DOSSIER DE PRESSE
Rapport du Conseil national du Numérique

IDENTITÉS NUMÉRIQUES

Clés de voûte de la citoyenneté numérique

Le 15 juin 2020

Sommaire

Mots des membres du groupe de travail

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.

À 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 fidèles 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 vœux 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, co-pilote du groupe de travail
Mohammed Boumediane, co-pilote du groupe de travail
Gilles Babinet
Olivier Clatz
Gaël Duval
Jean-Michel Mis

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 ou ses travaux sur la citoyenneté numérique de 2013.

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 oeuvre 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], 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. »

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 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-gouvernement. 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) ;
- 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 58 personnalités issues des administrations, du monde économique et du monde universitaire.

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'Etat 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'Etat. En effet, qu'il s'agisse d'Alicem, de la CNIe ou de FranceConnect, 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 FranceConnect. 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 formations 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'information 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 « dite-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.

35 recommandations pour orienter le Gouvernement et son administration

Le Conseil national du Numérique propose au Gouvernement 35 recommandations orientées autour de quatre axes :

1. Favoriser une solution inclusive et frugale qui rend service aux usagers
2. Faire preuve de pédagogie et initier l'ensemble des citoyens au numérique
3. Opter pour une gouvernance partagée qui replace l'usager au centre
4. Assurer une sécurité de tous

Axe 1 - Favoriser une solution inclusive et frugale qui rend service aux usagers

N°	Thème	Recommandation
1	**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.** Cette cartographie, qui pourrait être calquée sur celle du SIILAB, devra illustrer les différents points de médiation sur une carte, en fonction des besoins de l'usager (écrivain public numérique, travailleur social, Maison France Service…).
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.

3	AidantConnect	Encadrer par un socle de droits et garanties légales pour protéger le développement d'AidantsConnect. : – 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.
4	Design et tests utilisateurs	Imposer des critères d'accessibilité et d'inclusion dans la conception des services s'appuyant sur l'identité numérique qui soient régulièrement testés.
5	**Design, sécurité et fluidité**	**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**, pour la réutilisation des briques d'authentification existantes dans les terminaux mobiles était retenue. Ce cahier des charges pourra notamment servir lors de la conception de services à forte valeur, aux services privés dérivés à l'identité numérique, ainsi qu'aux parcours locaux territoriaux.
6	**Inclusion - Lieu d'enrôlement**	**Faire des mairies (et les collectivités territoriales) les principaux lieux d'enrôlement des identités numériques pour soutenir la confiance en l'État.** Si cet enrôlement devait être délégué à des acteurs de confiance, le Conseil recommande que ces délégations soient précédées d'un cahier des charges précis engageant les agents en charge de l'enrôlement : – Obligation d'assermentation et de formation des agents dédiés à l'enrôlement ; – Protection du citoyen via un cadre juridique particulier ; – Possibilité pour le citoyen de vérifier et modifier les informations relevées lors de l'enrôlement ; – Possibilité de tracer l'enrôlement (notamment pour prévenir les usurpations d'identité) ; – Les fournisseurs d'identité privés rattachés à FranceConnect doivent pouvoir garantir le même niveau de sécurité que les fournisseurs d'identité publics.

Axe 2 - Faire preuve de pédagogie et initier l'ensemble des citoyens au numérique

7	**Communication**	**Créer une réelle communication autour de FranceConnect et la création de la CNIe, comportant :** – Des informations simplifiées et non techniques sur la sécurité des infrastructures publiques qui hébergent des données personnelles et sur les mécanismes employés pour en garantir la confidentialité ; – Des infographies, vidéos, textes pédagogiques… sur la simplicité d'utilisation et les bénéfices que les citoyens peuvent retirer de FranceConnect, en prenant au besoin exemple sur certains fournisseurs d'identités privés ; – Un rappel que le projet d'identité numérique est au service d'une large inclusion des publics considérés comme éloignés du numérique ; – Des explications sur le rôle de la société civile et les droits de chaque citoyen de contrôler et de tracer l'usage qui est fait de ses données.
8	Communication - Fonctionnement service public et gestion des informations dématérialisées	Communiquer massivement sur le fonctionnement des services publics et de la gestion des informations dématérialisées pour répondre aux craintes des usagers vis-à-vis de potentiels abus et du manque de transparence de la puissance publique : – (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.
9	Communication - Données personnelles - CNIL	Informer les citoyens sur leurs droits vis-à-vis de leurs données personnelles. En plus d'un apprentissage sur le long terme à destination des 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.

10	**Communication FranceConnect**	**Engager FranceConnect 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.** En particulier, cette réflexion pourrait être l'occasion de remettre en lumière certains concepts centraux tels que : – Le fait qu'un fournisseur d'identité ne sait pas quel est le fournisseur de service qui est en train de l'appeler (et réciproquement) ; – Le fait que seules les données d'état civil (permettant d'éviter les personnes en doublons) et une adresse email sont communiquées entre fournisseurs d'identité et de services.
11	Formation des élus	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.
12	**Formation adultes**	**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 sur les thématiques suivantes :** – Hygiène informatique et de sécurité ; – Fonctionnement des services publics et gestion des informations dématérialisées ; – Multiplicité des identités numériques ; – Consentement et lisibilité des CGU.

13	**Formation continue**	**Créer un parcours de formation qui corresponde aux besoins de citoyenneté numérique pour les élèves de primaire et du secondaire**, jusqu'à l'âge de 15 ans correspondant à la majorité numérique selon la loi, afin que ceux-ci soient armés pour leurs premiers usages autonomes (inscription à Parcours Sup, au Crous…) en reprenant les axes proposés dans la recommandation 12.
14		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.

15	Transparence	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'offre 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)
16	Gouvernance partagée	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.
17	**Gouvernance sociétale**	**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) qui occuperait des missions :** – *a priori* pour évaluer les demandes des fournisseurs de services à accéder aux services du dites-le-nous-une-fois ou à FranceConnect et évaluer la légitimité de leur demandes d'informations. – *a posteriori* pour : – Évaluer les audits externes ; – Mettre à jour les programmes pédagogiques à destination des citoyens ; – Organiser des forums citoyens pour questionner la société civile sur la thématique et favoriser la participation citoyenne (cf. infra, 1.2.2.) ; – Saisir la CNIL pour sanctionner les fournisseurs d'identité ou de services qui ne respectent pas le cadre préalablement établi.

18	Gouvernance sociétale - Forum citoyens	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.
19	**Contrat pour les fournisseurs d'identité privés au titre d'une délégation de service public et consentement des usagers**	**Soumettre les fournisseurs d'identité privés** (en lien avec des fournisseurs de service publics) **à un contrat qui définisse la délégation du service public qu'ils effectuent en fonction du type d'action qu'ils prennent en charge** (par exemple, enrôlement physique, activation de certificats étatiques) et les outils sur lesquels ils s'appuient pour certifier les identités des citoyens. **Ce contrat 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. Le contrat de délégation de service public** devrait dès lors contenir : – Une obligation de mise en œuvre des moyens d'enrôlement inclusif ; – La formation des personnels en charge de l'enrôlement des populations au service d'identité numérique à l'éthique et l'inclusion (cf. supra, Chapitre I) ; – La formation des personnels en charge de l'enrôlement à la lutte contre définition des standards de mise en lisibilité et de compréhension des conditions générales d'utilisation selon plusieurs critères : lisibilité, version compréhensible par le grand public, test de lisibilité par des panels, emploi de la langue française facile à lire et à comprendre, information plus complète et non ambiguë sur la destination, les utilisations et destinataires des données ; – Le type de données transmises et stockées dans les relations entre le fournisseur d'identité et un service public ; – Le rappel de la possibilité de contrôle impromptu par la CNIL du fournisseur d'identité ; – La mise en place de contrôle *a posteriori* par la DINUM et l'ANSSI

20	Open data	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.
21	**Contrôle législatif**	**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.).**
22	Cadre règlementaire (1) mésusages	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.
23	« Dites-le nous une fois » et partage de données.	S'appuyer sur les recommandations du Conseil de 2015 soit : – « Permettre à chaque usager de visualiser les échang es 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. »

Axe 4 - Assurer une sécurité de tous

24	Souveraineté - Présence dans les instances supra nationales	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. .
25	Souveraineté - Capacité d'évaluation des technologies	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.
26	**Révision du règlement eIDAS**	– **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.**
27	Révision du règlement eIDAS	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.
28	**eIDAS - noeud d'interopérabilité**	**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 FranceConnect 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.**
29	eIDAS - niveau substantiel	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.
30	**Homogénéisation des niveaux de sécurité des démarches**	**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.** Cette doctrine pourrait être ensuite proposée au niveau européen en vue d'une possible harmonisation entre États membres.
31	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.

32	**Evaluation scientifique**	En complément des recommandations concernant l'implication de la communauté scientifique dans le processus de normalisation (cf. 1.1.), le Conseil souhaiterait remettre à l'ordre du jour une recommandation issue de son avis sur le fichier TES. Pour le Conseil, il est nécessaire que l**a communauté scientifique soit consultée, 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**
33	Souveraineté	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.
34	**TES - audits réguliers du système**	**Effectuer de manière régulière et impromptue des audits et des contrôles du fichier TES et des usages qui en sont faits par l'ANSSI et la CNIL.**
35	CNIe - certificats pour permettre la poursuite du Dites-le-nous une fois dans les parcours multicanaux	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).

Qu'est-ce que le CNNum ?

Le Conseil national du numérique est une commission consultative indépendante. Think-tank de l'intérêt général, 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 du CNNum
presse@cnnumerique.fr / 01 44 97 25 08