besoin, des formateurs sur l'ensemble du territoire à cette fin, en particulier dans les lieux de délivrance de l'identité numérique.

Recommandation n° 16 : Déployer des formateurs sur l'ensemble du territoire, notamment dans les lieux de délivrance de l'identité numérique.

EduConnect : un service d'authentification dans le domaine de l'éducation

EduConnect est un service d'authentification interfacé avec FranceConnect et ayant vocation à faciliter le suivi, par les parents, de la scolarité de leurs enfants. Il remplace les différents comptes de suivi des résultats scolaires précédemment utilisés par les parents.

L'enrôlement nécessite l'utilisation du numéro de téléphone donné par les parents lors de l'inscription scolaire des enfants.

EduConnect donne accès à un ensemble de services, parmi lesquels les démarches en ligne pour la demande de bourses, la mise à jour de la fiche de renseignements, le livret scolaire unique (LSU) et l'accès à l'espace numérique de travail (ENT).

Actuellement disponible pour les représentants légaux des élèves du CP au CM2, EduConnect devrait être généralisé pour les niveaux (collège et lycée) dans toutes les académies à partir de la rentrée 2020.

Source : ministère de l'éducation nationale.

B. DÉFINIR UN MODÈLE ÉCONOMIQUE PERTINENT DE L'IDENTITÉ NUMÉRIQUE

1. Garantir un large choix de services et de fournisseurs d'identité aux citoyens

Le succès du développement de l'identité numérique repose en grande partie sur **le nombre de services qui seront disponibles pour les citoyens-consommateurs nationaux**. Au-delà des seuls services publics disponibles en ligne, **l'apport du secteur privé est indispensable pour compléter la solution offerte par l'État, et proposer non seulement un accès sécurisé à un nombre croissant de services privé**s (en ce qui concerne les fournisseurs de services), mais aussi **un ensemble d'offres à valeur ajoutée susceptibles de correspondre aux attentes des utilisateurs du côté des fournisseurs d'identité** (coffre-fort numérique par exemple).

Il paraît donc important à la mission de réaffirmer que **la définition du modèle économique doit permettre à l'utilisateur de conserver le choix entre un fournisseur d'identité public et des fournisseurs d'identité privés**. Il s'agit là, en effet, d'un principe de confiance permettant de respecter les préférences de chacun. Afin de ne pas concurrencer l'offre privée, l'identité numérique régalienne doit être considérée comme une brique de niveau supérieur de FranceConnect. Elle ne serait appelée que si nécessaire dans le parcours des opérations de l'utilisateur. Elle serait donc un support « sécuritaire élevé » des offres privées mais n'aurait pas vocation à être utilisée « par défaut » dans les applications où un niveau faible ou substantiel suffit.

Recommandation n° 17 : Favoriser l'apparition d'offres de fournisseurs d'identité privés sur le marché de l'identité numérique, afin de donner le choix aux citoyens dans ce domaine.

Le rôle principal de l'État doit donc être de garantir la sécurité des données d'identité pivot contenues dans les titres d'identité physiques et de permettre leur dérivation par des fournisseurs d'identité privé, en plus des fournisseurs d'identité publics. À cet effet, il a été confirmé à la mission qu'il serait possible de dériver à partir d'une identité numérique régalienne d'autres identités numériques privées, en rebond. La question de l'accès direct de certains fournisseurs d'identité privés, voire de certains fournisseurs de services aux données d'identité numérique peut également être posée, à la stricte condition de respecter le cadre du RGPD et donc le consentement de l'utilisateur.

Le parcours d'identification mis en place doit répondre aux trois attentes principales des acteurs économiques pour être adopté, à savoir :

– une sécurisation accrue, étant donné qu'il s'appuie sur l'identité régalienne ;

– une ouverture réelle, c'est-à-dire qu'il doit permettre la dérivation d'identités de niveau inférieur publiques et privés, sur toutes sortes de supports et adaptées aux différents usages ;

– une interopérabilité, le nœud eIDAS devant permettre son usage dans l'ensemble des pays de l'Union européenne sans difficulté.

Recommandation n° 18 : S'appuyer sur des standards ouverts permettant l'intégration de l'identité numérique régalienne dans les solutions des fournisseurs de services pour faciliter le parcours de l'utilisateur.

2. Une identité numérique gratuite pour les citoyens et les fournisseurs de services publics mais payante pour les acteurs privés

Le déploiement réussi de l'identité numérique régalienne en France implique la gratuité de son usage pour les citoyens, qui refuseront de payer pour un service dont le bénéfice immédiat n'est pas encore complétement intégré. La

mission soutient donc l'idée d'une identité numérique gratuite pour les citoyens et les fournisseurs de services publics.

L'identité numérique régalienne doit néanmoins être payante pour les acteurs privés, afin de permettre la consolidation de l'offre privée dans ce domaine. Une gratuité de l'identité numérique publique pour les fournisseurs de services aurait pour effet de « refermer » le marché pour les fournisseurs d'identité privés. Si une phase de gratuité peut éventuellement être envisagée, il convient néanmoins de réaliser des études sur les risques qu'elle entrainerait vis-à-vis des acteurs privés souhaitant consentir des investissements dans ce domaine et qui pourraient y renoncer. Les acteurs économiques souhaitent que le modèle économique de l'identité numérique repose sur la transaction entre les fournisseurs d'identité et les fournisseurs de services. Il s'agit également d'un enjeu d'innovation et de robustesse, face au risque de défaillance de sécurité d'une solution unique, lequel ne peut jamais être réduit à zéro.

Recommandation n° 19 : Définir un modèle économique garantissant la gratuité de l'usage de l'identité numérique pour les citoyens afin d'assurer son déploiement rapide et massif, mais dans lequel le recours, par des fournisseurs de services, aux solutions régaliennes serait payant, afin de consolider le marché de l'identité numérique.

3. La valorisation des données : une question qui doit être tranchée

La valorisation économique des données d'identité est **une demande qui a été formulée au cours des auditions par un certain nombre d'acteurs économiques**. Elle permettrait selon eux de **renforcer l'attrait du marché de l'identité numérique**, et, en conséquence, de **proposer un choix de fournisseurs d'identité et de fournisseurs de services plus important pour le citoyen.**

À l'heure actuelle, cette valorisation est néanmoins exclue par les conditions générales d'utilisation de la plateforme FranceConnect. Cette interdiction est une garantie de confiance pour l'utilisateur et une distinction forte vis-à-vis d'autres fournisseurs d'identité numérique, comme Google ou Facebook par exemple, dont le modèle économique repose notamment sur cette valorisation, directe ou indirecte.

Interroger la valorisation des données d'identité numérique revient à poser la question de la possibilité, pour les fournisseurs d'identité, de partager des données complémentaires (au-delà des six données pivot) avec des fournisseurs de services. Si cet objectif est louable, pour enrichir le modèle et simplifier la vie des citoyens, **il pourrait susciter des résistances légitimes et limiter le caractère nouveau de la solution proposée par l'État**. En l'absence d'information complémentaire sur ce sujet, la mission souhaite insister sur l'impératif de protection des données personnelles (consentement de l'utilisateur, utilisation de ses données conforme aux objectifs présentés par l'acteur privé), d'une part, et sur la nécessité de s'assurer, en cas d'accord, que cette possibilité présente réellement un avantage du point de vue de l'utilisateur.

En tout état de cause, il apparaît à la mission que **les pouvoirs publics doivent fournir aux acteurs privés les éléments principaux du modèle économique envisagé pour l'identité numérique**, en précisant ce point en particulier. Il est important que les acteurs privés disposent d'une certaine visibilité dans ce secteur, vecteur de croissance économique pour notre pays (1).

Recommandation n° 20 : Présenter les éléments principaux du modèle économique de l'identité numérique retenu, afin de permettre aux acteurs économiques d'orienter leurs investissements dans ce domaine.

Il n'est pas nécessaire, en revanche, de figer le modèle économique de l'identité numérique, cet écosystème étant encore largement en cours de construction. Il faut néanmoins impérativement intégrer le déploiement de l'identité numérique au sein du plan de relance à venir, en raison de son impact important sur un grnd nombre de secteurs de l'activité économique.

Recommandation n° 21 : Intégrer le déploiement de l'identité numérique en France dans le cadre du prochain plan de relance.

C. ACCOMPAGNER LES FRANÇAIS, LEVER LES INQUIÉTUDES ET PROMOUVOIR UNE SOLUTION INCLUSIVE ET RESPONSABILISANTE

1. Donner à chaque Français les moyens de comprendre et maîtriser son identité numérique

a. Spécifier les enjeux liés à l'identité numérique dans les enseignements scolaires

L'éducation nationale s'est déjà considérablement modernisée et le numérique est désormais intégré dans les usages et dans les enseignements.

De nouveaux outils, tels que l'Éduthèque et les banques de ressources numériques, permettent aux enseignants d'accéder à des ressources pédagogiques en ligne et dotent ces enseignants et leurs élèves d'une culture numérique des usages absolument nécessaire aujourd'hui. Les programmes scolaires intègrent également des enseignements dont l'objectif est de développer les compétences numériques des élèves. C'est notamment le cas pendant le quatrième cycle d'enseignement – correspondant aux classes de 5ème, 4ème et 3ème – durant lequel les élèves bénéficient d'une éducation aux médias et à l'information et d'un enseignement relatif à l'informatique. Au lycée, les élèves de seconde générale et technologique reçoivent un enseignement consacré au numérique et à la technologie, à raison d'une heure et demie par semaine.

(1) Les analystes soulignent que l'identité numérique pourrait dégager une valeur économique comprise entre 3 % (économies matures) à 13 % (économies en développement) du PIB en 2030 si le programme d'identification numérique s'étend à de multiples cas d'usages de grande valeur et atteint des niveaux d'utilisation élevés.

Le numérique est également traité dans les programmes d'éducation civique et morale comme un enjeu de citoyenneté. L'identité numérique y est d'ailleurs abordée dans un enseignement plus large consacré aux composantes de l'identité. **Les questions relatives à la protection des données personnelles et à l'usurpation d'identité semblent toutefois peu traitées**.

La sensibilisation des futurs citoyens à ces préoccupations est considérée par l'ensemble des acteurs ayant participé aux travaux de la mission d'information comme un enjeu essentiel de l'identité numérique de demain. La chercheuse Danièle Bourcier estime nécessaire de **développer une éducation consacrée au contrôle, à la gestion et à l'utilisation des données personnelles**. Pour la professeure Bevière-Boyer, cet enseignement devrait être dispensé dès la maternelle et tout au long de la formation de l'étudiant.

Plusieurs internautes ayant participé à la consultation en ligne de l'Assemblée nationale sur l'identité numérique ont également souligné l'importance de l'éducation au numérique, certains considérant d'ailleurs que ces enseignements ne sont aujourd'hui pas suffisants.

Dans son rapport consacré aux identités numériques, le Conseil national du numérique partage cette préoccupation, observant qu'« *il est essentiel que les élèves acquièrent un bagage de culture numérique qui leur permette d'appréhender les grands enjeux de la société numérique. La formation continue des jeunes publics doit leur fournir les appuis intellectuels et les connaissances techniques, de façon à devenir des citoyens éclairés d'une société numérique*. » (1)

La mission d'information préconise donc **le renforcement de ces formations à toutes les étapes de la vie scolaire** afin de doter les élèves, futurs citoyens, d'une forme d'**hygiène numérique**. Elles doivent traiter spécifiquement de la question de l'identité numérique, de l'usurpation d'identité et de la protection des données personnelles, afin de **permettre le développement d'une véritable citoyenneté numérique**.

Recommandation n° 22 : Poursuivre les efforts en matière d'éducation au numérique dans les établissements scolaires, y compris dans les programmes d'enseignement moral et civique, en mentionnant spécifiquement les enjeux de protection des données personnelles et d'usurpation d'identité soulevés par l'identité numérique.

(1) Conseil national du numérique, rapport Identités numériques : clés de voûte de la citoyenneté numérique*, juin 2020, page 125.*

b. Un enjeu de formation continue

Afin de faciliter le déploiement des moyens d'authentification électroniques mis en place par les pouvoirs publics, l'Estonie a développé **une offre de formations au numérique pour adultes** complémentaire de celle dispensée dans le cadre scolaire, relative tant aux compétences en programmation qu'en littérature numérique (1).

La mise en place d'une initiative similaire en France a été plébiscitée par plusieurs personnes auditionnées par la mission d'information. Mme Bévière-Boyer préconise par exemple d'**ouvrir à tous les citoyens l'accès aux formations au numérique dispensées dans les universités françaises**.

La formation massive des Français de tous les âges est un prérequis à l'émergence d'une culture citoyenne du numérique. Cet effort doit ainsi être partagé par l'ensemble des acteurs du numérique, « *et pas seulement* [par] *l'exécutif, ni à l'inverse quelques associations militantes,* [afin de clarifier] *les enjeux qui s'attachent à l'identité numérique (de souveraineté, de croissance économique, de maîtrise des données, de lutte contre l'usurpation d'identité), les solutions possibles, ou non, les choix à opérer, les usages à développer, les mesures d'accompagnement nécessaires* » (2).

Ces initiatives pourraient ainsi être organisées par des structures telles que le **collectif Educnum**, fondé en 2013 par la CNIL, rassemblant des personnalités issues du monde de l'éducation, de la recherche, de l'économie numérique, de la société civile, de fondations d'entreprises et d'autres institutions, afin d'initier des actions de sensibilisation et de partage d'expériences de tous les publics, en y associant les acteurs économiques (3). Elles peuvent s'inspirer du format du cours en ligne de l'ANSSI relatif à la sécurité des systèmes d'information, plébiscité par un contributeur de la consultation en ligne de l'Assemblée nationale sur l'identité numérique (4). **Elles doivent en tout cas spécifiquement traiter des enjeux de l'identité numérique**.

Le numérique étant désormais indispensable à l'insertion professionnelle, les formations continues, les parcours d'insertion et les bilans professionnels doivent également systématiquement comprendre un volet numérique.

---

(1) Voir le compte-rendu de la table ronde relative à « la transformation numérique de l'école en Estonie et en France » co-organisée par France Stratégie et l'ambassade d'Estonie en France le 5 mai 2017.

(2) Contribution écrite de Mme Valérie Peneau aux travaux de la mission d'information.

(3) Sur son site internet, Educnum met à la disposition des internautes de nombreuses ressources numériques. Des ateliers et événements de sensibilisation sont également organisés par les membres du collectif.

(4) « L'ANSSI présente Secnumacadémie, sa formation en ligne sur la sécurité informatique gratuite et ouverte à tous », communiqué de presse du 18 mai 2017.

Recommandation n° 23 : Renforcer la formation continue aux outils numériques, en y intégrant les questions relatives à l'identité numérique, et mettre en place un volet numérique dans tous les parcours d'insertion professionnelle et dans les bilans professionnels.

Lors de son audition, Mme Elsa Hajman, responsable du pôle « inclusion et accès aux droits fondamentaux » de la Croix-Rouge française, a rappelé que **le déploiement du numérique entraîne une charge accrue pour les bénévoles**, qui se substituent à l'État **sans bénéficier de la même expertise que les travailleurs sociaux**.

Cette sollicitation nécessite, selon la Croix-Rouge française, un effort financier plus important de l'État pour soutenir le corps associatif dans cette mission dont il hérite.

L'État doit également renforcer les guides, les outils et les formations des bénévoles afin de permettre leur montée en compétences et un accompagnement plus efficace et respectueux des données personnelles des publics pris en charge par les associations. Des outils ont déjà été développés et gagneraient à être généralisés, à l'instar du kit de la CNIL à destination des travailleurs sociaux, qui pourrait utilement être décliné pour les bénévoles [(1)].

Les pouvoirs publics pourraient **consacrer une partie des économies réalisées du fait de la dématérialisation des services publics** à cette fin.

Recommandation n° 24 : Assurer la formation du corps associatif et des aidants numériques afin de garantir aux publics fragiles un accompagnement au numérique de qualité.

Recommandation n° 25 : Accroître les financements aux associations qui assurent l'accompagnement numérique des publics fragiles.

c. Instaurer un parcours citoyen d'identité numérique

i. L'identité numérique des personnes mineures

Le décret du 22 octobre 1955 instituant la carte nationale d'identité [(2)] dispose que « *la carte nationale d'identité est délivrée sans condition d'âge à tout Français qui en fait la demande* » (article 2). Il est néanmoins nécessaire que le mineur soit accompagné « *par une personne exerçant l'autorité parentale* » qui présente sa demande (article 4-4).

Toutefois, la délivrance d'un moyen d'identification électronique nécessite de recueillir le consentement des mineurs au traitement de leurs données personnelles.

(1) Travailleurs sociaux : un kit d'information pour protéger les données de vos publics*, site internet de la CNIL, 23 janvier 2019.*

(2) Décret n° 55-1397 du 22 octobre 1955 instituant la carte nationale d'identité.

L'article 8 du RGPD relatif aux conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information prévoit que les enfants âgés de plus de seize ans peuvent licitement consentir au traitement de leurs données personnelles, cet âge pouvant être abaissé jusqu'au seuil de treize ans par les États membres.

En France, l'article 45 de l'ordonnance du 12 décembre 2018 prise en application de l'article 32 de la loi du 20 juin 2018 relative à la protection des données personnelles [(1)] prévoit qu'**un mineur peut consentir seul au traitement de ses données personnelles à compter de l'âge de quinze ans**.

En revanche, **lorsque l'enfant a moins de quinze ans**, le **consentement** au traitement de ses données personnelles n'est licite que dans la mesure où il est donné **conjointement par le mineur concerné et le ou les titulaires de l'autorité parentale** à l'égard de ce mineur (article 45).

L'article 8.2 du RGPD précise que « *le responsable du traitement s'efforce raisonnablement de vérifier, en pareil cas, que le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant, compte tenu des moyens technologiques disponibles* ».

Dans sa contribution écrite, la CNIL précise que « *la question de la vérification de l'âge et des consentements est particulièrement complexe* » car « *tout système de vérification d'âge pose la question de son efficacité et du degré de facilité de son contournement. Il pose également des questions en termes de traitement des données personnelles, y compris des données sensibles* ».

La CNIL a engagé **une consultation publique** concernant les droits des mineurs sur leurs données personnelles, dont les résultats devraient être rendus publics à l'automne 2020.

La question de l'identité numérique des mineurs ne semble pas aujourd'hui traitée de façon satisfaisante. Un certain nombre de questions doivent encore être approfondies et débattues. Faut-il, comme en Allemagne, attendre l'âge de 15 ans pour délivrer une identité numérique aux enfants ? Certains usages pourraient-ils être ouverts dans un cadre scolaire, ce qui aurait également une portée éducative ?

Les mineurs peuvent exercer leur droit à l'effacement de leurs données personnelles lorsqu'ils atteignent leur majorité, mais faut-il nécessairement attendre cette majorité pour exercer ce droit en toute circonstance ?

Si la mission d'information appelle les pouvoirs publics à demeurer attentifs à la protection des mineurs dans la création et dans l'usage de leur identité numérique, elle souhaite qu'une réflexion globale sur le parcours

(1) Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel.

d'identité numérique du mineur soit mise en place. Cette réflexion pourrait correspondre à une ouverture progressive de droits et de responsabilités dans un cadre de formation à la citoyenneté numérique.

ii. Une identité numérique qui pourrait être délivrée à tous les moments clés de la vie

La création d'une identité numérique devrait pouvoir être proposée aux citoyens à tous les âges, et à l'occasion de moments clés de la vie, comme l'entrée au collège, la journée défense et citoyenneté et l'inscription sur les listes électorales (1).

Le service national universel (SNU), expérimenté depuis le mois de juin 2019, et dont la généralisation devrait intervenir progressivement à partir de 2021, doit également être l'occasion **de proposer aux jeunes filles et garçons la création de leur identité numérique** pendant ce temps fort.

Recommandation n° 26 : Proposer la délivrance d'une identité numérique à tous les moments clé de la vie du citoyen, y compris à l'occasion du service national universel.

Recommandation n° 27 : Lancer une réflexion interministérielle sur les mineurs et l'identité numérique.

iii. L'identité numérique des personnes décédées

L'article 84 de la loi « Informatique et liberté » pose pour principe **l'extinction des droits personnels** promus par la loi (accès, modification, *etc.*) **avec le décès de la personne**. Néanmoins, l'article 85 prévoit que « *toute personne peut définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès* ».

Ces directives peuvent être **générales**, lorsqu'elles portent sur l'ensemble des données concernant une personne, ou **particulières** lorsqu'elles ne concernent que certains traitements de données spécifiques. Elles peuvent désigner une personne chargée de leur exécution.

Le compte Alicem au décès de son utilisateur

L'utilisation du moyen d'identification électronique Alicem prévoit l'interrogation systématique de DOCVERIF afin de vérifier la validité du titre d'identité. Cette vérification permet à Alicem d'être informée du décès de l'utilisateur, et de procéder au blocage de son compte. En outre, un compte inactif pendant six ans est automatiquement fermé et les données qui y sont rattachées sont supprimées.

(1) Cette proposition est formulée par le think tank *Renaissance numérique dans sa note* Identité numérique : Passer à une logique citoyenne *de janvier 2019.*

S'agissant des directives générales, la loi prévoit qu'elles peuvent être enregistrées auprès d'un tiers de confiance numérique certifié par la CNIL. Son article 85 dispose que « *les références des directives générales et le tiers de confiance auprès duquel elles sont enregistrées sont inscrites dans un registre unique dont les modalités et l'accès sont fixés par décret en Conseil d'État, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés* ».

Dans sa contribution écrite aux travaux de la mission d'information, la CNIL observe qu'à ce jour, « *aucun décret n'a été pris sur ce point* ». Pourtant, « *l'adoption d'un décret permettrait d'apporter des précisions sur ces dispositions et de rendre le dispositif pleinement opérationnel* ».

Recommandation n° 28 : Afin de garantir la pleine effectivité du dispositif juridique de l'identité numérique des personnes décédées, publier le décret prévu à l'article 85 de la loi « Informatique et libertés » concernant les directives générales qu'une personne décédée peut définir à propos de la conservation, l'effacement et la communication de ses données personnelles.

En l'absence de directives générales ou particulières, l'article 85 permet également aux héritiers de la personne décédée d'exercer certains droits, notamment afin d'organiser le règlement de sa succession.

2. Réaffirmer des évidences pour garantir la confiance

a. Des principes fondamentaux à protéger : l'anonymat sur internet, la protection des données personnelles

i. Le maintien de l'anonymat sur internet

Le projet de développement d'une identité numérique régalienne est parfois **confondu avec une volonté de supprimer l'anonymat sur internet**.

Ces inquiétudes ont été exprimées dans les contributions de la consultation en ligne de l'Assemblée nationale sur l'identité numérique. De nombreux commentaires soulèvent la nécessité de maintenir l'anonymat en ligne et de développer des solutions respectueuses de la vie privée de leurs utilisateurs.

La mission d'information réaffirme que ses travaux n'ont jamais cherché à tendre vers cet objectif, par ailleurs fermement écarté par M. Cédric O et Mme Valérie Peneau lors de leurs auditions. L'identité numérique devra uniquement permettre aux usagers d'un service public ou aux clients d'une entreprise d'attester de leur identité afin de bénéficier d'une prestation ou d'un service qui nécessite au préalable cette vérification. Il n'est ainsi pas question d'utiliser l'identité numérique pour s'authentifier sur un réseau social, par exemple.

Recommandation n° 29 : Faire de l'anonymat la situation par défaut et réserver l'authentification en ligne aux seuls services qui nécessitent de connaître l'identité de l'utilisateur.

ii. La pertinence des principes du RGPD en matière de protection des données personnelles

L'article 5 du RGPD pose six principes qui s'imposent au responsable de traitement afin de protéger les données à caractère personnel des utilisateurs, et qui s'appliquent donc également aux données personnelles collectées dans le cadre de l'utilisation d'un dispositif d'identité numérique :

- **licéité, loyauté et transparence du traitement** au regard de la personne concernée ;

- **limitation des finalités** : les données collectées doivent l'être « *pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités* » ;

- **minimisation des données**, qui doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* » ;

- **exactitude** : ces données doivent être « *exactes et, si nécessaire, tenues à jour* » ;

- **limitation de conservation** : elles doivent être « *conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées* » ;

- **intégrité et confidentialité** : les données doivent ainsi être « *traitées de façon à garantir une sécurité appropriée des données à caractère personnel* ».

Pendant ses travaux, la mission d'information a constaté que **ces principes sont respectés par les pouvoirs publics**. Afin de garantir à l'avenir la confiance des citoyens dans les dispositifs d'identité numérique régalienne existant et en cours de développement, ils doivent continuer de guider l'action du Gouvernement.

Il importe d'assurer la transparence des moyens utilisés et des données collectées, tout en associant l'expertise citoyenne et universitaire au contrôle des outils et de la conformité des données recueillies aux objectifs poursuivis.

b. Une réflexion nouvelle sur la protection des droits numériques

L'enjeu de protection des données personnelles prend une ampleur considérable aujourd'hui et continuera à l'avenir d'être un sujet majeur des politiques publiques.

Pendant ses travaux, **la mission d'information s'est interrogée sur la pertinence d'introduire des modifications d'ordre constitutionnel**, notamment pour réaffirmer les principes de protection, de minimisation et de proportionnalité des données personnelles.

Certains acteurs sollicités par la mission d'information sont favorables à une telle initiative, à l'instar des professeurs Laura Draetta, Valérie Fernandez et Mickaël Bardin. **D'autres y opposés**, comme les professeurs Bénédicte Bevière-Boyer et François Pellegrini.

Lors de l'examen en première lecture du projet de loi constitutionnel relatif à une démocratie plus représentative, responsable et efficace par l'Assemblée nationale en juillet 2018, plusieurs députés avaient déposé un amendement étendant le domaine de la loi précisé à l'article 34 de la Constitution en y ajoutant « l*a protection des données à caractère personnel* » (1).

Constatant que « *les données personnelles des citoyens se retrouvent en effet collectées, traitées et utilisées dans des bases de données, objets d'appropriation privative par des structures commerciales, qui les détiennent comme de simples actifs et les négocient ensuite, souvent sans traçabilité* », les signataires avaient estimé que cette matière relevait, de par sa nature, du domaine de la loi.

Cette première réflexion pourrait être poursuivie jusqu'à son terme dans la perspective d'un prochain projet de loi constitutionnel.

Recommandation n° 30 : Inscrire la protection des données personnelles dans le domaine de la loi à l'article 34 de la Constitution.

c. Tirer les leçons d'Alicem : prévoir une alternative physique à la reconnaissance faciale

Dans sa délibération du 18 octobre 2018 portant avis sur le projet de décret Alicem, la CNIL a souhaité qu'une alternative à l'utilisation de la reconnaissance faciale lors de l'enrôlement à Alicem soit mise en place.

Cette alternative permettrait de **passer outre la méfiance encore vive vis-à-vis de cette technologie**, même si la mission d'information regrette qu'elle repose souvent sur une méconnaissance du dispositif et sur **une confusion entre l'authentification et l'identification biométrique**.

(1) Amendement n° 2047 présenté par M. Houlié.

Des modalités d'enrôlement « en présentiel » faciliteraient l'accessibilité des solutions d'identité numérique régaliennes en réduisant les étapes de création du compte et en permettant à l'utilisateur en difficulté de bénéficier d'un accompagnement dans la création de son identité numérique. L'État s'assurerait ainsi d'un nombre potentiel d'utilisateurs plus important.

Comme le relève le Conseil national du numérique, l'enrôlement est en effet un moment crucial qui conditionne les usages ultérieurs de la solution. Dans son rapport sur les identités numériques, le Conseil préconise de rendre l'enrôlement « *le moins frictionnel possible, puisque c'est le premier contact du citoyen avec l'administration numérique, ce qui déterminera fortement l'acceptabilité des outils et l'accession aux usages ultérieurs. Cela implique de créer un environnement de confiance (sécurité et simplicité d'usage) permettant d'authentifier la personne qui s'enrôle*. » (1)

En outre, la **mise en place d'une alternative à la reconnaissance faciale semble nécessaire pour garantir un niveau de sécurité élevé** au sens du règlement eIDAS, eu égard aux récents avis du réseau de coopération eIDAS concernant l'utilisation de la biométrie pendant la phase d'authentification.

Recommandation n° 31 : Mettre en place une alternative physique à la reconnaissance faciale dans le cadre de la phase d'enrôlement des solutions d'identité numérique régaliennes.

3. Donner à la CNIL les moyens de mieux assurer ses missions

Le rôle de la CNIL est un gage de confiance dans le développement des identités numériques de demain. La mission d'information constate que **son budget est en augmentation sur les quatre dernières années**. En 2020, il est en hausse de près de 9 % en autorisation d'engagement et en crédits de paiement, permettant le recrutement de 10 postes supplémentaires, ce qui portera ses effectifs de 215 en 2019 à 225 aujourd'hui.

BUDGET DE LA CNIL (1)

2017	17 362 855 €
2018	17 658 988 €
2019	18 791 573 €
2020	20 444 923 €

(1) En crédits de paiement.

Source : rapports annuels de la CNIL et loi de finances pour 2020.

Cette hausse continue traduit la place croissante occupée par la CNIL dans le paysage institutionnel français, notamment depuis l'entrée en vigueur, le 25 mai 2018, du RGPD, qui s'est accompagnée de la désignation de nombreux délégués à la protection des données. La mission d'information relève d'ailleurs que

(1) Conseil national du numérique, rapport Identités numériques : clés de voûte de la citoyenneté numérique*, juin 2020, page 49.*

le nombre de plaintes enregistrées par la CNIL a augmenté de 27 % entre 2018 et 2019 (1).

Si cette augmentation des moyens est nécessaire, **elle demeure néanmoins aujourd'hui insuffisante pour permettre à la CNIL d'assurer pleinement sa mission** de régulateur des données personnelles. Dans sa contribution aux travaux de la mission d'information, la CNIL observe que « *l'autorité polonaise compte 250 agents pour 37,98 millions d'habitants, le Royaume-Uni 696 pour 66,19 millions d'habitants, l'Allemagne plus de 700 pour 82,85 millions d'habitants* ».

Ainsi, « *les effectifs de la CNIL demeurent en-deçà du niveau minimal requis pour absorber l'ensemble des missions qui lui ont été confiées par le législateur. En particulier, la capacité de conseil aux acteurs publics et privés n'est pas adaptée au besoin exprimé par les administrations et les entreprises. De même, les ressources dédiées à la chaîne répressive ne suivent manifestement pas la tendance continue d'augmentations des saisines de la CNIL. Le manque de moyens obère la capacité d'action de l'institution en ce secteur. De plus, les ressources dédiées à la cybersécurité doivent aussi être renforcées, en lien notamment avec les nouvelles obligations découlant du RGPD en matière de notifications de violations de données* ».

L'augmentation substantielle des moyens du régulateur français des données personnelles doit donc lui permettre de remédier à son actuel sous-dimensionnement.

Recommandation n° 32 : Renforcer les moyens de la CNIL.

4. Mettre en œuvre un écosystème inclusif et responsabilisant

a. Faire de l'identité numérique de demain un facteur d'inclusion

i. Des solutions qui doivent être accessibles

Les associations entendues par la mission d'information, notamment Emmaüs Connect, la Croix-Rouge française et la fondation Petits frères des Pauvres (2) , ont salué **le potentiel inclusif des solutions d'identité numérique**.

Ces solutions pourraient faciliter la gestion des identifiants et des mots de passe pour les publics les plus éloignés du numérique et mieux sécuriser leurs droits. Ainsi que l'a rappelé Mme Elsa Hajman, ces publics ont aujourd'hui tendance à confier la gestion de leurs comptes en ligne à des membres de leur famille et à des aidants professionnels ou bénévoles, ce qui les expose à **des risques d'usurpation d'identité plus importants**.

(1) Rapport d'activité 2019 de la CNIL.

(2) Audition de représentants de l'association Emmaüs Connect, La Croix-Rouge française et la fondation Petits frères des pauvres par la mission d'information le mercredi 15 janvier 2020.

Pour permettre à l'identité numérique de devenir un facteur d'*e*-inclusion, il convient de s'assurer que les solutions développées demeurent compréhensibles du plus grand nombre. Lors de son audition, M. Tom-Louis Teboul, responsable « développement et partenatriat » d'Emmaüs Connect, a regretté l'emploi d'un champ lexical complexe sur les sites internet permettant d'accéder à un service public en ligne. L'utilisation de termes tels que « login » ou « identifiant » peut sembler anodine, mais elle dissuade certains utilisateurs peu familiers avec le champ lexical de la navigation en ligne.

Lors de son audition la Croix Rouge a par ailleurs insisté sur la nécessité de produire une littérature accessible à tous, notamment **des documents** relatifs à l'identité numérique et à la protection des données **rédigés en français et en langues étrangères**, afin d'offrir à chacun un égal accès à l'information relative au numérique.

Cet avis est partagé par le Conseil national du numérique, qui rappelle que « *la dématérialisation des démarches administratives doit prendre en compte la fracture numérique et l'inégalité entre les territoires* » [(1)]. Il invite ainsi le législateur à **développer un parcours d'identité numérique « facile à lire et à comprendre »** (FALC), recommandation à laquelle la mission d'information souscrit pleinement.

Ces solutions doivent également être accessibles aux personnes en situation de handicap.

La Croix-Rouge française **préconise un accompagnement dans la création de l'identité numérique** au sein des maisons France Service, ainsi que le maintien des solutions itinérantes afin de toucher les publics habitant dans des zones blanches ou grises [(2)], des territoires ruraux ainsi que des espaces urbains où les services publics sont moins nombreux, et donc moins accessibles.

Ces alternatives sont d'autant plus nécessaires que **des freins à l'acquisition du matériel numérique persistent** pour de nombreux Français. Dans sa contribution écrite, le Défenseur des droits observe que 19 % d'entre eux n'ont pas d'ordinateur à domicile et 27 % n'ont pas de *smartphone*.

Recommandation n° 33 : Développer des solutions d'identité numérique inclusives qui prennent en compte les besoins et les fragilités des publics les plus éloignés du numérique.

Recommandation n° 34 : Maintenir des alternatives physiques à la dématérialisation des services publics.

(1) Conseil national du numérique, rapport Identités numériques : clés de voûte de la citoyenneté numérique*, juin 2020, page 43.*

(2) Dans sa contribution écrite aux travaux de la mission d'information, le Défenseur des droits rappelle que 0,7 % des Français n'ont toujours pas accès à une connexion internet, soit 500 000 personnes.

ii. Le Pass Numérique, un dispositif innovant dont la montée en charge doit être poursuivie

L'augmentation des usages numériques en cours et à venir nécessite de renforcer la formation continue des citoyens les plus éloignés du numérique. Comme l'ont rappelé le Défenseur des droits dans sa contribution écrite aux travaux de la mission, et M. Pierre-Louis Rolle, directeur du programme « Société numérique » au sein de l'Agence nationale de la cohésion des territoires, il existe en effet **13 millions de Français en difficulté avec le numérique, dont 6,7 millions d'entre eux qui ne se connectent jamais à internet**.

C'est pour lutter contre cette fracture numérique, déplorée par toutes les associations entendues dans le cadre de la mission d'information, **que l'État a entamé le déploiement, en 2019, du Pass Numérique**, développé par la mission Société Numérique dans le cadre du plan national pour un numérique inclusif.

Ce dispositif permet à des publics vulnérables d'accéder, dans des lieux préalablement qualifiés par le biais d'une labellisation par les pouvoirs publics, **à des services d'accompagnement et de médiation numériques**. Cofinancés par l'État à hauteur de 10 millions d'euros l'an dernier, ces chèques numériques sont destinés à un achat par les collectivités territoriales, qui en financent ainsi une partie. Ils sont ensuite distribués par les collectivités et permettent d'accéder à dix, voire à vingt heures de formation.

Cette initiative innovante a été plébiscitée par l'association Emmaüs Connect lors de son audition par la mission d'information, qui préconise d'y recourir plus massivement.

Dans son rapport sur la dématérialisation des services publics de 2019 [(1)], le Défenseur des droits salue cette initiative, mais identifie néanmoins **trois difficultés** qu'il convient de résoudre :

– le nombre d'heures de formation serait insuffisant pour permettre aux publics fragiles d'être totalement autonomes ;

– les pouvoirs publics doivent veiller à imposer des critères de labellisation exigeants pour déterminer les lieux de médiation numérique ciblés par le dispositif et en assurer une répartition équilibrée sur le territoire national ;

– l'engagement financier mobilisé aujourd'hui par l'État paraît insuffisant pour répondre à la demande de formation des millions de Français encore éloignés du numérique, et cela nécessite un effort budgétaire plus important dans les années à venir.

(1) Défenseur des droits, Rapport Dématérialisation et inégalités d'accès aux droits*, 2019.*

Les pouvoirs publics devront prendre en compte ces difficultés s'ils souhaitent faire du Pass Numérique une réussite.

Recommandation n° 35 : Étendre le recours au Pass Numérique.

b. Accompagner la transformation des services publics

L'identité numérique devrait permettre de simplifier et de dématérialiser des démarches administratives.

Le **projet Grand Lyon Connect** est un exemple de cette ambition. Mis en place en décembre 2018, ce dispositif permet à l'usager de s'authentifier une fois, puis d'accéder à un portail de services sans avoir à recommencer le processus d'authentification. Cette facilité concerne aujourd'hui de nombreux services publics comme la gestion de l'état civil, la santé (dossier médical partagé, carnet de vaccination en ligne), l'éducation (signature électronique des bulletins de notes, inscription aux examens et concours, diplômes), les services municipaux (crèches, écoles, cantines), la possibilité d'une pré-plainte en ligne, disponible avant la dématérialisation du processus de dépôt de plainte depuis la loi de programmation 2018-2022 et de réforme pour la justice [(1)], et le traitement des actes à distance auprès des magistrats, avocats, huissiers et notaires.

Ce bouleversement des modalités de l'action publique n'est pas neutre pour les administrations. Le *think tank* Renaissance numérique considère que « *la dématérialisation appelle à une nouvelle organisation territoriale, dans laquelle la puissance publique doit repenser sa présence et sa valeur ajoutée* » [(2)]. Il s'inquiète des répercussions de la dématérialisation sur les agents, qui ne disposent pas toujours des compétences ou de l'équipement pour répondre aux exigences nouvelles des administrés.

Renaissance numérique propose **l'engagement d'une large réflexion associant élus et agents de l'administration** afin de rapprocher les agents publics et les concepteurs des solutions numériques, ces derniers pouvant partager leur « *culture "moderne"* » des usages auprès des agents publics afin de favoriser leur montée en compétences. La mission d'information estime que cette réflexion doit s'accompagner d'un plan de formation ambitieux des agents publics sur les sujets numériques.

Recommandation n° 36 : Mettre les solutions d'identité numérique au cœur des réflexions sur la dématérialisation des services publics, qu'elles doivent faciliter.

Recommandation n° 37 : Élever le niveau de l'ensemble des personnels de la fonction publique sur les sujets numériques par un vaste plan de formation.

(1) Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.

(2) Note Identité numérique : Passer à une logique citoyenne*, janvier 2019.*

c. Développer des solutions responsabilisantes qui permettent à l'utilisateur de mieux maîtriser ses données personnelles

i. Permettre aux utilisateurs de mieux visualiser le cheminement de leurs données personnelles

La feuille de route Tech.gouv de la DINUM prévoit 35 projets et actions prioritaires pour les années 2019-2021, afin d'accélérer la transformation numérique du service public.

L'une de ces actions, relative à l'inclusion numérique, ambitionne notamment de « ***mettre en œuvre une stratégie d'accès étendu aux services publics grâce au numérique*** ». Cette feuille de route prévoit la création d'un dossier numérique citoyen durant le second semestre 2020. Il pourrait permettre à ses utilisateurs de « *consulter la liste des informations dont les administrations disposent sur les citoyens ; suivre les échanges de données que les administrations effectuent entre elles pour faciliter les démarches ; développer une fonction de notifications permettant d'informer les citoyens de l'avancement du traitement de leurs dossiers* » (1).

Pour le directeur interministériel du numérique (2), il s'agit de rendre aux citoyens la pleine possession de leurs données, en leur offrant un tableau de bord présentant la manière dont les données peuvent être transférées d'une administration à une autre dans le cadre du programme de simplification des démarches administratives « *dites-le nous une fois* ».

Dans sa contribution écrite aux travaux de la mission d'information, **l'Association des départements de France conditionne la réussite du développement d'une identité numérique régalienne à la mise en place de cette initiative**. Elle relève en effet que « *l'approche publique de l'identité numérique est encore trop partielle pour être massivement adoptée par les citoyens : la CNIe n'existe pas encore, les usages de FranceConnect ne sont pas encore généralisés… Ce n'est qu'avec la mise en place de modules apportant réellement un bénéfice pour l'usager, comme les services permis par le projet de "dossier numérique du citoyen" qui s'appuie sur le "dîtes le nous une fois", que ces services seront éventuellement massivement adoptés* ».

La mission d'information préconise le développement et la mise en service rapide de cette initiative, qui s'inscrit résolument dans **un mouvement de prise de contrôle par les citoyens de leurs données personnelles**, et contribue à ce titre à la création d'un écosystème sain et responsabilisant de gestion de ces données.

---

(1) Tech.gouv, Accélérer la transformation numérique du service public, stratégie et feuille de route 2019-2021*, octobre 2019.*

(2) Audition de M. Nadi Bou Hanna, directeur interministériel du numérique, par la mission d'information le lundi 15 juin 2020.

La mission d'information estime également nécessaire d'**aller plus loin en permettant aux utilisateurs**, quelle que soit la solution qu'ils utilisent, **de savoir quel fournisseur d'identité utilise leurs données** et les conditions de partage de ces données à des tiers.

Recommandation n° 38 : Déployer rapidement le dossier numérique du citoyen.

Recommandation n° 39 : Développer des solutions d'identité numérique transparentes, qui informent les utilisateurs sur le cheminement et les conditions d'accès et de partage de leurs données personnelles avec des tiers.

ii. L'identité numérique auto-souveraine et la *blockchain*

Le recours aux technologies de la *blockchain* (ou « chaîne de blocs ») pourrait également être envisagé, comme complément ou comme alternative d'une identité numérique sécurisée garantie par l'État (1). Le rapport parlementaire des députés Laure de la Raudière et Jean-Michel Mis les définit comme « *des technologies de stockage et de transmission d'informations, permettant la constitution de registres répliqués et distribués (*distributed ledgers*), sans organe central de contrôle, sécurisées grâce à la cryptographie, et structurées par des blocs liés les uns aux autres, à intervalles de temps réguliers* » (2).

La *blockchain* permet aux citoyens de recourir à un protocole décentralisé qui leur offre un accès direct à leurs données ainsi qu'une vision globale de la façon dont elles sont partagées et réutilisées par des tiers. La *blockchain* offre ainsi un réseau stable et sécurisé, sans intervention de l'État, qui n'a pas à gérer une base de données centralisées.

L'association de la *blockchain* avec la **preuve à divulgation nulle de connaissance** (*zero knowledge proof*), qui consiste en un protocole sécurisé « [permettant] *à un utilisateur, appelé prouveur, de démontrer à un autre utilisateur, appelé vérifieur, qu'un certain fait est vrai, sans révéler aucune information, si ce n'est la véracité de ce fait* » (3), permettrait de **partager des données entre plusieurs parties sans avoir à transmettre les informations associées à la transaction**.

Le recours à la *blockchain* est notamment défendu par Mme Danièle Bourcier, qui la considère comme incontournable en ce qu'elle consiste en un système de certification décentralisé, sans intermédiaire, qui pourrait séduire un public méfiant ou en recherche de solutions très sécurisées et autonomes.

---

*(1) Cette recommandation était déjà formulée dans le rapport d'information n° 1501 de Mme Laure de La Raudière et M. Jean-Michel Mis sur les chaînes de blocs (*blockchains*), Assemblée nationale, XV*ème *législature, 12 décembre 2018.*

(2) Ibid.*, page 11.*

(3) Fabrice Benhamouda, « Divers modules et preuves à divulgation nulle de connaissance », Bulletin de la société informatique de France*, numéro 10, avril 2017.*

La notion émergente d'identité numérique auto-souveraine repose sur cette technologie. Présentée par la professeure Primavera de Filippi durant son audition (1), elle permet à l'utilisateur de **dévoiler sélectivement certains attributs, tout en choisissant les entités de certification qu'il souhaite** (2). Le *Gemalto Trust ID Network*, qui permet à l'utilisateur de bénéficier d'un contrôle total des accès à ses données personnelles, constitue une application industrielle intéressante de ce concept (3).

Le recours à la *blockchain* pourrait néanmoins être écarté en matière d'identité numérique des mineurs s'il s'avérait que cette technologie ne peut pas garantir avec certitude le droit à l'oubli ou à l'effacement des données.

Recommandation n° 40 : Favoriser le développement d'alternatives à l'identité numérique régalienne, comme l'identité numérique auto-souveraine, en exploitant les possibilités offertes par la *blockchain*.

d. Mettre en place une gouvernance transparente

La question de **la gouvernance des solutions d'identité numérique** de demain a été posée à plusieurs reprises par de nombreux acteurs entendus par la mission d'information, qui ont souhaité que les citoyens et le corps associatif soient mieux intégrés aux dispositifs mis en place.

Pour les chercheurs Valérie Fernandez et Laura Draetta, **les technologies sur lesquelles reposent les solutions d'identité numérique ne sont pas neutres**, mais sont au contraire le produit construit de la réflexion d'ingénieurs, qui évoluent parfois en milieu clos. **L'association des acteurs privés, des régulateurs publics, du corps associatif et des utilisateurs à la construction, au fonctionnement et à l'amélioration des dispositifs, ainsi qu'aux modèles économiques qui seront développés, est donc nécessaire.**

Les solutions d'identité numérique doivent également évoluer en fonction des usages. Ainsi que le relève le *think tank* Renaissance numérique, qui préconise **la création d'instances de dialogue avec les utilisateurs**, « *ces nouvelles fonctionnalités devront être développées sur la base d'une observation fine des usages qui évolueront au fur et à mesure, en même temps que l'appropriation de l'identité numérique et des choix politiques nouveaux.* » (4)

Mme Danièle Bourcier a également proposé que la régulation technique de l'identité numérique fasse l'objet d'un vote par **une assemblée d'experts du numérique**.

---

(1) Table ronde de professeurs réunissant Mme Primavera de Filippi et MM. Jean-Gabriel Ganascia et François Perea, organisée par la mission d'information le mardi 21 janvier 2020 – voir la vidéo de la table ronde sur le site de l'Assemblée nationale.

(2) Fenny Wang, Primavery De Filippi, « Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion »*, 2020.*

(3) Voir L'identité numérique sécurisée auto-souveraine *sur le site internet de l'entreprise Thales.*

(4) Renaissance numérique, rapport Identité numérique : Passer à une logique citoyenne*, janvier 2019, page 33.*

Une solution similaire a également été proposée par un contributeur de la consultation en ligne de l'Assemblée nationale sur l'identité numérique, qui suggère « *la mise en place d'**un comité éthique sur l'identité numérique** ayant une capacité d'audit, pouvant missionner des tests d'intrusions, pouvant auditer les comptes, s'assurer que les budgets sont suffisants pour* [garantir] *la sécurité du dispositif, pouvant auditer les prestataires techniques et ordonner l'arrêt momentané de la solution en cas de risque majeur* ». Plusieurs internautes préconisent en outre de **faire reposer les dispositifs sur des standards ouverts** et de **publier les codes source** des solutions mises en place.

Cette préoccupation a également été relevée par le Conseil national du numérique, dont le rapport sur les identités numériques « *estime crucial de replacer l'usager au centre, de ne pas limiter les identités numériques à des problématiques de sécurité intérieure, de créer des chaînes de confiance pour faire émerger une citoyenneté numérique* ». Il préconise notamment la création d'une « *instance de contrôle et de supervision indépendante et multi parties prenantes (académiques, associatifs, administratifs,* etc.*)* » qui aurait des missions de surveillance et de contrôle *a priori*, ainsi qu'un rôle d'évaluation et d'audit. Elle serait également chargée d'une « *mission spécifique d'interrogation et de construction de la citoyenneté numérique basée sur les principes de la participation citoyenne et qui devraient obligatoirement comporter des modalités de participation "*hors-ligne*"* » (1).

Le récent rapport du professeur Didier Truchet sur l'expertise publique en matière de santé, d'environnement et d'alimentation relève qu'un « *un fossé se creuse entre les agences en charge de l'expertise publique et la société civile, entendue comme le public, les associations concernées par les problèmes étudiés et la presse* » (2).

Il importe de permettre **l'émergence d'une expertise citoyenne** en matière d'identité numérique en nommant des experts indépendants et en mettant en place des processus d'évaluation et de contrôle transparents. Il convient également d'assurer la présence, au sein des comités d'expertise, de membres de la société civile, afin de « *diversifier la composition des comités et enrichir la palette des opinions qui s'y expriment, améliorer le partage et la discussion contradictoire des connaissances* [et] *mieux faire connaître la réalité, et la loyauté du processus d'expertise* » (3).

La mission d'information rappelle que les citoyens peuvent déjà **saisir directement la CNIL** pour toute question relative à la protection de leurs données personnelles et **s'adresser à l'ANSSI** pour déclarer une faille de sécurité ou une

---

(1) Conseil national du numérique, rapport Identités numériques : clés de voûte de la citoyenneté numérique*, juin 2020, pages 70-71.*

(2) Didier Truchet, rapport L'expertise publique, santé, environnement et alimentation*, 18 décembre 2019.*

(3) Ibid.

vulnérabilité. En ce qui concerne les autres acteurs qui assurent un suivi des sujets numériques (CNNum, CSNP, CESE), force est de constater un manque de lisibilité dans l'articulation de leurs actions. Une réflexion sur la gouvernance globale des sujets numériques apparaît souhaitable.

Recommandation n° 41 : À l'étape de la conception des solutions d'identité numérique, associer les citoyens, les universitaires et les acteurs et groupements du numérique à la définition des besoins et des attentes des utilisateurs.

Recommandation n° 42 : Engager une réflexion sur la gouvernance du numérique pour assurer davantage de lisibilité et un niveau de confiance plus élevé des citoyens.

5. Instaurer un cadre législatif protecteur

L'adoption d'un projet ou d'une proposition de loi n'est aujourd'hui pas nécessaire pour mettre en place l'écosystème de l'identité numérique régalienne.

Dans sa décision concernant la loi du 27 mars 2012 relative à la protection de l'identité, le Conseil constitutionnel a estimé que le législateur avait méconnu l'étendu de sa compétence en ne précisant pas la nature des données collectées, les « *garanties assurant l'intégrité et la confidentialité de ces données* », ainsi que « *les conditions dans lesquelles s'opère l'authentification des personnes mettant en œuvre ces fonctions, notamment lorsqu'elles sont mineures ou bénéficient d'une mesure de protection juridique* » (1).

Depuis 2012, l'adoption du règlement eIDAS, de son règlement d'exécution du 8 septembre 2015 (2), puis du RGPD, ont précisé ces éléments. Ainsi, lors de son audition par la mission d'information, M. Cédric O estimait qu'un encadrement législatif n'était aujourd'hui plus nécessaire, mais qu'un débat au Parlement pourrait être organisé afin d'associer pleinement la Représentation nationale aux travaux du Gouvernement.

Toutefois, **la complexité du sujet et les risques d'incompréhension, ainsi que la méfiance vis-à-vis de l'appareil étatique, semblent rendre cet encadrement nécessaire**. Cet avis est partagé par le Conseil national du numérique, dont l'une des recommandations consiste à « *soumettre au débat une loi d'orientation définissant l'identité numérique et ses finalités et assurant le respect des droits des citoyens en rappelant les cadres d'utilisation des données d'identité numérique pour prévenir des dérives (surveillance, fichages,* etc.*)* » (3).

---

(1) Décision n° 2012-652 DC du 22 mars 2012, considérant 14.

(2) Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

(3) Conseil national du numérique, rapport Identités numériques : clés de voûte de la citoyenneté numérique*, juin 2020, pages 73-74.*

L'identité numérique soulève également des **enjeux en matière de libertés individuelles**, qui suppose que le législateur demeure attentif à la transparence de ses finalités et aux effets des solutions développées.

Recommandation n° 43 : Évaluer la pertinence d'un encadrement législatif des solutions d'identité numérique.

TRAVAUX DES COMMISSIONS

Lors de leur réunion du mercredi 8 juillet 2020, la commission des Lois et la commission des Affaires économiques ont examiné ce rapport d'information et, à l'unanimité, en ont autorisé la publication.

Ces débats ne font pas l'objet d'un compte rendu. Ils sont accessibles sur le portail vidéo du site de l'Assemblée à l'adresse suivante :

http://assnat.fr/9dOeba

LISTE DES RECOMMANDATIONS

- **Déployer rapidement et massivement une solution d'identité numérique régalienne s'appuyant sur FranceConnect**

Recommandation n° 3 : Adjoindre une fonction de signature électronique certifiée au dispositif d'identité numérique en cours de développement.

Recommandation n° 4 : Poursuivre l'ouverture de FranceConnect à un nombre croissant de services publics et privés, en continuant de contrôler de façon transparente le respect des conditions générales d'utilisation de la plateforme par ses différents partenaires.

Recommandation n° 5 : Intégrer la solution d'identité numérique régalienne au sein du fédérateur d'identité FranceConnect.

Recommandation n° 10 : Travailler à l'élaboration de parcours d'identité numérique fluides, à partir de FranceConnect, en particulier dans le cas où un niveau d'authentification supplémentaire est nécessaire pour réaliser, sur le site d'un même fournisseur de services par exemple, une tâche nécessitant un niveau de sécurité plus élevé.

Recommandation n° 11 : Fixer des objectifs ambitieux de déploiement de la CNIe, en privilégiant une cible inférieure à 10 ans (4 à 5 ans au maximum) afin de combler le retard français en matière d'identité numérique.

Recommandation n° 18 : S'appuyer sur des standards ouverts permettant l'intégration de l'identité numérique régalienne dans les solutions des fournisseurs de services pour faciliter le parcours de l'utilisateur.

Recommandation n° 36 : Mettre les solutions d'identité numérique au cœur des réflexions sur la dématérialisation des services publics, qu'elles doivent faciliter.

- **Mobiliser les acteurs économiques pour garantir le succès de l'identité numérique**

Recommandation n° 1: Encourager les utilisations à titre expérimental de l'identité numérique régalienne par les acteurs privés, afin de leur permettre de s'approprier cette nouvelle solution.

Recommandation n° 17 : Favoriser l'apparition d'offres de fournisseurs d'identité privés sur le marché de l'identité numérique, afin de donner le choix aux citoyens dans ce domaine.

Recommandation n° 19 : Définir un modèle économique garantissant la gratuité de l'usage de l'identité numérique pour les citoyens afin d'assurer son déploiement rapide et massif, mais dans lequel le recours, par des fournisseurs de services, aux

solutions régaliennes serait payant, afin de consolider le marché de l'identité numérique.

Recommandation n° 20 : Présenter les éléments principaux du modèle économique de l'identité numérique retenu, afin de permettre aux acteurs économiques d'orienter leurs investissements dans ce domaine.

Recommandation n° 21: Intégrer le déploiement de l'identité numérique en France dans le cadre du prochain plan de relance.

- **Créer les conditions de la confiance**

Recommandation n° 2 : Réaliser un bilan public d'Alicem afin de garantir la confiance dans les solutions d'identité numérique développées par le Gouvernement.

Recommandation n° 7 : Réaffirmer le principe de l'interdiction de l'utilisation des données personnelles traitées par les solutions d'identité numérique régaliennes à des fins commerciales, publicitaires et sécuritaires posant problème quant à la protection des droits des citoyens, et l'indiquer clairement aux utilisateurs.

Recommandation n° 8 : Mettre en place des contrôles réguliers du respect des engagements pris par les partenaires de FranceConnect et assurer la publicité de leurs résultats selon une périodicité déterminée.

Recommandation n° 9 : Assurer un travail de veille sécuritaire constant sur la carte nationale d'identité électronique, en lien avec les acteurs experts de ce domaine.

Recommandation n° 12: Renforcer la communication au sujet de FranceConnect et de la future solution d'identité numérique régalienne, pour en expliciter l'intérêt pour le citoyen, les garanties et l'ensemble des usages offerts à court et moyen termes.

Recommandation n° 28 : Afin de garantir la pleine effectivité du dispositif juridique de l'identité numérique des personnes décédées, publier le décret prévu à l'article 85 de la loi « informatique et libertés » concernant les directives générales qu'une personne décédée peut définir à propos de la conservation, l'effacement et la communication de ses données personnelles.

Recommandation n° 29 : Faire de l'anonymat la situation par défaut et réserver l'authentification en ligne aux seuls services qui nécessitent de connaître l'identité de l'utilisateur.

Recommandation n° 30 : Inscrire la protection des données personnelles dans le domaine de la loi à l'article 34 de la Constitution.

Recommandation n° 31 : Mettre en place une alternative physique à la reconnaissance faciale dans le cadre de la phase d'enrôlement des solutions d'identité numérique régaliennes.

Recommandation n° 32 : Renforcer les moyens de la CNIL.

Recommandation n° 38 : Déployer rapidement le dossier numérique du citoyen.

Recommandation n° 39 : Développer des solutions d'identité numérique transparentes, qui informent les utilisateurs sur le cheminement et les conditions d'accès et de partage de leurs données personnelles avec des tiers.

Recommandation n° 40 : Favoriser le développement d'alternatives à l'identité numérique régalienne, comme l'identité numérique auto-souveraine, en exploitant les possibilités offertes par la *blockchain*.

Recommandation n° 41 : À l'étape de la conception des solutions d'identité numérique, associer les citoyens, les universitaires et les acteurs et groupements du numérique à la définition des besoins et des attentes des utilisateurs.

Recommandation n°42 : Engager une réflexion sur la gouvernance du numérique pour assurer davantage de lisibilité et un niveau de confiance plus élevé des citoyens.

Recommandation n° 43 : Évaluer la pertinence d'un encadrement législatif des solutions d'identité numérique.

- **Donner une vraie place aux collectivités locales pour inscrire l'identité numérique au sein des territoires**

Recommandation n° 13 : Renforcer l'association des collectivités au projet d'une identité numérique régalienne en leur garantissant un niveau d'information élevé et en les incluant dans la mise en place de la délivrance de cette identité.

Recommandation n° 14 : Définir précisément, en concertation avec les collectivités, une « feuille de route » pour le déploiement de la CNIe en leur sein, afin de favoriser la création de synergies. Créer un comité de pilotage chargé de coordonner son déploiement, en lien avec les collectivités.

Recommandation n° 15 : Créer des équipes-projets, en lien avec l'équipe centrale, travaillant spécifiquement au déploiement de la CNIe sur le terrain.

- **Mettre la formation et l'inclusion au cœur de l'identité numérique**

  - ***Formation***

Recommandation n°16 : Déployer des formateurs sur l'ensemble du territoire, notamment dans les lieux de délivrance de l'identité numérique.

Recommandation n° 22 : Poursuivre les efforts en matière d'éducation au numérique dans les établissements scolaires, y compris dans les programmes d'enseignement moral et civique, y en mentionnant spécifiquement les enjeux de

protection des données personnelles et d'usurpation d'identité soulevés par l'identité numérique.

Recommandation n° 23 : Renforcer la formation continue aux outils numériques, en y intégrant les questions relatives à l'identité numérique et mettre en place un volet numérique dans tous les parcours d'insertion professionnelle et dans les bilans professionnels.

Recommandation n° 24 : Assurer la formation du corps associatif et des aidants numériques afin de garantir aux publics fragiles un accompagnement au numérique de qualité.

Recommandation n° 35 : Étendre le recours au Pass Numérique.

Recommandation n° 37 : Élever le niveau de l'ensemble des personnels de la fonction publique sur les sujets numériques par un vaste plan de formation.

- ***Inclusion***

Recommandation n° 6 : Valoriser les retours d'expérience issus des expérimentations d'AidantsConnect et déployer ce service avant la fin de l'année 2020 sur l'ensemble du territoire national. Garantir pour la personne aidée la transparence des décisions prises en son nom par l'aidant.

Recommandation n° 25 : Accroître les financements aux associations qui assurent l'accompagnement numérique des publics fragiles.

Recommandation n° 26 : Proposer la délivrance d'une identité numérique à tous les moments clé de la vie du citoyen, y compris à l'occasion du service national universel.

Recommandation n° 27 : Lancer une réflexion interministérielle sur les mineurs et l'identité numérique.

Recommandation n° 33 : Développer des solutions d'identité numérique inclusives qui prennent en compte les besoins et les fragilités des publics les plus éloignés du numérique.

Recommandation n° 34 : Maintenir des alternatives physiques à la dématérialisation des services publics.

LISTE DES PERSONNES ENTENDUES ET DES CONTRIBUTIONS ÉCRITES REÇUES

I. LISTE DES PERSONNES ENTENDUES

Chercheurs et universitaires

- M. Stéphane Chauvier, professeur de philosophie morale et politique
- Mme Daniele Bourcier, directrice de recherche émérite au CNRS
- Mme Betty Mehri, doctorante au CNRS
- M. Fabrice Mattatia, docteur en droit
- Mme Bénédicte Bévière-Boyer, maître de conférences HDR en droit privé
- M. Michaël Bardin, maître de conférences en droit public
- Mme Valérie Schafer, professeure d'histoire européenne contemporaine
- Mme Fanny Georges, maître de conférences en sciences de l'information et de la communication
- M. François Pellegrini, informaticien et professeur à l'université de Bordeaux,
- Mme Valérie Fernandez, professeure, co-présidente de la Chaire internationale de recherche dédiée à l'identité numérique responsable (INR)
- Mme Laura Draetta, professeure, co-présidente de la Chaire internationale de recherche dédiée à l'identité numérique responsable (INR)
- M. Guy de Felcourt, consultant en matière d'identification numérique et de gestion des données, auteur de l'ouvrage *L'usurpation d'identité ou l'art de la fraude sur les données personnelles*
- M. Pierre-Antoine Chardel, professeur à l'Institut Mines-Télécom (IMT-BS), chercheur invité au MédiaLab EA 7033, Sciences Po-Paris, membre de l'Institut interdisciplinaire d'anthropologie du contemporain
- M. Thibault Douville, professeur de droit à l'université de Caen
- Mme Claire Levallois-Barth, enseignante-chercheure en droit à Télécom ParisTech
- M. Dominique Boullier, sociologue, professeur à l'Institut d'études politiques de Paris
- M. Emmanuel Netter, membre du réseau Trans Europe experts
- Mme Fabienne Jault-Seseke, membre du réseau Trans Europe experts
- M. Jean-Gabriel Ganascia, professeur d'informatique à la faculté des sciences de Sorbonne Université

- Mme Primavera De Filippi, chercheuse au CNRS
- M. François Perea, professeur à l'université Paul-Valéry – Montpellier 3
- M. Baptiste Robert, chercheur en informatique spécialisé dans la recherche de vulnérabilités logicielles

Associations et *think tanks*

- **« None of your business », organisation à but non lucratif**
  - — Mme Juliette Leportois, membre
  - — M. Gaëtan Goldberg, membre
- **Fondation Petits Frères des Pauvres**
  - — M. Philippe Lacroix, directeur
  - — Mme Ludivine Grimber, responsable du pôle projets
- **Croix Rouge**
  - — Mme Emily Rowley, chargée de mission inclusion numérique
  - — Elsa Hajman, responsable du pôle inclusion sociale
- **Emmaüs Connect**
  - — Mme Charlotte Bougenaux, directrice adjointe
  - — M. Tom-Louis Teboul, responsable du développement et des partenariats
- M. Lucien Castex, secrétaire général d'Internet Society France
- **Renaissance Numérique**
  - — M. Philippe Régnard, secrétaire général
  - — Mme Jennyfer Chrétien, déléguée générale
- **Social Media Club France (SMCF)**
  - — M. Emmanuel Parody, directeur des publications du groupe mind-FrontlineMedia,
  - — Mme Johana Sabroux
- Mme Estelle Massé, analyste politique à Access now

- Mme Chloé Berthélémy, *Policy Advisor* à European Digital Rights
- **GenerationLibre**
  - — Mme Isabelle Landreau, docteur en droit, expert GenerationLibre et co-auteur du rapport *Mes data sont à moi* (janvier 2018)
  - — Mme Mathilde Broquet-Courboillet, directrice de la stratégie et du développement du *think tank*
  - — M. Christophe Seltzer
- **La Quadrature du Net**
  - — M. Martin Drago, juriste
  - — M. Benoît Piédallu, membre

Administrations

- M. Cédric O, secrétaire d'État chargé du numérique
- **Autorité de régulation des communications électroniques et des postes**
  - — M. Serge Abiteboul, membre du collège
  - — M. Jean Cattan, conseiller du président
- M. Jérôme Letier, directeur de l'Agence nationale des titres sécurisés
- M. Pierre-Louis Rolle, directeur de la Mission Société Numérique
- Mme Bérengère Aujard, intrapreneuse Aidants Connect.
- Mme Stéphanie Combes, présidente du Health Data Hub
- **Caisse nationale d'assurance maladie**
  - — M. Bruno Noury, responsable du département SESAM-vitale au sein de la Direction déléguée à la gestion et à l'organisation des soins (DDGOS)
  - — M. Claude Gissot, directeur de la stratégie, des études et des statistiques
  - — M. Alain Issarni, directeur délégué des systèmes d'information
  - — Mme Véronika Levendof, responsable département juridique
- Mme Kristel-Amelie Aimre, conseillère chargée des affaires économiques à l'Ambassade d'Estonie en France
- M. Tore Keller, conseiller chargé des affaires politiques et économiques à l'Ambassade du Danemark en France

- **Service public fédéral belge de l'intérieur**
  - — M. Thierry de Grunne, conseiller au cabinet du ministre de la sécurité et de l'intérieur de Belgique,
  - — M. Bart Vrancken, chef de service de la transformation digitale et innovation
- Mme Sophie Kwasny, responsable protection des données à la direction générale des Droits de l'Homme et État de droit du Conseil de l'Europe
- **Commission nationale de l'informatique et des libertés**
  - — Mme Marie Laure Denis, présidente
  - — M. Bertand Pailhès, directeur des technologies et de l'innovation
  - — Mme Émilie Seruga-Cau, cheffe du service des affaires régaliennes et des collectivités territoriales
  - — Mme Tiphaine Havel, conseillère pour les questions institutionnelles et parlementaires
- **Délégation ministérielle du numérique en santé**
  - — M. Dominique Pon, responsable stratégique de la transformation du numérique en santé
  - — M. Raphaël Beaufret, directeur de projet « identification »
- M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information
- Mme Valérie Peneau, directrice du programme interministériel France Identité numérique
- M. Nadi Bou Hanna, directeur interministériel du numérique

<u>Acteurs économiques</u>

- **Cisco**
  - — M. Guillaume Sauvage de Saint Marc, directeur de l'innovation
  - — Bruno Bernard, directeur des affaires publiques
- M. Alexandre Breining, responsable conformité de Betclic.fr
- **MAÏF**
  - — M. Guillaume Rincé, directeur de la technologie
  - — M. Stéphane Tisserand, responsable des affaires publiques

- **IDEMIA**
  - — M. Pierre Lelièvre, senior vice-président des activités relatives à l'identité digitale
  - — Mme Céline Stierlé, responsable des relations presse et des affaires publiques
- **Alliance pour la confiance numérique (ACN)**
  - — M. Alban Féraud, président du groupe de travail sur l'identité numérique
  - — M. Yoann Kassianides, délégué général
- **Française des jeux**
  - — M. Charles Lantieri, directeur général délégué
  - — Mme Sophie Metras, directrice clients
  - — Mme Marion Huge, directrice de la régulation et des affaires publiques
  - — Mme Nadjet Boubekeur, responsable des affaires parlementaires
- **Association pour le développement des actifs numériques**
  - — M. Simon Polrot, président
  - — M. Alexandre Stachtchenko, directeur général de Blockchain Partner
  - — M. François-Xavier Thoorens, président d'Ark Ecosystem
- **IN Groupe**
  - — M. Bruno Chappert, vice-président exécutif
  - — M. Patrick Montliaud, vice-président exécutif
  - — M. Romain Galesne-Fontaine, directeur des relations institutionnelles
- **Docapost**
  - — M. Olivier Vallet, président directeur général
  - — Mme Candice Dauge, directrice du programme « identité numérique » du groupe La Poste
  - — Mme Smara Lungu, déléguée aux affaires territoriales et parlementaires
- **Conseil supérieur du notariat**
  - — M. Jean François Humbert, président
  - — M. David Ambrosiano, premier vice-président
- **Conseil national des greffiers des tribunaux de commerce**
  - — Mme Sophie Jonval, présidente
  - — M. Thomas Denfer, vice-président

- **Conseil national des barreaux**
  - — Mme Sandrine Vara, présidente de la commission numérique
  - — M. Louis Degos, président de la commission prospective
  - — Mme Sophie Ferry-Bouillon, membre de la commission Libertés et droits de l'homme.
- Mme Beatrice Oeuvrard, chargée des affaires publiques de Facebook France
- **Google France**
  - — M. Olivier Esper, *Public Policy, Senior Manager*
  - — Mme Floriane Fay, *Public Policy Manager*
  - — Mme Charlotte Radvanyi, *Policy Senior Analyst*
- **Orange**
  - — Mme Amelia Newsom-Davis, directrice des services payants
  - — M. Éric Mora, directeur mobile et sécurité
  - — Mme Claire Chalvidant, directrice adjointe des affaires publiques
  - — M. Simon Becot, responsable du projet de recherche Identité de l'Orange Labs service

II. LISTE DES CONTRIBUTIONS ÉCRITES REÇUES

- Secrétariat général des affaires européennes
- Défenseur des droits
- Association des départements de France
- Fédération internet nouvelle génération (Finc)
- American Express
- MasterCard
- Commission européenne – DG Connect
- Groupement des cartes bancaires CB
- Syntec Numérique