RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

conseil national du numérique

Rapport
Juin 2020

Identités numériques
Clés de voûte de la citoyenneté numérique

SOMMAIRE

ÉDITORIAL

En France, depuis la création de l'état civil, en 1792, la gestion de l'identité est une prérogative de l'État. Les mutations économiques, sociales et politiques induites par l'immiscion du numérique dans toutes les étapes de notre vie nous invite à refondre les formes de notre citoyenneté, de notre compétitivité, de notre mode de vie, de notre vivre-ensemble en préservant des valeurs et un modèle de société qui nous ressemblent.

Nous voyons se tisser sous nos yeux chaque jour un monde numérique qui investit et transforme notre quotidien parfois insidieusement, et qui bouleverse et redéfinit les liens et les valeurs à l'aune d'usages nouveaux et de préoccupations originales.

Cela impose que ce lien entre l'identité, garantie par l'État, et l'identité numérique, jusque-là plutôt associée aux fournisseurs de services privés, soit réinstauré et affirmé avec force.

Le contexte actuel –nous y reviendrons- impose de redéfinir en profondeur les liens qui nous unissent individuellement à l'État, mais aussi aux autres, dans ce qui constitue notre modèle de société et nos valeurs communes. Aujourd'hui, il existe un trop grand nombre de sites demandant au grand public de prouver son identité en ligne. Par une harmonisation du biais par lequel l'identité réelle de la personne est assurée en ligne, l'identité numérique offrira plus de garanties de sécurité aux citoyens pour de nombreux usages publics et privés.

Par ailleurs, nous ne pouvons faire l'économie de l'impact créé par les nombreuses affaires médiatiques récentes (Cambridge Analytica, fuites de données massives, ...) qui ont altéré la confiance que les citoyens accordent aux fournisseurs d'identité privés. De la même manière, les mésusages, usurpations d'identité et autres fraudes en ligne ont créé chez les citoyens un besoin accru de protection de la part de la puissance publique. À l'ère où le numérique s'immisce dans nos usages quotidiens, de façon souvent peu lisible dans ses enjeux, les questions de surveillance généralisée et de protection des données se ravivent avec force et la prise en compte de cet écueil nous semble un préalable indispensable pour renforcer la confiance des citoyens dans le numérique.

Aujourd'hui, alors que 92,4 % des Français utilisent internet, et que 59 % utilisent les réseaux sociaux, à l'heure où l'administration sera entièrement dématérialisée à l'horizon 2022, il est indispensable de travailler et réfléchir à construire une identité numérique maîtrisée et sécurisée. Ces chiffres ne prennent pas en compte les citoyens pas ou peu à l'aise avec les outils numériques, qu'il convient d'accompagner dans l'acquisition d'une littératie numérique leur permettant d'être autonomes dans leurs démarches en ligne. C'est à ces conditions que de nouveaux usages pourraient être conçus et développés en jouissant d'une assise d'usagers en capacité de les mobiliser et de les développer pleinement. L'identité numérique est la clef de voûte de cette nouvelle réalité. Il s'agit de l'élément pivot qui déterminera de quelle manière chacun de nous pourra accéder à la multiplicité des usages qui forment notre vie quotidienne, dans le respect de sa liberté, de son intégrité et de son individualité.

L'identité numérique régalienne doit permettre tant à la fois de simplifier la vie des Français, de faciliter leurs démarches administratives tout en

protégeant leur vie privée. Nous sommes pleinement convaincus que seule une mise en perspective croisée entre la voix de la société civile et les acteurs de cet écosystème dédié à l'identité numérique peut nous aider à prendre la bonne direction.

A ce titre, nous plaidons, au Conseil National du Numérique, pour que l'identité numérique régalienne soit appréhendée et conçue en tant que service public à part entière, engageant dans ses principes les valeurs de protection de l'usager, de frugalité des données, de confiance et d'égalité de tous les citoyens dans l'accès aux droits et à la puissance publique.

Un contexte inédit qui interroge avec force l'identité numérique de demain

L'identité numérique étant fortement liée à la vie civique et à la vigueur des liens de confiance réciproque entre les citoyens et l'État, nous avons choisi, au Conseil, de tenir compte du contexte inédit de la pandémie du COVID-19 survenue en fin d'année 2019. Il ne s'agit pas, dans ce rapport, de tirer des conclusions hâtives, mais bien d'illustrer que la relation de confiance doit préexister à toute démarche d'urgence, car elle garantit l'adhésion et la pleine participation des citoyens.

Par ailleurs, ce rapport de confiance participe à construire un pouvoir d'agir des citoyens dans la résolution collective des problèmes rencontrés dans des cas de crise majeure tels que celui-ci, en plaçant le citoyen comme l'un des pivots de la résolution de la crise, ne serait-ce que par sa délégation de confiance à l'État et son appui aux solutions mises en place.

Les conditions drastiques de cette crise (confinement strict, contrôle de la circulation des citoyens, système de santé en tension…) et la numéricité croissante que celle-ci impose (télétravail généralisé, expansion rapide de l'économie numérique des biens et services, mise en place de nouveaux processus de mise en arrêt maladie…) ont accéléré l'accès à des usages nouveaux publics ou privés. Cette mise en tension révèle aussi la place proéminente de l'État dans la gestion de cette crise et l'indispensabilité criante d'un numérique de confiance pour que la vie continue d'avancer malgré les conditions les plus strictes jamais connues dans l'ère contemporaine en France. Ce contexte inédit nous aura permis de mettre à la lumière criante de cette crise les liens réciproques qui unissent les citoyens à l'État.

Nous pensons, au Conseil national du numérique, que l'identité numérique est l'outil majeur qui nous permettra d'éclairer notre rapport à l'État et aux nouveaux acteurs émergents. Pour nous, l'identité numérique permettra de dessiner la voie juste, utile et efficace d'une administration dématérialisée de confiance, inclusive et accessible au service de l'usager. Par ailleurs, la crise du COVID-19 a mis en lumière la puissance des solutions développées par des acteurs privés étrangers et l'urgence, pour la France, de développer des réponses souveraines et fidèle à nos valeurs.

Eu égard à la situation actuelle, une identité numérique bien pensée pourrait également, à l'avenir, faciliter, au moins partiellement, certains enjeux posés par des contextes de crises comme celui que nous vivons

actuellement. Elle pourrait également, comme l'appelle de ses voeux l'écosystème que nous avons consulté, dégager de très fortes externalités positives qui seraient bénéfiques à tous : innovation, emplois, attractivité française… Nous sommes confiants dans la capacité de la puissance publique à faire les choix éclairés qui sauront accompagner la mise en place d'une identité numérique citoyenne, de confiance, inclusive, dynamique et propice au développement d'innovations : soit *une identité numérique à la française.*

Karine Dognin-Sauze et Mohammed Boumediane,
pilotes du groupe de travail

Gilles Babinet, Olivier Clatz, Gaël Duval, Jean-Michel Mis,
membres du groupe de travail.

Leila Amanar et Nathalie Bouarour,
rapporteures du groupe de travail.

SYNTHÈSE DU RAPPORT

Ce rapport a été commandé par le secrétaire d'État chargé du Numérique dans une saisine de juillet 2019. Il commence par un propos introductif permettant de qualifier et de définir le lien entre citoyenneté et identités numériques (1). Ces définitions établies, l'accent est mis sur la perspective européenne, et les différentes actions menées par la Commission (2). Cette perspective permet d'éclairer l'historique national des différents projets d'identité numérique et le cadre légal associé (3). Enfin l'accent est mis sur les leviers de l'identité numérique qui ont permis à l'étranger de faire émerger une identité numérique, support d'une forme de citoyenneté (4).

Alors que ce rapport établit d'entrée de jeu que l'identité numérique publique est un service public qui se doit d'être universel, le premier chapitre s'intéresse aux actions à mettre en œuvre pour assurer l'égalité de tous devant ce service ainsi que la continuité et l'adaptabilité. En gardant à l'esprit que tous les citoyens n'ont pas la même culture numérique, une cartographie actualisée des points de médiations ainsi que du type de formation disponible dans chacun de ces points doit être proposée à l'usager (recommandation n°1 & 2). Les aidants ont une place primordiale et décisive dans le lien entre citoyens et administration ainsi que dans la transmission de la confiance. Ces derniers doivent être formés aux bonnes pratiques ainsi que protégés à travers un cadre juridique et des outils particuliers. (recommandation n°3).

La fracture numérique doit être prise en compte dans la dématérialisation des démarches administratives, ainsi que les inégalités territoriales en termes de couverture et d'accès au numérique. Cette pratique doit s'inscrire dès la conception des technologies d'identité numérique et de la dématérialisation des démarches et des parcours, en testant l'accessibilité et l'inclusion des designs (recommandation n°4). Ces retours d'expérience sont précieux puisque les parcours et les briques technologiques les plus accessibles pourraient être utilisés pour faire émerger des modèles de référence pour les développements technologiques futurs (recommandation n°5).

La suite de ce chapitre établit que la première interaction entre un individu et son identité numérique est une étape cruciale du processus. Cette étape, l'enrôlement, se doit d'être inclusive, encapacitante (i.e qu'elle leur donne les capacités d'en faire un usage libre et éclairé) et inscrite dans des lieux de confiance pour maintenir la relation entre identité et citoyenneté. Pour se faire il est nécessaire de s'appuyer sur les lieux historiques de l'enrôlement à la carte nationale d'identité que sont les mairies. De plus, si le gouvernement choisissait de déléguer l'enrôlement à un acteur extérieur, il paraît important de définir cette procédure dans un cahier des charges protégeant les citoyens et les personnels (recommandation n°6). En clôture de ce premier chapitre, la communication et la formation sont identifiées comme les deux leviers pouvant mettre en valeur le rôle de l'État face aux identités numériques dans une ère de dématérialisation.

En premier lieu, il conviendrait d'apporter plus de clarté et de transparence à propos des différents projets de l'État. En effet, qu'il s'agisse d'Alicem, de la CNIe ou de France Connect, le manque de communication facilement assimilable par le plus grand nombre nuit

encore trop souvent au projet global (recommandations n°7 et 10). Plus généralement, une médiatisation du fonctionnement des services publics numériques serait bénéfique (recommandation n°8), et pourrait répondre aux différentes craintes éprouvées par les citoyens sur la gestion de leurs données personnelles ainsi que la maîtrise de ces dernières (recommandations n° 9).

En second lieu, et de concert avec le déploiement des identités numériques, les citoyens doivent être formés et acculturés largement au numérique pour développer une réelle citoyenneté numérique. Ces formations auront un impact si elles s'adressent à toutes les classes d'âge (recommandations n°12 et 13). Enfin, étant mandataires d'un pouvoir impactant leurs concitoyens, les élus doivent être formés au numérique (recommandation n°11).

Pour poursuivre sur l'ambition de proposer une identité numérique de confiance, le second chapitre du rapport développe des notions de transparence et de gouvernance, ainsi que de sécurité et de souveraineté. Dans une perspective organisationnelle, la transparence à travers une gouvernance partagée est utile à l'émergence d'outils de confiance auditables et responsables (recommandation n°15).

C'est l'objet de la première partie de ce chapitre, qui veut par la gouvernance, replacer le citoyen au centre du projet d'identité numérique. Si l'administration doit, pour des raisons évidentes, maintenir une vision holistique des projets d'identité numérique déployés, celle-ci ne peut agir seule sans l'appui d'un secteur économique structuré et de collectivités territoriales dotées de ressources humaines, financières et logistiques suffisantes (recommandation n°16).

Par ailleurs, la généralisation des identités numériques permettant de faire valoir sa citoyenneté est un enjeu suffisamment impactant pour recourir à l'instauration de nouveaux dispositifs de gouvernance sociétale comprenant des missions de contrôle et de consultation de la société civile (recommandation n°17 et 18). En effet, faire émerger une instance jouant le rôle de garde-fou permettrait de soutenir des acteurs reconnus, tout en limitant les possibilités de dérives. Enfin, dans cette optique de transparence, le système bénéficierait d'une ouverture des métadonnées issues des connexions des individus au titre de l'open data (recommandation n°20).

Les possibles dérives de l'identité numérique ayant été fréquemment mises en avant lors des consultations, celles-ci doivent être cadrées par des textes législatifs. En premier lieu, en assurant un meilleur encadrement des fournisseurs d'identité privés connectés à la plateforme France Connect. En effet, ces derniers effectuent une partie du service public, notamment au moment de l'enrôlement des usagers. Dans ce cadre, des critères stricts de formation des personnels, de lisibilité des services, de transmissions et stockages des données, de contrôle doivent leur être demandés (recommandation n°19). En second lieu, une loi d'orientation de l'identité numérique soumise au débat démocratique serait bénéfique pour assurer aux citoyens que l'outil a été pensé pour eux et avec eux (recommandation n°21). En dernier lieu, la capacité de mésusages du système par les personnels autorisés est une grande source de défiance. Tout en proposant un système de permissions, pour une meilleure traçabilité, les mésusages

et les détournements de finalité doivent être fortement pénalisés (recommandation n°22).

Dans une approche servicielle et en accord avec le décret sur le « dites-le-nous une fois », il convient de mettre en place les mécanismes garantissant la transparence du système, la traçabilité des accès et le respect du consentement (recommandation n°23).

Alors qu'il est admis que l'architecture et la sécurité sont à prendre en compte pour obtenir un système respectueux des libertés des citoyens, la souveraineté technologique influe elle aussi sur la sécurité du système. C'est l'enjeu de la seconde partie du deuxième chapitre. Dans les réflexions sur l'identité numérique et les schémas d'identification, les normes et les standards sont définis dans des cénacles internationaux dans lesquels une présence française forte doit être maintenue (recommandation n°24). Pour assurer un déploiement pérenne de l'écosystème de l'identité numérique, les normes et les certifications européennes sont à privilégier (recommandation n°25).

Par ailleurs l'Europe, à travers le règlement eIDAS, a déjà une position forte sur le sujet. L'imminence de la révision du règlement pourrait être l'occasion de proposer des améliorations pour assurer le système de revue et de notification, et donc la sécurité des citoyens qui seront bientôt confrontés à des identités numériques extra nationales (recommandations n°26 et 27). De plus, l'ouverture prochaine d'un point d'interopérabilité questionne et nécessite une meilleure documentation sur les développements en cours et les futurs usages (recommandation n°28). Si le règlement propose trois niveaux de sécurité, chacun souhaite proposer le système le plus sûr possible afin de faire correspondre les usages et les services aux niveaux de garantie idoines. De fait, il paraît indispensable de favoriser le développement d'une solution d'identité étatique de niveau substantiel (recommandations n°29 et 30).

Si la maîtrise de la souveraineté technologique a toute son importance dans les instances internationales et européennes, elle est aussi primordiale sur le territoire et au sein même de l'administration. La sous-traitance dans certains domaines peut comporter un grand nombre de risques si l'administration ne fait pas l'effort de recruter des profils techniques compétents, avec des plans de carrière longs, pour être sûre de garder une maîtrise sur les savoirs-faire (recommandations n°31 et 33). Il s'agit donc aussi plus globalement d'impliquer la communauté scientifique pour questionner les choix faits en termes de sécurité par l'Etat (recommandation n°32) ainsi que pour participer à la certification de briques technologiques ou de technologies d'identité numérique.

Dans la perspective où les choix scientifiques sont des choix politiques, quelques arbitrages technologiques sont mis en avant dans la fin du second chapitre afin de réduire les risques sur les libertés individuelles :

- Tout d'abord, il conviendrait d'utiliser une architecture de stockage des informations décentralisée et de chiffrer des données ;
- Les audits, notamment celui du fichier TES qui stocke les données biométriques de la CNIe, mériteraient de voir leur fréquence augmenter (recommandation n°34). De plus, et pour répondre en partie à cette première proposition, il est nécessaire d'augmenter

les ressources et missions de la CNIL puisqu'elles pourraient être davantage sollicitées.

- Ensuite, il serait intéressant que le dispositif CNIe offre des moyens de vérification d'informations sans diffusion des données d'identité des citoyens sur la théorie du zero knowledge proof (ZKP) ;
- Pour finir, faire de la CNIe, un vecteur de la citoyenneté numérique et du principe du « dites-le-nous une fois » pour les usagers multicanaux (recommandation n° 35).

Ce rapport conclut que pour faire émerger une identité numérique « à la française », il faut être attentif à ce que celle-ci soit conçue comme le principal levier d'une citoyenneté numérique. Cette citoyenneté risque d'être interrogée et redéfinie dans les années à venir par des nouveaux usages accompagnés de nouvelles solutions techniques. Les arbitrages et les prises de positions du gouvernement, ainsi que la révision du règlement eIDAS dans les mois à venir vont surement bousculer quelque peu ce rapport, rendant obsolètes certaines de ses parties. Néanmoins, à date, les positions exprimées par le Conseil national du numérique reflète des idéaux en matière de numérique portés depuis de nombreuses années par la société civile et les écosystèmes avec lesquels il est en lien étroit.

LISTE DES RECOMMANDATIONS

Favoriser une solution inclusive et frugale qui rend service aux usagers

Recommandation n°1

Thème : Médiation et cartographie

Recenser les points de médiation numérique dans une cartographie accessible tout au long du parcours utilisateur dans les démarches administratives afin que les usagers puissent s'y référer en cas de difficulté lors de leurs démarches en ligne.

Recommandation n°2

Mettre en place des formations à destination des éloignés du numérique dans des lieux dédiés disposant de moyens conséquents :

- enrôlement sécurisé et formation aux usages les plus simples,
- formation des agents,
- mise à disposition de matériel en libre service,
- harmonisation des offres de formation à l'usage des citoyens en fonction des besoins rencontrés sur le territoire,
- prise en compte des différents niveaux de littératie.

Recommandation n°3

Thème : Aidant Connect

Encadrer par un socle de droits et de garanties légales le développement d'Aidants Connect pour protéger :

- les usagers contre les risques d'usurpation d'identité et les risques de détournement de leurs identités ;
- la responsabilité des aidants lorsqu'ils doivent effectuer des démarches pour les usagers.

Recommandation n°4

Thème : Design et tests utilisateurs
Acteurs : DINUM

Imposer des critères d'accessibilité et d'inclusion dans la conception des services s'appuyant sur l'identité numérique qui soient régulièrement testés.

Recommandation n°5

Thème : Design, sécurité et fluidité
Acteurs : DINUM

Formuler un cahier des charges à destination des fournisseurs d'identités posant un certain nombre d'exigences en termes de sécurité et de fluidité, tout en garantissant des bénéfices d'usages déjà acquis.

Recommandation n°6

Thème : Inclusion–Lieu d'enrôlement

Faire des mairies (et des collectivités territoriales) les principaux lieux d'enrôlement des identités numériques pour soutenir la confiance en l'État

Faire preuve de pédagogie et initier l'ensemble des citoyens au numérique

Recommandation n°7

Créer une réelle communication autour de France Connect et la création de la CNIe.

Recommandation n°8

Thème : Communication–Fonctionnement service public et gestion des informations dématérialisées
Acteurs : Programme interministériel–Ambition 2022

Pour répondre aux craintes des usagers vis-à-vis de potentiels abus et du manque de transparence de la puissance publique, et en lien avec les recommandations 15 à 18 et 21 et 22, le Conseil recommande de communiquer massivement sur le fonctionnement des services publics et de la gestion des informations dématérialisées :

- Obligations légales encadrant les solutions techniques déployées pour le stockage des informations et en particulier des données personnelles ;
- Obligations légales définissant les informations relatives aux usagers qui peuvent être transmises entre administrations centrales et locales. Choix des mécanismes de frugalité pour en garantir la confidentialité ;
- Existence d'instances de contrôle vérifiant que les obligations légales sont respectées.

Recommandation n°9

Thème : Communication–Données personnelles–CNIL
Acteurs : CNIL

Puisqu'elles contribuent au fondement de leurs identités numériques au sens large, le Conseil recommande d'informer les citoyens sur leurs droits vis-à-vis de leurs données personnelles. En plus d'un apprentissage sur le long terme à destination de élèves du primaire et du secondaire, le Conseil recommande qu'un budget soit alloué à la CNIL pour réaliser des campagnes de communication sur les données personnelles dans des grands médias et à des heures de grande écoute.

Recommandation n°10

Thème : Communication–France Connect
Acteurs : DINUM
Engager France Connect dans une réflexion sur la manière dont il explique :

1. Son architecture ;
2. Les rapports entre les différents fournisseurs d'identité et fournisseurs de services ;
3. Les différents niveaux de sécurité eIDAS ;
4. Le nœud d'interopérabilité européen.

Recommandation n°11

Former l'ensemble des élus et des personnels des collectivités au numérique, en s'appuyant sur des parcours de formation obligatoires inscrits dans un répertoire national de formation régulièrement mis à jour.

Recommandation n°12

Thème : Formation adultes
Acteurs : MSAP avec fonds spécifiques alloués, Mission société numérique et Agences des territoires

Pendant les cinq premières années de déploiement du dispositif, le Conseil recommande que l'État mette en place des formations gratuites en dehors des périodes de travail à destination des publics majeurs.

Recommandation n°13

Acteurs : Détacher des ressources de l'Éducation Nationale pour avoir une cohérence avec la formation des mineurs

Créer un parcours de formation qui corresponde aux besoins de citoyenneté numérique pour les élèves de primaire et du secondaire, afin que ceux-ci soient armés pour leurs premiers usages autonomes.

Recommandation n°14

Thème : Formation continue–Éducation nationale
Acteurs : DNE, Éducation civique

En complément des formations, nous recommandons que l'État mette en place :

- Une plateforme regroupant l'ensemble des cours à destination des publics adultes, ainsi que les textes en lien avec la thématique ;
- Que soit organisé, annuellement, un programme de communication sur le sujet sur les médias de forte audience. Le premier cycle devrait traiter de l'identité numérique en lien avec les décisions de l'État concernant la dématérialisation des services publics.

Opter pour une gouvernance partagée qui replace l'usager au centre

Recommandation n°15

Thème : Transparence
Acteurs : A destination de l'instance jouant un rôle de garde fous CSGIN

Mettre en place des outils de transparence et de contrôle démocratique déjà utilisés dans d'autres cadres. Notamment :

- Publication de bilan annuel par les opérateurs d'identité numérique : coûts et investissements dans l'identité numérique, explication des choix technologiques, appels d'offres publics, formations des personnels administratifs et extérieurs, etc. ;
- Audit externe annuel des systèmes les plus critiques par l'ANSSI et la CNIL, en complément des audits de l'usabilité des systèmes (cf. recommandation n°1)

Recommandation n°16

Thème : Gouvernance partagée
Acteurs : Ministère du Territoire, DINUM, Ministère de l'Intérieur, Programme interministériel

Établir une feuille de route, associée à un budget propre, sur le déploiement par les mairies de l'identité numérique, co-construite avec les territoires sous le pilotage de la mission interministérielle, en lien étroit avec les ministères de l'intérieur et de la cohésion des territoires et des relations avec les collectivités territoriales.

Recommandation n°17

Thème : Gouvernance sociétale
Acteurs : Création d'un nouvel acteur : Commission de Suivi et de Gestion des Identités Numérique (CSGIN)

Créer une instance de contrôle et de supervision indépendante et multi parties prenantes (académiques, associatifs, administratifs, etc.), nommée Commission de Suivi et de Gestion des Identités Numériques (CSGIN).

Recommandation n°18

Thème : Gouvernance sociétale–Forum citoyens
Acteurs : CSGIN

Accorder à l'instance 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 ». De plus, la CSGIN pourrait soutenir l'animation locale des débats en aidant les acteurs territoriaux tels que les Maisons France Service.

Recommandation n°19

Thème : Contrat pour les fournisseurs d'identité privés au titre d'une délégation de service public et consentement des usagers
Acteurs : DINUM (pour l'intégration à FC), Ministère de l'Intérieur si utilisation des certificats présents sur la CNIe.

Soumettre les fournisseurs d'identité privés à un contrat qui définisse la délégation du service public qu'ils effectuent en fonction du type d'action qu'ils prennent en charge. Le contrat de délégation de service public devrait être guidé par un principe de loyauté dans l'intérêt général et dans l'intérêt des utilisateurs qui participe plus largement du principe de loyauté des relations contractuelles.

Recommandation n°20

Thème : Open data
Acteurs : DINUM

Rendre public, au titre de l'open data, les métadonnées issues des connexions des individus, de manière anonyme et agrégée, de sorte à :

- Éviter qu'une structure (plus importante qu'une autre) ne bénéficie des externalités positives d'un système créé par l'État sans redistribution ;
- Permettre de favoriser l'innovation et la recherche.

Recommandation n°21

Thème : Contrôle législatif
Acteurs : Parlementaires

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.).

Recommandation n°22

Thème : Cadre règlementaire
Acteurs : Parlementaires

Instaurer un cadre réglementaire qui permette notamment une pénalisation rapide des mésusages, en particulier des personnes en capacité d'abuser de leurs prérogatives professionnelles. Pour dissuader toutes formes de mésusages, le Conseil recommande que des sanctions fortes (amendes, pénalisation, etc.) soient renforcées et précisées.

Recommandation n°23

Thème : « Dites-le nous une fois » et partage de données.
Acteurs : DINUM

S'appuyer sur les recommandations du Conseil de 2015 soit :

- « *Permettre à chaque usager de visualiser les échanges de données entre les administrations pour la délivrance d'un service, ainsi que leur durée de conservation ;*
- *Prévoir le consentement de l'usager par défaut pour l'échange d'informations personnelles entre les administrations, sous réserve des cas d'échanges sans autorisation prévus par la loi ou par décret.* »

Assurer une sécurité de tous

Recommandation n°24

Thème : Souveraineté–Présence dans les instances supra nationales
Acteurs : MAE

Renforcer la représentation française dans les instances de normalisation européennes et internationales. Celles-ci constituent un lieu stratégique d'influence et de création de normes autour de l'identité numérique. Il s'agit d'un rôle essentiel du ministère des Affaires Étrangères de suivre ces thématiques et d'allouer les ressources nécessaires pour effectuer un travail de veille et d'influence éclairés, avec l'appui des autres ministères concernés.

Recommandation n°25

Thème : Souveraineté–Capacité d'évaluation des technologies
Acteurs : ETSI, CEN

S'appuyer sur des standards qui proviennent d'instituts de normalisation européens (ETSI, CEN) qui seraient reconnus nationalement comme le propose la Commission Européenne. En effet, « *dans le cadre du Mandat M/460, ayant pour objectif de fournir une réponse coordonnée sur le sujet du déploiement d'un marché européen digital unique, l'ETSI (European Telecommunications Standards Institute) et le CEN (Comité Européen de Normalisation) se sont vus confier la mission d'élaborer des normes relatives aux services de confiance prévus par eIDAS.* » Dans un second temps, la certification devrait être effectuée par des organismes évoluant avec les mêmes règles de droit que les entreprises en quête de validation et que les organismes promoteurs de normes.

Recommandation n°26

Thème : Révision du règlement eIDAS
Acteurs : ANSSI, Commission Européenne

Clarifier les exigences du règlement eIDAS pour les niveaux de garantie substantiel et élevé.

1. Standardiser le processus d'examen par les pairs notamment en terme de référentiel documentaire et de méthodologie, et clarifier son objet et son périmètre ;
2. Définir un corpus documentaire reprenant les informations qui doivent être automatiquement communiquées par les États membres sur leurs schémas d'identification électronique

Recommandation n°27

Thème : Révision du règlement eIDAS
Acteurs : ANSSI, ComMission Européenne

Préciser dans le règlement eIDAS les critères minimaux relatifs à l'identification à distance. Une harmonisation et des modalités d'évaluation de la fiabilité des méthodes d'identification à distance (par exemple, le nombre de défis à effectuer par l'utilisateur dans le cadre de la reconnaissance faciale, ou encore une standardisation du taux de faux positifs/faux négatifs impactant le pourcentage d'identification) seraient bienvenues afin d'harmoniser les pratiques mises en œuvre dans les États membres.

Recommandation n°28

Thème : eIDAS–noeud d'interopérabilité
Acteurs : DINUM, ANSSI

Publier davantage d'informations concernant la mise en place du nœud eIDAS français. De plus, il paraît nécessaire que celui-ci ne soit pas supporté uniquement par le service en charge de France Connect au sein de la DINUM mais que des ressources spécifiques y soient dédiées. Enfin, il doit être construit en étroite collaboration avec l'ANSSI et la CNIL.

Recommandation n°29

Thème : eIDAS–niveau substantiel
Acteurs : ANSSI, Commission Européenne, Programme interministériel

Revaloriser le niveau de garantie substantiel grâce à une solution d'identité numérique publique correspondante (après avoir déterminé les cas d'usage type pour ce niveau. Cf. recommandation n°30)

De plus il serait pertinent d'inciter les États ayant déjà une solution de niveau élevé à faire émerger une solution de niveau substantiel. La France pourrait dès à présent s'engager dans cette voie.

Recommandation n°30

Thème : Homogénéisation des niveaux de sécurité des démarches
Acteurs : DINUM, ANSSI, sous le pilotage des administrations concernées

Définir, sous le pilotage des administrations concernées, les niveaux de garantie nécessaires pour chaque service en ligne et créer une doctrine à destination des administrations pour leur permettre d'établir aisément le niveau de garantie des nouveaux services publics.

Recommandation n°31

Thème : Compétences techniques

S'assurer que les compétences que l'État sollicite à l'extérieur soient aussi maîtrisées en interne afin de ne pas se retrouver dans des situations de dépendance vis-à-vis des sous-traitants, de mise en risque de la pérennité du système, de perte de l'historique technique du système (erreurs, correction des erreurs, motifs et choix d'architecture, etc.).

Il est nécessaire que des compétences techniques soient recrutées massivement avec un plan de carrière leur permettant de s'inscrire sur le long terme dans l'administration, et que ces nouveaux agents soient intégrés à la mission identité numérique idoine de la DINUM.

Recommandation n°32

Thème : Evaluation scientifique (issue de TES)
Acteurs : ANSSI, INRIA

Consulter la communauté scientifique en appui de l'instance de gouvernance, concernant les choix de sécurité pour les technologies déployées par l'État notamment à travers :

- Une analyse de la solution
- L'évaluation des risques et des coûts
- L'élaboration de l'architecture

Recommandation n°33

Thème : Souveraineté

Attribuer des budgets pour la certification de technologies d'identité numérique, et/ou de briques technologiques liées à l'identité numérique. Il est nécessaire de répondre aussi aux besoins des entreprises de l'écosystème qui ne souhaitent pas proposer un schéma complet d'identité numérique mais seulement une brique technologique. De fait, des fonds définis précédemment permettraient d'alimenter une certification sous le principe de revue par les pairs, en lien avec les pôles d'excellence académique nationaux, l'ANSSI et la CSGIN.

Recommandation n°34

Thème : TES–audits réguliers du système
Acteurs : ANSSI, CNIL

Effectuer de manière régulière et impromptue des audits et des contrôles (par l'ANSSI et la CNIL), du fichier TES et des usages qui en sont faits.

Recommandation n°35

Thème : CNIe–certificats pour permettre la poursuite du Dites-le-nous une fois dans les parcours multicanaux
Acteurs : Programme intérministériel, Identité numérique

Insérer dans la carte nationale d'identité électronique (CNIe) un certificat d'autorisation à destination des personnels administratifs, pour accéder en guichet à des informations déjà connues de l'administration sans que l'usager ait besoin d'apporter ses documents. Néanmoins, il faudra mettre en place une forme de consentement explicite à cette transmission dans les parcours administratifs (par exemple la signature sur écran).

SAISINE DU CONSEIL NATIONAL DU NUMÉRIQUE ET MÉTHODOLOGIE DE TRAVAIL

Le Conseil national du numérique a entamé dès janvier 2019 une réflexion sur l'identité numérique fort d'avis en lien avec le sujet tel que sur le fichier TES de 2016[1] ou ses travaux sur la citoyenneté numérique de 2013[2]. Il a été saisi en juillet 2019 par le secrétaire d'État auprès du ministre de l'Économie et des Finances et du ministre de l'Action et des comptes publics, chargé du Numérique pour :

- « *explorer et développer le concept de citoyenneté numérique, nationale et européenne, dont l'identité numérique est porteuse ;*
- *proposer, en fonction des besoins identifiés, des éléments de communication et de pédagogie qui accompagneront la mise en œuvre de l'identité numérique afin d'en améliorer la compréhension et favoriser son caractère inclusif ;*
- *s'assurer, sur la base des expérimentations conduites par le programme interministériel[3], de l'ergonomie, de la facilité d'usage et de la qualité des supports utilisateurs associés aux solutions retenus, afin de s'assurer de leur adoption par le plus grand nombre d'utilisateurs, dans une démarche d'inclusion.* » [4]

Pour répondre à ces questionnements, le Conseil s'est appuyé sur la littérature scientifique ainsi que les divers rapports publiés ces dernières années. Il a organisé dès janvier 2019 une première journée collaborative sur la thématique de l'identité numérique qui a permis à 24 experts d'échanger autour de trois axes de réflexion : marché et usages, protection des données et cybersécurité, et citoyenneté. Les membres du groupe de travail ainsi que les rapporteures ont effectué un voyage d'étude en Estonie où ils ont pu échanger avec les personnels[5] de l'e-Governance Academy, l'Autorité des systèmes d'Information (RIA), la Commission de la Police et des Gardes-frontières, e-Estonia Briefing Center, le bureau du vote Électronique, et le Foresight Centre dédié aux scénarios prospectifs de l'e-government. Il a aussi réalisé une étude comparée internationale des différentes solutions choisies par les États et un déplacement à Bruxelles.

De plus sept consultations dans différentes villes de France (Paris, Lyon, Montpellier et Douai) ont été organisées. Ces consultations ont été articulées comme suit :

- les consultations de citoyens (ouvertes à tous sans pré-requis, médiatisées au plus grand nombre sur les réseaux sociaux et à travers la mailing-list du Conseil) ;
- les consultations d'experts (sur invitation).

Dans ce cadre, plus de 150 personnes ont pu s'exprimer sur le sujet.

Enfin, le Conseil a auditionné 57 personnalités issues des administrations, du monde économique et du monde universitaire. Une liste exhaustive est disponible en annexe.

1 Avis du Conseil national du numérique sur le fichier TES, décembre 2016.
2 Rapport du Conseil national du Numérique, Jules Ferry 3.0., octobre 2014.
3 Le programme interministériel a été officiellement installé en janvier 2019 comme le précise la lettre de mission.
4 Voir la lettre de saisine en annexe.
5 Le Conseil remercie particulièrement l'Ambassadeur de France en Estonie, M. Éric Lamouroux, ainsi que ces équipes qui ont participé à l'organisation de ces rencontres.

INTRODUCTION
LES IDENTITÉS NUMÉRIQUES : DE L'EUROPE AU MODÈLE FRANÇAIS

1. L'IDENTITÉ NUMÉRIQUE : UN SUJET COMPLEXE QUI FAIT RÉAGIR LES CITOYENS

1.1. De la citoyenneté numérique au service public de l'identité numérique

Un lien entre une nation et un citoyen se retrouve en partie dans la citoyenneté. Un citoyen est défini comme personne ayant la nationalité française et jouissant de ses droits civils et politiques (par exemple le droit de vote)[6]. La citoyenneté peut prendre de multiples formes dans le quotidien des individus : au-delà de la gestion de la population et l'allocation des prestations sociales par l'État, un pan primordial de la citoyenneté s'inscrit dans la participation individuelle et collective à la vie sociétale, politique, associative, etc.

Par extension, la citoyenneté numérique[7] peut être définie comme le rapport au politique, à la participation et à l'exercice de la citoyenneté médié par les technologies numériques. La démocratie numérique se fait aussi avec outils qui permettent la « *capacitation des citoyens, leur permettant d'interpeller les élus, de participer aux débats et d'exprimer leurs opinions ou accéder à des informations pluralistes* »[8]. De plus, elle peut être vue comme une série de compétences issues d'une culture numérique. C'est la définition que choisit le Conseil de l'Europe pour qui la citoyenneté numérique représente « *le maniement efficace et positif des technologies numériques (créer, travailler, partager, établir des relations sociales, rechercher, jouer, communiquer et apprendre), la participation active et responsable (valeurs, aptitudes, attitudes, connaissance) aux communautés (locales, nationales, mondiales) à tous les niveaux (politique, économique, social, culturel et interculturel), l'engagement dans un double processus d'apprentissage tout au long de la vie (dans des structures formelles, informelles et non formelles) et la défense continue de la dignité humaine* »[9]. Enfin, les usages et des pratiques du numérique individuelles contribuent à définir la citoyenneté.

La dématérialisation croissante des services publics ainsi que certaines conditions particulières[10] entraînent les citoyens à accorder une part de plus en plus grande au numérique dans leurs pratiques citoyennes. Dans ce contexte les identités numériques sont des outils essentiels pour la faire valoir en faisant perdurer le lien entre la nation et ses citoyens. Les identités numériques peuvent bousculer les différents pans de la citoyenneté numérique tant en facilitant les formes d'expression des uns qu'en réduisant les accès à la citoyenneté des autres. De fait, l'identité numérique, qui donne accès aux droits civils et politiques, doit être en partie appréhendée, gérée et pensée comme un bien public qui doit être inclusif et accessible à tous.

6 Site web, Vie Publique, « En quoi la citoyenneté est-elle une manifestation d'une identité commune ».
7 Voir notamment GREFFET, Fabienne, WOJCIK, Stéphanie, « *La citoyenneté numérique. Perspectives de recherche* », Réseaux, 2014/2 (n° 184-185), p. 125-159.
8 LINC, décembre 2019, *Civil tech, données et Demos*, Cahier Innovation et prospective, n°7, p 11.
9 Site web du Conseil de l'Europe, article « Citoyenneté numérique et éducation à la citoyenneté numérique ».
10 La crise sanitaire mondiale du premier semestre 2020 a notamment mis en avant l'importance des outils numériques pour maintenir des relations sociales, professionnelles ainsi qu'avec l'administration.

1.2. L'identité numérique : une notion sibylline

L'identité est une notion complexe puisqu'il s'agit d'une notion évolutive, dépendante de l'acteur qui l'attribue ainsi que du champ dans lequel cette attribution est faite.[11]

Liée avec le terme numérique, elle fait référence en premier lieu à l'identifiant (par exemple nom d'utilisateur), choisi pour ou par le détenteur et permettant–souvent associé à un mot de passe–d'accéder à des services (publics, privés ou professionnel, locaux, nationaux ou internationaux). L'identité numérique peut être déclarative (comme sur Twitter où le pseudo est choisi) ou imposée par le service (comme sur le site de l'assurance maladie où l'identité se fait par l'état civil), en rapport avec l'état civil ou non. Il existe alors une multiplicité d'identités numériques propres aux pratiques numériques[12] de chaque individu.

En second lieu, l'identité numérique peut aussi être perçue comme le reflet des comportements en ligne des individus : soit l'ensemble des traces (données, métadonnées) qu'un individu peut laisser en surfant sur internet, et qui permettront de définir une cartographie de ces comportements et de faire entrer celui-ci dans une typologie.

C'est selon le premier niveau, une identité attribuée, que l'identité numérique sera abordée dans ce rapport. Celle-ci intervient lorsqu'une relation a besoin d'un certain niveau de confiance, de certitude concernant les caractéristiques des interlocuteurs, pour perdurer. L'État est un acteur historique pour identifier les parties prenantes, de par sa prérogative régalienne de tenue à jour des actes de naissance et de décès des citoyens à travers l'état civil.

1.3. Identité numérique de confiance : un état civil en ligne ?

À travers les registres d'état civil, l'État fournit à ses citoyens une identité légale qui leur permet d'exercer des droits et plus généralement structure la relation de droits et de devoirs entre État et citoyens. Cette action d'apposition[13] ou d'enregistrement de caractéristiques d'une identité civile est prise en charge par les mairies à travers les registres d'état civil. Ils sont le support pour la distribution des titres d'identité.

En France, la carte d'identité, ou le titre d'identité, n'est pas obligatoire[14]. Néanmoins, sans titre d'identité, de nombreuses démarches deviennent extrêmement complexes, voire impossibles : créer un compte en banque,

11 Pour plus de précision sur la définition de l'identité numérique se référer à des ouvrages récents comme FOURMENTRAUX Jean-Paul (Dir), Identités numériques, Expressions et traçabilité, Les Essentiels d'Hermès, CNRS éditions, 2015.. Ou KHATCHATOUROV, Armen, CHARDEL Pierre-Antoine, FEENBERG Andrew et PEIRES Gabriel, Les identités numériques en tension entre autonomie et contrôle, Volume 3, ISTE Editions, 2019.
12 Nous utiliserons souvent les termes identité numérique au singulier. Néanmoins, cela ne veut pas dire que nous réduisons les identités numériques à une identité numérique qui devrait être uniquement proposée par l'État, même si nos travaux s'intéressent aux conditions nécessaires à l'émergence d'une ou des plusieurs identités numériques certifiées par l'État.
13 Nous choisissons ici volontairement les termes «*d'apposition de caractéristiques*» *de l'identité civile pour faire écho à un champ de recherche et de contestations autour de l'identité de genre et du droit à l'autodétermination qui met en avant le rapport de domination dans la définition de l'identité par les autorités régaliennes et dans l'attribution de caractéristiques biologiques et physiques éloignées de la définition que l'individu donne de lui-même. Voir par exemple les positions de l'association Aides* «Autodétermination, santé, droits pour les personnes trans et/ou intersexes 20 ans que la France (nous) piétine !», novembre 2016.
14 Loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité.

souscrire une assurance, louer un logement… Ils permettent de facto un accès aux droits pour l'individu.

Avec la dématérialisation des services publics, et la possibilité d'accéder avec le numéro d'identification d'un service à un autre service (à travers l'agrégateur France Connect), les identités civiles (numéro de sécurité sociale, numéro fiscal, numéro étudiant) sont utilisées comme des identités numériques.

Néanmoins, il faut tenir compte du fait que l'association entre les identités numériques et l'identité civile mène souvent à un raccourci qui lie identités numériques aux titres d'identité électronique. Or, les deux ne sont pas forcément concomitants. En effet, l'identité numérique ne nécessite pas forcément un titre électronique (un identifiant et un mot de passe suffisent pour les cas d'usage les moins sensibles) pour se développer et le titre électronique ne sous-entend pas de fait, une identité numérique (des informations sur une carte à puce ne font pas forcément une identité numérique) car l'objectif initial du titre électronique est de lutter contre la fraude documentaire et faciliter les contrôles.

2. LA CITOYENNETÉ NUMÉRIQUE AU PRISME EUROPÉEN : LE POIDS DE L'EUROPE DANS LE PAYSAGE ACTUEL ET LES NORMES VÉHICULÉES AUTOUR DE L'IDENTITÉ NUMÉRIQUE[15]

Dans l'Union Européenne, la citoyenneté passe par une appartenance au marché commun, par la circulation des personnes, des biens, des services et des normes. Depuis la fin des années quatre-vingt-dix, l'Union Européenne s'est emparée de cette thématique, associée à une compétence régalienne des États membres, en mettant en place un cadre d'interopérabilité (*European Interoperability Framework*)[16] visant à promouvoir le transfert de services et données entre les administrations publiques de la communauté à travers différentes couches d'interopérabilité[17].

C'est dans ce contexte que l'Union a souhaité se positionner sur le sujet souverain de l'identité numérique, notamment en s'appuyant sur une série de textes et de programmes entre 2010 à 2020[18].

L'identité numérique constitue alors une brique d'un projet plus large : comme le soulignait le député européen Carlos Zorrinho dans son discours de présentation du programme du deuxième volet du programme « *Interoperability solutions for public administrations, businesses and citizens* » : « *Derrière tout le travail réalisé se cache une ambition sous-jacente : contribuer à la construction d'une identité numérique européenne, qui permet de créer de meilleures conditions pour le développement d'administrations publiques efficaces, capables de soutenir les entreprises et les citoyens dans leurs besoins quotidiens, mais aussi dans leur entrée en compétition sur les marchés mondiaux des entreprises.* » [19] [20]. Pour répondre à ces objectifs, plusieurs logiques ont été promues au niveau européen telles que la reconnaissance mutuelle des identités numériques de chaque pays, l'interopérabilité [des services de confiance utilisés par les administrations] et le soutien d'une identité européenne.

Une tentative de faire émerger l'appartenance à une citoyenneté européenne se retrouve dans les initiatives développées pour les

15 WAHNICH Sophie, « *L'identité nationale, une question européenne* », Dans Vacarme 2010/1 (N° 50), pp. 86 à 90.
16 European Interoperability timeline
17 Quatre couches, technique, sémantique, organisationnelle et légale.
18 À partir de 2010, plusieurs programmes ont permis de déployer ces politiques publiques tels que : ISA programme (2010-2015) relatif à l'interopérabilité des solutions pour les administrations publiques ; la communication sur les données ouvertes pour améliorer l'innovation, la croissance et la transparence des gouvernements (2011) ; la révision de la directive PSI pour l'utilisation des informations du secteur public (2013) ; le règlement eIDAs (2014) portant sur l'identification électronique et les services de confiances dans les transaction électroniques au sein du marché intérieur ; la seconde version du programme ISA qui s'entend jusqu'en 2020.
19 « ISA2–In the Heart of Europe » Discours de Carlos Zorrinho, à la conférence de présentation du programme.
20 « *Behind all the work made was an underlying ambition to contribute to the construction of a European digital identity, which allows for the creation of better conditions for the development of efficient public administrations that can support companies and citizens in their daily needs, but also in their competitive entrance in global markets of businesses.* »

étudiants et les personnels académiques : la fédération des identités à travers des programmes comme RENATER[21] ; la création d'une identité étudiante européenne[22] ; un partage de ressources et une facilitation d'intégration de nouveaux services eduGAIN[23].

Du point de vue légal, c'est le règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (dit eIDAS) [24] qui traite de l'identité numérique avec pour objectif d'assurer l'interopérabilité des systèmes d'identification et d'authentification des solutions d'identité numérique. Cette interopérabilité passe par une classification des moyens de mise en œuvre de différents niveaux de garantie (faible, substantiel et élevé)[25]. Il promeut un principe de reconnaissance mutuelle des moyens d'identification électroniques des différents pays européens. *« Pour bénéficier de cette reconnaissance mutuelle un moyen d'identification électronique doit :*

1. *Avoir été délivré conformément à un schéma d'identification électronique notifié par l'État membre concerné et figurant sur la liste publiée par la Commission. […] ;*
2. *Avoir un niveau de garantie égal ou supérieur à celui requis par l'organisme du secteur public concerné pour accéder à ce service en ligne, à condition que ce niveau soit substantiel ou élevé. Cette reconnaissance mutuelle ne concerne ainsi que les organismes du secteur public qui exigent, pour accéder à l'un de leurs services en ligne, une identification électronique répondant au moins aux exigences du niveau substantiel. » [26]*

En février 2020, quinze pays européens ont notifié leurs schémas d'identification électronique auprès de l'Union après un examen par les pairs des États membres.[27]

En plus d'aborder l'identité numérique par la reconnaissance mutuelle[28], l'Europe harmonise les différents titres d'identité à travers le règlement (UE) 2019/1157[29]. C'est pour répondre à ce règlement que l'État français multiplie les efforts pour mettre en place un titre électronique répondant aux mêmes critères que le passeport d'ici août 2021. Ce titre apparaît comme un support possible de l'identité numérique régalienne (cf. 3.1).

L'identité numérique n'est donc pas uniquement une question de prérogative de souveraineté, mais aussi une question supranationale qui régule et homogénéise le marché unique européen, son accès et sa fluidification. L'important ici réside dans un ensemble de mesures, hétérogènes, ayant le même portage politique et la même ambition : l'interopérabilité et la fédération des services européens.

21 Site web de Renater, article sur la fédération : L'accès authentifié et sécurisé aux ressources de la communauté.
22 Site web de Erasmus.
23 Site web de Geant, article sur l'initiative eduGAIN.
24 Règlement (UE) No 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 et abrogeant la directive 1999/93/CE
25 Site web de l'ANSSI, article sur le règlement eIDAS.
26 idem.
27 Overview of pre-notified and notified eID schemes under eIDAS.
28 Le principe de reconnaissance mutuelle du règlement eIDAS propose qu'une identité numérique développée dans un État membre puisse être reconnu par un autre État membre et permette l'accès aux services publics préalablement identifiés. Ce principe ne s'applique que pour les niveaux de garantie substantiel et élevé.
29 Règlement du Parlement européen et du Conseil 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.

3. DIFFÉRENTS PROJETS D'IDENTITÉ NUMÉRIQUE NATIONALE : HISTORIQUE ET LÉGISLATION

3.1. Historique des projets : du titre électronique à l'identité numérique

La création de la Commission nationale de l'informatique et des libertés (CNIL), par la loi du 6 janvier 1978, répond au projet d'automatisation des fichiers administratifs et du répertoire des individus par le biais du numéro INSEE, et a été grandement documentée. Cette histoire, qui fige l'importance de la séparation des numéros administratifs d'identification citoyens, a marqué l'ensemble des projets politiques de création de carte d'identité électronique[30] et dans une certaine continuité, de l'identité numérique.

En effet, divers projets d'identité numérique ont été menés par le Gouvernement français au cours des vingt dernières années. Ces développements ont permis par exemple de faire émerger la signature électronique à destination des entreprises à partir de 2000[31] ainsi que les cartes d'identité professionnelle dans les professions réglementées, notamment pour les professionnels de la santé ainsi que dans plusieurs ministères[32].

Alors que jusqu'en 2005, il est possible de constater une faible évolution en termes d'avancées technologiques, les échecs à répétition ont fait émerger des critiques récurrentes autour du développement de l'identité numérique :

- De nombreuses réticences[33] ainsi qu'un manque de confiance qui avaient été mis en avant dans les débats citoyens[34] autour du projet d'Identité Nationale Électronique Sécurisée (INES). Ce projet est présenté en 2003 par Nicolas Sarkozy, alors ministre de l'Intérieur. L'émergence du programme s'appuie à l'époque sur un constat : la difficulté de l'administration centrale à certifier l'identité d'une personne, autrement que par l'acte de naissance facilement falsifiable, conduisant à l'obtention indue de vrais documents d'identité au moyen d'une fraude à l'état civil[35]. Pour remédier à ce problème et lutter contre la fraude à l'identité, il est alors proposé d'instaurer un titre d'identité électronique qui serait lié à plusieurs fichiers centraux ainsi que des éléments biométriques inscrits dans la puce. Le projet est suspendu par le gouvernement en 2005 ;

30 Pour des précisions sur l'histoire de la carte d'identité française, notamment en amont de l'émergence de la carte électronique, voir PIAZZA, Pierre, 2004, Histoire de la carte nationale d'identité, Odile Jacob, 2004, 462 p.
31 En 1997, le Programme d'action gouvernemental pour la société d'information (PAGSI) est instauré, afin de « *créer les conditions d'une société de l'information pour tous* ». Ce programme a abouti à la mise en place de la signature électronique principalement à destination des entreprises.
32 Les cartes d'identité professionnelles, notamment dans les professions réglementées comme les métiers de la santé sont les premières cartes d'identité électroniques à voir le jour. Les cartes CSP#, apparaissent vers la fin des années-quatre-vingt-dix portées par le programme SEASAM-Vitale et le ministère de la Santé. Elles permettent de valider les informations de l'identité professionnelle du titulaire de carte ainsi que de fluidifier les relations avec l'Assurance maladie et de porter des certificats d'authentification et de signature électronique du titulaire.
33 PIAZZA Pierre, « *Les résistances au projet INES* », Cultures & Conflits [En ligne], 64 | hiver 2006.
34 Le Forum des droits sur internet, Rapport : le projet de carte nationale d'identité électronique, 16 juin 2005.
35 LECERF Jean-René, Rapport d'information n° 439, Identité intelligente et respect des libertés, Sénat, 2004-2005.

- L'absence de périmètre d'usage bien défini de l'identité numérique. L'identité numérique est mentionnée dans le cadre législatif avec la loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité. Néanmoins, l'article qui mentionne les nouvelles fonctionnalités en rapport avec l'identité numérique de la carte nationale d'identité électronique est rejeté par la décision n° 2012-652 DC du 22 mars 2012 du Conseil constitutionnel notamment en raison du manque d'information concernant « *la nature des « données » au moyen desquelles ces fonctions peuvent être mises en œuvre […] les garanties assurant l'intégrité et la confidentialité de ces données ; […] les conditions dans lesquelles s'opère l'authentification des personnes mettant en œuvre ces fonctions* » [36] ;
- Le manque de soutien politique de certains projets : c'est le cas en 2009 avec le projet Idénum qui finit par s'enliser après la création du consortium économique avec les acteurs privés. Ce projet ambitionnait à nouveau de faire émerger un titre électronique, avec un niveau de sécurité et de confiance suffisamment fort pour pouvoir être utilisé à distance. La stratégie consiste alors à s'appuyer sur un GIE[37]. Un organisme central se charge d'établir les règles appliquées par les émetteurs, qui émettent des identités homologuées selon des niveaux de sécurité similaires. Le fournisseur de services qui bénéficie de l'identité numérique certifiée du client, rétribue l'émetteur de cette identité. Ce projet donnera naissance en 2013 à la société Idénum. Portée par l'État (à travers la Caisse des dépôts à 32 %), le Crédit Mutuel, le CIC, Pages Jaunes, SFR et le groupe La Poste, cette société a pour pour objectif de « *Fédérer en France le plus grand nombre d'acteurs du web afin de définir et promouvoir des solutions d'identité numérique universelles pour les professionnels comme les particuliers* » comme l'annonçait Fleur Pellerin dans son discours au FIC en 2013.

À partir de 2014, une approche nouvelle est choisie par le gouvernement et l'administration, décorrélant l'identité numérique du titre et, de fait, de l'idée d'une identité numérique unique. L'identité numérique se pense dorénavant d'abord en fonction des services auxquels elle permet l'accès.

C'est dans cette philosophie que France Connect est créé en 2015[38]. L'objectif est de « *proposer au public de s'identifier et de s'authentifier, auprès de partenaires, fournisseurs de téléservices et de services en ligne, au moyen de dispositifs mis en œuvre par des fournisseurs d'identité partenaires* » [39], et « *repose sur une fédération d'identités et permet :*

- *De simplifier des démarches et formalités administratives effectuées par le public et d'en assurer la traçabilité et le suivi ;*

36 Conseil Constitutionnel, décision n°2012-652 DC du 22 mars 2012, Loi relative à la protection de l'identité. [Non conformité partielle]
37 Selon l'exemple du GIE CB qui a permis le développement massif des technologies de carte à puce dans le secteur bancaire
38 Arrêté du 24 juillet 2015 portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication d'un téléservice dénommé « FranceConnect ».
39 Arrêté du 8 novembre 2018 relatif au téléservice dénommé « France Connect » créé par la direction interministérielle du numérique et du système d'information et de communication de l'État.

– *De sécuriser le mécanisme d'échange d'informations entre autorités administratives prévu par les articles L. 113-12 et L. 114-8 du code des relations entre le public et l'administration susvisés. Le téléservice assure uniquement une fonction de mise en relation des autorités administratives, sans traiter des données susceptibles d'être échangées dans ce cadre ;*

– *De simplifier l'accès du public aux services en ligne proposés par les entités partenaires ;*

– *Au public, d'accéder à des téléservices d'autres États membres en respectant les dispositions prévues par le règlement du 23 juillet 2014 susvisé, notamment les exigences relatives au niveau de garantie requis par le téléservice concerné.*
L'adhésion au téléservice « France Connect » est facultative. »

L'enjeu du projet est d'offrir un service permettant de répondre aux besoins des citoyens et de moderniser l'État, tout en laissant libre choix aux individus sur le principe de la fédération des identités. Le modèle permet aux citoyens de choisir parmi plusieurs fournisseurs d'identités pour accéder à un service qui a intégré l'option France Connect. Ce modèle se veut plus respectueux des principes structurants de la loi informatique et libertés, et de ces évolutions, sur le numérique notamment parce que : les identités ont toutes la même valeur (pour chaque niveau de garantie eIDAS) et sont interchangeables ; aucun stockage de données d'identité n'est fait par France Connect (qui se contente de faire passer les informations du fournisseur d'identité au service) ; le fournisseur de service ne sait pas quel est le fournisseur d'identité (et réciproquement), etc.

Au départ ouvert uniquement aux services publics, puis à certains services privés à partir de novembre 2018, l'arrêté du 11 mai 2020 relatif à « l'*expérimentation visant à étendre le périmètre des partenaires du téléservice « FranceConnect »* »[40] permet d'entamer une réflexion - incluant la CNIL - sur l'élargissement du téléservice France Connect à de nouveaux acteurs privés.

Depuis le règlement eIDAS, le titre d'identité est à nouveau souvent lié à l'identité numérique[41]. En France cette relation se retrouve à travers le service d'Authentification en ligne certifiée sur mobile (Alicem) [42], porté par l'Agence nationale des titres sécurisés (ANTS) et le ministère de l'Intérieur. Instauré par décret en mai 2019, ce service a pour objectif « *d'assurer une certification de l'identité dans un monde digital complémentaire au monde physique* », « *de contribuer à la simplification des démarches administratives* », « *de développer la première solution d'identité de numérique visant le niveau de garantie élevé au sens du règlement eIDAS* », et « *de contribuer à la lutte contre l'usurpation d'identité en ligne* ».[43]

40 Arrêté du 11 mai 2020 relatif à l'expérimentation visant à étendre le périmètre des partenaires du téléservice « FranceConnect ».
41 Néanmoins ce n'est pas une obligation puisque plusieurs États ont notifié des schémas d'identification électronique où le lien avec un titre d'identité est bien plus faible. On observe notamment une tendance à la généralisation de l'identité numérique sur mobile, et, Alicem, avec la lecture systématique du passeport, fait figure d'exception.
42 Décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile ».
43 Ministère de l'Intérieur, « Alicem, la première solution d'identité numérique régalienne sécurisée », 16 décembre 2019. op. cit.

Cet historique permet de constater les deux relations de confiance nécessaires à l'émergence de l'identité numérique : d'une part, la confiance accordée à l'État par la population au regard de la sécurisation de ses données et d'autre part, la confiance dans le titre fourni par l'État, qui se transforme en levier de certification de l'identité numérique, même chez certains fournisseurs d'identité privés.

Bien entendu, les diverses propositions gouvernementales autour de l'identité numérique ne sortent pas ex nihilo des administrations. C'est pour répondre à la multiplication, voire l'explosion, des usages en phase avec la croissance des technologies et des relations médiées par le numérique, que les gouvernements successifs ont cherché à se saisir du sujet de l'identité numérique. Face à l'économie numérique de la donnée, les identités numériques vérifiées sont des biens de première valeur qui mettent en avant des grands acteurs de l'économie numérique ayant la possibilité de prendre le marché remettant en cause la position souveraine des Etats dans le rapport à l'identité.

3.2. Un encadrement juridique varié

En parallèle des projets d'identité numérique nationaux, plusieurs décisions législatives ou projets de loi ont impacté le cadre de l'identité numérique, soit parce qu'ils délimitent et cadrent l'identité numérique, soit parce qu'ils font émerger de nouveaux usages pour cette identité.

À titre d'exemple, le règlement général pour la protection des données (RGPD) définit l'utilisation qui peut être faite des données à caractère personnel. Il fait émerger au niveau européen des notions de minimisation, de nécessité et de proportionnalité de la collecte et du traitement des informations des citoyens par l'État. Ces obligations, proches de celles du modèle français de la loi Informatique et Libertés, se retrouvent dans les choix et l'architecture de France Connect.

En parallèle, le programme Action publique 2022 ambitionne de « *repenser le modèle de l'action publique en interrogeant en profondeur les métiers et les modes d'action publique au regard de la révolution numérique qui redéfinit les contours de notre société* » [44] et accentue l'importance du développement des identités numériques des Français. De plus, certains objectifs (tels que la signature électronique) sont porteurs de nouveaux usages, en attente d'une identité numérique à la hauteur des exigences de sécurité et de confiance qui leur sont appliquées.

Enfin, le programme « dites-le-nous-une-fois » [45], s'inscrit dans la continuité même de France Connect puisqu'il a été réfléchi par le même service de modernisation de l'État pour compléter les propositions du service France Connect. Ce service[46] vise à dispenser les citoyens de fournir plusieurs fois les mêmes pièces justificatives[47]. La loi du 10 août

44 Gouvernement, Action Publique 2022 : pour une transformation du service public, Mis à jour le 30 octobre 2018.
45 Site web Modernisation.gouv, septembre 2013, « « Dites le nous une fois » : un programme pour simplifier la vie des entreprises ».
46 Décret nº 2019-33 du 18 janvier 2019 fixant la liste des pièces justificatives que le public n'est plus tenu de produire à l'appui des procédures administratives en application de l'application de l'article L. 113-13 du code des relations entre le public et l'administration.
47 Décret nº 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 nº 2018-727 du 10 août 2018 pour un État au service d'une société de confiance.

2018 pour un État au service d'une société de confiance, dite ESSOC[48], prolonge cette initiative, en facilitant les interactions et réduisant le nombre de requêtes de justificatifs.

Cet ensemble de lois et de mesures doit être mis en parallèle avec les actions diverses et variées des territoires et de leurs représentants. En effet, l'identité numérique liée à l'état civil des individus est aussi un levier particulièrement utile pour les localités qui souhaitent rendre de meilleurs services à leurs administrés. Leurs pratiques participent à l'émergence de nouveaux usages et d'un savoir social autour de l'identité numérique.

48 Loi n° 2018-727 du 10 août 2018 pour un État au service d'une société de confiance, dite ESSOC.

4. REVUE DES LEVIERS HABITUELS DE L'IDENTITÉ NUMÉRIQUE

Les travaux du Conseil montrent que les autres pays qui ont développé une identité numérique s'appuient généralement sur trois leviers : le titre obligatoire, un numéro unique d'identification et un registre centralisé des populations. Aucun de ces leviers ne peut être sollicité au regard de l'histoire et du cadre législatif français. Néanmoins, il convient de se demander si dans les différents pays ayant créé leur identité numérique grâce à ces leviers, une citoyenneté numérique a pu apparaître avec la démocratisation de l'identité numérique, ou si cet outil ne sert que de véhicule pour améliorer la prestation de services.

4.1. Une architecture française fondée sur le respect des droits des citoyens

En France, le modèle d'identité numérique France Connect a été développé en correspondance avec la logique d'État plateforme[49]. L'objectif premier est de rendre des services aux citoyens tout en facilitant l'interaction avec les administrations et le travail de ces dernières dans un processus de dématérialisation. « *La puissance publique peut désormais agir en facilitant l'accès à différentes ressources, biens publics, biens communs, infrastructures cognitives, au lieu de prétendre réguler par l'interdiction. En donnant accès à ses données, à ses logiciels, à ses simulateurs, à une identité authentifiée (à travers France Connect), à une monnaie.* » [50]

Dans ce système, France Connect est un trousseau d'accès–les fournisseurs d'identité représentant des clés–pour accéder à des ressources. Ce service s'est développé pour proposer une solution alternative aux géants privés comme Facebook Connect, qui commençaient à proposer leur solution à des services publics mettant en cause la souveraineté nationale.[51]

Au niveau européen, l'Italie est un des pays qui a développé le schéma d'identification proche du modèle français, en choisissant de s'appuyer sur une fédération d'identité[52]. Il a été notifié à la Commission européenne aux trois niveaux de garantie eIDAS (faible, substantiel, élevé). Le schéma italien s'appuie le Systema Pubblico per la gestione dell Identita Digitale (SPID), un système de fédération d'identités géré par l'Agence pour l'Italie Digitale (AgID). Il permet de faire communiquer des fournisseurs d'identité et des fournisseurs de services. Sur le même modèle que France Connect, qui s'est ouvert depuis novembre 2018 aux services privés, notamment bancaires et assurances, des services privés sont accessibles à travers la fédération italienne.

49 PEZZIARDI Pierre et VERDIER Henri, Janvier 2017, Des startups d'État à l'État plateforme, Fondation pour l'innovation politique.
50 ibid. p. 31.
51 Même s'il est improbable qu'on puisse un jour payer en se connecter au site des impôts via Facebook Connect, d'autres services connexes proposent ce type de connexion, comme par exemple les plateformes de démocratie participative
52 En plus de l'Italie, les Pays-Bas (eHerkenning), la Belgique (FAS) et le Royaume-Uni (Gov.uk verify) ont aussi fait le choix de s'appuyer sur des mécanismes de fédérations.

4.2. Le titre d'identité : un support qui n'est pas obligatoire pour les citoyens français

Le titre d'identité (par exemple la carte nationale d'identité ou le permis de séjour) offre un avantage. S'il était universel, il donnerait à son porteur une identité certifiée par l'État avec un très haut niveau de garantie et à partir de laquelle celui-ci peut dériver d'autres identités. C'est le choix fait par l'Allemagne : à travers cet outil le pays a cherché à démocratiser l'utilisation de l'identité numérique à partir de 2010 en rendant le titre d'identité électronique obligatoire.

Cette carte d'identité électronique allemande est payante et délivrée en mairie. Le citoyen peut choisir lui-même s'il souhaite l'option d'authentification électronique pour un coût supplémentaire. Elle est utilisée pour des services publics comme privés et permet des usages comme l'accès en ligne à des services publics (prestations sociales, déclaration et paiement des impôts, l'emploi, etc.), privés (banques, assurances) et la signature électronique de documents. Si l'État est bien fournisseur d'identité numérique via le portail Mein Service-bw, les acteurs privés peuvent aussi fournir une identité en ligne : ainsi la société Allianz propose 'Meine Allianz' et la Deutche Post propose le portail 'Postident'.

La carte d'identité peut donc s'avérer être un véritable levier pour le développement de l'identité numérique. Néanmoins, elle n'est pas l'outil principal d'une citoyenneté numérique, en particulier lorsque le choix d'en disposer n'est pas libre. En France, le titre d'identité reste optionnel et l'accès aux droits et à la citoyenneté ne concerne pas que les personnes de nationalité française (étrangers vivant en France, demandeurs d'asile…).

4.3. Le numéro d'identification unique : prohibé par la loi informatique et liberté, mais utilisé dans d'autres pays

Le numéro d'identification unique, tout comme la carte d'identité électronique, est un levier utile à la démocratisation de l'identité numérique puisqu'il permet de facilement croiser des données des citoyens entre les différentes administrations, évitant d'avoir une identité par citoyen et par service.

C'est la structure sur laquelle s'est appuyée l'Estonie pour développer l'identité numérique de ses citoyens. Ce pays est souvent présenté comme étant le pays le plus avancé en termes d'e-gouvernement et d'identité numérique. Il génère d'ailleurs un marché particulier autour de la question à destination des professionnels qui souhaiteraient en apprendre plus sur la « digital society » estonienne[53]. Le modèle bien documenté relève d'une véritable stratégie d'État[54]. Il fonctionne grâce à un numéro d'identification unique de chaque citoyen et résident[55]. Le fichier associé est géré par le ministère de l'Intérieur et contient toute

53 Site web e-Estonia.
54 CHAMPETIER DE RIBES Violaine et SPIRI Jean, Demain tous Estoniens ? L'Estonie, une réponse aux GAFA, Cent Mille Milliards, Hachette, septembre 2018.
55 Ce numéro peut évoluer au cours de l'existence d'un individu, notamment en cas de changement sexe biologique.

l'information concernant la personne, de la date de naissance jusqu'aux informations relatives aux sanctions pénales. De plus, le fichier contient l'identité de l'agent qui a ajouté l'information dans le fichier. Il faut noter que la politique de la donnée est très différente en Estonie et en France.

Le système, considéré comme décentralisé (chaque administration détenant une partie des informations) [56], permet un niveau de sécurité homogène et de protection des données. L'État fait preuve d'une grande transparence vis-à-vis des citoyens qui peuvent suivre en temps réel les informations et les demandes d'informations effectuées par chaque administration à travers une plateforme idoine. Pour éviter les usages malintentionnés de personnes ayant des permissions d'accès, ceux-ci sont fortement sanctionnés.

Outre l'accès à des services à travers une plateforme similaire à France Connect, l'identité numérique estonienne permet l'accès automatique à certaines prestations sociales et au vote en ligne.

Néanmoins, plusieurs limites peuvent être mises en avant concernant la citoyenneté numérique estonienne. Dans son effort d'apporter toujours plus de services aux citoyens, le gouvernement ne prend parfois pas le temps de consulter sa population sur l'intérêt qu'elle éprouve pour un nouveau service[57]. De plus, l'émergence de l'identité numérique s'est faite en réponse à un besoin de diminuer les coûts de fonctionnement de l'administration dans les années quatre-vingt-dix dans un pays ayant une faible population et des experts en informatique importants. L'administration estonienne a agit de manière verticale et a déployé sa solution en plusieurs étapes, sans réaction forte de la part de la population. Dans cette optique, les notions d'inclusion et d'acceptabilité n'ont pas toujours été mises en avant malgré des efforts de pédagogie tant à travers des programmes de formations spécifiques que des programmes pédagogiques sur le temps long.

En France le numéro d'identification unique va à l'encontre des principes légaux issus de la loi informatique et libertés, ainsi que des usages des citoyens qui ont l'habitude de cloisonner les identifiants et les services[58].

4.4. Le registre de la population : une centralisation qui n'existe pas sur le territoire, qui s'avère être un levier pour d'autres pays

Le registre de population permet de centraliser les données d'identité de toute la population et de proposer une identité numérique à l'ensemble des citoyens. En Belgique, cet outil a considérablement facilité la mise en place de l'eID même si il est confronté à des limites.

56 Le système est supporté par la Xroad et piloté par le RIA
Site web de l'Information System Author ity (RIA) de la république d'Estonie.
57 Notre visite à e-Estonia Briefing Centre le 15 octobre 2019 a ainsi montré que les services sont développés sur le POC, et rapidement implémenté en phase de test sur l'ensemble de la population. À titre d'exemple, le service permettant aux parents de voir les notes de leurs enfants en temps réel avaient suscité de grands questionnements de la part de la population. Ce service apparaissait pour certain comme trop coercitif pour les élèves. Il a néanmoins été conservé par le gouvernement. Les statistiques montrent qu'une majorité des parents s'y connectent une trentaine de fois par mois.
58 Voir par exemple l'étude de législation comparée du Sénat sur « *le numéro unique d'identification des personnes physiques* ».

L'identité numérique belge a été déployée massivement à partir de 2004, où elle est délivrée par les communes[59]. Le citoyen reçoit un courrier de convocation en mairie où un agent active son identité numérique et les trois composantes d'identification de la carte, c'est-à-dire l'authentification numérique, signature électronique et validité du titre. Concomitamment à la mise en place d'une identité numérique, la Belgique a déployé une plateforme de services tirant bénéfice de cette identité. La plateforme du site my.belgium.be propose des services publics variés tant au niveau national qu'au niveau local–consulter et gérer son dossier fiscal, remplir et envoyer sa déclaration d'impôt, consulter son dossier de pension retraite, de santé, enregistrer un contrat de bail, faire une déclaration en ligne auprès de la police, etc.

Cette identité numérique nécessitait à l'origine l'usage d'un boîtier dédié dans lequel l'utilisateur devait insérer sa carte, ce qui a conduit à des taux d'utilisation très bas. Avec l'arrivée d'Itsme[60], moyen d'identification électronique sur mobile ne nécessitant plus d'équipement dédié (comme un lecteur de carte), l'usage de l'identité numérique a nettement augmenté. Les usages de cette identité par des services privés se sont de plus beaucoup développés.

Néanmoins, ici encore, la question de la citoyenneté numérique, liée à l'identité numérique, n'est pas complètement prise en compte. En premier lieu, en termes d'inclusion et de fracture numérique puisque la solution proposée comporte un certain nombre de biais. La société Itsme a d'ailleurs récemment fait appel à des experts[61] du sujet pour améliorer la distribution du service auprès de l'ensemble de la population. En second lieu, le portage par une entreprise privée questionne sur la portée de la citoyenneté numérique qui peut être atteinte à travers cette solution. Enfin, la citoyenneté est aussi une question d'échelle (locale/nationale), et de perception d'individu concernant sa relation à l'État, des droits et des devoirs, et son implication dans la vie de la cité.

Ce rapport propose des recommandations face aux enjeux qui ont été soulevés dans les ateliers et rencontres quant à l'avenir de la citoyenneté à l'ère des déploiements de l'identité numérique.

L'urgence d'offrir une solution d'identité numérique régalienne s'explique par la crainte, justifiée, de voir arriver des acteurs systémiques extra nationaux sur le marché à travers une solution non-souveraine, peu ou pas respectueuse des valeurs européennes. Cette urgence se fait d'autant plus ressentir chez les citoyens qui n'ont pas une grande maîtrise du numérique et qui ne sont pas en mesure de se doter, d'eux-mêmes, de solutions d'identification respectueuses de leurs droits. Dans un contexte de dématérialisation croissante des services publics, proposer une offre étatique accessible et inclusive qui permette de répondre aux besoins de l'ensemble des citoyens est primordial pour favoriser l'adhésion et la participation éclairée à une future citoyenneté numérique (chapitre 1). De plus, dans une modernité numérique marquée par les affaires et les scandales entourant des pratiques abusives, il est nécessaire de se doter d'une solution souveraine dont la gouvernance est maîtrisée au profit des libertés fondamentales de chacun et en replaçant le citoyen au centre (chapitre 2).

59 Service public fédéral Intérieur belge, Documents d'identité, eID, FAQ.
60 Site web d'Itsme.
61 La Fondation Roi Baudouin et WeTechCare ont été sollicités par Itsme en juin 2019 pour «*réduire la fracture numérique*».

CHAPITRE I
L'IDENTITÉ NUMÉRIQUE, PILIER DE LA CITOYENNETÉ NUMÉRIQUE

Favoriser une solution inclusive et frugale qui rend service aux usagers

L'approche de la citoyenneté numérique est définie, en introduction, dans les compétences pour une culture de la démocratie élaborées par le Conseil de l'Europe[62], qui rappelle que les compétences nécessaires à tout citoyen pour pouvoir participer efficacement à une culture de la démocratie ne sont pas acquises de manière automatique, mais doivent être apprises et pratiquées dans les meilleures conditions.

La citoyenneté numérique consiste donc à prendre en compte les modifications profondes que la technologie induit en termes d'information, d'expression, et d'investissement citoyen, en évitant l'écueil de la réduire aux moyens technologiques et aux usages qui en découlent. L'usage du numérique a permis aux populations d'investir, par divers moyens, les sujets politiques et a vu émerger de nouvelles formes de citoyenneté et d'engagement public (participation citoyenne en ligne, consultations, vote des projets urbains d'intérêt général, pétitions en ligne…). Ces formes de participation sont encourageantes, car elles répondent à des besoins citoyens et contribuent à garantir, par leur existence, les valeurs de liberté d'expression, d'opinions et de croyances qui président à la vie démocratique de notre pays.

L'État a ainsi tout intérêt à développer et se saisir de la question de la citoyenneté numérique, en agissant de concert avec les citoyens, les collectivités locales, le tissu associatif et politique, en co-construisant des passerelles d'expression publique et citoyenne dans de bonnes conditions.

Aussi, se dégage une interdépendance entre la gestion publique de ces garanties et l'opportunité de se saisir de ces nouvelles modalités d'expression publique qui renouvelle avec force la volonté citoyenne de « peser » dans les orientations publiques.

Le Conseil propose donc de prendre une acception large de la citoyenneté numérique au prisme des relations entre l'État, les collectivités locales et les citoyens, en mobilisant des usages numériques à forte valeur ajoutée déjà existants (notamment relatifs à la justice) et prospectifs ou avec des enjeux de sécurité élevée (pétitions en ligne, vote en ligne des citoyens de l'étranger, procuration de vote). Cette conception de la citoyenneté numérique permettrait aux citoyens d'accéder à une agentivité pleine et entière dans l'exercice de leurs droits ou l'expression de leur participation démocratique, tout en bénéficiant des usages liés à l'identité numérique.

L'objet de ce présent rapport est de proposer des pistes pertinentes pour la mise en oeuvre d'une identité numérique « à la française ». L'appréhension d'une identité numérique réussie nécessite de la concevoir comme un service public à part entière, et non plus seulement comme une passerelle d'accès aux services publics numériques, en accord avec les principes fondamentaux définis par la Constitution :

62 Site web du Conseil de l'Europe, article « Citoyenneté numérique et éducation à la citoyenneté numérique », op.cit.

principe d'égalité de tous devant le service public, principe de continuité et principe d'adaptabilité[63].

En effet, la mise en œuvre du premier axe du Plan Action Publique 2022 sur la dématérialisation s'est faite sans prendre suffisamment en compte l'inclusion et l'accessibilité, selon plusieurs rapports et études constatant l'ampleur de la « fracture numérique »[64]. De la même manière, le deuxième axe de la « plateforme numérique de l'État » souffre d'une carence dans la mise en œuvre d'une adaptabilité qui prenne en compte les besoins des citoyens, leurs retours utilisateurs ainsi que les nouveaux usages à venir.

La logique de l'État plateforme ne saurait s'accomplir que sur son volet technique et institutionnel, et appelle de ses vœux à ce que l'identité numérique publique soit définie et considérée comme un service public à part entière.

L'identité numérique publique impose en effet de calibrer son ambition pour l'exercice d'une citoyenneté numérique, poursuivant ainsi deux objectifs : redéfinir avec force le périmètre et les conditions de l'accès aux services publics, et rappeler les missions et principes des services publics à l'aune de la concurrence induite par les plateformes numériques, comme le suggère le Conseil d'État dans son rapport : « *dresser la cartographie des activités de service public concurrencées par les plateformes* », en « interrogeant la pertinence de leur maintien » [65].

En effet, si l'émergence de l'État plateforme prend d'ores et déjà en compte les mutations dans les principes d'organisation administrative, le Conseil appelle à recentrer la conception des services publics numériques autour des besoins des usagers. Tout en facilitant la prise en compte rapide des mesures de simplification décidées, le Conseil national du numérique souhaiterait qu'elle s'articule avec une redéfinition de la logique du service public à l'aune des usages de l'identité numérique, suivant les mutations induites par le numérique dans la relation entre l'État et ses administrés, et suivant les principes de cohésion sociale qu'elle doit atteindre.

Cet engagement semble primordial pour tenir les nombreux enjeux qu'engage l'identité numérique. Le Conseil souhaite rappeler, dans ce premier chapitre, que les enjeux d'inclusion, d'accessibilité, et d'acceptabilité de l'identité numérique ne pourront s'accomplir qu'en adoptant une démarche « usager-centrée » et une pédagogie encapacitante, en ceci qu'elle dote les citoyens de compétences leur permettant de comprendre et se saisir de l'outil, de pouvoir exprimer leurs retours utilisateurs. Pour répondre à ces enjeux majeurs, le CNNum considère comme primordiale la prise en compte de la question de l'enrôlement de tous, des publics «éloignés du numérique» et des mineurs.

63 Ce dernier principe est défini comme tel : « *Présenté comme un corollaire du principe de continuité, il s'agit davantage d'assurer au mieux, qualitativement, un service plutôt que de sa continuité dans le temps. Cela signifie que le service public ne doit pas demeurer immobile face aux évolutions de la société ; il doit suivre les besoins des usagers (par exemple souplesse d'organisation des services publics) ainsi que les évolutions techniques (par exemple passage, au début du XXe siècle, du gaz à l'électricité)* ». Site web Vie Publique, Fiche thématique « La notion de service public ».
64 Cf. rapport du Défenseur des Droits, rapport Crédoc, op. cit.
65 CONSEIL D'ÉTAT, Étude annuelle 2017, Puissance publique et plateformes numériques : accompagner l' « ubérisation », principe n°15.

1. LA DÉMATÉRIALISATION DOIT AVOIR UNE DÉMARCHE INCLUSIVE ET ACCESSIBLE POUR TOUS LES CITOYENS

L'identité numérique peut constituer une opportunité pour faciliter l'accès des citoyens aux services publics, dans un contexte où ceux-ci sont de plus en plus dématérialisés dans le cadre de la mise en oeuvre du plan Action Publique 2022. Plutôt qu'« à marche forcée » [66], cette dématérialisation doit être faite en s'assurant de son accessibilité pour tous les citoyens[67].

Ainsi, le Défenseur des droits, dans son rapport « Dématérialisation et inégalités d'accès aux droits » paru en 2019[68] décrit la dématérialisation comme un « enfer numérique », privant de nombreux citoyens du recours à leurs droits ou à la résolution de problèmes administratifs classiques :

« *La dématérialisation offre de nouveaux moyens d'accès aux services publics et permet de simplifier l'accès aux informations et aux documents administratifs pour une majorité d'usagers mais, si les facultés de chacun ne sont pas réellement prises en compte, elle comporte un risque de recul de l'accès aux droits et d'exclusion pour de très nombreux usagers* » [69].

Pire, cet « enfer numérique » tend à fragiliser les usagers les plus éloignés du numérique et accentue la distance entre les citoyens et l'administration. Selon une étude Arcep / Crédoc parue en 2019[70], 25 % déclarent que les démarches en ligne sont trop complexes et 20 % reconnaissent un manque d'aisance numérique pour mener à terme leurs démarches en ligne.

Pour que les utilisateurs se sentent à même de tirer profit des usages, notamment associés aux parcours administratifs, il est nécessaire de faire en sorte que ces usages soient simples à prendre en main. Le Conseil national du numérique, dans une note sur la modernisation de l'administration, a ainsi plaidé en 2019 pour une dématérialisation centrée sur les besoins des usagers[71].

L'inclusion, définie comme la mise en oeuvre d'une accessibilité et d'une compréhension du numérique pour tous, est un élément fondamental de la citoyenneté numérique. Cette inclusion implique que les parcours administratifs dématérialisés intègrent dans leur conception, les problématiques d'accessibilité et de simplification qui sont indispensables à l'adhésion du plus grand nombre. En particulier, dans son rapport publié en février 2020 « *l'accessibilité numérique, entre nécessité et opportunité* » [72], le Conseil national du numérique a estimé que la numérisation des services publics demeurait une opportunité qu'il restait à exploiter pour garantir l'inclusion numérique des personnes en situation de handicap. Aussi, dans son rapport, le Conseil a proposé 50 recommandations pour faciliter le déploiement de l'accessibilité dans la société numérique.

66 Défenseur des droits, op. cit. p. 13.
67 Libération, « *L'administration numérique ne doit pas accélérer l'exclusion sociale* », 22 novembre 2016.
68 Défenseur des droits, op.cit.
69 Défenseur des droits, op.cit.
70 Arcep, Baromètre du numérique 2019.
71 Conseil national du numérique, Transformation de l'État Dépasser la norme par la pensée design, novembre 2019.
72 Conseil national du numérique, L'accessibilité numérique, entre nécessité et opportunité, février 2020.

1.1. La dématérialisation des démarches administratives doit prendre en compte la fracture numérique et l'inégalité entre les territoires

Jacqueline Gourault, ministre de la Cohésion des territoires et des Relations avec les collectivités territoriales auprès du ministre de l'Intérieur, a présenté l'identité numérique comme un « droit fondamental » dans la perspective d'une dématérialisation totale des parcours administratifs lors des Assises de l'identité numérique organisées par le programme interministériel sur l'identité numérique le 25 et 26 avril 2018.

Or, les parcours dématérialisés, tels qu'ils sont conçus actuellement, nécessitent un investissement des usagers en équipements (ordinateur ou terminal mobile) et présupposent d'accéder facilement à Internet. Si le Plan France Très Haut Débit[73] et l'Agence d'aménagement numérique des territoires prévoient une couverture de « bon haut débit » en 2020 sur tous les territoires, et la généralisation du très haut débit à horizon 2022, la persistance de « zones blanches » [74] et la nécessité d'un équipement et d'une connexion internet fiables restent des écueils au développement généralisé de la dématérialisation.

Outre la question de la couverture du réseau au niveau national, la question des équipements et de l'accès à internet détermine fortement la possibilité d'un « plein usage » des services publics et conséquemment, l'accès aux droits sociaux, qui peut constituer une part importante des ressources de nombreux citoyens.

Au-delà de l'aspect matériel, les démarches nécessitent un niveau de littératie[75] numérique suffisant pour accéder et comprendre les requêtes, manipuler les outils et faire aboutir les démarches jusqu'au bout, selon une enquête de la Mission Société Numérique[76] qui rappelle que les niveaux d'éducation et les faibles revenus constituent des facteurs d'aggravation de la fracture numérique. Cela plaide pour un parcours d'identification numérique en français «facile à lire et à comprendre» (FALC), en particulier lorsque l'incitation à faire des démarches dématérialisées peut conduire à un non-recours aux droits ou prestations sociales pour les personnes « éloignées du numérique », c'est à dire ne disposant pas des moyens matériels, intellectuels ou le niveau de littératie suffisant pour accomplir des démarches numériques simples. Ces préalables sont indispensables à la pleine réalisation des ambitions de la Mission Société Numérique[77] et aux préconisations du Conseil dans son rapport de 2013 « *Citoyens d'une société numérique : Accès, Littératie, Médiations, Pouvoir d'agir, pour une nouvelle politique d'inclusion* » [78].

73 Site web du gouvernement, « Le Plan France très haut débit », mai 2017.
74 Arcep, Les déploiements mobiles dans les zones peu denses, Observatoire des déploiements mobiles en zones peu denses, 24 février 2020.
75 La littératie est définie dans le rapport de l'OCDE « *La littératie à l'ère de l'information » comme étant « l'Aptitude à comprendre et à utiliser l'information écrite dans la vie courante, à la maison, au travail et dans la collectivité en vue d'atteindre des buts personnels et d'étendre ses connaissances et ses capacités* ».
76 Site web de la Mission société numérique, article « *13 millions de français en difficulté avec le numérique, Le numérique ne bénéficie pas encore à l'ensemble de la population* ».
77 Site web de la Mission société numérique.
78 Conseil national du numérique, Citoyens d'une société numérique. Accès, Littératie, Médiations, Pouvoir d'agir : pour une nouvelle politique d'inclusion, Octobre 2013.

1.2. Penser les usages dématérialisés en impliquant les collectivités locales

La numérisation d'un panel très large de services a entraîné une multiplication des usages d'identités numériques pour accéder à des ressources et effectuer des actions. Cette massification touche autant les personnes physiques que les personnes morales. Dans ces nouveaux usages, les identités numériques permettent de participer aux interrogations sur l'allocation du budget participatif d'un territoire[79] ou encore de réunir sur un seul support l'ensemble des services de mobilités et de culture multipartenaire d'une localité[80]. Elles sont aussi un levier pour les personnes morales puisqu'elles permettent à des responsables d'associations ou d'entreprises d'effectuer des démarches et déclarations à distance. Dans une certaine prospective, les certificats de signature électronique associés aux identités numériques permettraient de nouveaux usages pour les personnes physiques comme morales allant de la signature d'un bail à la signature d'un contrat de travail ou un virement d'un montant important. Enfin elles pourraient permettre dans une certaine mesure un accès aux aides sociales de fait.

Penser les usages dématérialisés au niveau national ne permet pas de tenir compte des spécificités des différentes régions et des collectivités ni de mobiliser leur expertise et expérience dans le déploiement des politiques d'inclusion sur le territoire. En effet, depuis plusieurs années les collectivités territoriales se sont modernisées pour répondre quotidiennement aux besoins des usagers. Elles ont fait évoluer leur processus de travail et d'interaction avec les usagers en dématérialisant les procédures autant qu'elles ont fait émerger des nouveaux usages s'appuyant sur des identités numériques comme par exemple des refontes des services de mobilités. Elles ont en ce sens développé un savoir-faire spécifique sur les besoins des usagers en terme d'identité numérique et les possibilités pour répondre à de multiples situations, sur des territoires variés, composés individus ayant des sensibilités différentes face aux outils numériques. Les collectivités territoriales, en lien de proximité avec les acteurs locaux de la médiation, ont une réelle expertise métier qui bénéficierait à la réflexion sur l'inclusion des citoyens aux nouveaux usages liés à l'identité numérique.

Les régions peuvent être en tête de la coordination du dispositif, à savoir créer, promouvoir, animer et évaluer les dispositifs de politique d'inclusion articulés à l'échelle locale. Cet échelon nous paraît particulièrement important à investir, du fait de ses compétences en matière de solidarité territoriale par la mobilisation des Centres Communaux d'Actions Sociales (CCAS), des intercommunalités et communes.

C'est par ailleurs le propos majeur du Manifeste pour l'inclusion de l'association des Interconnectés[81] qui appelle à mobiliser les expertises et compétences des villes et communes pour la mise en œuvre de la politique globale d'inclusion numérique.

79 Site web du budget participatif de la ville de Paris.
80 Site web de la carte Trabool.
81 Les Interconnectés, 12 et 13 février 2020, Manifeste des territoires innovants.

1.3. Recenser, renforcer et développer les points d'accueil en guichet pour enrôler, acculturer et soutenir les citoyens éloignés du numérique

L'identité numérique pourrait être un véhicule de facilitation et de confiance entre les citoyens et l'administration, notamment par l'encapacitation des citoyens via les outils de traçabilité et de recours, la fluidification des parcours et l'inscription de l'identité numérique tout au long de la vie citoyenne (de l'identité numérique pour mineurs à l'âge adulte). Cela implique d'articuler les besoins des citoyens et des opérateurs de médiation numérique en prenant en compte les différences selon les territoires, de subvenir aux revendications des points de médiation par des dotations publiques calibrées, de soutenir l'effort de formation des aidants, et d'augmenter le nombre d'heures prévues par le Pass Numérique.

1.3.1. Identifier les guichets

Le principe du choix laissé aux citoyens dans leur recours à l'administration et leur relation à l'identité numérique est primordial pour que la dématérialisation ne soit pas vue comme une contrainte ou une complexité supplémentaire et menée « à marche forcée ». Ainsi, pour les citoyens les moins dotés en littératie numérique, la persistance d'un réseau de guichets implantés sur le territoire leur permettant d'utiliser leur identité numérique pour accomplir et mener à terme des formalités administratives est une nécessité qui doit être pourvue et garantie par l'État au nom du droit à l'accès aux services publics pour tous[82].

Or, en pratique, parmi les difficultés rencontrées par les citoyens, celle de ne plus trouver d'interlocuteur humain a été fortement relevée pendant les consultations menées par le Conseil entre octobre et décembre 2019, mais aussi à la suite du Grand Débat consécutif à la crise des Gilets Jaunes[83], ce qui peut donner lieu à une perception très verticale de l'administration à l'ère de la dématérialisation. Ce constat a déjà fait l'objet d'une partie importante du rapport du Commissariat Général du Plan dit Plan Lasserre[84] selon lequel le rapport de confiance entre usagers et administrations doit se construire de façon mutuelle, dès lors que l'usager est en pleine possession des moyens d'accéder aux services publics dont il a besoin. Le rapport réaffirme que « *l'administration [...] ne saurait être une administration tout électronique qui mettrait une partie de sa population de côté* [85] ».

Ainsi, le Conseil recommande de construire un plan d'inclusion numérique qui passe par la confiance dans les relais, par l'élaboration d'une stratégie forte et cohérente à l'échelle du territoire, et par des moyens développés autour des acteurs publics (État, collectivités, CCAS et autres organismes sociaux) et privés (fournisseurs de services, associations...). Une première étape de ce plan consiste à rendre plus visibles et identifiables les points de médiation numérique.

82 En droit, le principe de l'égalité devant le service public découle du principe d'égalité devant la loi, consacré dès la Déclaration des droits de l'Homme et du citoyen du 27 août 1789. Il signifie que toute personne a un droit égal à l'accès au service, dès lors que celle-ci participe de manière égale aux charges financières résultant du service. Progressivement, ce principe a acquis une valeur constitutionnelle, c'est-à-dire qu'il s'agit désormais d'un principe dégagé par le Conseil constitutionnel et dont le respect s'impose à tous les organes de l'État, y compris le législateur.
83 France Infos, « *Conséquence du Grand Débat national, 460 maisons de services publics ouvrent en 2020* », 16 novembre 2019.
84 LASSERRE Bruno, L'Etat et les technologies de l'information : Vers une administration à accès pluriel, décembre 2000.

Recommandation n°1

Recenser les points de médiation numérique dans une cartographie accessible tout au long du parcours utilisateur dans les démarches administratives afin que les usagers puissent s'y référer en cas de difficulté lors de leurs démarches en ligne.

1.3.2. Éviter l'engorgement en formant les usagers

L'engorgement des guichets de médiation numérique a été plusieurs fois évoqué lors des auditions menées par le Conseil dans le cadre de ses travaux, et relevé également dans le rapport du Défenseur des Droits[86]. Du fait d'un niveau de littératie insuffisant pour accéder aux usages les plus simples des usagers, ces guichets consacrent une partie de leurs ressources à la résolution de problèmes simples (comme l'oubli d'un mot de passe) ce qui impacte mécaniquement leurs missions originelles et les subventions qui y sont associées.

Ainsi, les dispositifs publics de médiation numérique, en l'état, ne permettent pas aux citoyens d'accéder à un niveau de littératie suffisant dans la perspective d'une administration intégralement dématérialisée. D'après un bilan de la Gazette des Communes (développée par la Caisse de Dépôts et Consignations) [87] auprès de centres de médiation labellisés « Maisons France Service », ces espaces pallient aux difficultés immédiates rencontrées par les usagers, en leur apportant un soutien idoine pour débloquer un problème ou accéder à un droit, mais ne sont pas suffisamment dotés de moyens financiers et humains pour aller au-delà de ces situations d'urgence.

Afin de désengorger ces guichets, le Conseil recommande la mise en place d'une formation des usagers aux outils numériques et services dématérialisés (Pass Numérique, mobilisation des Espaces Publics Numériques…) consécutive, par exemple, à la création d'une identité numérique afin de réduire la « fracture numérique ». Cette formation pourrait donner droit automatiquement à l'un des dispositifs prévus par le « Plan pour un numérique inclusif » [88], comme l'attribution d'un Pass Numérique.

Les guichets de médiation numérique pourraient ainsi devenir des lieux-ressources consacrés à la formation et à l'acquisition des usages, à la résolution des points de friction et à l'accompagnement des usagers dans les parcours administratifs. Cette démarche implique de repenser le plan pour un Numérique Inclusif présenté en 2018 en comblant les écarts créés entre la désaffectation des guichets des opérateurs de services publics, et la mise en place de Maisons France Service.

86 Défenseur des droits, Rapport Dématérialisation et inégalités d'accès aux droits, 2019.
87 La gazette des communes, article « *Maisons de services au public : pourquoi il faut faire mieux* », juillet 2019.
88 Site web vie publique, "E-administration : quelle politique pour les exclus du numérique ? ".

Recommandation n°2

Mettre en place des formations à destination des éloignés du numérique dans des lieux dédiés disposant de moyens conséquents :

- enrôlement sécurisé et formation aux usages les plus simples ;
- formation des agents ;
- mise à disposition de matériel en libre service ;
- harmonisation des offres de formation à l'usage des citoyens en fonction des besoins rencontrés sur le territoire ;
- prise en compte des différents niveaux de littératie.

1.3.3. Établir les garanties permettant d'instaurer la confiance

Du point de vue des aidants, la formation autour des bonnes pratiques (notamment en sécurité, confidentialité etc) de la protection juridique de l'aidant et de l'usager doit impérativement s'accompagner d'outils performants permettant de garantir que l'enrôlement, comme l'accompagnement, se fassent dans les meilleures conditions possibles. Pour cela il est nécessaire d'établir les garanties légales permettant de protéger les usagers ayant recours aux aidants (notamment contre des usages non consentis de leur identité numérique), mais aussi de protéger les aidants lorsque ceux-ci effectuent des démarches pour l'usager (notamment en évitant que leur responsabilité ne soit engagée). Le Conseil rappelle que la question de la confiance passe par la démonstration que la dématérialisation s'inscrit dans une démarche qui ne laisse pas le citoyen sans un socle de garanties en cas de mésusage, ce dont les aidants sont le relais sur le terrain.

Recommandation n°3

Encadrer par un socle de droits et de garanties légales le développement d'Aidants Connect pour protéger :

- les usagers contre les risques d'usurpation d'identité et les risques de détournement de leurs identités ;
- la responsabilité des aidants lorsqu'ils doivent effectuer des démarches pour les usagers.

2. ÉLARGIR L'IDENTITÉ NUMÉRIQUE AU PLUS GRAND NOMBRE : L'ENRÔLEMENT

2.1. Engager un design centré sur l'utilisateur dans la mise en œuvre des démarches non encore dématérialisées

Si la formation au numérique, notamment dans ses usages administratifs est une condition essentielle à l'acceptation de l'identité numérique et au plein accomplissement du Plan Action Publique 2022, la simplification des parcours est le deuxième véhicule indispensable pour atteindre une pleine « société numérique » [89].

La mise en œuvre des démarches dématérialisées restant[90] pour accomplir le Plan Action Publique 2022 lancé en 2017[91] s'engagera de manière concomitante à la généralisation des identités numériques publiques, voire de la distribution d'une Carte Nationale d'Identité électronique (CNIe) prévue pour 2021[92]. À ce titre, en réponse aux alarmes de Jacques Toubon, Défenseur des Droits, sur la « *rupture d'égalité entre les citoyens dans leur accès aux droits* » [93], l'identité numérique pourrait permettre de renouer avec l'ambition d'une simplification administrative bénéfique à la fois pour les citoyens et l'administration, selon Cédric O, secrétaire d'État chargé du numérique : « *L'identité numérique contribuera grandement à faciliter les démarches en ligne dans les années à venir* » [94].

Cette ambition implique de penser la transformation des services publics à travers l'ergonomie des parcours utilisateurs, plutôt qu'à travers une numérisation pensée d'abord au bénéfice des processus internes aux administrations. La simplification des démarches pourrait permettre aux plus éloignés du numérique de s'approprier une identité numérique facilitant l'accomplissement de leurs démarches administratives. Pour cela, le parcours devra être conçu autour de l'utilisateur (« user-centric »), de ses besoins, et d'une refonte des étapes identifiées comme sources de frictions (au sens du design) et menant à un fort taux d'abandon des démarches dématérialisées. Cela nécessite que ces parcours soient co-construits avec des designers et un panel de citoyens aux niveaux d'autonomie et de compétences différents qui pourraient identifier les problèmes, proposer des alternatives et tester les solutions retenues. Les designers impliqués dans ces processus pourraient ainsi défaire les points de friction complexes liés à l'identification et l'authentification aux services.

89 Site web du Gouvernement, article « *Pour une République numérique* », novembre 2018.
90 D'après l'observatoire des démarches en ligne, 31 % des démarches n'étaient pas dématérialisées en octobre 2019. Voir le rapport.
91 Site web du Gouvernement, 30 octobre 2018, article « *Action Publique 2022 : pour une transformation du service public* ».
92 ANDRE Michèle, Rapport d'information n° 486 (2008-2009), La nouvelle génération de titres d'identité : bilan et perspectives, Sénat, juin 2009.
93 Propos tenus dans un entretien du journal Les Echos, qui reprend les éléments du rapport déjà cité.
94 Propos tenus sur le compte Twitter du Ministre.

Recommandation n°4

Imposer des critères d'accessibilité et d'inclusion dans la conception des services s'appuyant sur l'identité numérique et qui soient régulièrement testés.

Les usages les plus fréquents de l'identité numérique doivent faire l'objet d'un soin particulier. En effet, ces usages pourraient permettre aux utilisateurs de développer les automatismes (créer et retenir des mots de passe et/ou identifiants, par exemple) et d'inscrire, dans leur quotidien, le recours aux services administratifs numériques.

Dans la même dynamique, la simplification doit s'articuler avec les niveaux de sécurité de l'identification idoines[95]. Ces mécanismes pourront s'appuyer sur les briques d'authentification existantes sur mobiles qui mobilisent des gestes simples et sont acquis aux usages les plus simples.

Recommandation n°5

Formuler un cahier des charges à destination des fournisseurs d'identités posant un certain nombre d'exigences en termes de sécurité et de fluidité, tout en garantissant des bénéfices d'usages déjà acquis.

2.2. L'enrôlement est déterminant pour favoriser l'acceptabilité

Dans le contexte de la dématérialisation et de la mise en place d'une identité numérique pour tous, l'enrôlement demeure une étape importante.

L'enrôlement est l'étape de création de l'identité numérique d'une personne. Elle peut être réalisée par une autorité publique de délivrance de titre, un tiers de confiance (La Poste qui enrôle, en tant que fournisseur d'identité fédéré à France Connect, par exemple[96]) ou de manière automatisée et autonome comme c'est le cas avec la solution « Mobile Connect et moi », fournisseur d'identité privé de France Connect, ou encore la solution publique Alicem, via un dispositif de reconnaissance faciale[97], avec des exigences plus ou moins fortes de sécurité selon le niveau de garantie visé. Ainsi, l'enrôlement doit être 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.

95 cf. Chapitre 2, partie 1.2.4
96 Site web Etat plateforme, "Avec la Poste, France Connect s'enrichit d'un second fournisseur d'identité", octobre 2015.
97 Notons qu'à date de publication du rapport, la solution Alicem n'est pour le moment pas mise à disposition du public.

Cette étape permet de définir avec les citoyens leurs moyens d'authentification, mais aussi de les introduire aux usages futurs de leur identité numérique. Pour créer les conditions d'une acceptabilité et d'une utilisation généralisée de ces usages, le Conseil recommande que cet enrôlement se fasse avec le moins de friction possible et que soient garanties les possibilités de révocation et de vérification de l'accès des citoyens à leur identité numérique à la suite de cet enrôlement.

C'est lors de cette étape fondamentale que sont rencontrés beaucoup des écueils relatifs à l'inclusion et la confiance. Pour tenir ces engagements d'inclusion et d'accessibilité, qui sont des obligations légales, la mobilisation des lieux de confiance de la vie publique (mairies, sous-préfectures…) doit être au coeur des stratégies d'enrôlement à une identité numérique publique : il importe que les citoyens, même les plus éloignés du numérique, puissent s'enrôler de manière simple, sereine et que cet enrôlement consacre ou renforce un lien de confiance entre le citoyen et les administrations. Pour ce faire, le Conseil recommande que l'enrôlement se fasse dans les lieux emblématiques que sont les mairies et les sous-préfectures, à en croire un sondage de l'Institut français d'opinion publique (IFOP) sur le lien entre les citoyens et les élus qui consacre les maires comme catégorie d'élus préférée des Français à 87 % [98], ce qui en fait le « symbole par excellence de l'élu de proximité ». L'étude du CEVIPOF sur la confiance des Français dans leurs institutions est venue confirmer que les échelons territoriaux (mairies, conseil départemental, conseil régional…) sont des vecteurs de confiance importants dans la vie des citoyens[99].

Si, pour des motifs logistiques ou organisationnels, l'enrôlement à une identité numérique publique devait être délégué à des acteurs tiers (privés, publics, associatifs…), il convient de s'assurer que ces acteurs évoquent et répondent à un cahier des charges assurant un niveau de confiance équivalent à celui des mairies.

Ainsi, s'il était décidé que l'enrôlement des citoyens soit délégué à un acteur privé, le Conseil recommande que cette mission soit assortie d'une délégation de service public[100] s'appuyant sur un socle de garanties et de conditions au moins aussi exigeantes que celles s'appliquant aux guichets des pouvoirs publics.

En effet, les décrets d'application de la délégation de service public devront encadrer l'enrôlement par tiers en garantissant un socle de protection de l'usager (sécurité des informations relevées, possibilité de révocation et de modifications des informations, ….) ainsi qu'un effort de formation harmonisé avec celui des agents publics de médiation numérique (guide des bonnes pratiques, protection de l'agent, assermentation). Ainsi, le Conseil recommande que l'assermentation des agents soit obligatoire, afin de participer à la mise en place d'un environnement de confiance pour l'usager.

98 Ifop, Sondage août 2019, Les français et leurs élus.
99 Cevipof, En quoi les Français ont-ils confiance aujourd'hui ? -Le baromètre de la confiance politique, février 2020.
100 L'article L.1121-3 du Code de la commande publique s'attache à préciser en quoi consiste la délégation de service public.

Recommandation n°6

Faire des mairies (et des collectivités territoriales) les principaux lieux d'enrôlement des identités numériques pour soutenir la confiance en l'État.

2.3. L'identité numérique pour les mineurs

L'identité numérique des mineurs[101] soulève des problèmes spécifiques, notamment en ce qu'elle nécessite d'arbitrer les responsabilités et les choix qui, avant cet âge, relèvent des tuteurs légaux et ceux qui relèvent des mineurs.

Le passage à la majorité, dans son application, pose des questions relatives à son articulation avec le droit à l'oubli et au transfert des responsabilités numériques des parents vers l'enfant. Différents événements de la vie civique des mineurs pourraient servir à accompagner ce passage vers la majorité (notamment la Journée d'Appel à la Défense Nationale ou l'inscription à Parcours Sup) et sont autant d'occasions de procéder à l'enrôlement si le passage à la majorité nécessite la création d'une nouvelle identité.

Ces problématiques sont plus largement étudiées par la mission parlementaire d'information sur l'identité numérique de l'Assemblée nationale qui rendra ses conclusions prochainement.

101 La majorité numérique est fixée à 15 ans par application du RGPD. Pour plus de précisions voir site web de la CNIL.

3. UNE PÉDAGOGIE VISANT À RÉDUIRE LA FRACTURE NUMÉRIQUE PERMET L'ENCAPACITATION ET LA CONFIANCE DES CITOYENS

Faire preuve de pédagogie et initier l'ensemble des citoyens au numérique

3.1. La communication devrait être un véhicule de la pédagogie orientée vers les citoyens : le cas Alicem

Alicem : un moyen d'identification électronique

Qu'est-ce qu'Alicem ?

« *Alicem atteste l'identité de manière sécurisée au moyen d'un processus rigoureux. L'utilisateur s'inscrit depuis son smartphone avec son titre d'identité (passeport ou titre de séjour) dont la puce est lue par lecture sans contact NFC (communication en champ proche) et dont l'authenticité et la validité sont vérifiées auprès des services de l'État. Grâce à une technologie de reconnaissance faciale, l'utilisateur prouve qu'il est le titulaire légitime du titre d'identité.*

Après cette phase d'inscription, Alicem permet d'accéder de manière simplifiée, mais toujours sécurisée, à l'ensemble des services partenaires de France Connect. Pour ce faire, l'utilisateur s'authentifie depuis son smartphone avec son code de sécurité. Pour certains usages, une lecture NFC de la puce du titre est également nécessaire. » [102]

Comment l'application fonctionne ?

Pour créer une identité numérique de niveau élevée l'individu devra télécharger l'application sur la plateforme Android[103]. Puis une série d'étapes comme la lecture de la puce de son passeport biométrique et la réalisation de défis de reconnaissance faciale vont permettre à l'individu de créer son identité. La validité du titre sera vérifiée par une interrogation de DocVérif.

Une fois l'enrôlement effectué, l'utilisateur pourrait utiliser Alicem pour accéder à différents services à travers France Connect, que ce soit sur un ordinateur ou un mobile.

Quelle utilisation de la reconnaissance faciale dans Alicem ?

La reconnaissance faciale est utilisée pour vérifier que l'individu qui crée une identité numérique de niveau élevé via l'application Alicem est bien le détenteur du titre biométrique associé cette identité. Il s'agit d'une comparaison du gabarit présent sur le passeport avec celui généré depuis les défis de reconnaissance faciale (preuve de vivacité). Pour des questions de cybersécurité, cette comparaison est faite hors du téléphone, sur des serveurs du ministère de l'Intérieur. Une fois la validation effectuée, les données biométriques sont détruites de l'espace servant à faire la comparaison.

Que se passe-t-il en cas de perte ou de changement de mobile ?

En cas de perte de téléphone, l'utilisateur pourra supprimer son compte. en fonction de son estimation du risque il pourrait alors réinitialiser son compte sur un nouveau mobile avec une carte SIM similaire ou créer un nouveau compte (en supprimant le précédant). Il faut noter qu'un changement de compte ou de carte SIM entraîne la perte de l'ensemble des informations de relatives au compte.

Les controverses autour de l'application Alicem

Plusieurs controverses ont émergé suite à la publication du décret Alicem.

La CNIL a émis plusieurs réserves concernant cette application. Dans son article de novembre 2020 sur la reconnaissance faciale, elle rappelait qu'elle ne s'opposait pas à l'utilisation des données biométriques et plus particulièrement à l'utilisation de la reconnaissance faciale dans le cadre de l'application[104]. En revanche, sa 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[105] mettait en avant une réserve concernant le consentement libre à la reconnaissance faciale en l'absence d'alternative en vue de la création d'une identité numérique au niveau de garantie élevé[106], et des interrogations sur l'accessibilité des différents défis dans la procédure d'enrôlement.

La Quadrature du Net a déposé en juillet 2019 un recours devant le Conseil d'État[107] contre le décret Alicem. Le recours a pour objet : « *Un projet d'identité numérique, fondé sur un dispositif de reconnaissance faciale obligatoire (au mépris du RGPD) et ayant pour objectif avoué d'identifier chaque personne sur Internet pour ne plus laisser aucune place à l'anonymat ne peut qu'être combattu.* »

104 CNIL, Reconnaissance faciale : pour un débat à la hauteur des enjeux, 15 novembre 2019, p. 9.
105 Demande d'avis n° 18008244.
106 Pour répondre à la problématique d'alternative soulevée par la Commission Nationale Informatique et Libertés, la mission interministérielle sur l'identité numérique a imaginé a un parcours utilisateur où le face à face pourrait être effectué hors ligne, dans des lieux spécifiques comme les mairies.
107 Recours de la Quadrature du net devant le Conseil d'État contre le décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile ».

La présentation du projet Alicem a davantage mis en avant son aspect innovant, technique et sécurisé que l'émergence de nouveaux usages, d'opportunités de développement d'un marché de services hautement sensibles assorti de garanties solides pour l'usager. Cette communication trop technicienne n'a pas aidé à la bonne réception de cet outil par le grand public.

Les consultations menées auprès de citoyens et d'experts ont permis de constater une appréhension de l'identité numérique difficile pour les premiers, 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[108]. Ces consultations ont en effet été concomitantes à la communication gouvernementale au sujet d'Alicem[109], critiquée par la presse[110] [111] et par les associations de défense des droits numériques (comme La Quadrature du Net, qui a déposé un recours auprès du Conseil d'État[112]). Le recours à la reconnaissance faciale dans cette application ainsi que l'utilisation des données ont bousculé la communication en laissant peu d'espace pour les autres interrogations sur les usages possibles de l'application.

De fait, lors des consultations menées par le Conseil, Alicem s'est imposé comme un sujet fortement anxiogène et difficile à appréhender pour les non-experts. Ainsi, de nombreux recours à des références culturelles grand public[113] tendent à rapprocher la biométrie à une volonté de l'État de centraliser et collecter des informations à des fins sécuritaires. Cette crainte rappelle à l'État son devoir de pédagogie envers ses citoyens, comme le rappelait déjà en 2001 le rapport Carcenac sur l'e-administration qui « *ne doit pas être prétexte à plus de contrôle sur les citoyens* » [114]. Pour se démarquer de tels scénarios, l'État doit orienter sa communication en tenant compte des craintes des citoyens et communiquer sur les projets législatifs liés à l'identité numérique.

Recommandation n°7

Créer une réelle communication autour de France Connect et la création de la CNIe.

108 Pour rappel, le Conseil dans son avis sur le fichier TES avait considéré qu'il était urgent d'ouvrir une réflexion publique et globale sur la question de l'identité à l'heure du numérique, en recommandant un débat public : « *l'objectif de ce débat est de porter une réflexion globale sur les facettes de l'identité à l'ère numérique (rôles respectifs et articulation entre France Connect, chaîne de traitement des passeports et de la CNI, identités numériques publiques et privées), qui prenne en compte la généralisation des smartphones et l'état de l'art en matière d'architectures (web services, interfaces de programmation et informatique en nuage). Le Conseil avait appelé le gouvernement à encourager la recherche publique sur les sujets de l'identité numérique — encore peu soutenue en France — de la biométrie et des moyens de sa sécurisation.* », Avis du Conseil national du numérique sur le fichier TES, décembre 2016, page 6.
109 Il s'agit d'un hasard.
110 Nextinpact, REES Marc, " ALICEM : la biométrie de l'identité numérique sur mobile fait tiquer la CNIL ", mai 2019.
111 Les Echos, DEDES Florian, " Alicem : démarrage chaotique pour l'identité numérique à la française. ", mai 2019.
112 La Quadrature du net, « *La Quadrature du Net attaque l'application ALICEM, contre la généralisation de la reconnaissance faciale* », juillet 2019.
113 Par exemple, à la série britannique Black Mirror, qui présente un futur technologique dystopique dans lequel les outils numériques remplissent bien souvent des fonctions de discipline et de contrôle. Cette série incarne à l'heure actuelle de nombreuses critiques adressées aux nouvelles technologies. Voir par exemple : Oihab Allal Cherif, « Black Mirror » ou le côté obscur de la technologie, The Conversation, 29 mai 2019.
114 CARCENAC Thierry, Rapport Pour une administration électronique citoyenne, sur la modernisation de l'Administration électronique, Avril 2001.

3.2. Un problème de confiance historique qui nécessite un effort de pédagogie conséquent et une prise en compte des réticences des citoyens

Du projet de Système Automatisé pour les Fichiers Administratifs et Répertoires des Individus (SAFARI) de 1974, au débat houleux sur le fichier des Titres Électroniques Sécurisés (TES) en 2016, la société française entretient, comme cela est rappelé en introduction, une longue tradition de méfiance vis-à-vis des volontés de centralisation d'informations sur les citoyens, et ce pour des raisons évidentes héritées de l'Histoire.

C'est d'ailleurs à la suite de l'échec de la mise en place de SAFARI, appelé à l'époque « SAFARI ou la chasse aux Français » [115] par le journal Le Monde, que le ministre de la Justice de l'époque, M. Jean Lecanuet, présentera le projet de loi « Informatique et Libertés » [116].

Le Conseil souhaite insister sur le fait que l'idée de la surveillance généralisée, qui s'appuierait sur l'identité numérique, a été mentionnée dans l'ensemble des consultations qui ont été organisées. Cette surveillance est souvent mise en parallèle avec deux autres points : la centralisation des informations et la crainte d'être tracé[117], pisté, « fliqué », avec une identité numérique étatique alors que la multiplicité des identités numériques actuelles leur permet de jongler en fonction des situations et des usages. Ces craintes apparaissent comme l'un des premiers freins à l'usage d'une identité numérique, qu'elle soit formalisée par une plateforme ou par une carte. A cette crainte s'ajoute celle que la sécurité des administrations et infrastructures hébergeant ces informations ne soit pas suffisante.

Pour répondre à cette méfiance, un effort de pédagogie semble nécessaire pour rendre transparent le fonctionnement des services de l'État et rassurer les citoyens sur la sécurité et la durée du stockage de leurs données. Afin qu'il soit pleinement efficace, cet effort de pédagogie doit être adapté pour répondre aux craintes de tous les citoyens, qu'ils soient technophiles et à la recherche de détails techniques ou qu'au contraire ils ne disposent pas d'appétence particulière pour ces sujets.

Ainsi, le gouvernement gagnerait à amplifier l'effort d'une pédagogie inclusive et sécurisante, dans une démarche d'encapacitation des citoyens sur les différents outils mis en place.

En effet, les citoyens ne peuvent pas accorder inconditionnellement leur confiance à la mise en place de l'identité numérique si les principes de simplification, de sécurité et de protection de l'usager ne sont pas clairement et massivement communiqués à l'ensemble de la population.

Le Conseil rappelle qu'il s'agit d'un prérequis indispensable à la confiance et l'émergence d'une pleine citoyenneté numérique.

115 Création de la Commission nationale de l'informatique et des libertés.
116 Adopté le 6 janvier 1978 et qui donnera naissance à la CNIL, voir introduction.
117 En rapport à la traçabilité et au « flicage », certains citoyens ont évoqué certains dispositifs anxiogènes comme les compteurs Linky en plus du déploiement des CCTV (Closed-Circuit TeleVision).

Recommandation n°8

Pour répondre aux craintes des usagers vis-à-vis de potentiels abus et du manque de transparence de la puissance publique le Conseil recommande de communiquer massivement sur le fonctionnement des services publics et de la gestion des informations dématérialisées :

- Les obligations légales encadrant les solutions techniques relatives le stockage des informations et en particulier des données personnelles ;
- Les obligations légales définissant les informations relatives aux usagers qui peuvent être transmises entre administrations centrales et locales.
- Existence d'instances de contrôle vérifiant que les obligations légales sont respectées.

3.2.1. La question des données personnelles

Lors des consultations, plusieurs citoyens ont fait part de leurs craintes de voir leurs données personnelles exploitées pour des finalités dont ils n'auraient pas connaissance. En ce sens, le traitement médiatique d'Alicem est représentatif des craintes qu'ont les citoyens de voir la numérisation de leur identité servir de prétexte à de nouvelles formes d'exploitation de leurs données personnelles.

La controverse sur l'exploitation des données personnelles rattachées aux identités numériques privées peuvent venir alimenter ces craintes. Ainsi, l'article 154 de la loi finance 2020[118] permet à quelques administrations de collecter et traiter « *les contenus, librement accessibles sur les sites internet des opérateurs de plateforme en ligne [notamment les sites de vente en ligne et les réseaux sociaux]* » pour des besoins de recherche de manquements et d'infractions. S'il ne s'agit pas d'une exploitation des données personnelles directement liée à l'identité numérique telle qu'elle est traitée dans ce rapport, le traitement des données liées aux identités numériques privées (un compte Facebook ou Twitter, par exemple) ne favorise par une réception positive de l'identité numérique publique par les citoyens. Dans ce contexte, la création d'une identité numérique régalienne pourrait être perçue par les citoyens comme une opportunité de simplifier l'agrégation des données personnelles des citoyens grâce à un identifiant unique.

La volonté qu'ont les citoyens d'éviter que leurs données personnelles fournies par les fournisseurs d'identité privés ne se trouvent associées à leur identité publique s'illustre déjà au travers de leur utilisation de France Connect. En effet, d'après un acteur auditionné, les citoyens évitent d'avoir recours au site des impôts comme fournisseur d'identité lorsqu'ils se connectent à leur banque, et préfèrent utiliser un autre fournisseur d'identité public (comme Ameli). Un tel comportement pourrait être motivé par la crainte de voir les services des impôts accéder directement aux informations bancaires grâce à cet identifiant.

118 Loi n° 2019-1479 du 28 décembre 2019 de finances pour 2020.

Ces comportements découlent entre autres d'une méconnaissance des citoyens de leurs droits et de la façon dont leurs données personnelles peuvent être traitées. Un des leviers pour répondre à ces craintes est, outre un effort de communication accru concernant les nouveaux traitements de données personnelles mis en place par l'État, une meilleure information et formation des citoyens pour leur permettre de comprendre et de mieux gérer l'accès à leurs données personnelles.

Recommandation n°9

Il est nécessaire d'informer sur la maîtrise qu'ont les citoyens vis à vis de leurs données personnelles, fondement de leurs identités numériques au sens large. En plus d'un apprentissage sur le long terme à destination de élèves du primaire et du secondaire, le Conseil recommande d'un budget soit alloué à la CNIL, pour réaliser des campagnes de communications sur les données personnelles dans des grands médias et à des heures de grandes écoutes.

3.2.2. Le fonctionnement des services publics

Outre le sentiment de défiance vis-à-vis de certains nouveaux services développés par l'État, et déjà mentionnés plus haut, les consultations ont fait ressortir que certains citoyens craignent de voir leurs données transférées entre les services déjà existants sans en être informés. Dès lors, même si certaines initiatives telles que le « dites-le-nous une fois » 119 permettent de simplifier la vie des usagers, l'impression que leurs données pourraient transiter d'un service public à un autre peut suffire à les dissuader de s'en servir.

France Connect, en ce qu'il sert de hub entre les différents services et fournisseurs d'identités, doit être mis au centre de l'effort pédagogique qu'il convient de faire pour que les citoyens comprennent comment les données sont utilisées par différents services. En effet, la richesse de la fonctionnalité qu'offre la plateforme et sa position à l'intersection de différents services publics en font l'exemple idéal pour communiquer sur le fonctionnement des fournisseurs de services et leur accès restreint aux seules données.

De plus, cette communication doit être articulée à différents échelons d'acteurs de confiance : relais institutionnels, réseau de médiation numérique, collectivités territoriales… Celle-ci doit s'appuyer sur une communication forte de la part de la DINUM, notamment sur les évolutions de France Connect.

119 Simplification des démarches administratives : « Dites-le-nous une fois » passe à la vitesse supérieure.

Recommandation n°10

Engager France Connect dans une réflexion sur la manière dont il explique :

- Son architecture ;
- Les rapports entre les différents fournisseurs d'identité et fournisseurs de services ;
- Les différents niveaux de sécurité eIDAS ;
- Le nœud d'interopérabilité européen (cf. Chapitre 2, partie II. 1.2.2.).

3.3. La formation de tous : un prérequis à l'émergence de l'identité numérique

La pédagogie et la communication sont deux éléments importants pour faire émerger une citoyenneté numérique et donner aux individus les capacités de choisir leurs identités numériques, en particulier pour interagir avec les services publics. Néanmoins, ces éléments sont à accompagner d'un effort conséquent sur la formation à trois niveaux : la formation des élus qui prennent des décisions en matière d'identité numérique, la formation des adultes pour éviter le creusement d'un écart générationnel et enfin la formation des mineurs pour les acculturer aux pratiques numériques respectueuses de la vie privée et de l'individualité de chacun.

3.3.1. Les collectivités locales pour plus de souveraineté et pour faire des choix éclairés

Dans une intervention au Forum International de la Cybersécurité 2020, Anne Le Henanff[120] élue du Morbihan expliquait comment les élus, confrontés à une attaque de leur système en 2016, avaient appris l'importance de certaines règles en matière de protection des données personnes et d'hygiène informatique.

Les auditions de plusieurs acteurs des collectivités territoriales menées par le Conseil lors du « Forum des Interconnectés » ont mis en avant l'importance de la formation au numérique des citoyens qui sont amenés à faire des choix impactant un grand nombre d'individus : qu'il s'agisse de la solution de gestion d'identité des comptes de la bibliothèque municipale ou des procédures d'inscription à la cantine scolaire pour un foyer comptant trois mineurs. Dans ces circonstances, c'est la capacité de choix des prestataires, des services, qui est impactée autant que la modernisation des processus pour répondre aux différentes lois en vigueur.

Les élus sont accompagnés de personnels experts et compétents. En raison de leurs pouvoirs conférés par l'élection, ce sont les représentants des citoyens qui arbitrent et font des choix qui vont impacter les citoyens. Par exemple, pour faire vivre le débat citoyen, la province de

120 Voir présentation sur le site de Villes Internet.

Namur propose aux différentes collectivités un outil numérique de participation citoyenne, reposant sur un gestionnaire d'identité privé. En effet, à l'époque de sa création, le recours à ce fournisseur d'identité paraissait simple, d'autant qu'il était fortement utilisé par les usagers, et permettait d'évacuer la problématique de la gestion des identités. Cette série de choix pose maintenant de grands enjeux pour faire évoluer l'outil, en particulier sur le type de fournisseur d'identité à proposer.

Le cas belge est un peu éloigné du cas français puisque les services de France Connect ont très tôt été proposés aux différentes collectivités. Néanmoins certains élus[121], ainsi que les personnels administratifs, se sentent éloignés des sujets numériques et, parfois, peu en capacité de prendre des décisions relatives à l'identité numérique, ses gestionnaires, et son architecture.

En janvier 2020, un rapport des inspections générales des Finances et de l'Administration (IGF/ IGA) sur la formation des élus[122] proposait d'effectuer une refonte des possibilités de formations via la création d'un compte de formation de l'élu local (CFEL), « *ouvrant des droits pour tous les élus locaux, mobilisable par les élus et par la collectivité [et qui] financerait uniquement des formations à l'exercice du mandat rattachées à un répertoire national de formation des élus locaux (RFEL) mis à jour régulièrement […]* » [123]

Le Conseil considère comme opportun d'intégrer à ce répertoire un panel de formations obligatoires traitant du numérique et plus particulièrement de l'identité numérique et de ses enjeux, dotant les élus d'un bagage numérique leur permettant d'assurer au mieux leurs missions.

Recommandation n°11

Former l'ensemble des élus et des personnels des collectivités au numérique, en s'appuyant sur des parcours de formation obligatoires inscrits dans un répertoire national de formation régulièrement mis à jour.

3.3.2. Inclure l'ensemble de la population à travers la formation des adultes

Comme cela a été explicité en début de ce chapitre (partie I du chapitre I), un grand nombre de lieux associatifs ou de lieux de médiation numérique prennent en charge une partie de la formation au numérique des publics demandeurs. Ces formations peuvent aller de l'utilisation d'une boîte mail à l'utilisation d'outil d'administration en passant par des

121 DURAND-TORNARE Florence, MELIN Anna, Le choix de l'élu dans une France numérisée, Cités en réseaux 2020, Association Ville internet.
122 ACAR, Bruno, GIGUET, Xavier, SCHECHER François, MORIN Gabriel, janvier 2020, Rapport La formation des élus locaux, IGA, IGF.
123 ibid, Recommandation n°4.

réflexions sur la gestion des informations personnelles et des traces sur internet[124].

Alors que ces formations sont indispensables et nécessaires, elles sont confrontées à deux limites :

- leur financement par appels d'offres pour répondre à des problématiques spécifiques sur des outils ;
- les lieux de formations, souvent associés à des centres sociaux ou des espaces d'aide sociale, qui paraissent stigmatisants pour certains.

Dans ces conditions et pour développer le socle d'une culture numérique homogène dans l'ensemble de la population et nécessaire pour répondre aux enjeux de l'identité numérique, le Conseil estime qu'il est important d'accentuer les efforts sur la formation des adultes. Ces formations pourraient être pilotées par la Mission société numérique et l'Agence des territoires en lien étroit avec l'éducation nationale pour qu'il y ait une cohérence avec les parcours de formation des mineurs.

On peut ainsi s'inspirer de l'exemple Estonien : associer au déploiement de l'identité numérique la mise à disposition de temps de formation pour les adultes hors des périodes de travail.

Recommandation n°12

Pendant les cinq premières années de déploiement du dispositif, le Conseil recommande que l'État mette en place des formations gratuites en dehors des périodes de travail à destination des publics majeurs.

3.3.3. Préparer les générations futures : l'enjeu de la formation des mineurs

Il convient de nuancer la croyance selon laquelle toutes les personnes nées après l'an 2000 seraient spontanément à l'aise avec les outils numériques[125]. Les jeunes publics sont, tout autant que les adultes, soumis aux exigences de formation nécessaire pour une appropriation de la citoyenneté numérique. L'Éducation nationale se doit non seulement d'inculquer un socle de connaissances solides à l'ensemble des élèves, mais aussi de poursuivre d'autres buts, tels que la concrétisation du principe d'égalité et la fabrique de la citoyenneté. Un enseignement du numérique pour tous les élèves de seconde se doit de servir ces objectifs, sur la base d'éléments généraux sur le numérique. 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.

125 Voir notamment les travaux sociologiques les plus récents sur ces questions Jen Shradie, ou Dominique Pasquier, L'internet des familles modestes : Enquête dans la France rurale, Paris : Presse des Mines, 2018

Depuis cette rentrée, les lycéennes et lycéens en classe de seconde générale et technologique bénéficient donc obligatoirement, une heure et demie par semaine, de ce nouvel enseignement de « Sciences Numériques et Technologie » (SNT), avec l'objectif de « *permettre d'appréhender les principaux concepts des sciences numériques, mais également de permettre aux élèves, à partir d'un objet technologique, de comprendre le poids croissant du numérique et les enjeux qui en découlent.* » [126]

S'appuyer sur la citoyenneté numérique, c'est aussi prendre en compte l'éducation civique des individus. Le parcours scolaire instruit les mineurs aux définitions et enjeux de la citoyenneté, plus particulièrement dans le cadre d'un enseignement spécialisé dès le collège.

Dans ce cadre, l'introduction du concept de citoyenneté numérique pour les mineurs permettrait de diffuser auprès des élèves les notions de responsabilité, de sécurité et de protection des données personnelles en prenant appui sur les règles juridiques françaises et européennes, en rappelant les principes fondamentaux en la matière (notamment issus du RGPD et de la loi Informatique et Liberté).

Ainsi, le Conseil recommande d'intégrer les enjeux de l'identité numérique tout au long de la scolarité, en l'intégrant au socle « Enseignement moral et civique » enseigné dès le collège, et en agrémentant cet enseignement d'outils d'encapacitation des futurs citoyens en devenir auxquels pourraient être associés des acteurs déjà identifiés et travaillant sur ces thématiques comme le CLEMI[127] ou les réseaux éduCNUM de la CNIL[128].

Recommandation n°13

Créer un parcours de formation qui corresponde aux besoins de citoyenneté numérique pour les élèves de primaire et du secondaire, afin que ceux-ci soient armés pour leurs premiers usages autonomes.

Recommandation n°14

En complément des formations, mettre en place :

- Une plateforme regroupant l'ensemble des cours à destination des publics adultes, ainsi que les textes en lien avec la thématique ;
- Que soit organisé, annuellement, un programme de communication sur le sujet sur les médias de forte audience. Le premier cycle devrait traiter de l'identité numérique en lien avec les décisions de l'État concernant la dématérialisation des services publics.

126 Réponse du ministre de l'éducation nationale et de la jeunesse au CSP du 3 juillet 2018.
127 Voir site web du Clemi.
128 Voir site web d'educNUM.

CHAPITRE II
LA CONFIANCE : UNE CONSTRUCTION BASÉE SUR LA GOUVERNANCE ET LA SÉCURITÉ

Développer un environnement de confiance basé sur une maîtrise de la souveraineté et une responsabilisation des différentes parties-prenantes

L'identité numérique ne pourra être un levier de la citoyenneté numérique que si les individus sont en mesure de se saisir des usages qui y sont associés. Malheureusement, nos pratiques numériques dans des environnements fermés et souvent opaques ont entraîné une délégation des savoirs néfaste à la prise en main des outils numériques. Pour le Conseil, il est primordial de créer une relation de confiance afin que les citoyens se saisissent de ces technologies de leur propre initiative.

Cette confiance ne peut pas uniquement découler d'une délégation aveugle du citoyen à l'État, mais devrait se développer sur la base de pratiques vertueuses émanant des pouvoirs publics, sur lesquelles des efforts de communication doivent être faits[129] (cf. chapitre 1). De plus, comme le Conseil l'expliquait en 2015 dans le rapport Ambition numérique, « *la dématérialisation des services publics et la multiplication des données personnelles collectées par l'administration peuvent potentiellement conduire à des dérives […]* ».

Par conséquent, « *l'État doit faire preuve d'exemplarité pour garantir les droits et libertés fondamentaux numériques* » [130]. Ce dernier a des responsabilités supérieures à celles des entreprises du numérique qui, elles, peuvent se prévaloir d'avoir été « choisies » par les utilisateurs. Dans cette ambition de créer une identité numérique de confiance, quatre principes directeurs sont à prendre en compte.

La gouvernance peut être définie comme : « *les formes de pilotage, de coordination et de direction des individus, des groupes, des secteurs, des territoires, et de la société, au-delà des organes classiques du gouvernement. […] avec trois points centraux : l'idée de donner une direction à la société, de mobiliser une coalition et enfin d'exercer une contrainte, soit trois dimensions essentielles du politique.* » [131] Pour l'identité numérique, les enjeux sont son but (et la philosophie générale du modèle d'identité numérique), le partage de la gouvernance entre les différentes parties prenantes et le cadre législatif qui lie et contraint les acteurs.

La sécurité et le sentiment de sécurité, absolument nécessaires pour la construction d'un climat de confiance. Ce lien est mis en exergue par l'Union Européenne pour qui « *l'instauration d'un climat de confiance dans l'environnement en ligne est essentiel au développement économique et social* » [132]. En effet, si « *les consommateurs, les entreprises et les autorités publiques n'ont pas confiance, notamment en raison d'un sentiment d'insécurité, ils hésiteront à effectuer des transactions par voie électronique et à adopter de nouveaux services* »[133]. Cette notion de sécurité est au centre des normes de reconnaissance mutuelle dans le champ européen.

129 La communication étatique autour du numérique a été plutôt mal accueillie par la population et la société civile, mettant en avant une forte méfiance, comme cela a pu être relayé dans la presse thématique comme l'article 154 du projet de loi de finances, le décret Alicem, les projets d'expérimentation de reconnaissance faciale ou encore plus récemment l'application GendNote.
130 Ambition numérique page 103.
131 LE GALÈS, Patrick. "Gouvernance." In Dictionnaire des politiques publiques, edited by Laurie BOUSSAGUET, Sophie JACQUOT, and Pauline RAVINET, 5e édition., 299–308. Paris : Presses de Sciences Po, 2019.
132 Règlement (UE) No 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 et abrogeant la directive 1999/93/CE.
133 Idem.

Par ailleurs, d'après les chercheurs Milad Doueihi et Jacopo Domenicucci, la confiance représente une relation alors que la sécurité est une réalité qui se concrétise par des dispositifs d'assurance[134]. Une sécurité maximale des données sacrifiant l'expérience de l'utilisateur ou la facilité d'usage des services serait contre-productive. De plus, une approche trop centrée sur la sécurité ne participera pas à convaincre des utilisateurs déjà méfiants.

La souveraineté de l'identité numérique soulève une question : comment l'État–qui en faisant jouer une prérogative régalienne, celle de l'identité, dans un environnement transnational soumis à un grand nombre de risques et une forte concurrence–peut-il garder la maîtrise de sa souveraineté ? Alors que classiquement la souveraineté se traduit par l'existence de monopoles étatiques et de l'application de la loi, elle est questionnée par le numérique. Selon Pierre Trudel[135], la souveraineté dite numérique ne devrait pas être un état sanctuarisé, immuable, mais devrait être vue comme un processus. Dans ce contexte, « *[l]'Union Européen représente le modèle le plus achevé de mutualisation de souveraineté par des États-nations démocratiques au moyen d'institutions supranationales.* » [136]

En fonction de ces différentes définitions, il est possible de constater que la confiance s'inscrit dans une imbrication d'éléments nécessaires à l'émergence d'une citoyenneté numérique médiée par l'identité numérique. Elle va de pair avec la question de la cohérence des mesures mises en place par l'État. Elle fait appel à la responsabilité des acteurs ainsi qu'à la transparence du système (cf. chapeau de cette introduction).

134 DOUEIHI Milad et DOMENICUCCI Jacopo Domenicucci, La confiance à l'ère numérique, Berger-Levrault, avril 2018.
135 TRUDEL, Pierre, « La souveraineté en réseaux » dans Annie Blandin-Obernesser, Droits et souveraineté numérique en Europe, Bruxelles, Bruylant, 2016, pp. 5-14.
136 ibid. p. 13.

1. UNE GOUVERNANCE PARTAGÉE QUI REPLACE LE CITOYEN AU CENTRE

Opter pour une gouvernance partagée qui replace le citoyen au centre

Le Conseil estime crucial de replacer l'usager au centre, de ne pas limiter les identités numériques à des problématiques de sécurité intérieure, et de créer les chaînes de confiance pour faire émerger une citoyenneté numérique.

Placer l'usager au centre implique de redonner du pouvoir aux citoyens afin de mieux maîtriser leurs identités numériques. Cette maîtrise peut se faire au niveau individuel (quelle identité pour quel service) ou à un niveau plus général à travers la gouvernance de l'identité numérique. Pour que cette gouvernance ne soit pas médiée « par les instruments » [137], deux leviers sont utiles pour replacer le citoyen au cœur des processus : la transparence et le contrôle citoyen.

À travers ces deux leviers, l'objectif est de réaffirmer l'État de droit, comme le Conseil le proposait déjà dans son rapport de juin 2015 Ambition numérique[138].

1.1. Transparence et confiance : piliers d'une citoyenneté numérique qui s'appuie sur une gouvernance partagée de l'identité numérique

Il apparaît de plus en plus que la transparence est un levier pour l'acceptation par les citoyens et le déploiement des identités numériques. Les processus adéquats doivent être mis en place pour répondre à cet enjeu.

Recommandation n°15

Mettre en place des outils de transparence et de contrôle démocratique déjà utilisés dans d'autres cadres. Notamment :

- Publication de bilan annuel par les opérateurs d'identité numérique : coûts et investissements dans l'identité numérique, explication des choix technologiques, appels d'offres publics, formations des personnels administratif et extérieurs, etc. ;
- Audit externe annuel des systèmes les plus critiques par l'ANSSI et la CNIL, en complément des audits de l'usabilité des systèmes (cf. recommandation n°1)

137 LASCOUMES, Pierre, LE GALES, Patrick (dir.), Gouverner par les instruments, Presse de Sciences Po, 2004.
138 op. cit, p. 79.

1.1.1. Une vision globale et réfléchie de concert : un rôle pour toutes les parties prenantes

1.1.1.1. L'administration doit s'assurer d'avoir une vision holistique pour assurer une bonne gestion des coûts

Les différentes auditions les consultations que le Conseil a mené ont fait émerger un questionnement autour de la gestion globale des coûts de l'identité numérique quand celle-ci se retrouve dans différents projets sectoriels. À titre d'exemple, alors que l'État développe une carte nationale d'identité électronique (CNIe), les réflexions parallèles autour de l'e-Carte vitale questionnent puisque les finalités de cette dernière pourraient chevaucher les potentielles évolutions de la CNIe[139].

Dans ces conditions, la dilution des budgets dans plusieurs programmes avec des composantes similaires laisse craindre une perte d'efficacité et d'impact si des pistes de mutualisation n'étaient pas retenues. Alors qu'une mission sur l'identité numérique[140] est portée par le programme interministériel sur l'identité numérique sur commande des ministres de l'Intérieur et de la Justice, il serait étonnant de voir émerger des initiatives sectorielles qui ne soient pas rattachées à cette mission. L'identité numérique devrait au contraire être coordonnée interministériellement, en prenant en compte les problématiques sectorielles de chaque partie prenante, pour éviter les effets de double emploi de différentes solutions étatiques et le manque de cohérence des solutions proposées.

Pour répondre à cette question de gouvernance globale et de cohérence du modèle proposé, les projets de création d'identité numérique devraient être portés à la connaissance de la mission interministérielle. Sur le long terme, il est nécessaire de pérenniser cette mission en une politique publique, qui pourrait être portée conjointement par le ministère de l'Intérieur et la DINUM, et chargée du suivi de l'ensemble des projets d'identité numérique pour :

- vérifier le périmètre d'action de chaque dispositif et s'interroger sur une mutualisation potentielle de certains dispositifs ;
- proposer des standards d'interopérabilité dans l'optique de possibles évolutions des systèmes.

1.1.1.2. Gouvernance économique : structuration des acteurs économiques et soutien du gouvernement

Les acteurs économiques et les industriels proposant des solutions d'identité numérique, se sont structurés depuis plusieurs années dans des groupements autour des questions de cybersécurité (par exemple, Hexatrust ou l'Alliance pour la confiance numérique). Néanmoins, le projet « identité numérique de confiance », présent dans le Contrat stratégique de filière cyber[141], signé en janvier 2020 démontre le besoin de ces acteurs d'avoir des sas d'échange dédiés avec le gouvernement. En effet, les auditions du Conseil, ainsi que les consultations avec les

139 Pour autant le programme interministériel a pu rapporter au Conseil que le ministère de la santé était intégré depuis le début au comité de pilotage et qu'une solution dérivée de l'identité numérique régalienne serait sûrement proposée.
140 Lettre de saisine de la mission identité numérique, janvier 2018.
141 Contrat stratégique de la filière Industries de sécurité 2020/2022, 29 janvier 2020.

experts, ont mis en avant l'importance pour les industriels de connaître les arbitrages gouvernementaux[142] en matière d'identité numérique pour pouvoir développer des solutions techniques, favoriser l'innovation et maintenir leur compétitivité face à leurs concurrents étrangers.

Le Contrat de filière cherche à répondre à ces besoins à travers un engagement des deux parties :

- « *Les industriels s'engagent à :*
  - *définir une spécification unique de l'OS de la future CNIe ;*
  - *construire rapidement des solutions et services enrichis permettant de viser directement le développement d'usages opérationnels à grande échelle et les mettre en service ;*
  - *développer des actions de sensibilisation et de communication vers les acteurs du secteur privé.*
- *L'État s'engage à :*
  - *déployer la CNIe dès 2021 ;*
  - *poursuivre en 2020 les travaux normatifs assurant les conditions de succès de l'identité numérique publique et privée-poursuivre le déploiement du fédérateur d'identité FranceConnect.* » [143]

Le Conseil salue cette initiative qu'il estime bénéfique pour la richesse de l'offre de solutions qui sera proposée aux citoyens. Il espère qu'elle pourra répondre aux enjeux de soutien de l'innovation et de multiplication de l'offre d'identités numériques à destination des utilisateurs. Il regrette néanmoins que les fournisseurs de services n'aient pas été associés à l'initiative dans le but de développer des solutions tournées vers les usagers. De plus, il estime qu'un positionnement rapide de l'État concernant les fournisseurs de services privés accessibles avec la solution d'identité numérique régalienne permettrait à d'autres acteurs privés de développer des offres commerciales à l'attention de cet écosystème sans risquer d'entrer en concurrence avec l'offre étatique.

1.1.1.3. Les collectivités territoriales : des acteurs de confiance pour l'identité numérique

La gouvernance de l'identité numérique ne peut être pensée sans les acteurs qui vont la déployer au quotidien : les collectivités, à travers les mairies. Celles-ci sont au premier poste dans la distribution des cartes nationales d'identité et le déploiement de l'identité numérique de niveau élevé supportée par ces cartes. De plus, en tant qu'opérateur de services publics, les collectivités territoriales sont un maillon crucial.

Les enjeux entourant l'enrôlement, la formation des personnels administratifs et la mise en place de nouveau processus de travail ont été mis en avant dans le chapitre I. Néanmoins, il est nécessaire de rappeler que les collectivités territoriales ne peuvent pas être vues comme les opérateurs d'une politique centrale, appliquée de manière pyramidale :

142 Cela peut sembler être une évidence, mais la lenteur de la prise de décision et de communication a pu par le passé fortement ralentir un secteur industriel très innovant.
143 Ibid. p. 36

elles doivent être parties prenantes du processus de gouvernance de l'identité numérique.

Les auditions effectuées ont révélé que les territoires et les collectivités pourraient être d'importants maillons de la chaîne de confiance soutenant l'identité numérique, qu'elle soit ou non portée par la CNIe.

Ces acteurs doivent être intégrés en amont aux réflexions afin de ne pas subir de décisions centralisées en matière d'identité numérique. Leur expérience de terrain sera précieuse pour évaluer le budget nécessaire au déploiement par la CNIe ainsi que l'organisation et le maillage territorial de cette délégation de service. Une réflexion collective avec des acteurs tels que les Interconnectés, la France urbaine ou encore l'Association des Maires de France permettra de fixer un mode de déploiement acceptable qui ne sera pas vécu comme une décision unilatérale de l'État. Cette coordination avec les territoires pourra être le fait de la nouvelle agence de cohésion des territoires, l'ANCT.

Recommandation n°16

Établir une feuille de route, associée à un budget propre, sur le déploiement par les mairies de l'identité numérique, co-construite avec les territoires pour le déploiement de l'identité numérique sous le pilotage de la mission interministérielle, en lien étroit avec les ministères de l'intérieur et de la cohésion des territoires et des relations avec les collectivités territoriales.

1.1.2. Gouvernance sociétale : la nécessité de créer des instances mixtes pour suivre les usages et l'évolution des outils, en accord avec les aspirations citoyennes

1.1.2.1. Instauration d'une instance multi parties prenantes qui joue le rôle de garde-fou sur l'identité numérique pour assurer la transparence

Pour répondre au besoin de confiance dans le système et son opérateur, les citoyens et les experts consultés suggèrent de créer une instance jouant le rôle de garde-fou qui permettrait d'éviter les dérives pouvant apparaître avec la démocratisation des identités numériques : Commission de Suivi et de Gestion des Identités Numériques (CSGIN)

En complément des missions qui incombent déjà à la CNIL et à l'ANSSI, cette instance aurait des missions de surveillance et de contrôle a priori, et a posteriori dans un rôle d'évaluation, d'audit. Si la CSGIN est en charge du contrôle et du suivi, elle n'est pas en charge de l'application des sanctions sur le mauvais traitement des données personnelles, qui font partie des missions de la CNIL. En revanche, de par son expertise et les ressources quotidiennes qu'elle mobilise sur la gestion et la suivi de l'identité numérique, elle sera en capacité de recueillir des preuves en cas de mésusage, de constituer un dossier, et de saisir la CNIL pour que celle-ci applique la législation en vigueur et les sanctions adéquates. Elle sera aussi en charge de consultations thématiques et d'organisation

du débat citoyen autour de l'identité numérique, sa gestion et ses innovations (cf. infra 1.2.2.).

Afin de maintenir son indépendance, cette instance pourrait être, entre autre, financée par les redevances découlant de l'utilisation de l'identité numérique[144]. En effet certains citoyens et experts ont mis en avant que le niveau de confiance serait moins important si cette instance tirait son budget directement de l'État.

Une composition multi parties prenantes est nécessaire pour signifier que cette instance n'a pas vocation à légitimer les actions du gouvernement mais bien à répondre à l'impératif de transparence. Elle serait composée de chercheurs, de la société civile et du Défenseur des droits. Les missions de la CSGIN recoupant certaines missions actuelles du programme interministériel identité numérique, la Commission pourrait une fois les missions du programme remplies, récupérer une partie des ressources. Des personnels administratifs pourraient être détachés ponctuellement au sein de l'instance, pour venir informer des évolutions de l'identité numérique. Un lien particulier serait maintenu avec l'ANSSI et la CNIL grâce à des réunions trimestrielles dans un premier temps, puis biannuelles par la suite.

Recommandation n°17

Créer une instance de contrôle et de supervision indépendante et multi parties prenantes (académiques, associatifs, administratifs, etc.), nommée Commission de Suivi et de Gestion des Identités Numériques (CSGIN).

1.1.2.2. Forum de participation citoyenne pour soutenir le tiers de confiance.

Dans le système politique français, la gouvernance s'inscrit dans une réflexion démocratique. Pour faire vivre cette réflexion sur l'identité numérique il paraît donc opportun de prendre appui sur les principes effectifs de la démocratie participative à travers l'introduction de forum de participation citoyenne sur l'identité numérique. Comme le rappelle le chercheur Loïc Blondiaux, les modalités de discussions doivent : « *[…] prendre au sérieux les conditions matérielles de discussion […], encourager l'émergence d'acteurs capables d'animer le débat de façon neutre, promouvoir une constitution démocratique mixte […], jouer sur la complémentarité des dispositifs, faire en sorte que le rôle de la participation ne demeure pas uniquement consultatif, et pallier enfin les logiques d'exclusion sociale caractéristiques du fonctionnement démocratique actuel.* » [145]

Sous le pilotage de la CSGIN, l'instance ayant le rôle de garde-fou, cet espace de débats avec les citoyens permettra d'obtenir des retours sur les dispositifs d'identité numérique, leurs usages, leur philosophie,

144 Selon les aménagements prévus par la LOLF (articles 16 et suivants) pour ne pas aller à l'encontre du principe d'universalité budgétaire et de non-affectation des recettes.
145 RODET, Diane, « Loïc Blondiaux, Le nouvel esprit de la démocratie. Actualité de la démocratie participative », Lectures, Les comptes rendus, 2008.

leur périmètre, ainsi que l'évolution de la citoyenneté numérique. La synthèse de ces débats, rapportée par l'instance, permettra une agilité du dispositif à travers un processus itératif.

Recommandation n°18

Accorder à l'instance 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 ». De plus, la CSGIN pourrait soutenir l'animation locale des débats en aidant les acteurs territoriaux tels que les Maisons France Service.

1.1.3. Des règles claires pour les fournisseurs d'identité privés et les fournisseurs de services privés : la loyauté des fournisseurs dans l'intérêt des citoyens

En 2015, dans son rapport Ambition numérique, le Conseil proposait un concept de loyauté des plateformes. La loyauté se définit comme « *[visant] à obliger les acteurs économiques à assurer de bonne foi les services qu'ils proposent sans chercher à les détourner à des fins contradictoires à l'intérêt de leurs utilisateurs, qu'ils soient particuliers ou professionnels.* » [146]. Dans son rapport de 2017 précité sur les enjeux éthiques des algorithmes et de l'IA[147], la CNIL proposait d'introduire un principe de loyauté qui pourrait s'inscrire dans une nouvelle génération de garanties et de droits fondamentaux à l'ère numérique, des « droits-système » organisant la gouvernance mondiale de notre univers numérique. Cela signifie que tout service numérique devrait être loyal envers ses utilisateurs, non pas seulement en tant que consommateurs, mais également en tant que citoyens, voire envers des communautés ou de grands intérêts collectifs dont l'existence pourrait être directement affectée.

Dès lors, le principe de loyauté est utilement mobilisable dans le cas de l'identité numérique. Ce principe devrait donc être matérialisé dans la relation tripartite État, citoyens, fournisseurs d'identité et pourrait être inscrite dans la délégation de service public[148]. La mission d'intérêt général et de facto de l'intérêt des citoyens aurait alors la primauté. Dans le cadre des missions qui sont déléguées aux fournisseurs d'identité par l'État, celui-ci doit s'assurer de leur bonne gouvernance, en établissant des règles et un cadre strict de leur relation avec les usagers ainsi que les services privés avec lesquels ils traitent. Pour l'instant, cette relation est contractualisée par les conditions générales d'utilisation de la plateforme France Connect[149], ce qui ne semble pas suffisant aux regards des enjeux que soulève la généralisation des identités numériques. De plus, les

146 op. cit, p. 59.
147 CNIL, 2017, rapport précité Comment permettre à l'homme de garder la main.
148 Pour rappel, la délégation de service public est « *un contrat par lequel une personne morale de droit public confie la gestion d'un service public dont elle a la responsabilité à un délégataire public ou privé, dont la rémunération est substantiellement liée au résultat de l'exploitation du service. Le délégataire peut être chargé de construire des ouvrages ou d'acquérir des biens nécessaires au service.* ».
149 Les fournisseurs d'identité sont actuellement soumis aux conditions générales d'utilisation de la plateforme France Connect.

liens[150] avec les fournisseurs de services qui accèdent à la plateforme France Connect ainsi que les types de fournisseurs de services sont à étudier, notamment pour s'assurer de la qualité et du respect des droits des citoyens sur leur service. France Connect est perçu par les citoyens comme une marque étatique, et à ce titre, la confiance doit y être maintenue.

Cette délégation doit être suivie par l'instance de contrôle ainsi que la DINUM, dans ses relations avec les fournisseurs d'identité et de services qui sont intégrés à l'agrégateur France Connect. De plus, le ministère de l'Intérieur aura un devoir de transparence auprès de la CSGIN pour le suivi du respect des droits d'utilisation des certificats d'authentification qu'il va fournir, que ce soit par des titres ou par une interaction avec la plateforme DocVérif [151]. L'instance de contrôle pourra demander à tout moment un état des lieux de ces utilisations.

Il faut garder à l'esprit que l'écosystème de l'identité numérique va grandir et se développer en fonction des choix, et des prises de positions du gouvernement. Établir un contrat qui a pour objet l'exécution d'un service relatif à l'identité numérique permet de maintenir des garanties fortes aux parties contractantes et aux citoyens et représente par conséquent une caution profitable à tous.

Recommandation n°19

Soumettre les fournisseurs d'identité privés à un contrat qui définisse la délégation du service public qu'ils effectuent en fonction du type d'action qu'ils prennent en charge. Le contrat de délégation de service public devrait être guidé par un principe de loyauté dans l'intérêt général et dans l'intérêt des utilisateurs qui participe plus largement du principe de loyauté des relations contractuelles..

Recommandation n°20

Rendre public, au titre de l'open data, les métadonnées issues des connexions des individus, de manière anonyme et agrégée, de sorte à :

- Éviter qu'une structure (plus importante qu'une autre) ne bénéficie des externalités positives d'un système créé par l'État sans redistribution ;
- Permettre de favoriser l'innovation et la recherche.

150 Conditions générales d'utilisation de la plateforme France Connect pour les fournisseurs de service.
151 Arrêté du 13 mai 2019 modifiant l'arrêté du 10 août 2016 autorisant la création d'un traitement automatisé de données à caractère personnel dénommé « DocVérif ».

1.2. Redonner le contrôle aux citoyens à travers la maîtrise des données de l'identité numérique

Le principe d'autodétermination informationnelle (qui englobe la maîtrise des données par les citoyens) et le rapport savoir-pouvoir que ce principe sous-tend est au coeur du déploiement de l'identité numérique.

Le droit à l'autodétermination informationnelle[152] a été décrit par le rapport Ambition numérique du Conseil[153], et consacré par la nouvelle rédaction la loi informatique et liberté en 2019. Ce droit, au prisme de l'identité numérique, permet de redonner le contrôle aux citoyens en actant les contours et les conséquences de l'utilisation de leur identité numérique dans une ambition de faire émerger une citoyenneté numérique. En 2015, « *Le Conseil consid [érait] que le principe d'autodétermination informationnelle, opposable aux acteurs privés, dev [ait] s'appliquer de manière différenciée aux administrations.* » [154]

Une des suites du droit à l'autodétermination informationnelle[155] appliqué à l'identité numérique pourrait se trouver dans des solutions de self sovereign identity[156]. Malgré l'intérêt que le Conseil porte à ce type de solutions technologiques, qui ont été promues par plusieurs experts en raison de leur capacité à laisser le citoyen détenteur et gestionnaire de son identité, il n'est pas en mesure de recommander ces solutions qui ne semblent pas correspondre aux besoins et aux niveaux de maîtrise de l'ensemble de la population. Ces technologies pourront être envisagées dans un second temps, à la suite d'une première phase de déploiement, de pédagogie et de communication autour de l'identité numérique.

1.2.1. La représentation démocratique comme socle de la citoyenneté : définir un véhicule législatif propre à l'identité numérique

Différents échanges avec des experts ont mis en avant un manque de consultation démocratique[157] sur le développement de l'identité numérique. Les experts se sont questionnés sur les formes légales qui ont supporté le développement des différents systèmes d'identité numérique. En effet, jusqu'à présent les différentes solutions supportant l'identité numérique ont été inscrites au journal officiel (JO) à travers des décrets, à l'instar du fédérateur d'identités France Connect ou de la solution Alicem.

Cette problématique a été l'objet des questions de la mission parlementaire sur l'identité numérique lors de l'audition du secrétaire d'État chargé du Numérique. Selon l'analyse des services juridiques de l'administration, un texte de loi spécifique n'est pas nécessaire pour

152 Voir l'explication du droit dans l'article de la CNIL sur les changements du à la loi république numérique.
Sur le site de la CNIL.
Voir la Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (1).
153 Ambition numérique, op. cit., p.50.
154 ibid, p.130.
155 op. cit.
156 Dans le principe de Self Sovereign Identity, l'utilisateur, grâce aux technologies décentralisées de blockchain, conserve la propriété des données qui servent à prouver son identité de même qu'il décide du niveau de partage et des accès aux informations le concernant.
157 Le Conseil salue les travaux de la mission d'information parlementaire sur l'identité numérique qui a débuté en novembre 2019, et qui répond en partie aux besoins de consultation démocratique. Cette mission est présidée par Marietta Karamanli, assisté des co-rapporteurs Christine Hennion et M. Jean-Michel Mis (nommé pour remplacer Paola Forteza depuis mars 2020).

déployer les identités numériques répondants au règlement eIDAS. Pour autant, le secrétaire d'État a mis en avant qu'un débat parlementaire n'était pas exclu.[158]

Pour le Conseil, un texte de loi spécifique serait bénéfique pour définir les grands principes et la gouvernance de l'identité numérique. Il redonnerait une forme de contrôle aux citoyens en mettant les parlementaires au centre du processus de discussion et de décision. Il permettrait aussi de rappeler l'encadrement de la transmission des données (déjà présente dans le décret France Connect et le règlement d'exécution eIDAS 2015/1502) ainsi que de leur utilisation, d'établir le schéma de gouvernance de l'identité numérique, mais aussi de décrire son périmètre et ses finalités[159]. La protection des citoyens serait de fait mieux assurée tout en permettant l'innovation. Le Conseil national du numérique encourage la mission parlementaire sur l'identité numérique à proposer un projet de loi allant dans ce sens.

Recommandation n°21

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.).

1.2.2. Confiance par et pour les citoyens : instance de contrôle et outils de contestation

Dans sa prise de parole devant la mission parlementaire, Pierre-Louis Rolle, directeur de la mission Société Numérique[160] expliquait que la crainte autour de l'exploitation des données à caractère personnel est devenue un frein à l'utilisation d'internet par les citoyens ces trois dernières années. Ce constat est confirmé par les enquêtes Baromètre numérique de l'Arcep[161], et l'étude CAPUNI du groupe Marsouin[162] qui montrent, entre autres, que cette crainte pousse un certain nombre d'individus à limiter leur accès à internet, ce qui impacte aussi l'accès aux services publics en raison de leur dématérialisation. C'est en partie pour répondre à ces problématiques que le Conseil estime qu'il faut renforcer les droits des citoyens à travers trois mesures : la traçabilité des actions et des accès, la prise en compte du droit à l'erreur et le soutien aux acteurs garants des libertés.

1.2.2.1. La traçabilité, le droit de regard et la pénalisation des mésusages sont des vecteurs de confiance pour les citoyens

Lors des consultations, les citoyens ont été interrogés sur leurs craintes concernant le déploiement de l'identité numérique, associé au

158 Mission d'information sur l'identité numérique : audition de M. Cédric O, secrétaire d'État chargé du numérique, minute : 01 : 02 : 32. [Retranscrit par nos soins].
159 C'est l'absence de périmètre de l'identité qui avait entraîné le Conseil constitutionnel à supprimer l'article 3 de la loi de 2012, déclarant la loi en non conformité partielle. décision n°2012-652 DC du 22 mars 2012.
160 Mission parlementaire sur l'identité numérique, minute 00 : 19 : 50.
161 Baromètre du numérique 2012, 18ème édition, Arcep, Conseil général de l'Économie, Mission société numérique.
162 Enquête Individus 2019, CAPUNI, Observatoire Omni du groupe Marsouin.

principe du « dites-le-nous une fois ». Ceux-ci mettent en avant des peurs de mésusages de leurs données par des personnels autorisés ou plus largement par le gouvernement. Ces craintes font écho à la problématique de la perte de confiance des citoyens dans leurs institutions. Néanmoins, face aux risques d'usurpation d'identité ou de mésusages, c'est vers l'État que les citoyens se retourneront pour assurer la protection et la garantie de leur identité pivot.

En Estonie, les informations relatives aux individus sont systématiquement liées à leur identité numérique et enregistrées par l'administration concernée, sous le pilotage du RIA (Riigi Infosüsteemi Amet). Les employés de chaque administration ont des permissions limitées dans leurs accès aux informations des citoyens ; ils n'ont accès qu'aux informations qui leur sont nécessaires pour effectuer leur mission d'intérêt général ; et les accès à ces informations sont suivis et enregistrés afin qu'ils puissent être contrôlés par l'administration ainsi que, dans une version limitée[163], par le citoyen. En complément de cette transparence et pour limiter les cas de mésusages (comme par exemple les usages illicites ou sans consentement de l'utilisateur), le détournement des permissions par les personnels autorisés est fortement pénalisé[164]. Les conséquences sont des pertes de permission, de droit d'exercer pour les professions réglementées et des amendes de plusieurs dizaines de milliers d'euros.

En parallèle, et de sorte à répondre aux attentes de transparence, une plateforme conférant à chaque citoyen un droit de regard en temps-réel sur les traitements dont il est l'objet pourrait être mise en place.

Recommandation n°22

Instaurer un cadre réglementaire qui permette notamment une pénalisation rapide des mésusages, en particulier des personnes en capacité d'abuser de leurs prérogatives professionnelles. Pour dissuader toutes formes de mésusages, le Conseil recommande que des sanctions fortes (amendes, pénalisation, etc.) soient renforcées et précisées.

Recommandation n°23

S'appuyer sur les recommandations du Conseil de 2015 soit :

- « *Permettre à chaque usager de visualiser les échanges de données entre les administrations pour la délivrance d'un service, ainsi que leur durée de conservation ;*
- *Prévoir le consentement de l'usager par défaut pour l'échange d'informations personnelles entre les administrations, sous réserve des cas d'échanges sans autorisation prévus par la loi ou par décret.* »[165]

163 Le citoyen peut suivre l'ensemble des procédures en cours dans les différentes administrations, ainsi que : quelle administration a accédé à quelle donnée, et les demandes d'accès entre administrations.
164 2007, Estonia Personal data act.
165 Ambition numérique, op.cit, p.128.

Enfin, la transparence et l'audit a posteriori ne sont pas les uniques éléments nécessaires à l'émergence de la citoyenneté numérique : le consentement est un prérequis. Dans le cadre de l'ouverture de France Connect à des services fournis par des acteurs privés, le Conseil rappelle qu'aucune transmission automatique de documents à des acteurs privés ne doit être effectuée sans le consentement explicite de l'usager. Une autorisation implicite, via les conditions générales d'utilisation, ne saurait être suffisante[166].

1.2.2.2. Utiliser l'identité numérique sans crainte en renforçant les droits des citoyens : appliquer le droit à l'erreur et une réversibilité des actions

La loi n° 2018-727 du 10 août 2018 pour un État au service d'une société de confiance[167] dite « ESSOC », acte la nécessité d'instaurer une confiance de l'administration envers les citoyens. Elle s'inscrit sur deux piliers que sont le droit à l'erreur et l'allégement des démarches ainsi que la facilitation des parcours pour les usagers. « *Le droit à l'erreur repose sur un a priori de bonne foi : la charge de la preuve est inversée, il reviendra à l'administration de démontrer la mauvaise foi de l'usager. C'est la possibilité pour chaque Français de se tromper dans ses déclarations à l'administration sans risquer une sanction dès le premier manquement. Chacun doit pouvoir rectifier–spontanément ou au cours d'un contrôle– lorsque son erreur est commise de bonne foi. Le droit à l'erreur n'est toutefois pas une licence à l'erreur : il ne s'applique ni aux récidivistes ni aux fraudeurs. Le droit à l'erreur n'est pas non plus un droit au retard : les retards ou omissions de déclaration dans les délais prescrits n'entrent pas dans son champ d'application.* » [168]. Le second pilier, la simplification met en avant que « *si des erreurs de bonne foi interviennent, c'est souvent parce que notre réglementation et nos procédures sont complexes. Si le « droit à l'erreur » atténue les effets, le projet de loi pour un État au service d'une société de confiance tend aussi à traiter les causes : complexité, manque de lisibilité et surabondance de la norme.* » [169]

Ces principes répondent aux réticences d'utilisation de l'identité numérique que les citoyens ont pu signaler lors des consultations organisées par le Conseil. En effet, beaucoup mettaient en avant une peur que l'identité numérique–associée à la dématérialisation, l'automatisation des actions- et l'interconnexion des administrations– entraîne une perte de leurs droits en cas d'erreurs de leur part ou de l'administration sur l'une des procédures.

Aujourd'hui plusieurs chantiers ont été lancés sur l'expérimentation de la loi ESSOC. Le Conseil national du numérique ne peut que saluer cette décision législative. Il estime qu'il est nécessaire que les principes de la loi ESSOC soient efficients au moment du déploiement des identités numériques dérivées de la CNIe.

166 Idem.
167 Loi n° 2018-727 du 10 août 2018 pour un État au service d'une société de confiance (1).
168 Le portail de l'Économie, des Finances, de l'Action et des Comptes publics, « *Droit à l'erreur : loi pour un État au service d'une société de confiance (ESSOC)* », 30 août 2018.
169 idem.

1.2.2.3. S'appuyer sur un acteur déjà reconnu : la CNIL

Plusieurs acteurs sont en charge de la protection des droits des citoyens. Concernant les questions numériques, la CNIL[170] est un acteur incontournable puisqu'une de ses missions est « d'informer et de protéger les droits » [171]. De par cette mission elle possède un pouvoir de contrôle et de sanction qu'il faudra articuler avec les actions de la nouvelle CSGIN comme cela a été présenté plus haut.

Au regard des différentes recommandations sur l'identité numérique formulées par le Conseil qui convoquent les missions de la Commission, il paraît nécessaire que ses ressources soient augmentées. En effet, sans étendre le champ de leur mission, le déploiement de l'identité numérique augmentera le nombre de cas (notamment avec la multiplication des fournisseurs de services et la création de nouveaux fournisseurs d'identité) et donc la quantité de ressources nécessaires pour les traiter.

170 Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
171 Site web de la CNIL, « Mission (1) : Informer, protéger les droits ».

2. LA SÉCURITÉ : UNE EXIGENCE POUR LA SOUVERAINETÉ

Architecture et sécurité du système pour une identité numérique respectueuse des libertés des citoyennes

Pour les citoyens comme pour les experts[172], l'identité numérique soulève de nombreuses questions en termes de sécurité, que ce soit au sujet du système et de l'architecture qui le supporte, des données à caractère personnel, des technologies, mais aussi de la perception qu'ont les individus du respect de la sécurité de leurs informations personnelles. Ces inquiétudes ont été mises en avant à de nombreuses reprises dans les consultations organisées par le Conseil national du numérique.

Lorsque les citoyens sont interrogés sur les avantages et les inconvénients des dispositifs d'identité numérique, tous pointent les risques de failles de sécurité à travers des termes comme : « le piratage des systèmes », « la fuite de données », ou « les portes dérobées » (*backdoors* en anglais) qui entraîneraient des failles de sécurité. Ces termes–souvent utilisé dans les médias–sont mentionnés à plusieurs reprises lors des consultations. Les citoyens font fréquemment référence à des scandales de fuite de données qui ont pu avoir lieu[173]. Pour beaucoup, l'État ne serait pas en capacité de mettre en place une architecture répondant à des principes de sécurité élevée et, plus particulièrement, de mettre l'ensemble de son administration à un niveau de sécurité qu'ils jugent acceptable. C'est la capacité de l'État à répondre aux besoins de sécurité soulevés par l'identité numérique qui est interrogée.

Selon la définition de la souveraineté donnée en introduction de ce rapport, la sécurité est l'un des atouts pour son maintien et sa maîtrise. En s'appuyant sur des savoirs-faire partagés et des normes définies multilatéralement, les États réaffirment leurs prérogatives de souveraineté tant en termes d'identité numérique (choix des technologies répondant à leur besoin de sécurité, rappel de leur position face à des géants de numériques, etc.) qu'en termes de défense (protection des systèmes et des citoyens contre les cyberattaques), tout en mettant en avant leur pouvoir normatif sur une thématique transversale.

Pour le Conseil national du numérique, le Gouvernement doit assurer la sécurité des citoyens au regard de l'identité numérique tout en maintenant sa souveraineté : au regard des normes et des standards internationaux et en faisant valoir ses valeurs dans les échanges européens (1), mais aussi à travers ses choix technologiques tout en maintenant un pôle de connaissances (2) ainsi que des positions et des technologies déjà éprouvées (3).

172 cf. Introduction de ce rapport.
173 L'affaire Cambridge analytica a notamment été mentionnée pendant les consultations.

2.1. De la norme imposée à la co-construction européenne pour la sécurité de tous

2.1.1. Les normes et standards internationaux

« *L'État se trouve désormais de plus en plus concurrencé par d'autres entités productrices de normativités.* » [174] Il est donc légitime de se questionner sur la place laissée à la souveraineté en termes de sécurité face à l'élaboration de normes internationales. À titre d'exemples non exhaustifs, depuis plusieurs décennies, différents groupements internationaux de la filière du transport ont eu des impacts sur l'identité numérique (et sa sécurité) dans le but d'optimiser la sécurité de leurs services[175].

Par exemple, en juin 2016, l'Organisation de l'aviation civile internationale (OACI, agence spécialisée de l'ONU) a débuté des travaux, pilotés par l'Australie, portant sur les certificats de voyage numériques ainsi qu'une réflexion pour faire évoluer les normes du passeport électronique ; l'International Air Transport Association (IATA) travaille depuis 2017 au projet OneID afin de « *diriger l'industrie dans ses efforts pour assurer aux passagers une expérience sûre, sans heurt et efficiente d'un bout à l'autre. Le projet OneID fait appel aux technologies de gestion de l'identité et de reconnaissance biométrique pour simplifier le trajet du passager.* » [176]

Cet intérêt est aussi porté par les instituts de normalisation internationaux comme nationaux depuis de nombreuses années. Le groupe ISO/IEC JTC 1/SC 17[177], portant sur les cartes et dispositifs de sécurité pour l'identification des personnes[178] a publié 107 normes depuis 1995179. Il est en cours de réflexion sur des thématiques comme les permis de conduire mobiles ou la biométrie[180]. L'institut américain de standardisation (NIST) s'intéresse aussi à l'identité numérique et a publié en juin 2017 ses « Digital Identity Guidelines » [181].

La normalisation de l'identité numérique se fait aussi à travers des groupements d'intérêt pour des protocoles de sécurité ou des architectures spécifiques comme c'est le cas pour l'alliance FIDO[182] (fast IDentity Online portée par des industriels) ou le W3C (qui poursuit des réflexions sur l'identifiant décentralisé).

Ces différentes normes promues par les organisations internationales, des groupes d'industriels, des groupements scientifiques et des organisations non-gouvernementales servent de références dans les textes communautaires traitant de l'identité numérique. En effet, le règlement d'exécution de la directive eIDAS note que « *les spécifications et les procédures établies dans le présent acte d'exécution se fondent notamment sur la norme internationale ISO/CEI 29115, qui est la principale*

174 Voir TRUDEL, Pierre., ibid.
175 Parfois par le biais de la normalisation des informations présents dans les titres électroniques.
176 IATA, Communiqué n°52, septembre 2019.
177 La France y est représentée par l'AFNOR.
178 Documents d'identification et documents connexes, les cartes, et les dispositifs de sécurité et les jetons ainsi que l'interface associée à leur utilisation dans les applications intersectorielles et les échanges internationaux
179 Normes du ISO/IEC JTC 1/SC 17, Cartes et dispositifs de sécurité pour l'identification des personnes..
180 idem.
181 NIST, Digital identity Guide Lines, Juin 2017.
182 Site web de l'alliance FIDO.

norme internationale disponible dans le domaine des niveaux de garantie pour les moyens d'identification électronique. » [183]

En notant que la plupart de ces organisations sont transnationales, localisées hors de l'espace de l'Union européenne, certains industriels auditionnés[184] et experts consultés se sont questionnés sur l'impact que pourrait avoir la délégation de la normalisation technique sur la souveraineté technologique en termes d'identité numérique.

Le Conseil national du numérique souhaite que les réflexions et l'intelligence collective issues des échanges multipartites, internationaux soient valorisées en laissant une place stratégique aux scientifiques et experts techniques des sujets.

Recommandation n°24

Renforcer la représentation française dans les instances de normalisation européennes et internationales. Celles-ci constituent un lieu stratégique d'influence et de création de normes autour de l'identité numérique. Il s'agit d'un rôle essentiel du ministère des Affaires Étrangères de suivre ces thématiques et d'allouer les ressources nécessaires pour effectuer un travail de veille et d'influence avisé, avec l'appui des autres ministères concernés.

Recommandation n°25

S'appuyer sur des standards qui proviennent d'instituts de normalisation européens (ETSI, CEN) reconnus nationalement. En effet, « *dans le cadre du Mandat M/460, ayant pour objectif de fournir une réponse coordonnée sur le sujet du déploiement d'un marché européen digital unique, l'ETSI (European Telecommunications Standards Institute) et le CEN (Comité Européen de Normalisation) se sont vus confier la mission d'élaborer des normes relatives aux services de confiance prévus par eIDAS.* » [185] Dans un second temps, la certification devrait être effectuée par des organismes évoluant avec les mêmes règles de droit que les entreprises en quête de certification et que les organismes promoteurs de normes.[186]

La souveraineté en matière de sécurité doit être exprimée au niveau européen pour pouvoir peser dans les sphères d'échange internationales. L'Europe a déjà prouvé sa capacité à édicter des normes en matière de numérique, notamment avec le règlement général sur la protection des données. Différentes auditions ont mis en lumière que le règlement eIDAS était lui aussi un instrument de référence, intéressant des pays hors de l'Union Européenne participant aux groupes de travail qui leur sont ouverts, cité par d'autres gouvernements et pris comme référence par des industriels dans leur développement vers des marchés internationaux.

183 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) no 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.
184 Audition réalisée par le conseil et consultation expert organisé à Paris en décembre 2019.
185 Site de l'ANSSI, article sur le règlement eIDAS.
186 Pour plus de précision voir la sous-partie 2.2. cette partie sur la sécurité, traitant de l'audit.

2.1.2. L'Europe comme vecteur de norme : le poids du règlement eIDAS

Le règlement eIDAS[187] a été un facilitateur dans la diffusion de l'identité numérique dans l'Union Européenne. Tout en étant une avancée pour la souveraineté européenne (cf. supra), il soulève aussi pour la France un certain nombre d'enjeux de sécurité à travers le principe de reconnaissance mutuelle des schémas d'identification électronique et l'interopérabilité des services de confiance. Le Conseil national du numérique valide ces deux principes et souhaite proposer de les compléter selon quatre axes.

2.1.2.1. La révision du règlement eIDAS : l'occasion d'apporter des améliorations

Avant le 1er juillet 2020, la Commission doit procéder à un réexamen de l'application du règlement eIDAS et ainsi rendre compte au Parlement européen et au Conseil, via un rapport technique. Pour ce faire, la Commission aura recours à une consultation publique en ligne ouverte à tous ainsi qu'à une étude ciblée pilotée par quatre cabinets de conseil ayant pour mission d'auditionner les parties prenantes dans les États membres.

L'ANSSI, est chargée d'évaluer la bonne atteinte des niveaux de garantie revendiqués par les schémas d'identification électronique notifiés par la France et participe aux examens par les pairs qui visent à évaluer les schémas d'identification (et leur niveau de garantie) notifiés par les États membres. Ces examens par les pairs sont un processus d'évaluation collégial, d'une durée de trois mois, qui repose sur la participation volontaire des États membres. L'examen par les pairs se base notamment sur un corpus documentaire décrivant les schémas d'identification que l'État souhaite notifier. La décision d'exécution 2015/1984 du 3 novembre 2015 définit les circonstances, les formats et les procédures relatives à la procédure de notification. Toutefois, les détails du corpus documentaire fourni par les États membres, ainsi que la publication des informations entourant la notification des schémas d'identification, sont laissés à la libre appréciation de l'État membre comme le montre ce commentaire par Marie Eichholtzer[188] collaboratrice de la Commission travaillant sur le déploiement des solutions d'identité numérique : « *Les États membres décident des documents à rendre publics ou non en ce qui concerne leur notification. Dans le cas de l'eID Belge, seul le formulaire de pré notification a été rendu public* » [189] [190].

Une audition avec les personnes en charge de l'application du règlement eIDAS[191] au sein de l'ANSSI a mis en avant les problèmes que pouvaient poser le fait de se reposer sur le volontarisme des États membres ainsi que la disparité des informations produites[192] sur la qualité de l'examen par les pairs qui se doit pourtant d'établir un avis sur le niveau de garantie atteint par le schéma d'identification conformément aux exigences du règlement eIDAS.

187 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 et abrogeant la directive 1999/93/CE.
188 Voir le profil utilisateur de Marie Eichholtzer.
189 Opinion No.7/2018 of the Cooperation Network on the Belgian eID scheme, commentaire du 18 juin 2019.
190 « *Member States are deciding which document to make public or not regarding their notification. In the case of Belgium eID, only the pre-notification form has been made public* ».
191 Audition réalisée par le Conseil dans le cadre de ces travaux sur l'identité numérique.
192 Une lecture des diverses opinion de réseaux de coopération permettent de s'apercevoir de la disparité des sources sur lesquelles s'appuient ces opinions. Opinion of the Cooperation Network..

Recommandation n°26

Clarifier les exigences du règlement eIDAS pour les niveaux de garantie substantiel et élevé.

- Standardiser le processus d'examen par les pairs notamment en terme de référentiel documentaire et de méthodologie, et clarifier son objet et son périmètre ;
- Définir un corpus documentaire reprenant les informations qui doivent être automatiquement communiquées par les États membres sur leurs schémas d'identification électronique

En cela, le Conseil rejoint les recommandations portées par l'ANSSI autour de la révision du règlement eIDAS pour unifier les pratiques au sein des États membres en termes de sécurité et ainsi promouvoir les mécanismes de reconnaissance mutuelle et d'interopérabilité des schémas d'identification électronique. Il faut noter qu'il ne s'agit pas pour l'Agence de la priorité absolue de la révision du règlement qui estime qu'il faut commencer par la clarification des exigences mêmes du règlement pour les niveaux de garantie substantiel et élevé.

De plus, il existe aujourd'hui un vase communiquant entre les services de confiance[193] et l'identification électronique. Néanmoins, le règlement d'exécution (UE) 2015/1502 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique[194] ne spécifie pas de cadre technique pour les mécanismes recourant à l'identification à distance qui se multiplient avec l'augmentation des moyens d'identification électronique.

Recommandation n°27

Préciser dans le règlement eIDAS les critères minimaux relatifs à l'identification à distance. Une harmonisation et des modalités d'évaluation de la fiabilité des méthodes d'identification à distance (par exemple, le nombre de défis à effectuer par l'utilisateur dans le cadre de la reconnaissance faciale, ou encore une standardisation du taux de faux positif faux négatifs impactant le pourcentage d'identification) seraient bienvenues afin d'harmoniser les pratiques mises en œuvre dans les États membres.

193 La deuxième partie du règlement eIDAS traite des services de confiance. Ils sont définis comme des services électroniques normalement fournis contre rémunération qui consistent : a) en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services ; b) en la création, en la vérification et en la validation de certificats pour l'authentification de site internet ; ou c) en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services.
194 Règlement d'exécution (UE) 2015/1502 de la Commission, op.cit.

2.1.2.2. Le nœud d'interopérabilité européen proposé par le règlement eIDAS : des éléments à éclaircir

Le nœud d'interopérabilité prévu par le règlement eIDAS[195] est un point de connexion qui permet à l'infrastructure d'identification électronique nationale d'un État membre de fonctionner avec les infrastructures d'identifications électroniques nationales d'autres États membres. C'est donc un levier pour la libre circulation dans l'espace européen qui donne à la revue par les pairs une importance toute particulière. Le règlement d'exécution 2015/1501 définit précisément les informations[196] qui circulent à travers ce nœud entre les fournisseurs d'identité et les fournisseurs de services européens ainsi que le type d'information qui sont stockées par les opérateurs du nœud. En France, ce nœud doit être rattaché à France Connect et la DINUM sera l'opérateur de ce nœud.[197]

La difficulté à obtenir des précisions sur le noeud eIDAS interroge le Conseil à plusieurs niveaux. Il estime qu'une communication doit être faite sur ce sujet pour deux raisons : tout d'abord pour permettre aux citoyens de faire des choix éclairés, notamment dans l'hypothèse où une solution d'identité numérique privée, notifiée par un autre État membre, serait disponible sur le territoire ; ainsi que pour améliorer la transparence, partager la gouvernance et permettre la mobilisation de la société civile.

Recommandation n°28

Publier davantage d'informations concernant la mise en place du nœud eIDAS français. De plus, il paraît nécessaire que celui-ci ne soit pas supporté uniquement par le service en charge de France Connect au sein de la DINUM mais que des ressources spécifiques y soient dédiées. Enfin, il doit être construit en étroite collaboration avec l'ANSSI et la CNIL.

Enfin, le Conseil précise que même s'il pourrait être judicieux d'engager une réflexion sur l'encadrement des informations d'identité qui seront en mesure de transiter par le nœud dans l'hypothèse où un fournisseur d'identité privé extra européen serait notifié à Commission, il paraît difficile d'imposer des restrictions supplémentaires au niveau national. En effet si un fournisseur d'identité extra européen est notifié à la Commission, il le sera nécessairement par un État membre qui en prendra la responsabilité, cela passera par un examen par les pairs, et in fine les mêmes obligations de reconnaissance mutuelle s'appliqueront. Dans ces conditions, c'est la révision du règlement qui paraît prioritaire.

195 Règlement d›exécution (UE) 2015/1501 de la Commission du 8 septembre 2015 sur le cadre d›interopérabilité visé à l›article 12, paragraphe 8, du règlement (UE) no 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.
196 Ibid, p. 6
197 Site web, Modernisation.gouv, État plateforme. Juin 2015, « France Connect eIDAS, vers une identité numérique européenne ».

2.1.2.3. La sécurité des schémas d'identification électronique : ne pas oublier le niveau substantiel

En s'intéressant aux dix-sept solutions qui ont été notifiées (ou pré-notifiées), on constate que douze États membres proposent uniquement des solutions de garantie élevée et que seul l'un d'entre eux propose les trois niveaux de garantie[198]. En France, selon les informations publiquement disponibles l'État développe une solution d'identité qui vise le niveau de garantie élevé[199] (en cours de notification par l'ANSSI) à travers Alicem. Le développement massif des solutions de niveau de garantie élevé peut être expliqué par plusieurs mouvements concomitants : un premier mouvement lié à l'idée de « qui peut le plus peut le moins » [200], un second lié au fait que, beaucoup d'États se sont dotés, avant le règlement eIDAS, de cartes d'identité électronique, pour des coûts souvent importants et une ergonomie souvent limitée. Ils ne peuvent décemment pas afficher à leur population qu'une telle solution n'atteint qu'un niveau de garantie substantiel. Enfin un dernier mouvement serait associé au risque de voir arriver sur le territoire national une solution extra européenne privée qui pourrait répondre à des usages de niveau de garantie élevé (comme par exemple la délivrance des titres d'identité à distance).

Néanmoins, pour répondre aux exigences du niveau de garantie élevé, beaucoup de schémas d'identification s'appuient sur des technologies biométriques, favorisant le développement de ces technologies qui pour certaines sont peu accessibles et peu inclusives. De plus, le manque d'exigences précises permettant de distinguer le niveau élevé du niveau substantiel des moyens d'identification[201], ainsi que le fait que le niveau de garantie de chaque usage (créer un compte, souscrire une assurance, payer une amende…) ne soit pas harmonisé interroge.

Recommandation n°29

Revaloriser le niveau de garantie substantiel grâce à une solution d'identité numérique publique correspondante (après avoir déterminé les cas d'usage type[202] pour ce niveau. Cf. recommandation n°30)

De plus il serait pertinent d'inciter les États ayant déjà une solution de niveau élevé à faire émerger une solution de niveau substantiel. La France pourrait dès à présent s'engager dans cette voie.

198 Overview of pre-notified and notified eID schemes, site web de l'Union Européenne.
199 « *Développer une première solution d'identité numérique visant le niveau de garantie «élevé» au sens du règlement européen sur l'identification électronique et les services de confiance pour les transactions électroniques, dit règlement «eIDAS»*. Site du ministère de l'Intérieur. « *Alicem, la première solution d'identité numérique régalienne sécurisée* » .
200 De manière plus générale, très peu d'Etats souhaitent afficher que les solutions mises à disposition de la population ne répondent pas aux exigences de sécurité les plus élevées.
201 Les « *caractéristiques et conception des moyens d'identification électronique* » sont définies en quelques lignes à la page quinze du règlement d'exécution. op.cit.
202 Une étude commandée par le programme interministériel et menée par la DITP, en 2019, a permis de circonscrire un certain nombre de cas d'usage pour l'identité numérique régalienne. C'est en s'appuyant sur le travail effectué que le Conseil estime qu'il est nécessaire de proposer une typologie des cas d'usage en fonction des niveaux de garantie attendus.

2.1.2.4. La mise en cohérence des actes et des démarches nationales avec les standards du règlement

Dans la continuité de la recommandation précédente, il paraît nécessaire de travailler sur une notion de proportionnalité entre les usages et les niveaux de garantie des schémas d'identification électronique.

Recommandation n°30

Définir, sous le pilotage des administrations concernées, les niveaux de garantie nécessaires pour chaque service en ligne et créer une doctrine à destination des administrations pour leur permettre d'établir aisément le niveau de garantie des nouveaux services publics.

Le Conseil soutient la proposition n°2 du rapport IGF, IGA et CGE de juillet 2018 qui recommandait : « *Sous le pilotage de la DINUM et avec l'appui de l'ANSSI, de recenser toutes les démarches publiques nécessitant une identification et une authentification et définir le niveau de garantie eIDAS attendu pour les démarches en ligne qui dépassent le niveau faible. Porter une attention particulière au domaine de la santé qui pourrait nécessiter un niveau de garantie important pour les usages récurrents.* » [203] [204]

2.2. La sécurité de tous se retrouve dans la maîtrise de la souveraineté technologique

2.2.1. Maîtrise des compétences techniques : internalisation et soutien aux universités et aux industriels

La maîtrise de la souveraineté qui a été évoquée en introduction se traduit aussi au niveau de l'État par la nécessité d'une internalisation des compétences ainsi qu'un soutien à la recherche et aux industriels. Le règlement d'exécution eIDAS 2015/1502[205] précise les exigences de sécurité relatives aux installations, au personnel et aux sous-traitants. Parmi ces exigences, la notion de maîtrise des savoir-faire est mentionnée dans ces termes :

1. « *Il existe des procédures garantissant que le personnel et les sous-traitants soient suffisamment formés, qualifiés et expérimentés eu égard aux compétences nécessaires pour exécuter les tâches qui leur sont confiées.*
2. *Le personnel et les sous-traitants doivent être en nombre suffisant pour faire fonctionner et gérer de manière adéquate le service conformément à ses politiques et procédures.*
3. *Les installations utilisées pour fournir le service sont surveillées en permanence et protégées contre les dommages causés par des événements environnementaux, l'accès non autorisé et d'autres facteurs susceptibles d'avoir une incidence sur la sécurité du service.*

203 Rapport IGF, IGA, CGE, Juillet 2018, Modèles économiques de l'identité numérique, Tome I.
204 Le programme porte à l'attention du Conseil que cette recommandation a donné lieu à l'étude de la DITP susmentionnée permettant de définir les cas d'usage.
205 op. cit.

4. *Les installations utilisées pour fournir le service garantissent que l'accès aux zones de conservation ou de traitement d'informations personnelles, cryptographiques ou autres informations sensibles est limité au personnel ou aux sous-traitants autorisés*».

Néanmoins, dans cette description, l'État revêt uniquement un rôle de surveillance et n'a pas d'obligation de maîtrise en interne des compétences qu'il délègue et sous-traite. Dans les schémas d'identité électronique nationaux, la DINUM sous-traite une partie du développement de la plateforme France Connect, pour l'agrégation des fédérateurs d'identité et le déploiement chez certains fournisseurs de services.

De la sorte, plusieurs auditions ont rapporté que le manque de compétences internes et le recours à des prestataires extérieurs faisait peser un risque sur le maintien en condition opérationnelle et de sécurité de France Connect. Les personnes auditionnées ont notamment appuyé sur les risques liés au changement de prestataires lors des appels d'offre de marchés publics.

Plusieurs actions[206] au cours de ces derniers mois ont rappelé l'importance de la valorisation des compétences nationales en matière d'innovation technologique, que ce soit dans les milieux de la recherche ou économique. Cette technique de valorisation par le soutien à la recherche a été éprouvée aux États-Unis avec la mise en place dans les années 80 du Bayh-Dole Act, permettant de favoriser grâce à des investissements publics et de la recherche, le maintien de la souveraineté dans les secteurs innovants. En France, c'est ce que propose le contrat Ambition 2023 de l'INRIA qui met en avant la nécessité de soutenir les politiques publiques liées à leur domaine d'expertise. Dans le monde économique, le Contrat stratégique de la filière cybersécurité place l'identité numérique de confiance au centre des préoccupations (cf. infra). Ces efforts partagés devraient permettre des échanges fructueux pour le secteur public.

Recommandation n°31

S'assurer que les compétences que l'État sollicite auprès de prestataires externes soient aussi maîtrisées en son sein afin de ne pas se retrouver dans des situations de dépendance (vis-à-vis des sous-traitants), de mise en risque de la pérennité du système et de perte de l'historique technique du système (erreurs, correction des erreurs, motifs et choix d'architecture, etc.).

Il est nécessaire que des compétences techniques soient recrutées massivement, avec un plan de carrière leur permettant de s'inscrire sur le long-terme dans l'administration, et que ces nouveaux agents soient intégrés à la mission identité numérique idoine de la DINUM.

206 Par exemple, les contrats stratégiques de filières cyber ou la signature du contrat d'ambition 2023 de l'INRIA .

2.2.2. Capacité d'évaluation des choix scientifiques et audit des systèmes

Comme évoqué dans le point 1.1. de ce chapitre, les normes sont souvent définies dans des sphères de discussions internationales. L'expertise technique et scientifique française sur l'identité numérique y est reconnue, notamment grâce à ses leaders industriels. Mais c'est aussi tout un écosystème d'entreprises de taille et de métiers divers qui évoluent autour des solutions d'identité numérique en proposant des solutions complètes ou simplement des briques logicielles.

La globalisation des normes pose la question de la certification des innovations technologiques ainsi que de la capacité d'audit en lien avec le développement des solutions d'identité numérique. La certification effectuée hors des frontières européennes doit être évaluée à l'aune du droit, des normes et des valeurs européennes. Il est important que la compétence de certification existe en Europe et/ou en France pour être sûr que celle-ci respecte nos valeurs (transparence, frugalité des données, non discrimination algorithmique, etc.).

À titre d'exemple, sur la certification de la biométrie, en particulier des briques de reconnaissance faciale, l'ANSSI ne teste aujourd'hui que la capacité de fraude de la technologie en la soumettant à des séries d'attaques. Elle n'effectue pas de travaux d'audit de l'algorithme sur des thématiques comme l'efficience de la technologie ou encore des questions de biais algorithmiques ou de base de données. En cas de nécessité, elle sous-traite cette tâche à d'autres. Ces problématiques ne rentrent pas dans les missions confiées à l'Agence, puisqu'il ne s'agit pas stricto sensu d'audit de la sécurité du système, mais de la recherche de potentiels biais du système.

Recommandation n°32

Consulter la communauté scientifique en appui de l'instance de gouvernance, concernant les choix de sécurité pour les technologies déployées par l'État notamment à travers :

- une analyse de la solution
- l'évaluation des risques et des coûts
- l'élaboration de l'architecture

Recommandation n°33

Attribuer des budgets pour la certification de technologie d'identité numérique, et/ou de briques technologiques liées à l'identité numérique. Il est nécessaire de répondre aussi aux besoins des entreprises de l'écosystème qui ne souhaitent pas proposer un schéma complet d'identité numérique mais seulement une brique technologique. De fait, des fonds définis précédemment permettraient d'alimenter une certification sous le principe de revue par les pairs, en lien avec les pôles d'excellence académique nationaux, l'ANSSI et la CSGIN.

2.2.3. Des règles de sécurité imposées aux fournisseurs d'identité privés de la plateforme France Connect

Comme mentionné dans la première partie du second chapitre, il est nécessaire d'imposer un cadre plus précis à destination des fournisseurs d'identité privés. Le décret d'application d'une délégation de service public permettrait de fixer le cadre à travers lequel ces fournisseurs opèrent et à rappeler les obligations de sécurité et d'auditabilité des systèmes (ex ante, ex post).

En janvier 2020, l'identité numérique de la Poste a été certifiée au niveau de garantie substantiel par l'ANSSI[207]. Cette certification est une avancée majeure pour l'identité numérique en France puisqu'il s'agissait, tant pour l'ANSSI que pour le fournisseur d'identité, de la première certification à un tel niveau de garantie. D'autres fournisseurs d'identité, privés et publics, sont actuellement en cours de certification au niveau substantiel, ce qui ne les empêche pas d'être intégrés à la plateforme France Connect depuis de nombreuses années.

Les conditions générales d'utilisation de la plateforme France Connect explicitent les règles d'usage et les niveaux de sécurité requis pour accéder à la plateforme. Comme cela a déjà été mentionné dans la recommandation n°19, le Conseil estime que ces documents doivent évoluer.

2.3. Des choix technologiques permettent de garantir la sécurité des citoyens

2.3.1. Silotage et chiffrement des informations : le Conseil n'est pas favorable à la centralisation des informations

La sécurité technologique a été grandement évoquée dans les consultations qui ont été menées par le Conseil national du numérique. Des exemples étrangers ainsi que des positions scientifiques ont fréquemment mis en avant qu'aucun système n'est en capacité d'être totalement sécurisé. Il est évident que des systèmes résilients sont à favoriser pour gérer les informations liées à l'identité numérique, notamment en partitionnant et en chiffrant l'information.

Pour répondre au principe du « dites-le nous une fois » [208], et à la nécessité d'un partage d'information entre administrations, les systèmes d'information doivent d'abord être pensés à travers leurs interfaces de programmation API[209], qui permettront ensuite des interconnexions entre les systèmes et le développement d'interfaces pour les utilisateurs. En aucun cas une centralisation des informations, liée à l'identité numérique des français et leur interaction avec un fournisseur de service, n'est souhaitable. Elle irait à l'encontre de choix historiques[210] et de la philosophie poursuivie par l'État depuis plusieurs années[211].

207 Site du ministère de l'Economie et des Finances, « *Le service d'identité numérique de La Poste est conforme au niveau de garantie « substantiel » de l'ANSSI* ».
208 Comme mentionné en introduction, ce principe vise à réduire la charge administrative et les redondances d'informations.
209 cf. l'exemple de l'Estonie, supra.
210 Comme par exemple la séparation du numéro fiscal et du numéro de sécurité social.
211 À l'image du modèle France Connect.

Concernant les données à caractères biométriques, le Conseil soutient la position de la CNIL[212] qui « *[…] a déjà eu l'occasion de reconnaître la légitimité et la proportionnalité de certains usages. Par exemple, et sans préjudice de ses appréciations concernant certaines modalités de mise en œuvre (s'agissant notamment du caractère libre du consentement recueilli pour le dispositif Alicem), elle a déjà admis, pour les dispositifs PARAFE ou Alicem, le recours à la reconnaissance faciale en cas d'exigence d'un niveau particulièrement élevé d'authentification des personnes et sous réserve de leur maîtrise sur leurs données biométriques.* » [213] Néanmoins, comme évoqué dans la partie 1.2. de ce chapitre, le Conseil estime qu'il est nécessaire en premier lieu qu'un cadre soit proposé pour définir les modalités et les moyens de la reconnaissance à distance, par exemple à travers un règlement d'exécution ; en second lieu, il est nécessaire que les niveaux de sécurité de chaque usage soient pensés pour éviter un usage trop fréquent du niveau élevé (cf. chapitre 2, partie II, 1.2.4.) et que des moyens d'authentification utilisant des données biométriques hautement sensibles se deviennent obligatoires pour l'ensemble des services.

Concernant le stockage des données biométriques[214], le Conseil réaffirme ses positions précédentes[215] et estime qu'il faut favoriser des solutions de stockage sur des supports chiffrés dont l'individu est en possession physique, comme ce sera le cas pour la CNIe.

Néanmoins, le stockage dans un base centrale existe depuis la création de la base TES concernant les passeports et les titres de séjour électronique. Depuis juin 2017[216], elle conserve aussi les empreintes digitales recueillies lors des procédures de délivrance des cartes nationales d'identité. Lors de son audition[217] devant la mission parlementaire sur l'identité numérique en février 2020, Jérôme Letier, directeur de l'ANTS, a fourni une description détaillée qui se veut rassurante sur le fonctionnement de la base des titres sécurisés.

Il y met en avant que le fichier TES est construit sur le principe du lien unidirectionnel : il est possible d'obtenir les informations biométriques d'une personne à partir de son état civil (nom, prénom…), mais il n'est pas possible d'obtenir les informations d'état civil à partir des données

212 CNIL, « *Reconnaissance faciale : Pour un débat à la hauteur des enjeux* », 15 novembre 2020.
213 Op. cit. page 9.
214 Les données biométriques sont définies à l'article 4 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
215 Avis du Conseil national du numérique sur le fichier TES, décembre 2016. op. cit.
216 « *Demande de carte d'identité : recueil et conservation des empreintes digitales* », 11 mai 2017, Site web du ministère de l'Intérieur.
217 Captation vidéo de l'audition de Jérôme Letier, directeur de l'ANTS devant la mission parlementaire sur l'identité numérique, 19 février 2020.
« *Le système d'information, TES, conserve en France ces informations [de délivrance de titre, ainsi que les informations contenues dans le titre notamment les données biométriques], dans des conditions d'usage, et même de non usage, qui sont extrêmement fortes, et qui a été audité il y a moins de trois ans par l'ANSSI et la DINUM et qui sont régulièrement vérifiées. La construction native de la base de données de TES fait que même si je souhaite de retrouver depuis une empreinte digitale [un individu], mon agence ne peut pas le faire. La base de donnée TES n'est pas un fichier de population. C'est une base de données des demandes de titres sécurisés. Donc si j'ai un numéro de titre ou un nom, je peux par des moyens sécurisés revenir à la demande, revenir à l'historique de la demande, revenir à la photo voire aboutir dans des conditions strictes à l'empreinte. C'est ce qui la distingue d'autres bases de la police judiciaire où le législateur a autorisé le ministère à revenir. Ce fichier TES, sert au recueil de la demande, qui est ensuite instruite dans un centre de recueil de décisions d'un agent préfectoral. Lorsque tout se passe bien il y a un badge qui part à l'imprimerie nationale côté passeport et côté CNI au ministère. Même processus de recueil pour les deux titres. Lorsque vous venez renouveler, l'autorité d'instruction à accès à l'historique pour voir s'il y a un droit d'accès.* »

biométriques.[218] À ce titre, le Conseil souhaite rappeler qu'il s'oppose au recoupement du fichier TES avec d'autres fichiers de police judiciaire et ou administrative. Il estime que l'ANSSI et la DINUM sont compétentes pour effectuer des audits de contrôle du fichier et que la CNIL[219] joue son rôle en contrôlant le respect des procédures de gestions des données personnelles et biométriques. Par ailleurs, notons que le système est en cours d'audition par l'ANSSI, pour la première fois depuis depuis trois ans.

Recommandation n°34

Effectuer de manière régulière et impromptue des audits et des contrôles (par l'ANSSI et la CNIL), du fichier TES et des usages qui en sont faits.

Néanmoins, le Conseil émet une forte inquiétude sur la taille de la base TES en raison du versement des informations (biométriques) issues des cartes nationales d'identité depuis mai 2017[220]. L'inquiétude du Conseil porte sur les usages futurs de l'identité numérique et les alternatives existantes. En effet, en raison des usages et des exigences de sécurité du règlement eIDAS, les identités numériques s'appuient de plus en plus sur les certificats d'authentification présents sur les titres (et une validation par DocVérif). Dans ces conditions, la base TES risque fortement de voir son nombre d'entrées augmenter drastiquement. Le Conseil exige qu'un engagement fort de l'État soit pris pour assurer que cette situation n'émerge pas. Il est nécessaire que :

- L'État, soutenu par la communauté scientifique et les industriels, développe une solution d'identité numérique décentralisée (a minima de niveau substantiel) qui ne s'appuierait pas sur un titre d'identité biométrique ;
- S'appuyer sur un véhicule législatif pour cadrer le périmètre de l'identité numérique, rappelant au passage le caractère facultatif des titres d'identité.

2.3.2. Grands principes de la sécurité des données des citoyens : conservation des données, frugalité des données et révocabilité

Il paraît nécessaire de s'appuyer sur les principes du RGPD pour répondre à la notion de sécurité entendue comme sécurité des individus et de leurs données. Néanmoins, le règlement d'exécution 2015/1502 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique rappelait l'importance d'utiliser des « *méthodes reconnues et de l'application des principes inscrits comme dans la norme ISO/CEI 20000*[221] **. ».**[222]

218 Audit du système « Titres électroniques sécurisés » par l'ANSSI et la DINSIC, 13 janvier 2017.
« *[Le système] permet d'associer à des données d'identification alphanumériques [ndla : nom, prénom, date et lieu de naissance] des données biométriques [ndla : p. ex. photo du visage, empreintes digitales], tout en empêchant que des données d'identification puissent réciproquement être associées à des données biométriques.* »
219 Site web de la CNIL, Rapport ANSSI / DINSIC Sur le fichier TES : une forte convergence avec l'avis de la CNIL, 23 janvier 2017.
220 Décret n° 2017-910 du 9 mai 2017 relatif aux conditions de recueil et de conservation des empreintes digitales des demandeurs de carte nationale d›identité.
221 Voir norme ISO/CEI 20000 sur le site web de ISO, dans sa version 2018.
222 op.cit.

2.3.2.1. Augmenter les ressources de la CNIL pour répondre aux problématiques de conservation des données

La conservation des données par l'administration est un enjeu majeur qui passe souvent au second plan des débats. Le débat sur la conservation des données de connexion de l'application Alicem entre le ministère de l'Intérieur et la CNIL est à ce titre particulièrement symbolique[223]. Conformément à ses missions, la CNIL doit être dotée de moyens suffisants pour répondre aux demandes qui vont être croissantes sur la conservation des données (cf. point 2.2.2. de la partie Gouvernance).

Le Conseil réitère les positions qu'il a tenu dans son avis sur le fichier TES[224]. De fait il estime qu'il faut être vigilant à ce que l'utilité de conserver des données biométriques pour atteindre les finalités avancées par les dispositifs d'identité numérique ainsi que le type de conservation (centralisée, non centralisée, etc.) fassent l'objet d'une analyse d'impact propre à chaque dispositif comme le veut la législation[225], même si ces dispositifs s'appuient sur des structures ou des schémas d'identification déjà existants.

2.3.2.2. Offrir des moyens de vérification d'information sans diffusions des données d'identité des citoyens à travers des solutions s'appuyant sur le zero knowledge proof

Afin que l'identité numérique réponde aux besoins des citoyens en termes de protection de la vie privée, et pour qu'elle puisse faire émerger des nouveaux usages respectueux, celle-ci doit pouvoir offrir des moyens de vérification d'information sans une diffusion complète des données d'identité des citoyens à travers des solutions s'appuyant sur le zero knowledge proof (ZKP, en français : preuve à divulgation nulle de connaissance) [226]. Il s'agit d'un prérequis pour répondre au principe de proportionnalité et à l'idée de frugalité des données.

En effet, le choix d'inclure ce type de technologies dans l'identité numérique permettrait d'améliorer le rapport de confiance qu'ont les individus à l'identité numérique répondant aux craintes de surveillance et au nécessaire besoin d'espace de vie privée. Combiné à une CNIe, l'utilisation du ZKP permettrait aux usagers d'accéder à certains services sans avoir à donner l'ensemble de leur identité qui est une information non pertinente pour l'usage visé. Par exemple, obtenir des tarif d'accès préférentiels aux équipements sportifs pour les habitants d'une collectivité locale sans avoir à révéler l'ensemble de leurs données d'identité.

223 Alors que la CNIL valide le temps de conservation des informations d'identité des individus conformément aux prérequis du règlement eIDAS, de sept ans, celle-ci s'interroge sur la conservation des traces d'accès à l'application ainsi que la conservation des historiques de transaction qu'elle estime manifestement disproportionnée. Voir la 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).
Le décret n° 2019-452 du 13 mai 2019 autorisant la création d›un moyen d'identification électronique dénommé « *Authentification en ligne certifiée sur mobile* » , op. cit., mentionne à l'art. 10 que les données qui sont conservées dans le cas du traitement centralisé par l'ANTS «sont supprimées à l'issue d'une période d'inactivité du compte de six ans ».
224 op. cit.
225 Voir notamment les CGU du service France Connect qui font références aux législations applicables.
Et plus spécifiquement sur la conservation des données biométriques le règlement général de protection des données à caractère personnel (RGPD).
226 Le zero knowledge proof désigne un protocole sécurisé dans lequel une entité, nommée « fournisseur de preuve », prouve mathématiquement à une autre entité, le « vérificateur », qu'une proposition est vraie sans toutefois révéler d'autres informations que la véracité de la proposition. Cela permet par exemple de vérifier qu'une personne en majeure, sans pour autant dévoiler son âge exact ou sa date de naissance.

Hypothétiquement, cette technologie pourrait aussi être utilisée pour certains services à travers la plateforme France Connect. Il faut noter que dans son fonctionnement actuel, le service France Connect effectue toujours la transmission d'un certain nombre de données de l'identité pivot au fournisseur de services. Plus largement, il serait–dans certains cas–plus pertinent que les fournisseurs de services listent les données d'identité dont ils ont besoin et qu'ils ne reçoivent que ces dernières.

Dans ces conditions le Conseil national du numérique estime que les identités numériques proposées par les pouvoirs régaliens doivent répondre à un principe de frugalité, tant dans le stockage que la transmission des informations d'identité. Pour ce faire, il recommande que soient déployées des solutions techniques permettant aux individus de prouver certains attributs d'identité sans dévoiler la totalité de leur identité.

2.3.2.3. L'importance de la révocabilité de l'identité numérique pour la sécurité des porteurs de l'identité numérique

Le Conseil estime que l'identité numérique doit être révocable, annulable à tout moment, pour répondre aux risques d'attaque, d'usurpation et de faille. Il salue les arbitrages du gouvernement[227] allant dans ce sens.

2.3.3. La structure de la CNIe : certificat d'authentification et signature sur demande des citoyens

Comme évoqué en introduction, la carte nationale d'identité électronique qui doit être déployée sur le territoire national d'ici août 2021 pourrait être un des supports de l'identité numérique.

Dans le rapport « Modèle économique de l'identité numérique » de juillet 2018[228], l'Inspection Générale des Finances proposait, après une étude des solutions européennes, de doter la CNIe de certificats d'authentification et de signature, pour favoriser le déploiement de l'identité numérique. Contrairement à la proposition des administrations en charge de l'écriture du rapport, pour qui les certificats doivent être activés automatiquement, le Conseil estime que cette activation doit se faire sur demande du citoyen pour qu'il reste en pleine maîtrise de son ou ses identités numériques. Insister sur le modèle de consentement à l'activation des certificats serait bénéfique pour la communication qui sera faite de l'identité numérique portée par la CNIe. Cette activation pourrait être proposée au citoyen lors de la délivrance de la carte, ce qui ne l'empêchera pas d'être effectuée plus tard, sur demande du citoyens, dans l'un des points dédiés à l'enrôlement (ex. mairie, préfecture, etc.).

De plus, alors que la solution envisagée est pour l'instant de niveau substantiel et élevé, associant la CNIe à l'application Alicem, il paraît nécessaire d'intensifier les efforts pour qu'elle puisse répondre à l'ensemble des usages d'une population très hétérogène en terme d'accès et de littératie numérique. En effet, des échanges avec les collectivités territoriales ont mis en avant la nécessité d'avoir un support

227 Prise de parole Valérie Péneau le 19 janvier 2020 lors de l'ID Forum au FIC à Lille. Site web de l'ID Forum.
228 op. cit.

de l'identité numérique qui puisse offrir un service identique quel que soit les modes d'interaction des citoyens avec l'administration en particulier dans les parcours multicanaux. En effet ces acteurs ont mis en avant l'apparition d'une rupture dans le principe du « dites-le-nous une fois » pour certains utilisateurs ayant des parcours multicanaux[229]. Selon eux, alors que le principe du « dites-le-nous une fois » est bien appréhendé dans les parcours numérique, il est très difficile de poursuivre celui-ci quand la démarche change de point d'entrée : les pièces justificatives étant bien souvent redemandées à l'usager.

Recommandation n°35

Insérer dans la carte nationale d'identité électronique (CNIe) un certificat d'autorisation à destination des personnels administratifs, pour accéder en guichet à des informations déjà connues de l'administration sans que l'usager ait besoin d'apporter ses documents. Néanmoins, il faudra mettre en place une forme de consentement explicite à cette transmission dans les parcours administratifs (par exemple la signature sur écran).

229 Un parcours multi canal est un parcours qui commence avec un outil (ex. internet), et se poursuit avec un autre (ex.téléphone, guichet, courrier).

CONCLUSION

Les identités numériques sont, par leur capacité de définition de nos individualités, et autant qu'elles peuvent être, très personnelles. Elles peuvent constituer également, comme cela a été décrit dans ce rapport, les outils d'une politique publique plus globale. Devenant les intermédiaires de l'accès aux services publics dématérialisés, le respect de principes constitutionnels d'égalité de tous devant le service public, de continuité et d'adaptabilité sont plus que jamais une priorité. Ces identités numériques — et pas uniquement celles portées par le gouvernement — doivent permettre de faire émerger un modèle français de la citoyenneté numérique.

Cette sensibilité et ces principes, se retrouvent dans toutes les recommandations et les orientations de ce rapport. Pour le Conseil, il paraît primordial que le Gouvernement prenne en compte quatre axes dans le développement de ce bien public : celui-ci ne sera acceptable que s'il est représentatif d'un modèle social ouvert, inclusif et prenant en compte les spécificités de chacun ; la citoyenneté numérique n'est pas une situation qui se décrète mais un processus qui nécessite un accompagnement de l'ensemble de la population indifféremment des âges, des localités, ou des situations sociales et professionnelles. La gouvernance de l'identité numérique doit être représentative de la démocratie, en prenant en compte l'ensemble des voix au chapitre et en proposant une position collégiale et éclairée. Enfin, la sécurité est un pilier de la confiance dans les identités numériques et des moyens proportionnés doivent être mobilisés.

Proposer des identités numériques largement acceptées et utilisées par tous, c'est permettre à des nouveaux services d'apparaître, à des processus d'être repensés ou inventés, à une économie de s'étendre, à des écosystèmes d'éclore, à des nouvelles technologies d'émerger. Ces évolutions seront sûrement une source de redéfinition de la citoyenneté qui, même si elle est un concept intemporel en lien avec l'État-nation, peut être requalifiée perpétuellement selon le vécu de chaque génération confrontée à son siècle, ses moments de crise et de cohésion.

BIBLIOGRAPHIE

Rapports

- ACAR, Bruno, GIGUET, Xavier, SCHECHER François, MORIN Gabriel, janvier 2020, Rapport La formation des élus locaux, IGA, IGF
- CNIL, LINC, décembre 2019, Civil tech, données et Demos, Cahier Innovation et prospective, n°7.
- CNIL, Reconnaissance faciale : pour un débat à la hauteur des enjeux, 15 novembre 2019.
- Conseil national du numérique, Citoyens d'une société numérique. Accès, Littératie, Médiations, Pouvoir d'agir : pour une nouvelle politique d'inclusion, Octobre 2013.
- Conseil national du numérique, Avis Fichier TES, décembre 2016.
- Conseil national du numérique, Avis Transformation de l'État Dépasser la norme par la pensée design, novembre 2019.
- Conseil national du numérique, Rapport L'accessibilité numérique, entre nécessité et opportunité, février 2020.
- Arcep, Conseil général de l'Économie, Mission société numérique, Baromètre du numérique, 18ème édition, Ambition numérique, 2015, Conseil national du numérique.
- LASSERRE Bruno, L'Etat et les technologies de l'information : Vers une administration à accès pluriel, décembre 2000.
- LECERF Jean-René, Rapport d'information n° 439, Identité intelligente et respect des libertés, Sénat, 2004-2005
- Le Forum des droits sur internet, Le projet de carte nationale d'identité électronique, 16 juin 2005.
- ANDRE, Michèle, Rapport d'information n° 486 (2008-2009), La nouvelle génération de titres d'identité : bilan et perspectives, Sénat, Juin 2009.
- CARCENAC, Thierry, Rapport Pour une administration électronique citoyenne, sur la modernisation de l'Administration électronique, Avril 2001.
- LONGUET, Gérard, MONTAUGÉ, Franck, Rapport de la commission d'enquête sur la souveraineté numérique, Sénat, Octobre 2019.
- IGF, IGA, CGE, Modèles économiques de l'identité numérique, Tome I, Juillet 2018.
- Renaissance numérique, Identité numérique : Passer à une logique citoyenne, janvier 2019
- Défenseur des droits, Dématérialisation et inégalités d'accès aux droits, 2019.
- OURAL Akim, Vers un modèle français des villes intelligentes, Juin 2018.

Littérature scientifique

- CHAMPETIER DE RIBES Violaine et SPIRI Jean, Demain tous Estoniens ? L'Estonie, une réponse aux GAFA, Cent Mille Milliards, Hachette, septembre 2018.
- DOUEIHI Milad et DOMENICUCCI Jacopo Domenicucci, La confiance à l'ère numérique, Berger-Levrault, avril 2018.
- FOURMENTRAUX Jean-Paul (Dir), Identités numériques, Expressions et traçabilité, Les Essentiels d'Hermès, CNRS éditions, 2015.
- GREFFET, Fabienne, WOJCIK, Stéphanie, « La citoyenneté numérique. Perspectives de recherche », Réseaux, 2014/2 (n° 184-185), p. 125-159.
- KHATCHATOUROV, Armen, CHARDEL Pierre-Antoine, FEENBERG Andrew et PEIRES Gabriel, Les identités numériques en tension entre autonomie et contrôle, Volume 3, ISTE Editions, 2019.
- LASCOUMES, Pierre, LE GALES, Patrick (dir.), Gouverner par les instruments, Presse de Sciences Po, 2004.
- PASQUIER, Dominique, L'internet des familles modestes : Enquête dans la France rurale, Paris : Presse des Mines, 2018.
- PEZZIARDI Pierre et VERDIER Henri, Janvier 2017, Des startups d'État à l'État plateforme, Fondation pour l'innovation politique.
- PIAZZA, Pierre, Histoire de la carte nationale d'identité, Odile Jacob, 2004, 462 p.
- PIAZZA, Pierre, « Les résistances au projet INES », Cultures & Conflits [En ligne], 64 | hiver 2006.
- Renaissance numérique, L'identité numérique, passer à une logique citoyenne, janvier 2019.
- RODET, Diane, « Loïc Blondiaux, Le nouvel esprit de la démocratie. Actualité de la démocratie participative », Lectures, Les comptes rendus, 2008.
- TRUDEL, Pierre, « La souveraineté en réseaux » dans Annie Blandin-Obernesser, Droits et souveraineté numérique en Europe, Bruxelles, Bruylant, 2016, pp. 5-14.
- WAHNICH Sophie, « L'identité nationale, une question européenne », Dans Vacarme 2010/1 (N° 50), pp. 86 à 90.

Textes législatifs et réglementaires (ordre chronologique)

Arrêtés

- Arrêté du 24 juillet 2015 portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication d'un téléservice dénommé « FranceConnect ».
  https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030972764&dateTexte=&categorieLien=id
- Arrêté du 8 novembre 2018 relatif au téléservice dénommé « FranceConnect » créé par la direction interministérielle du numérique et du système d'information et de communication de l'État.
  https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037611479&categorieLien=id

- Arrêté du 13 mai 2019 modifiant l'arrêté du 10 août 2016 autorisant la création d'un traitement automatisé de données à caractère personnel dénommé « DocVérif ». https://www.legifrance.gouv.fr/affichTexte.do ? cidTexte=JORFTEXT000038485802&dateTexte=20190722
- Arrêté du 11 mai 2020 relatif à l'expérimentation visant à étendre le périmètre des partenaires du téléservice « FranceConnect ». https://www.legifrance.gouv.fr/affichTexte. do?cidTexte=JORFTEXT000041897201&dateTexte=&categorieLien=id

Décisions

- Décision n° 2012-652 DC du 22 mars 2012, du Conseil Constitutionnel https://www.conseil-constitutionnel.fr/decision/2012/2012652DC.htm

Décrets

- Décret n° 2017-910 du 9 mai 2017 relatif aux conditions de recueil et de conservation des empreintes digitales des demandeurs de carte nationale d'identité. http://www.legifrance.gouv.fr/affichTexte.do ; jsessionid=DDBD9EDAEBD448ECD152E1 269BD9E52C.tpdila16v_1 ? cidTexte=JORFTEXT000034638566&dateTexte=&oldAction=rechJO&catego rieLien=id&idJO=JORFCONT000034630664
- Décret n° 2019-33 du 18 janvier 2019 fixant la liste des pièces justificatives que le public n'est plus tenu de produire à l'appui des procédures administratives en application de l'application de l'article L. 113-13 du code des relations entre le public et l'administration. https://www.legifrance.gouv.fr/affichTexte.do ? cidTexte=JORFTEXT000038029642&dateTexte=&categorieLien=id
- 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. https://www.legifrance.gouv.fr/affichTexte.do ? cidTexte=JORFTEXT000038029589&dateTexte=&categorieLien=id
- Décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé « Authentification en ligne certifiée sur mobile ». https://www.legifrance.gouv.fr/affichTexte.do ? cidTexte=JORFTEXT000038475477&categorieLien=id
- Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. https://www.legifrance.gouv.fr/eli/decret/2019/5/29/JUSC1911425D/jo/texte

Lois

- Loi n° 2018-727 du 10 août 2018 pour un État au service d'une société de confiance (1). https://www.legifrance.gouv.fr/affichTexte.do ; jsessionid=853C8147BBC226E07049DF2F6256B6B1.tplgfr26s_1 ? cidTexte=JORFTEXT000037307624&categorieLien=id
- Loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité https://www.legifrance.gouv.fr/affichTexte.do ? cidTexte=JORFTEXT000025582411&categorieLien=id
- Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (1) https://www.legifrance.gouv.fr/eli/loi/2016/10/7/ECFI1524250L/jo/texte

Règlements européens

- Règlement (UE) No 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 et abrogeant la directive 1999/93/CE https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32014R0910&from=FR
- Règlement d'exécution (UE) 2015/1501 de la Commission du 8 septembre 2015 sur le cadre d'interopérabilité visé à l'article 12, paragraphe 8, du règlement (UE) no 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. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32015R1501&from=FR
- 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) no 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. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32015R1502&from=FR
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données). https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679
- Règlement (UE) 2019/1157 du Parlement européen et du Conseil 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 https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32019R1157

ANNEXES

Lettre de saisine

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE ET DES FINANCES

MINISTÈRE DE L'ACTION ET DES COMPTES PUBLICS

SECRÉTARIAT D'ÉTAT CHARGÉ DU NUMÉRIQUE

LE SECRÉTAIRE D'ÉTAT

Paris, le - 9 JUIL. 2019

Madame la Présidente,

Le développement des usages numériques crée, pour nos concitoyens, de multiples besoins de s'identifier en ligne. De surcroît, certains services requièrent de pouvoir lier, avec un haut niveau de confiance, l'identité réelle de l'utilisateur avec son identité en ligne (ex. : signature d'un document, souscription d'un contrat).
Comme dans le monde physique, l'Etat doit pouvoir garantir l'identité de ses citoyens dans le monde numérique et ce lien de confiance est indispensable pour faciliter et sécuriser les usages numériques au quotidien.

C'est la raison pour laquelle a été créée, en janvier 2018, une direction de programme interministériel chargée de concevoir et mettre en œuvre un parcours d'identification numérique universel et inclusif sécurisé, plaçant les intérêts des utilisateurs « au cœur [des] démarches ». Ces travaux sont coordonnés avec les initiatives menées par direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC) notamment dans le cadre de FranceConnect.

Les travaux menés au cours de la première phase de ce programme, marquée notamment par le déroulement des Assises de l'identité numérique en avril 2018, ont permis de définir le scénario qui doit conduire à offrir à l'ensemble de la population une solution d'identification numérique avec un niveau de garantie élevé, au sens du règlement européen e-IDAS.

Madame Salwa TOKO
Présidente du Conseil national du numérique
6 rue Louise Weiss
75013 PARIS

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES
139 rue de Bercy - Télédoc 181 - 75572 Paris cedex 12

Réunis lors d'un comité stratégique du programme le 19 décembre dernier, ont été à cet égard actées les principales orientations suivantes :

1) compte tenu du règlement européen renforçant la sécurité des cartes d'identité, prochainement publié, se saisir de l'opportunité du déploiement d'une future carte nationale d'identité numérique (CNIe) pour offrir aux usagers un moyen d'identification numérique de niveau élevé (horizon été 2021) ;

2) prévoir que la future CNIe, support de l'identité numérique, puisse être « dérivée » par des fournisseurs d'identité privés pour faciliter une offre de solutions d'identification alternatives;

3) dans l'attente du déploiement de cette solution « universelle », mettre à disposition du public dès 2019 la solution expérimentale sur smartphone développée par le ministère de l'intérieur, dite ALICEM, et conduire les études complémentaires et les expérimentations nécessaires pour anticiper au mieux les besoins des utilisateurs, mobiliser les usages (publics et privés) et clarifier les fondamentaux du marché de l'identité numérique.

Afin d'éclairer le Gouvernement dans la mise en œuvre de ces orientation stratégiques, je souhaiterais m'appuyer sur l'avis du Conseil national du numérique, notamment dans le cadre d'une consultation publique citoyenne organisée par vos soins en étroite coordination avec le Secrétariat d'Etat au numérique.

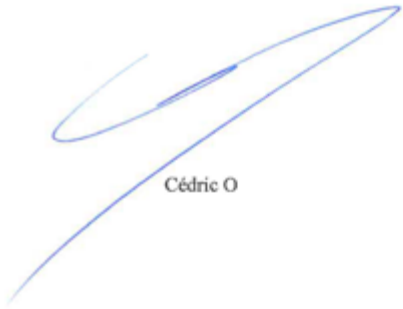
L'objectif de cette consultation sera de comprendre la perception de ce projet par les acteurs impliqués (citoyens, associations d'usagers, entreprises, collectivités territoriales, etc.). Ces travaux seront cruciaux pour anticiper au mieux les besoins de tous les utilisateurs et garantir l'appropriation collective de l'identité numérique, du niveau de garantie faible à celui élevé. Ils le seront également pour construire une vision collective et assurer le développement éclairé et responsable de l'identité numérique dans des délais resserrés.

Je souhaite donc que vous me fassiez parvenir, d'ici l'automne 2019, des propositions concernant la mise en place d'un tel dispositif permettant notamment de répondre aux trois grands enjeux suivants :

- explorer et développer le concept de citoyenneté numérique, nationale et européenne, dont l'identité numérique est porteuse;
- proposer, en fonction des besoins identifiés, des éléments de communication et de pédagogie qui accompagneront la mise en œuvre de l'identité numérique afin d'en améliorer la compréhension et favoriser son caractère inclusif;
- s'assurer, sur la base des expérimentations conduites par le programme, de l'ergonomie, de la facilité d'usage et de la qualité des supports utilisateurs associés aux solutions retenues, afin de s'assurer de leur adoption par le plus grand nombre d'utilisateurs, dans une démarche d'inclusion.

La direction de programme interministérielle chargée de l'identité numérique ainsi que la direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC) se tiennent bien entendu à votre disposition pour vous fournir tous les éléments utiles à la conduite de votre mission.

Je vous prie d'agréer, Madame la Présidente, l'expression de notre considération distinguée.



Cédric O

Copie à :
- Madame Valérie Péneau, inspectrice générale de l'administration, directrice du programme interministériel chargé de l'identité numérique
- Monsieur Nadi Bou Hanna, directeur interministériel du numérique et du système d'information et de communication de l'État (DINSIC)

Institutions

- ADLC : Autorité de la concurrence
- ANCT : Agence nationale de cohésion des territoires
- ANSSI : Agence nationale de sécurité des systèmes d'information
- ANTS : Agence nationale des titres sécurisés
- CGE : Conseil général de l'Économie
- CNNum : Conseil national du numérique
- CNIL : Commission nationale de l'informatique et des libertés
- CREDOC : Centre de Recherche pour l'Étude et l'Observation des Conditions de Vie
- CSA : Conseil supérieur de l'audiovisuel
- DDD : Défenseur des droits
- DINUM : Direction Interministérielle du numérique
- IGA : Inspection Générale de l'administration
- IGF : Inspection Générale des Finances
- LINC : Laboratoire d'innovation numérique de la CNIL
- SIILAB : Laboratoire pour l'Innovation et l'Investissement Social (Hauts-de-France)

Abréviations

- ALICEM : Authentification en ligne certifiée sur mobile
- CNI : carte nationale d'identité
- CNIe : carte nationale d'identité électronique
- ISA : Interoperability solutions for public administrations
- EIF : European Interoperability framework
- FI : Fournisseur d'identité
- FS : Fournisseur de service
- FC : France Connect
- MIE : Moyen d'identification électronique
- NIR : Numéro d'inscription au répertoire
- PKI : Public Key Infrastructure
- RNIPP : Répertoire national d'identification des personnes physiques
- TES : [fichier des] Titres électroniques sécurisés

Glossaire

- Authentification : Il s'agit de donner une preuve que l'identité que l'on utilise est bien à nous. En authentifiant on vérifie les données d'identification.
- Enrôler : acte de création d'une identité sur un service.
- Fédérateurs d'identité : entité publique ou privée capable de mettre à disposition de fournisseurs de services (publics et privés) une offre de plusieurs fournisseurs d'identité (publics et privés), et ceci en garantissant un point d'entrée unique à ces acteurs.
- Identification : fournir une preuve de son identité.
- Identité racine : Une identité fortement garantie, servant de base à la délivrance d'autres identités.
- Identité pivot : Une identité pivot est l'ensemble des données minimales nécessaire pour identifier une personne physique ou morale. Sur France connect il s'agit du nom/ prénom/ date de naissance / lieu de naissance / sexe / Pays de naissance.
- Moyens d'identification électronique (MIE) : Élément matériel (carte, clé USB) et/ ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne.
- Niveau de sécurité (au sens du règlement eIDAS) :
  - Faible : une identité numérique à réserver à des usages peu sensibles de type consultatifs. La vérification limitée de l'identité du demandeur.
  - Substantiel : Une identité numérique adaptée à des usages plus sensibles et engageants pour le citoyen. Il est suggéré d'effectuer une vérification de l'identité du demandeur notamment en vérifiant la possession d'une pièce d'identité et la validité de cette dernière
  - Élevé : Une identité numérique robuste pour des usages numériques qui auraient requis une présence physique.
- Schéma d'identification électronique : Un schéma d'identification électronique au sens d'eIDAS est l'ensemble du processus d'enrôlement, utilisation, et révocation de l'identité numérique.

SYNTHÈSE DES CONSULTATIONS

Résumé

Pour les citoyens

- Les consultations ont été l'occasion d'exprimer leur rapport à l'identité numérique – notion floue, qu'il a fallu expliciter et à laquelle certains se sont vivement opposés – et plus largement, de faire un bilan de la dématérialisation des démarches administratives.
- De fortes craintes, nourries par des références culturelles anxiogènes, ont été exprimées concernant : le fichage et la centralisation des données, la possibilité que les données soient cédées à des acteurs économiques, l'usurpation d'identité.
- Des questionnements ont aussi émergé sur les conséquences qu'une architecture qui permet le partage des données entre administrations pourrait avoir sur la perception des prestations sociales, notamment en cas de mésusages ou d'erreurs.
- Il est nécessaire de favoriser une simplification administrative associée à de meilleurs outils de communication et une protection dans les relations avec l'État.
- L'État a un rôle primordial à jouer dans la mise en place d'un outil de confiance, mais les bénéfices d'usages doivent être démontrés ainsi que la sécurité du système. Un tiers de confiance serait utile pour prendre en charge un volet pédagogique, voire jouer le rôle d'une institution d'arbitrage.
- La citoyenneté numérique ne pourra pas émerger sans l'instauration de gardes-fous, supports de la confiance.

Pour les experts

- Il y a une urgence à voir émerger des positions du gouvernement concernant l'identité numérique et sur lesquelles ils pourront s'appuyer pour développer les solutions répondant aux usages de demain et aux contraintes réglementaires (lutte contre la fraude fiscale).
- Les acteurs du marché ont fait état de leurs inquiétudes relatives au fait que le système ne serait pas efficient ou ne dégagerait pas suffisamment de bénéfices d'usages, au risque d'inciter les usagers à se tourner vers les fournisseurs d'identité privés.
- L'identité numérique sera l'occasion d'allier : une simplification administrative (notamment pour les personnes morales) et d'une inclusion citoyenne comme condition de l'acceptabilité des outils.
- Les enjeux de cybersécurité et de souveraineté nationale sont à en prendre en compte. Il faut garder à l'esprit qu'aucun système n'est à l'abri de cyberattaques et que l'appréhension des risques est une condition essentielle à la pérennité du dispositif.
- Le modèle de gouvernance et l'interopérabilité ont aussi suscité des questionnements.

Contexte

Le secrétaire d'État chargé du Numérique a saisi le Conseil en juillet 2019 afin que celui-ci explore et effectue des recommandations sur la thématique de l'identité numérique. Dans le cadre de ses travaux sur l'identité numérique, son déploiement ainsi que l'articulation de nouveaux outils avec les dispositifs déjà existants, le Conseil national du numérique (CNNum) a effectué sept consultations dans différentes villes de France (Paris, Lyon, Montpellier et Douai). Ces consultations ont été scindées comme suit :

- les consultations citoyennes (ouvertes à tous sans pré-requis, médiatisées au plus grand nombre sur les réseaux sociaux et à travers la mailing-list du Conseil)
- les consultations experts (sur invitation)

1. Représentations et appréciations de l'identité numérique par les citoyens : la vision angoissée supplante les bénéfices d'usage

Les différentes consultations citoyennes ont permis de mettre au jour les réactions contrastées des citoyens face au sujet. En premier lieu, un sentiment assez diffus de confusion et d'angoisse autour des termes « identité numérique » a été constaté. En effet, lorsque les citoyens sont interrogés sur les représentations qu'ils associent à l'identité numérique ainsi que leur motivation à participer à la consultation, certains participants convoquent des fictions (cf. Black mirror[230], Big brother), des affaires médiatiques (cf. Cambridge analytica, fuite de données, usurpations d'identité, deep fake…) ou des politiques étrangères sur l'usage de la biométrie et de la surveillance de masse (par exemple, la Chine).

En second lieu, les usages liés à l'identité numérique, et plus particulièrement les interactions avec l'administration, peuvent se faire à travers différents canaux qui influent sur le niveau d'acceptation et de crainte des citoyens. La plupart des individus utilisent plusieurs canaux, voire changent de canal au cours d'une même procédure lorsqu'un problème dans leur parcours utilisateur se présente (internet, téléphone, courrier, au guichet). Certains rappellent qu'ils effectuent les démarches en ligne par contrainte : elles leur permettent plus de flexibilité que les démarches au guichet ou par téléphone (horaires, disponibilité, déplacements, etc.) ou répondent à une disparition des points physiques auxquels s'adresser.

Outre ces premières considérations, des points saillants plus spécifiques sont remontés des consultations citoyennes, comme la difficulté à définir ou concevoir l'identité unique (1.1), la problématique de la confiance (1.2.), la thématique de la sécurité (1.3), un ensemble de peurs associées au sujet (1.4.), ainsi que des considérations plus spécifiques sur les dispositifs que sont la CNIe (1.5) et France Connect (1.6).

230 Note d'étonnement des rapporteures : bien souvent dans les consultations nous avons pu constater que les individus évoquent plus régulièrement la série Black mirror (2011) que la surveillance généralisée et omniprésente de type « orwellienne », « 1984 » ou « Bigbrother ». La distinction entre ces deux cadres de référence est que Black Mirror ne se concentre pas sur la surveillance généralisée dans un contexte de coercition totalitaire, mais articule au fur et à mesure des épisodes des dérives possibles du « numérique » (pris dans son sens général) pouvant bouleverser les structures de la société.

1.1. Difficulté à définir, ou concevoir, une identité unique pour les citoyens

La notion d'identité numérique a été relativement difficile à concevoir pour les citoyens, notamment l'idée d'une numérisation de l'identité racine (elle-même étant issue de l'état civil). Souvent cette identité numérique a été perçue comme une réduction ou une agrégation de leurs multiples identités numériques à une seule. Dans cet esprit, plusieurs questionnements ont été mis en avant notamment la gestion des traces, ainsi que les risques de traçabilité. De plus, la notion de donnée apparaît fréquemment pour définir l'identité numérique avec une interprétation plus ou moins large[231]. Ce qui apparaît comme important pour les citoyens est de cerner : quelles sont les informations embarquées dans l'identité numérique, quels sont les usages qui pourraient en découler et quels sont les risques auxquels ils s'exposent.

1.2. Le numérique, un médium qui impact la confiance dans l'État même si celui reste le garant de l'identité pivot

La difficulté à concevoir l'identité numérique ainsi qu'à l'accepter témoigne d'un manque de confiance[232] de la population. Ce sentiment se retrouve tant au niveau de la délégation de la mission à un tiers (fournir une identité aux citoyens) que dans un rapport ambigu à l'État. En premier lieu, l'outil qu'est le numérique leur pose problème, notamment en terme de sécurité ; néanmoins, face aux risques d'usurpation d'identité ou de mésusages, c'est à l'État que les citoyens renvoient la responsabilité de leur protection et de la garantie de leur identité pivot. En second lieu, ils remettent en cause la pérennité du périmètre d'application des outils en cas de changement du pouvoir politique pour un régime plus coercitif. Pour eux, « *il ne faudrait pas donner de passe-droits à l'État* ».

Lorsqu'on les interroge sur le moyen de restaurer ou de faire émerger cette confiance, deux solutions sont envisagées :

- l'importance d'une structure de contrôle indépendante qui prendrait soit la forme d'un consortium d'individus pouvant jouer le rôle de tiers de confiance, soit d'une autorité administrative indépendante ou parlementaire (même si certains questionnent l'indépendance d'une autorité administrative) ;
- la notion de choix revient aussi fréquemment comme moyen de restaurer la confiance, argumentant qu'il est nécessaire de pouvoir choisir les outils, les usages et en particulier des alternatives.

231 Pour certains les données correspondant regroupent : l'adresse e-mail, l'adresse postale, le numéro de téléphone, les données de santé, etc. Il n'y a pas de définition commune entre les participants.
232 En décembre 2018 France stratégie a publié un rapport intitulé « Expertise et démocratie, faire avec la défiance ». Il cite pour définir de la notion de confiance le sociologue G. Simmel, dans sa publication de Sociologie. Etudes sur les formes de la socialisation,, éd. PUF, 1908, un « *état intermédiaire entre le savoir et le non-savoir sur autrui. Celui qui sait tout n'a pas besoin de faire confiance. Celui qui ne sait rien ne peut raisonnablement même pas faire confiance* ». La confiance est selon eux synonyme d'une forme de savoir acquis mais aussi de dépendance.

1.3. La gestion de la sécurité : un corollaire de cette confiance

Dans la majorité des consultations, la question de la sécurité et tout particulièrement de la cybersécurité du système a été mise en avant très tôt dans les échanges. Sur l'ensemble des consultations et des exercices, lorsque les citoyens sont interrogés sur les avantages et les inconvénients des dispositifs proposés, tous mettent en avant les risques de failles de sécurité à travers des termes comme : le piratage, la fuite de données, les potentialités de hackage des systèmes ainsi que la notion de portes supplémentaires qui entraînerait des failles de sécurité. Le terme de backdoors souvent utilisé dans les médias est mentionné à plusieurs reprises. Il faut ajouter que les citoyens font fréquemment référence à des scandales de fuite de données qui ont pu avoir lieu. Pour beaucoup, l'État ne serait pas en capacité de mettre en place une architecture répondant à des principes de sécurité élevé et plus particulièrement de mettre l'ensemble de son administration à un niveau de sécurité acceptable.

Lorsqu'ils sont interrogés sur les solutions qui pourraient être mise en place pour diminuer ce qu'ils perçoivent comme des risques de sécurité, plusieurs options sont proposées :

- L'hygiène informatique devrait être enseignée tant aux usagers de l'identité numérique qu'au personnel administratif.
- La chaîne de blocs ou « blockchain » est souvent évoquée comme une forme de sécurité par les personnes les plus expertes dans les groupes de citoyens.
- Un niveau de sécurité et d'auditabilité est important pour un certain nombre de participants afin de vérifier la manière dont l'administration prendrait en charge leur identité numérique.

1.4. Surveillance généralisée, usurpation d'identité, accès aux droits : les autres interrogations et réticences des citoyens

L'idée de la surveillance généralisée, qui s'appuierait sur l'identité numérique a été mentionnée dans l'ensemble des consultations qui ont été organisées. Cette surveillance est souvent mise en parallèle avec deux autres points. Tout d'abord, la centralisation des informations (qui permettrait la surveillance) que les citoyens craignent et rejettent. De plus, ils mentionnent la peur d'être tracés[233], pistés, « fliqués », avec une identité numérique étatique (unique) alors que la multiplicité des identités numériques actuelles leur permet de jongler en fonction des situations et des usages. La surveillance apparaît comme l'un des premiers freins à l'usage d'une identité numérique, qu'elle soit formalisée par une plateforme ou par une carte. Cette crainte est subséquente à la perception du niveau de sécurité des informations.

De plus, les citoyens s'interrogent et s'inquiètent des conséquences que pourraient avoir une usurpation d'identité numérique, ou une perte ou un vol de l'identité numérique. Ils s'inquiètent aussi de la possibilité de suppression de l'ensemble de leurs données ou de vente de leurs

233 En rapport à la traçabilité et au « flicage », certains citoyens ont évoqué certains dispositifs anxiogènes comme les compteurs Linky en plus du déploiement des CCTV (Closed-Circuit TeleVision).

données personnelles. Pour eux, il est primordial de pouvoir révoquer l'identité numérique[234], d'être informé de son utilisation et d'avoir un parcours simplifié pour la réactiver au besoin.

Outre la surveillance ou l'usurpation, c'est aussi l'irréversibilité des actions et les potentiels impacts sur l'accès aux droits qui freinent les citoyens. Beaucoup s'imaginent qu'en ayant une identité numérique en ligne, si un problème survenait dans une interaction avec l'administration, cela pourrait impacter l'ensemble du système, notamment en cas de partages d'informations entre administrations. À titre d'exemple ils craignent qu'en cas d'erreur (de leur part ou de l'administration) au niveau de leurs impôts, cela impacte la perception d'allocations sociales et ce, avec des procédures de recours longues et laborieuses. De la même manière, l'idée que l'identité numérique puisse être un outil de lutte contre la fraude fiscale[235], ou de réduction du délai de paiement des amendes est perçu comme un risque qui pourrait induire un retrait des droits[236] (décisions verticales de l'administration, difficultés d'accéder à des moyens de contestation…).

Dans une certaine mesure, beaucoup de citoyens se sont interrogés sur le coût d'un tel système, qu'il s'agisse : d'une carte d'identité électronique et de sa production, d'une plateforme et de sa gestion, du maintien de la sécurité de l'ensemble du système, de la mise à niveau des infrastructures, de la formation des personnels administratifs et des utilisateurs. Plusieurs scénarii émergent pour la répartition du coût de l'identité numérique : pour certains, il faudrait qu'il soit également réparti entre tous les citoyens, pour d'autres, cela devrait être supporté uniquement par les personnes utilisant le système, à l'instar de la redevance audiovisuelle.

En parallèle du coût monétaire, des préoccupations écologiques ont été mentionnées à plusieurs reprises. Pour certains il s'agit d'évoquer le coût environnemental des démarches administratives sur formulaires papier, arguant que la dématérialisation serait plus respectueuse de l'environnement. Pour d'autres, il est question au contraire de l'impact écologique du numérique. Ils souhaitent que les décisions du gouvernement se fassent en fonction de ce critère en abordant des notions de frugalité et de « taille » du projet.

Enfin, lorsqu'il s'agit de lister les avantages et les usages qui pourraient accompagner le dispositif d'identité numérique, l'un des arguments les plus généralement admis est qu'il s'agit principalement d'une simplification, bien que certains demandent encore la preuve de son utilité, ce qui traduit que l'intérêt de l'outil au regard des dispositifs existants n'est pas toujours perçu.

Ainsi, l'outil est représenté comme un confort accru de l'expérience utilisateur mais pas forcément un service supplémentaire.

234 Ils imaginent en autre un système d'opposition, comme pour les cartes de paiement.
235 Les citoyens ont en particulier mentionné la manière dont l'administration pourrait se nourrir de leur vie sur les réseaux sociaux pour vérifier leurs déclarations. Ils ont explicitement fait référence à l'article 57 du PLF.
236 Ce système fait penser par exemple à la Schufa allemande (Schutzgemeinschaft für allgemeine Kreditversicherung) qui fait état des dettes et de la solvabilité des citoyens.

1.5. La nécessité de garde-fous pour faire émerger une citoyenneté numérique

Pour mieux comprendre ces peurs, questionnements et réticences des citoyens concernant le déploiement de l'identité numérique, ils ont été interrogés sur les éléments leur permettant de garantir et de restaurer la confiance en l'outil.

Tout d'abord, la grande majorité des citoyens interrogés insistent sur la mise en place d'une autorité de contrôle et de suivi de l'identité numérique qui doit être concomitante au déploiement de celle-ci. En effet, cette autorité doit servir de garde-fous pour protéger les droits et les libertés des citoyens, et s'assurer que l'État ne s'octroie pas de prérogatives de contrôle ou de centralisation des données qui ne seraient pas prévues dans le dispositif de départ.

Les différents participants ne s'entendent pas forcément sur la forme et sur son rattachement à l'organigramme de l'administration. Pour certains, seul un organisme public, plus précisément l'État peut garantir l'identité. Le principe régalien est notamment mis en avant ainsi que l'impossibilité de déléguer cette mission. D'autres mettent en avant l'incapacité d'une institution reliée à l'État (par son financement) à garantir son indépendance. De fait, ceux-là ne soutiennent pas le principe des autorités administratives indépendantes. Pour ces derniers, seuls les parlementaires pourraient jouer le rôle de contre-pouvoir. Enfin, une dernière proposition émerge sous la forme d'une société de gouvernance, s'appuyant sur une structure collégiale multi-acteurs[237] pour garantir l'impartialité et renforcer sa mission d'intérêt général. Ces propositions sont fortement liées à l'acceptation de l'outil comme passerelle vers une citoyenneté numérique.

Certains mentionnent aussi l'idée du rôle de tiers de confiance que devrait avoir cette instance. Il n'a pas été précisé si le tiers de confiance devait être l'autorité de contrôle, ou un acteur supplémentaire.

1.6. La carte nationale d'identité électronique, support de l'identité numérique

À la présentation du dispositif de carte nationale d'identité électronique[238], les participants s'accordent sur plusieurs considérations.

- En premier lieu, ce dispositif doit être simple dans son accès et vis-à-vis des usages qui pourront en être faits. Pour eux, le support physique ne suffit pas à répondre aux besoins de plus éloignés et aux exigences de l'inclusion. Un réel travail doit être fait dans la conception du dispositif et des parcours usagers tant pour sa délivrance, son utilisation que les modalités de son renouvellement.
- De plus, et comme mentionné précédemment, les citoyens estiment que ce dispositif ne doit pas être obligatoire, et que

237 L'exemple des coopératives multi-parties prenantes et des SIC est notamment mentionnée comme un modèle de gouvernance possible.
238 La description de la CNIe a été extraite d'un des documents de consultation de la DITP commandé par la mission interministérielle sur l'identité numérique.

son utilisation ou son attribution doit se faire par choix non contraint[239].

- Il serait intéressant que la CNIe réduise la « taille du portefeuille » notamment en embarquant d'autres titres (ex. le permis de conduire, titre de transport public, etc.). Néanmoins les citoyens sont vigilants concernant la carte vitale et les données de santé qui selon eux devraient être cloisonnées.
- La notion de « sans-contact » comme définie dans la présentation de la DITP a suscité de vives réactions de la part des usagers. Ce terme les projette dans des représentations liées à l'environnement bancaire et notamment un risque de vol d'informations d'identité, comme les cartes bancaires sans-contact[240].

Concernant les usages qui pourraient être faits de la CNIe, nous constatons un clivage qui dépend directement du niveau d'aisance numérique des individus. Les groupes revendiquant une bonne aisance numérique (auto-qualification entre 7 et 10 sur une échelle allant de 0 à 10) imaginent des usages répondant à leurs besoins de simplification : mariage, PACS, procuration, prise de rendez-vous médical, obtention ou renouvellement de la carte grise… Pour d'autres se qualifiant moins à l'aise dans les démarches administratives, et comme cela a été évoqué précédemment, les projections sont plus difficiles, et correspondent aux usages du titre comme moyen de répondre à un contrôle d'identité ou d'accéder à des droits. À travers ces différents positionnements et partant du principe que les usages font la pérennité du dispositif, il paraît nécessaire de mettre en lumière la volonté générale (toutes catégories confondues) de simplification.

1.7. France Connect, son évolution et le principe du « dites-le-nous une fois »

À la présentation d'évolutions du dispositif France Connect et du principe du « dites-le-nous une fois » [241], les participants s'accordent sur plusieurs considérations.

- Le principe du consentement est une notion centrale pour les citoyens consultés. Pour certains, le partage de données et de documents entre administrations devrait se faire avec un consentement explicite et éclairé du citoyen. Des principes de nudges ne devraient pas être utilisés sur ces fonctionnalités, même si cela sert à développer des bénéfices d'usage. D'autres accepteraient une certaine forme d'automatisation si une liste des informations que les administrations sont en mesure de se communiquer est définie et communiquée à l'avance.

239 Le choix contraint représenterait l'idée qu'il est nécessaire d'avoir cet outil pour accéder à un service public ou un service privé d'importance « vitale » ou bien que l'accès aux services est détérioré par l'absence du dispositif. Ils précisent aussi qu'il ne faut pas que le refus entraîne des pénalités ou la relégation en citoyen de « seconde zone ».. **240** « *Sans contact, ça veut dire qu'il faut aller demander la pochette en aluminium ?* » [pochette du principe de cage de Faraday] » Propos recueilli en consultation.
241 Le principe du « dites-le-nous une fois » est une corollaire de la réflexion autour de l'émergence de FranceConnect. Nous avons utilisé la description du principe présenté sur le site modernisation.gouv, datant de 2013. url : https://www.modernisation.gouv.fr/home/dites-le-nous-une-fois-un-programme-pour-simplifier-la-vie-des-entreprises [consulté en octobre 2019].

- Les systèmes de notification sont jugés utiles et assez appréciés des usagers. Beaucoup citent en exemple le système de France Connect, qui notifie l'usager lorsqu'une connexion est effectuée avec l'une de ses identités numériques.
- Concernant les publics éloignés, les citoyens rappellent l'importance de la délégation de confiance à des gens assermentés[242] dans des lieux spécifiques et ciblés.
- Le dispositif leur paraît positif s'il permet une attribution des droits sans avoir à faire des procédures. Certains évoquent le non-recours aux droits conséquent d'une méconnaissance de l'ensemble des aides existantes. D'autres abondent en mettant en avant la lourdeur des démarches administratives pour y accéder.
- Pour la majorité des participants, il est primordial de faire une séparation entre les acteurs publics et les acteurs privés. Les acteurs privés[243], même ceux dits « d'importance vitale » ne devraient pas accéder sans conditions drastiques à ce dispositif. Les services publics de santé[244] devraient également être distincts de ce système, eu égard à la sensibilité des données de santé.
- La notion de portabilité. Durant les différentes consultations, certains citoyens ont évoqué la portabilité et la possibilité de télécharger l'intégralité de leur dossier administratif comme une possibilité de « garder la main » sur les échanges, l'usage et/ou la circulation de leurs données.

Globalement, nous avons constaté une réelle difficulté des citoyens à visualiser le fonctionnement du « dites-le-nous une fois » sans multiplication des fichiers, ou centralisation de l'ensemble des données dans une base unique. Ils émettent des questionnements légitimes à propos du type d'informations qui pourraient circuler entre administrations et sont en demande d'éclairages et de garanties fortes.

2. Les questionnements des experts sur l'appropriation citoyenne et le développement du marché d'usages

Les consultations experts ont permis d'en savoir plus sur les besoins et attentes des acteurs de l'écosystème (banques, industriels, PME, startups, universitaires…). Nous avons choisi de ne relever ici que certains points spécifiques qui n'auraient pas été évoqués en première partie de cette synthèse.

2.1. Des arbitrages très attendus dans l'écosystème pour amorcer développement d'un marché d'usages

Tout d'abord, les arbitrages du gouvernement sont très attendus et pourraient déterminer certains positionnements stratégiques, de la part notamment des acteurs bancaires. Les acteurs ont en générale rappelé l'importance d'une identité numérique publique pour répondre aux enjeux de l'économie numérique (usurpation d'identité, concurrence avec les grandes acteurs du numérique) et des obligations réglementaires

242 L'association des centres sociaux de Douai fait partie des lieux pilote pour tester Aidants-Connect. Le dispositif a notamment été mentionné à l'occasion.
243 « *Public c'est normal, mais facture, non.* » Propos recueilli en consultation.
244 « *Ce qui est chez Améli doit rester chez Améli.* » Propos recueilli en consultation.

(lutte contre la fraude et le blanchiment d'argent). Ils ont à de nombreuses reprises soulevé l'urgence de mettre en place un système pérenne, agile et efficient pour ne pas prendre de retard sur les autres pays européens, ainsi que pour ne pas tarir les potentialités économiques qui pourraient émerger.

2.2. La souveraineté nationale et européen au coeur de la thématique de l'identité numérique

L'importance des référentiels (notamment la nécessité d'une interopérabilité répondant aux standards eIDAS[245]) a été évoquée comme un enjeu essentiel de la souveraineté sur le territoire européen, et de l'importance de choisir une solution d'identité numérique pouvant faire émerger des usages transnationaux (cf. EIF, ISAProgramme, eIDAS).

De plus, les experts ont mis en lien la notion de souveraineté entourant l'identité numérique avec les efforts de pédagogie et d'information qui doivent être fait auprès des acteurs territoriaux et des élus pour qu'ils fassent des choix éclairés dans les collectivités, et que le travail avec des personnes garantes soit facilité.

2.3. Sécurité du système et frugalité des informations : pour une architecture qui favorise l'acceptabilité

Plusieurs modèles et types d'architecture ont été débattus lors des consultations. La plupart des experts s'accordent sur la nécessité d'une identité racine garantie et gérée par l'État.

Abondant certaines remarques relevées lors des consultations citoyennes, certains acteurs rappellent qu'aucun système n'est totalement à l'abri des risques liés à des attaques cyber-sécuritaires d'ampleur. Ainsi, alors que l'identité numérique est considérée comme l'un des pivots de cette souveraineté à l'ère des GAFAM : la question de l'efficience du système a animé les débats de manière transversale.

La centralisation des données -qui avait été au coeur d'une controverse liée au fichier TES[246]- a été évoquée par les experts. Certains proposent que le système choisi ne puisse pas créer de perspective de fichage, et plaident pour la mise en place de garde-fous et d'une garantie de transparence à l'égard des citoyens. Pour eux, c'est un enjeu de l'environnement de confiance. Ils interpellent sur la tentation d'une centralisation qui exposerait les citoyens mais aussi la crédibilité de l'outil. Cette préoccupation est l'un des points communs les plus prégnants entre les consultations citoyennes et les consultations experts que nous avons menées.

De plus, certains experts plaident pour que l'identité numérique permettent une preuve à divulgation nulle de connaissance ainsi que la restriction des permissions d'accès aux informations d'identité en fonction du fournisseur de service comme le propose la CNIe allemande.

245 RÈGLEMENT (UE) No 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 et abrogeant la directive 1999/93/CE, dit « eIDAS »
246 Le Conseil national du numérique a publié en décembre 2016 un avis relatif au décret n°2016-1460 prévoyant la création d'une base de données des « Titres électroniques sécurisés » (TES).

Les experts ont aussi rappelé que la solution devait être suffisamment réactive (notamment via une mise à jour en temps réel) pour permettre la mise en conformité avec les règlements de lutte contre la fraude (inscription de la date de décès, par exemple).

Enfin, les experts ont rappelé que l'architecture devait répondre à un cahier des charges contenant des principes fort de notre société comme la sobriété écologique dès sa conception, l'inclusion pensée et designée en amont et la possibilité de faire émerger des logiques de plateforme multifaces / multicouches.

2.4. La gestion des données d'identité : un des enjeux économique du modèle

Le positionnement de l'État concernant le modèle économique de la solution est très attendus. Les experts s'interrogent sur les choix qui vont être fait en terme de gestion des permissions et d'accès aux données d'identité, afin de garantir une séparation des pouvoirs.

Certains experts ont plaidé pour la mobilisation des grands acteurs privés (par exemple, via la facturation des opérations d'authentification), expliquant que les bénéfices dégagés pourraient ainsi permettre au système de s'autofinancer. En revanche, d'autres pensent que faire payer une identité numérique pourrait orienter les entreprises à se raccrocher à des identités numériques gratuites, ce qui pourrait être un avantage concurrentiel d'ampleur pour certains acteurs privés.

2.5. L'identité numérique vecteur d'efficience pour personnes morales

Les acteurs ont rappelé l'importance, et la forte demande, pour embarquer la problématique des personnes morales dès le démarrage du programme. Ainsi, il faudra prendre en compte les besoins d'identité dans tous les cas de mise en relation entre entreprises (notions de mandats inter ou intra entreprises, avec notamment le cas des professions réglementées qui agissent pour le compte des entreprises), ainsi que dans le cas de mandats et d'interventions pour un tiers (mineurs, aidants, accompagnateurs sociaux, prêt de carte vitale etc.).

Il faudra envisager la fluidité des parcours entre ces différents besoins, pour être en capacité de faire le lien entre les personnes physiques et les personnes morales (ex : agriculteurs). Il sera d'autant plus important de prendre en compte cette dimension au vu du nombre croissant d'entrepreneurs et d'auto-entrepreneurs en France, qui revêtent aussi bien le statut de citoyen que de personne morale. Pour développer les usages de solutions d'identité numérique, il faut adresser en priorité les parcours à forte valeur d'usage pour les citoyens et les entreprises.

2.6. L'inclusion comme vecteur d'appropriation et de confiance dans l'outil : levier pour l'émergence des marchés d'usage

Les acteurs consultés ont rappelé que l'inclusivité, l'accessibilité et la confiance dans l'outil étaient les conditions indispensables à une appropriation commune par les citoyens. Les experts mettent en avant que l'identification des citoyens est une avancée majeure pour leur relation au service public et pour les perspectives de marché qui en découlent, mais qu'il y a un manque drastique sur la formation, voire « l'hygiène informatique primaire » des citoyens pour se prémunir des fraudes et des usurpations d'identité. Ces questions doivent rester au coeur du déploiement de l'identité numérique. Ces conditions sont essentielles pour faire émerger un marché d'usages conséquent au niveau national, voire européen.

Enfin, l'identité numérique est comprise par tous comme un enjeu majeur du lien de confiance entre les citoyens et l'État, mais aussi comme enjeu fort du dynamisme de l'écosystème.

L'inclusion numérique est une perspective de marché pour les acteurs privés, qui s'investissent déjà sur le sujet (ex : Google qui organise des sessions de formation au numérique). L'inclusion totale des citoyens permettrait de développer des usages à fort potentiel.

2.7. La nécessité d'un tiers de confiance sous la forme d'une institution indépendante

Sur ce sujet, à de nombreuses reprises les experts ont formulé l'idée d'un « tiers de confiance » qui pourrait être un acteur autonome, accessible pour les citoyens mais aussi pour les personnes morales. Les experts ont rappelé l'importance de « garde-fous » sur les données, sous forme d'une institution autonome, voire ad hoc. Cette institution jouerait le rôle d'un « tiers de confiance » et serait idéalement accessible aux citoyens en cas de mésusages, mais aussi pour les personnes morales et entreprises.

La mise en place d'un tiers de confiance permettrait de déléguer la complexité du schéma de maintien et de stockage des données pour les citoyens à une institution en mesure de comprendre les processus et d'approuver la conformité des processus et le respect de l'intérêt général. Pour certains, ce rôle pourrait être joué par les collectivités, ou par une extension du rôle de la CNIL qui jouit d'une reconnaissance par les citoyens. Cette question amène à réfléchir à la chaîne de responsabilité et à la nécessité d'une institution autonome, censée garantir le bon usage des données et jouer le rôle d'intermédiaire de confiance.

De plus, cette institution « tiers de confiance » pourrait avoir un rôle de pédagogue et d'acculturation générale pour que la sécurité soit perçue comme un gage de confiance, et que soient mieux compris les bénéfices d'usages qui découleront de l'identité numérique. Cela pourrait amener aussi à faire évoluer au fil du temps les standards pour améliorer la lisibilité et l'appropriation par tous de l'identité numérique.

2.8. Liberté de choix pour permettre à chacun d'utiliser l'identité numérique correspondant à ces besoins

Pour garantir la couverture des besoins de l'ensemble des publics et la liberté de choix, il émerge un consensus sur la nécessité de conserver une pluralité d'identités numériques et de laisser l'utilisateur choisir en fonction des situations, de ses préférences et de ses capacités. La multiplicité des identités numériques est également importante pour des raisons de sécurité et pour favoriser l'innovation technologique. Il se dessine ainsi un modèle d'écosystème de l'identité numérique caractérisé par une offre diversifiée, une pluralité de solutions d'identité, qu'il conviendra néanmoins de réguler, afin d'éviter le risque d'une trop grande complexité.

2.9. Une liberté transmise par le support de l'identité numérique

Plusieurs experts, dans différentes consultations, ont appelé à diversifier les supports et ne pas se limiter à des solutions sur smartphone :

- Une solution d'identité uniquement sur mobile risque d'exclure une partie de la population puisqu'elle pose la question de l'accès au support physique et au forfait associé, sans tenir compte du niveau d'autonomie nécessaire pour les usagers ;
- Elle pose aussi la question de la relation avec les opérateurs et les constructeurs ;
- Enfin, au vu de l'émergence des technologies, il est possible de se questionner sur la pérennité d'un tel système et le coût d'une maintenance à long terme.

Conclusion

Les participants ont souligné l'importance de tirer les leçons du passé pour la protection de l'identité, notamment des choix d'architecture préservant des risques inhérents à la constitution d'un fichier de population centralisé.

Ainsi, avec un périmétrage conséquent, un effort de pédagogie, de formation et d'inclusion, l'identité numérique pourrait être perçue non pas comme l'extension d'une administration complètement dématérialisée, mais plutôt comme le lien renforcé entre le citoyen et l'État qui garantit, protège et arme le citoyen face aux risques déjà relevés.

LISTE DES PERSONNES AUDITIONNÉES

- Pierre Saber, responsable de l'EPN du Picoulet
- Florian Delezenne, Responsable de l'incubateur de services publics numériques–beta.gouv.fr.
- Hélène Bizette, Coordinatrice, Pandas, Association Pimms Paris
- Hélène Garancher, Directrice, Association Pimms Paris
- Boris Chevrot, Dr. en sociologie-anthropologie
- Julien Kounowski, Inspecteur Hors Classe de l'Action Sanitaire et Sociale (IHC), Ministère des solidarités et de la santé
- Henri Verdier, Ambassadeur pour le numérique.
- Marc Norlain, CEO- co fondateur Ariadnext
- Bénédicte Revol, Expérience Client. Excellence opérationnelle. Programmes de transformation. Secteurs public et privé, DITP
- Jean Deydier, Emmaüs Connect
- Charlotte Bougenaux, Emmaüs Connect
- Nadi Bou Hanna, Directeur de la DINUM
- Côme Berbain, CTO de l'État.
- Frédéric Duflot, Association Open Law
- Lisa Allemand, Chargée de mission – Cadre réglementaire de la sécurité numérique, ANSSI
- Romain Santini, Sous-direction Stratégie, Division Management de la sécurité du numérique, Adjoint à la cheffe du bureau « Ingénierie du cadre normatif et réglementaire », ANSSI
- Emmanuelle Vivier, Présidente du CSIESR, Comité des services informatiques de l'Enseignement supérieur et de la recherche, DSI Université d'Amiens
- Serge Portella, Président de l'ADSI-ESR, l'association des DSI des universités et établissements, DSI Aix Marseille Universités.
- Pierre.Boulet, VP NUM Université de Lille et Professeur d'informatique.
- Sabine Jaume-Rajaonia
- Hervé Bourgault, RENATER
- Marie-Pierre Chalimbaud, ERASMUS+
- Jean-Paul Roumegas, CNOUS
- David Rongeat, Agence de Mutualisation des Universités et Établissements.
- Bertrand Mocquet, Agence de Mutualisation des Universités et Établissements.
- Céline Stierlé, directrice des Affaires publiques, Idémia,
- Vincent Bouatou, Directeur de l'innovation. Idémia
- Pierre Lelièvre, Identité digitale. Idémia
- Solenne Lepage, Directrice générale adjointe, Fédération des Banques Françaises
- Nicolas Bodilis Reguer, Directeur du département Relations institutionnelles France, Fédération des Banques Françaises
- Olivier Vandenbilcke, Regulatory & Innovation, BNP Paribas
- Yves Le Querrec, Directeur Relations Interbancaires, Direction des Paiements, La Banque Postale
- Frédérique Fagès, Chargée de mission numérique, FBF
- Olivier Senot, directeur du développement, Docapost
- Fabrice Mattatia, DPO Ministère de l'intérieur
- Didier Trutt, PDG, INGroupe
- Romain Galesne-Fontaine, directeur des affaires publiques, iNGroupe
- Philippe Regnard, Directeur des affaires publiques, Branche numérique, La Poste.
- Cécile Gautron, Directeur Identité Numérique, DG Docaposte IOT, La Poste.
- Jean-Marc Galland, Chef de la mission de délivrance sécurisée des titres DMAT.
- Jonathan Bloch, Chef du département des projets et de développement des applications, DMAT, Ministère de l'Intérieur.

- Christine Balian, Directrice du programme France Connect, cheffe mission IDNUM, DINUM
- Stéphane Mavel, Business développement/relations partenaires, DINUM
- Lionel Fouillen, Relations Partenaires FranceConnect, DINUM
- Martin Drago, Chargé d'analyses juridiques et politique, La Quadrature du Net
- Benoît Piédallu, membre, La Quadrature du Net
- Jean-Pierre Triquet, Directeur de la Communication et du Numérique, CU Dunkerque
- François Laureys, Gestionnaire de projets, Stratégie territoriale & Smart Cities, Développement territorial, Namur
- Nathalie Mondanel, Cheffe de projet e-administration et organisation, Ville de Rouen
- Guylaine Guillaumin, Responsable de la mission qualité et modernisation, Ville de Rouen.
- Nicolas Deffieux, Autorité de la concurrence
- Etienne Pfister, Autorité de la concurrence
- Bertrand Pailhès, Directeur innovation et technologies, CNIL
- Amandine Jambert, Experte technique, CNIL
- Valérie Péneau, Directrice du Programme interministériel sur l'identité numérique
- Frédéric Pichon, Directeur adjoint du Programme interministériel de l'identité numérique
- Gilles Coester, Chargé de mission Relations institutionnelles et Partenariats du Programme interministériel sur l'identité numérique

LISTE DES MEMBRES DU CONSEIL NATIONAL DU NUMÉRIQUE

Présidente

- Salwa TOKO

Vice-Président

- Gilles BABINET

Membres

- Yann ALGAN
- Maud BAILLY
- Annie BLANDIN-OBERNESSER
- Mohammed BOUMEDIANE
- Jérémie BOROY
- Patrick CHAIZE
- Théodore CHRISTAKIS
- Olivier CLATZ
- Nathalie COLLIN
- Vincent COSTALAT
- Maryne COTTY-ESLOUS
- Karine DOGNIN-SAUZE
- Gaël DUVAL
- Gérald ELBAZE
- Hind ELIDRISSI
- Florette EYMENIER
- Martine FILLEUL
- Sophie FLAK
- Henri ISAAC
- Tatiana JAMA
- Loubna KSIBI
- Anne LALOU
- Thomas LANDRAIN
- Constance LE GRIP
- Litzie MAAREK
- Laura MEDJI
- Françoise MERCADAL-DELASALLES
- Jean-Michel MIS
- Hervé PILLAUD
- Jean-Charles SAMUELIAN
- Christian VANIZETTE
- Alexandre ZAPOLSKY

Secrétariat général

- Charles-Pierre ASTOLFI, Secrétaire général
- Vincent TOUBIANA, Secrétaire général adjoint
- Eric BERNAVILLE, Assistant de direction

Rédactrices

- Leila AMANAR, rapporteure
- Nathalie BOUAROUR rapporteure

Relectures

- Myriam EL ANDALOUSSI, rapporteure
- Joséphine HURSTEL, rapporteure alternante
- Marylou LE ROY, responsable juridique et des affaires institutionnelles
- Jean-Baptiste MANENTI, rapporteur
- Ménéhould MICHAUD DE BRISIS, rapporteure
- Philippine REGNIEZ, rapporteure
- Hugo BESANCON, stagiaire
- Farah FEJJARI, stagiaire

À PROPOS DU CONSEIL NATIONAL DU NUMÉRIQUE

Le Conseil national du numérique est une commission consultative indépendante. Il est chargé d'étudier les questions relatives au numérique, en particulier les enjeux et les perspectives de la transition numérique de la société, de l'économie, des organisations, de l'action publique et des territoires.

Il est placé auprès du ministre chargé du numérique. Ses statuts ont été modifiés par décret du 8 décembre 2017. Ses membres sont nommés par arrêté du Secrétaire d'État chargé du numérique pour une durée de deux ans.

Contact presse : Charles-Pierre Astolfi, Secrétaire général, presse@cnnumerique.fr, 01 44 97 25 08

https://cnnumerique.fr | @CNNum