POLITIQUES, INSTITUTIONS ET DÉMOCRATIE

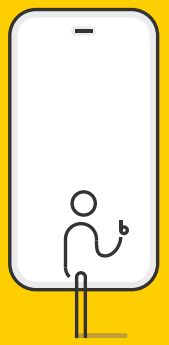
JANVIER 2019

IDENTITÉ NUMÉRIQUE : PASSER À UNE LOGIQUE CITOYENNE

RENAISSANCE numerique

TABLE DES MATIÈRES

INTRODUCTION



Alors que l'État soutient l'ambition d'une dématérialisation à 100% des services publics à horizon 2022[1], l'avènement d'un parcours d'identité numérique porté par l'État en France prend une dimension nouvelle.

L'identité numérique désigne ici l'attribution à une personne d'un identifiant unique sécurisé pour l'utilisation de l'ensemble des services en ligne nécessitant son authentification, et en particulier ses démarches administratives en ligne. Porté à l'échelle européenne dans le cadre du règlement sur l'identité numérique et les services de confiance, « eIDAS » (*electronic identification and trust services*)[2], il s'agit d'un projet de modernisation de l'administration aux implications potentiellement importantes, pour la vie publique et citoyenne, mais également pour le développement de l'économie et la confiance dans la transformation numérique de nos sociétés. Le règlement eIDAS vise à instaurer un mécanisme de reconnaissance mutuelle des moyens d'identification électronique des États membres sur l'ensemble des services en ligne des autres États membres. De nombreux modèles ont déjà été testés et mis en place en Europe, comme en Estonie, au Danemark, en Suisse, en Belgique ou en Allemagne, avec pour chacun ses particularités culturelles et de mise en application[3]. Le schéma d'identification électronique fait encore l'objet en France de débats techniques et juridiques importants, notamment quant à sa sécurisation, en vue d'aboutir à une proposition satisfaisante. Le 5 janvier 2018, Gérard Collomb, alors ministre de l'Intérieur, Nicole Belloubet, garde des Sceaux, et Mounir Mahjoubi, secrétaire d'État chargé du Numérique, ont signé une lettre de mission adressée à Valérie Peneau, inspectrice générale de l'administration, pour diriger l'équipe interministérielle chargée de conduire le programme visant à déployer un parcours d'identification numérique sécurisé, en vue de son ouverture et sa notifica-

1 « Dématérialisation, rémunération des fonctionnaires… la réforme de l'État dévoilée », Benoît Floc'h, *LeMonde.fr*, le 29 octobre 2018.

2 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 : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32014R0910&from=EN

3 Voir le Tableau 1 p 12.

tion à la Commission européenne à la rentrée 2019[4]. Il s'agit pour l'État de développer un dispositif stable et interopérable à l'échelle des administrations nationales et territoriales, et à l'échelle européenne, qui garantisse le respect des données générées par son utilisation, et apporte des garanties en termes de sécurité pour éviter notamment la fraude à l'usage.

Toutefois, au-delà de ces débats techniques indispensables, le déploiement attendu d'une identité numérique, dont le bénéfice pour les usagers semble clairement identifié par les acteurs en charge du projet, sera également conditionné par sa pertinence pour ses utilisateurs finaux : usagers de l'administration, citoyens, et peut-être à terme, consommateurs. Souvent éclipsée par les débats techniques et juridiques, la prise en compte de leurs attentes, au-delà du principe même de simplification des usages, conditionne pourtant le futur succès d'un tel dispositif.

DE L'IDENTITÉ À L'AUTHENTIFICATION : DES ENJEUX PREMIERS DE SÉCURITÉ

L'identité numérique fait référence à deux acceptions qu'il faut distinguer : d'une part l'existant, une identité numérique virtuelle « de fait », constituée de la somme des usages actuels de chaque individu en ligne ; d'autre part, un projet d'identité numérique « garantie », qui puisse permettre d'identifier avec certitude un déclarant au moyen d'un identifiant unique.

Pour atteindre cet objectif, des garanties de sécurité, de fiabilité et d'intégrité des données partagées sont nécessaires et établies en proportion des risques encourus pour chaque usage. Le règlement européen eIDAS[5] a imposé une classification des moyens mis en œuvre pour sécuriser une authentification en ligne. Cette classification comporte trois niveaux de sécurité : faible, substantielle et élevée.

Sont considérés comme « faibles » par la classification du règlement des moyens d'authentification qui ne nécessitent que la connaissance d'un identifiant ou d'un mot de passe. Faciles à usurper, ils présentent donc des risques de fraudes, ponctuelles ou massives, d'usurpation ou d'altération de l'identité. Une identité numérique « garantie » doit pouvoir permettre d'identifier objectivement et avec certitude une personne civile, via des processus homologués de sécurisation et de fiabilisation des données transmises, pour des actes plus sensibles (dans ses relations avec l'administration fiscale, son assurance maladie, etc.). L'exigence de sécurité dans ces cas est plus sécurisée. Une identification allant de « substantielle » à « élevée » du déclarant est alors nécessaire en vue de limiter et d'empêcher le risque d'utilisation abusive ou d'altération de l'identité, et appelle à des mesures d'authentification plus importantes. Dans le premier cas, on pourra par exemple exiger, en plus de la connaissance de l'identifiant et du mot de passe, la connaissance d'un secret ou la possession d'un objet (par exemple les trois chiffres de sécurité de sa carte bancaire) ou encore un mot de passe à usage unique (OTP - *one-time password*). Dans le second, pour une identité « élevée », on exigera la reconnaissance d'une preuve la plus inaltérable et infalsifiable de l'identité du déclarant. Par exemple, ses empreintes digitales ou rétiniennes, ou tout autre attribut biologique d'identité ultra personnalisé.

4 « Mise en place de solutions d'identité numérique sécurisée : lancement d'un programme », communiqué de presse commun de Gérard Collomb, ministre de l'Intérieur, de Nicole Belloubet, garde des sceaux, ministre de la Justice et de Mounir Mahjoubi, secrétaire d'État chargé du Numérique, le 5 janvier 2018.

5 Décryptage du règlement eIDas sur le site de l'ANSSI.

PÉRIMÈTRE DE L'IDENTITÉ NUMÉRIQUE : QUELLE AMBITION ?

En moyenne, chaque Français dispose de plusieurs dizaines d'identifiants en ligne, créés auprès de services de messagerie, de plateformes sociales, de sites marchands, de médias, de comptes administratifs, et plus encore selon les profils. Mais cet état de fait offre des garanties de sécurité à la fiabilité aléatoire et peu compatibles avec des exigences régaliennes d'identification et d'authentification. Pour comprendre l'identité numérique, il faut mesurer le périmètre de son ambition et le bénéfice qu'elle entend apporter à ses futurs usagers.

L'identité numérique unique adresse dans un premier temps des enjeux de simplification et de dématérialisation des démarches administratives :

- aux niveaux national et européen pour les contrôles aux frontières, la police et la justice, le vote des Français à l'étranger, etc. ;
- au niveau national pour ce qui relève de la relation avec les administrations, les impôts, l'Assurance maladie, Pôle emploi, les allocations sociales, etc. ;
- au niveau des collectivités territoriales pour ce qui relève de l'éducation, les services municipaux : crèches, écoles, état civil, bibliothèques, cantines scolaires, inscription sur les listes électorales, etc.

Elle pourrait ainsi générer de nouveaux usages et proposer à terme des fonctionnalités qui participeraient à redynamiser la vie publique, en capitalisant sur la confiance acquise dans son utilisation. En ce sens, des démarches sont déjà en œuvre dans le champ de la concertation.

Au-delà des administrations, l'identité numérique pourrait également constituer un relai fiable à l'identification en ligne auprès de l'ensemble des acteurs publics, privés et marchands, qui s'appuient sur une identification sécurisée pour leurs transactions. À ce titre, elle viendrait en alternative des dispositifs déjà existants mais fragmentés entre chaque acteur.

Dans le débat en cours, les parties prenantes du parcours d'identification numérique ne s'accordent pas nécessairement sur le périmètre de cette ambition. La dématérialisation annoncée du service public offre une rampe de lancement idéale pour le déploiement de l'identité numérique, qui pourrait donner du sens à cette démarche du point de vue des usagers. Les enjeux d'adoption sont donc d'abord liés au succès de cette dernière et son adéquation avec les usages attendus. Si aujourd'hui la mission semble se concentrer principalement sur ce périmètre, de nombreux acteurs anticipent déjà un développement ultérieur pour de nombreux services privés qui requièrent une identification sécurisée forte.

Le développement du parcours d'identification numérique pourrait ainsi permettre de faciliter la création de nouvelles offres, plus personnalisées, par l'ensemble des acteurs de l'économie. Par exemple, des offres de mobilité dites « MAAS » (*mobility as a service*), articulées autour de comptes personnalisés et hybrides de mobilité. Des territoires ont lancé des projets en ce sens, afin de combiner l'accès indistinct à des vélos, bus, tramways, covoiturages et autres moyens de transports et de simplifier les abonnements gérés par les collectivités.

UN DÉBAT ANCIEN QUI A EU DES DIFFICULTÉS À ÉMERGER TECHNIQUEMENT EN FRANCE

Vingt-trois États membres de l'Union européenne ont mis en place une identité numérique, dont la Finlande (la première en 1999), l'Allemagne, le Danemark, la Belgique et l'Estonie[6]. Alors que la France s'annonçait pionnière en 1997, avec l'annonce du programme d'action gouvernemental pour la société d'information (PAGSI) porté par le gouvernement de Lionel Jospin[7], le projet a eu plus de difficultés à émerger en pratique. Cette histoire chaotique a notamment été marquée par cinq initiatives qui ont toujours achoppé, que ce soit en raison de doutes vis-à-vis des conditions de sécurité déployées ou d'un manque de clarté autour du périmètre des différents projets et de leurs ambitions.

Un des premiers avatars de l'identité numérique avait été le programme public INES (Identité Nationale Électronique Sécurisée) en 1999, qui, outre le passeport biométrique, intégrait également une carte d'identité électronique offrant un accès à des services web. Ce deuxième volet a été abandonné en juin 2005. Mais le sujet a été relancé avec le projet de loi « protection de l'identité » en 2010, soutenant l'introduction dans la carte d'identité nationale de deux puces électroniques, l'une dite « régalienne », lisible uniquement par des agents de l'État habilités, l'autre facultative dite « vie quotidienne », qui incluait des services plus courants. La proposition de loi qui en a découlé a été censurée partiellement par le Conseil constitutionnel en 2012, en raison d'incertitudes quant à la sécurité et la vocation des données rassemblées par le dispositif.

Le projet pilote IdeNum (en partenariat avec la Caisse des dépôts, SFR, La Poste, le Crédit Mutuel-CIC et Les PagesJaunes/Solocal) lancé parallèlement à la loi « protection de l'identité » en 2010, et relancé en 2013, a repris le flambeau avec une ambition plus mesurée, avant d'être à nouveau abandonné en 2015 pour se fondre avec l'actuel FranceConnect, piloté à l'époque par le secrétariat général pour la modernisation de l'action publique (SGMAP).

6 Voir le Tableau 1 p 12.

7 Le gouvernement a lancé en 1997 le Programme d'action gouvernemental pour la société d'information (PAGSI), 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 dès 2000, principalement à destination des entreprises.

Le dispositif FranceConnect, qui a fait l'objet récemment d'un arrêté précisant son périmètre et ses usages[8], permet à l'usager d'utiliser l'identité numérique d'un fournisseur d'identité partenaire (notamment impots.gouv.fr, Ameli, La Poste, et les deux derniers arrivés, la Mutualité Sociale Agricole et Mobile Connect et moi) pour s'authentifier directement auprès des fournisseurs de services acceptant le bouton FranceConnect. En septembre 2018, FranceConnect revendiquait 6 millions d'utilisateurs inscrits et 350 fournisseurs de services partenaires[9].

Le cadre réglementaire pour la conception d'une architecture de réseau qui puisse délivrer une identité numérique fonctionnelle pour les citoyens existe. La volonté politique, maintenue depuis plusieurs années et pressante à mesure que l'agenda numérique européen se resserre, ne manque pas au gouvernement. Cependant, ce dispositif ne pourra remplir sa mission qu'à la condition d'être adopté par le plus grand nombre. Présents dans les discours, les citoyens semblent aujourd'hui éclipsés de sa conception. En interrogeant les conditions de son adoption, cette note vise ainsi à dépasser le débat autour de la stricte ingénierie technique de l'identité numérique, pour se pencher sur les attentes et le rôle des citoyens dans ce déploiement.

8 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, publié au Journal officiel.

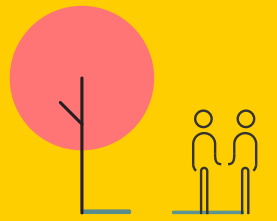
9 « *6 millions d'utilisateurs pour FranceConnect* », Mission Société Numérique, le 13 septembre 2018.

TABLEAU 1 : LES DISPOSITIFS D'IDENTITÉ NUMÉRIQUE EN EUROPE (BELGIQUE, DANEMARK, ESTONIE, SUÈDE, SUISSE)

	Belgique	Danemark	Estonie	Suède
Type de support(s) utilisé(s)	Depuis 2003 : carte d'identité électronique (obligatoire dès 15 ans) Depuis 2016 : l'application « *Itsme* » a permis le développement des usages en facilitant l'authentification sur smartphone	Depuis 2004 : numéro CPR (*Civil Registration System*), numéro unique donné à la naissance ou lors de l'installation dans le pays	Depuis 2002 : carte d'identité électronique obligatoire	Depuis 2002 : certificats électroniques distribués aux citoyens par six banques, le service de courrier postal suédois et un opérateur télécom
Adoption	99,85 % des plus de 12 ans	94 % des citoyens âgés de plus de 15 ans	98 % des habitants	+ de 7,5 millions d'utilisateurs actifs, soit près de 75% de la population

PARTIE 1

L'IDENTITÉ NUMÉRIQUE AU SERVICE D'UNE VIE PUBLIQUE RENOUVELÉE



UNE OPPORTUNITÉ POUR SIMPLIFIER LA RELATION AVEC LES ADMINISTRÉS

L'identité numérique a d'abord l'ambition d'accélérer la dématérialisation de la relation avec les administrations. Ce sujet renvoie directement à la réforme et à la modernisation de l'État, dans la lignée du « Grand Plan d'Investissement 2018-2022 », remis par Jean Pisani-Ferry au Premier ministre en septembre 2017, et qui prévoit de consacrer 1,9 milliard d'euros pour dématérialiser les démarches administratives[10]. C'est une thématique à double entrée : d'un côté, il y a un enjeu de simplification du millefeuille administratif et d'économies budgétaires ; de l'autre, une prise en compte de l'évolution des usages au profit de l'expérience des bénéficiaires. En ligne de mire : une meilleure accessibilité par la qualité de service rendu au citoyen, plus fluide et engageante, vers plus de personnalisation.

LA RELATION À L'ADMINISTRATION N'EST PLUS « GÉNÉRALISTE »

De fait, les attentes des administrés ont évolué sur l'ensemble des services dont ils peuvent bénéficier dans leur vie quotidienne, en écho à l'évolution de leurs usages sur Internet. Les services développés en ligne, et les équipements qui permettent de s'y connecter, ont connu une croissance phénoménale depuis 15 ans. Un constat que corrobore les chiffres du gouvernement qui avance que près de deux tiers des Français (65%) utilisent Internet pour réaliser leurs démarches administratives ou fiscales[11]. En découlent de nouveaux standards autour de la simplicité d'usage, de la fluidité dans les opérations et une rapidité d'exécution qui rendent archaïques d'autres lourdeurs administratives. Le projet d'identité numérique incarne ce changement de paradigme vers une exigence nouvelle de facilitation du service public. L'État doit être en mesure de fournir à chacun une qualité de service égale et digne, quel que soit le dispositif d'identité auquel l'usager a recours pour effectuer sa démarche. Dans cette lignée, la réalisation des démarches en présentiel doit elle-même être réinventée, alors qu'elle reste indispensable en termes d'inclusion pour accompagner les publics dans leurs usages, notamment les populations les plus éloignées du numérique. À ce titre, notons que pour la première fois cette année[12], la proportion des individus qui accomplissent les démarches administratives en ligne est en baisse : - 2 points par rapport à 2017[13].

En termes de conception, il s'agit bien de placer les usages au centre du futur parcours d'identification numérique. Cette évolution de paradigme doit néanmoins se garder de tomber dans l'écueil d'une relation trop consumériste vis-à-vis du service public, qui dénaturerait ou banaliserait le rapport à l'État, ou donnerait le sentiment de ne plus responsabiliser le citoyen face au caractère particulier de la relation qu'il entretient avec la chose publique.

FRANCECONNECT, UNE PREMIÈRE ÉTAPE

Les développements de FranceConnect semblent offrir des résultats satisfaisants en termes d'usage. Ce dispositif pose les bases d'une expérience du service public qui ne s'appuie pas simplement sur des considérations réglementaires et en rend l'accès plus intuitif. Néanmoins, chacun des sites qu'il rassemble offre une expérience de navigation hétérogène, qui trahit un besoin de coordination plus important entre les administrations qui s'y agrègent. Ce qui, au-delà du processus d'identification, invite à repenser le parcours d'usage à la faveur de plus d'homogénéité entre toutes les administrations.

Par ailleurs, la visibilité du dispositif reste relativement faible auprès des Français. Selon une étude conduite par l'IFOP pour Renaissance Numérique en avril 2018, le taux de notoriété de l'outil et encore plus son taux de connaissance, demeurent relativement bas.

15%

FranceConnect demeure ainsi un objet inconnu pour la grande majorité des répondants (59 %) et seuls 15% savent précisément de quoi il s'agit.

10 « L'État 100% numérique de Macron coûtera 9,3 milliards d'euros », Sylvain Rolland, *LaTribune.fr*, le 26 septembre 2017.

11 « Baromètre du numérique 2018 », Agence du Numérique, Autorité de Régulation des Communications Électroniques et des Postes (ARCEP) et Conseil Général de l'Economie, de l'Industrie, de l'Energie et des Technologies (CGE), décembre 2018.

12 « Baromètre du numérique 2018 », Agence du Numérique, Autorité de Régulation des Communications Électroniques et des Postes (ARCEP) et Conseil Général de l'Economie, de l'Industrie, de l'Energie et des Technologies (CGE), décembre 2018.

13 « Baromètre du numérique 2018 », Agence du Numérique, Autorité de Régulation des Communications Électroniques et des Postes (ARCEP) et Conseil Général de l'Economie, de l'Industrie, de l'Energie et des Technologies (CGE), décembre 2018.

Au-delà de leur adéquation aux usages, cela nous invite également à interroger les modalités de diffusion de ces dispositifs auprès des publics.

DE LA NÉCESSITÉ DE MUTUALISER LES RESSOURCES ET LES BONNES PRATIQUES ENTRE LES ADMINISTRATIONS

Une meilleure circulation des informations et des bonnes pratiques entre les administrations est nécessaire pour aboutir à une offre de services homogène en amont du déploiement de l'identité numérique. Cette dernière exige en effet une articulation des offres entre les administrations, jusqu'aux collectivités territoriales. L'annonce récente[14] de la création de la plateforme Tech.Gouv, présentée comme le premier réseau social qui réunit les « forces numériques » de l'État, semble aller dans ce sens. Dans son parcours en ligne, l'usager ne distingue pas nécessairement les différents échelons de l'administration engagés. Le cloisonnement entre administrations derrière l'interface ne doit donc pas contrevenir à la fluidité de son parcours. C'est d'ailleurs toute l'ambition de l'État plateforme, mais qui peine dans sa mise en œuvre car cela appelle à réorganiser tous les systèmes d'information construits en « silos ministériels ». Cette homogénéisation des parcours d'usage doit également permettre à terme l'optimisation des informations sur les bénéficiaires entre les services publics[15] et donc la création de services dématérialisés plus adaptés à la situation de chacun, en fonction de son statut et de ses besoins précis. Toutefois, cela passera nécessairement par le consentement explicite des citoyens et une attention devra être portée quant au besoin de la fragmentation de ces informations, afin de résoudre l'appréhension liée à leur centralisation.

14 « Lancement de Tech.Gouv et nominations du directeur du numérique de l'État et de l'ambassadeur pour le numérique », ministère de l'Économie et des Finances et ministère de l'Action et des Comptes publics, le 24 octobre 2018.

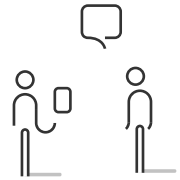
15 Sous réserve de conditions exemplaires de protection des données personnelles. Les conditions de sécurité des données sont validées par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et les processus d'anonymisation des données personnelles par la Commission nationale de l'informatique et des libertés (CNIL).

« DÎTES-LE-NOUS UNE FOIS »

Le principe du « *Single Sign On* », ou du « Dîtes-le-nous une fois », incarne bien cette plus-value d'usage pour l'administré. Il suffira de renseigner une première fois ses informations sur le site d'une administration, pour ne plus avoir à les renseigner par la suite auprès des autres administrations.

Concrètement, cela signifie pour le citoyen de ne pas avoir à fournir plusieurs fois des informations déjà détenues par l'administration. Cela permet par exemple l'accès à de nouveaux services comme le pré-remplissage des formulaires administratifs. Au-delà de la plus-value en termes de parcours pour l'usager, cela répond également avec la dématérialisation afférente, aux enjeux d'engorgement des guichets, qui deviennent ainsi plus accessibles pour des demandes plus sensibles à traiter. C'est aussi la possibilité pour le citoyen d'envoyer ou de recevoir ses documents ou ses données directement en ligne dans un coffre-fort numérique, qui aura la même valeur juridique qu'un document remis en présentiel.

À terme, un identifiant unique pourrait également servir à s'authentifier auprès de services qui remplissent une mission de service public, par exemple les régies de transports.



LE PROJET
GRAND LYON CONNECT

Le projet Grand Lyon Connect[16], lancé à Lyon en décembre dernier, témoigne de cette volonté de permettre à l'usager de pouvoir passer d'un portail de services à un autre sans avoir à re-signer. Cette simplification participe du développement de services à valeur ajoutée dans des domaines administratifs variés, et à tous les échelons du service public, par exemple :

- **la gestion de l'état civil**
  actes de naissance, mariages, divorces, adoption, décès, renouvellement de documents d'identité déclarés volés ou perdus, etc. ;
- **la santé**
  via notamment le dossier médical partagé, un carnet de vaccination en ligne, des ordonnances électroniques, des radiographies dématérialisées, etc. ;
- **la justice**
  pré-plainte en ligne, etc.[17] ;
- **l'éducation**
  signature électronique des parents sur des bulletins de notes électroniques, inscription aux examens, aux concours, certifications, diplômes, etc. ;
- **les collectivités territoriales**
  l'inscription sur les listes électorales, la gestion des services municipaux (crèches, écoles, bibliothèques, cantines scolaires, collecte de déchets...), etc. ;
- **le notariat et les professions juridiques**
  le traitement des actes à distance auprès des notaires, magistrats, avocats, huissiers, etc.

16 https://moncompte.grandlyon.com/login/?next=/accounts/

17 Le projet de loi Justice 2018-2022 actuellement en débat au Parlement vise à permettre notamment un « *règlement dématérialisé des petits litiges de la vie quotidienne* » pour l'ensemble du territoire national : « *Une procédure entièrement dématérialisée pourra se tenir pour certains litiges. Les justiciables pourront obtenir une décision dans un délai rapide, l'ensemble des échanges s'effectuant de manière dématérialisée* ». Ces services recoupent par exemple le fait de pouvoir porter plainte et de se porter partie civile par voie dématérialisée. « Projet de loi de programmation 2018-2022 et de réforme pour la Justice », Ministère de la Justice, Dossier de presse, avril 2018 : http://www.justice.gouv.fr/art_pix/dp_pjl_justice.pdf

L'IDENTITÉ NUMÉRIQUE PORTE LA PROMESSE D'UNE RELATION FACILITÉE AVEC L'ADMINISTRATION ET LES ÉLUS

VERS DE NOUVEAUX USAGES CITOYENS

Les opportunités de simplification sont nombreuses, mais attention à ne pas se reposer exclusivement sur la seule dimension technique. Pour envisager la modernisation du service public et son acceptabilité par les citoyens, il convient de donner du sens à ce processus, et imaginer un parcours d'identification numérique qui réinvente la relation avec l'État et les collectivités. À ce titre, il faut rappeler que l'identité numérique adresse dans un premier temps les pratiques de l'usager-consommateur, dans le cadre de la dématérialisation des services publics d'abord, mais également potentiellement en vue d'une utilisation plus large de l'identité numérique par des acteurs privés et marchands. Son périmètre a également vocation à s'élargir aux pratiques citoyennes, à l'instar du champ de la concertation. En assurant l'identité des participants, et donc l'intégrité du vote, à l'échelle locale ou nationale, elle pourrait permettre de garantir et de généraliser le recours aux dispositifs participatifs en ligne[18].

RÉINVENTER LA PROXIMITÉ

La diminution du recours au guichet, implicite dans le cadre du projet de numérisation des services publics et d'identité numérique, implique aussi une transformation de la présence des administrations sur l'ensemble du territoire. Réinventer ce rapport autour d'une expérience plus fluide et partagée avec les institutions doit inviter à redéfinir le cadre de la proximité, si l'on veut éviter l'écueil d'un consumérisme désincarné du service public. La dématérialisation appelle à une nouvelle organisation territoriale, dans laquelle la puissance publique doit repenser sa présence et sa valeur ajoutée. La politique actuelle d'État plateforme apporte un service public dématérialisé qui vient « d'en haut ». Cependant, à l'échelon local, tous les agents et les administrés, ne sont pas également compétents et équipés pour appréhender ces dispositifs. La dématérialisation menace de désœuvrer en partie les agents,

18 « Démocratie : le réenchantement numérique ? », Renaissance Numérique et Fondation Jean Jaurès, mars 2017.

qui doivent réinventer les modalités de leur action pour ne pas perdre le lien avec les administrés. Le numérique apporte cette faculté de pouvoir accéder à des services à distance, sans avoir à se déplacer. Avec une identité numérique sécurisée, ce phénomène pourrait s'accélérer. La question de l'accompagnement est nécessaire, autant qu'une réflexion sur la manière dont ces dispositifs peuvent servir à revivifier la relation des citoyens avec les services publics.

Dans cette optique, les élus et les agents doivent être mis à contribution pour repenser cette proximité et la valeur ajoutée de la puissance publique, car ils ont une vision très opérationnelle des besoins des citoyens et du rôle des services publics dans leurs territoires. La modernisation de l'action publique ne doit pas se faire au détriment de cet historique. La culture administrative n'est pas « agile ». À ce titre, les start-ups d'État ont beaucoup à faire pour diffuser une « culture du produit » au sein des administrations. Il s'agit de rester chevillé au plus près des besoins des usagers pour viser juste et assurer un service efficace, mais également et surtout qui puisse susciter la confiance des usagers.

VOIR LA SOCIÉTÉ TELLE QU'ELLE EST

L'identité numérique incarne la rencontre entre deux cultures de l'offre de service. D'un côté, les concepteurs de fonctionnalités numériques très compétents sur les dimensions techniques et les cycles de vie d'un produit ont pour eux cette culture « moderne » des usages, qui est primordiale, qui alimente depuis plusieurs années la dématérialisation des services marchands, qui bénéficient déjà d'une utilisation massive de dispositifs d'identification numérique. De l'autre, les agents publics, porteurs du sens du service public, doivent monter en compétence et réinventer leur rôle pour conserver le lien avec les administrés.

La volonté de simplification et de modernisation portée par l'identité numérique ne doit pas être aveugle aux réalités du terrain. Il faut voir la société telle qu'elle est, à la fois physique et numérique. Garder en tête la préservation du lien avec l'administration à toutes les étapes de la vie du citoyen est essentiel. La généralisation de l'identifiant numérique est l'opportunité de penser la société autour d'écosystèmes de proximité hybrides, à la fois physiques et en ligne. Cela permettra de donner du sens au déploiement et à une adoption progressive d'une identité numérique qui ne soit ni anxiogène ni exclusive.

Les usages citoyens de l'identité numérique

PERSONNALISER LA RELATION AVEC L'USAGER-CITOYEN

La circulation des informations entre les administrations permettra le développement de la personnalisation de la relation de l'usager aux services publics.

> « *Dans les données associées à l'usager, il peut y avoir des éléments de préférences. Aujourd'hui, les administrations s'organisent de manière très verticale. Il faut trouver LA page dans le site Internet qui recense le service auquel l'on veut accéder, idem pour les lignes de bus ou du Vélo'v*[19]*. Ce que l'on doit viser, c'est que l'usager puisse constituer lui-même son propre tableau de bord. L'enjeu est de lui présenter des données et des éléments contextualisés par rapport à ses intérêts, après soumission à son consentement.* »
>
> Hervé Groléas
> Directeur des systèmes d'information à la métropole de Lyon

La possibilité de cette personnalisation semble être la clé du développement massif de l'usage par les citoyens. Pour l'assurer, il faut également pouvoir garantir les conditions de cette personnalisation, que l'usager puisse avoir confiance dans le parcours d'identification numérique, et qu'il lui soit présenté de manière à ce qu'il puisse facilement l'intégrer.

19 Vélo'v désigne le système de vélos en libre-service mis en place dans la métropole de Lyon depuis 2005.

PARTIE 2

VERS L'ADOPTION DE L'IDENTITÉ NUMÉRIQUE

Le succès du service sera finalement sanctionné par son appropriation. Le projet d'identité numérique se situe au confluent d'enjeux multiples pour le développement du numérique et la transformation de notre société. En ce sens, il ne peut être un objet conçu que par « en haut », dont les indicateurs de succès seraient établis à l'aune de l'enthousiasme des parties prenantes à son développement. Le citoyen doit trouver sa place dans ce processus et appréhender la pertinence de ce projet.

LA CONFIANCE AU CŒUR DE L'ADOPTION

Pour encourager le développement de l'identité numérique, il faudra qu'elle soit utile, mais également que l'on puisse s'y fier. Il faut qu'elle inspire confiance et donc que l'on sache l'appréhender. Les détails techniques des architectures de réseaux qui garantiront la sécurité des données ne seront pas à la portée de la plupart des utilisateurs. Par ailleurs, l'informatique, comme le papier, ne sont pas des systèmes infaillibles en termes de sécurité. Quel que soit le parcours d'identification numérique qui sera développé et la nature de ses supports, il faudra assumer sereinement qu'une marge de risque existe toujours et savoir partager cette dimension avec les citoyens. La confiance provient de celui qui la délivre et non de l'outil technologique.

Par ailleurs, pour accepter cette marge, il faut que les usagers puissent avoir confiance dans l'objectif poursuivi par ce parcours d'identification numérique et donc savoir y donner un sens.

COMMENT PRÉSENTER L'IDENTITÉ NUMÉRIQUE AU CITOYEN ?

Si la confiance est un prérequis à l'adoption de tout dispositif, et ce au-delà même de l'identité numérique, il faut ensuite envisager sa stratégie de déploiement et notamment la manière dont elle sera présentée au citoyen. Il s'agit là d'un élément également soumis à des choix de confiance et de sécurité, mais qui ne peut s'y résumer.

À QUEL MOMENT ATTRIBUER UNE IDENTITÉ NUMÉRIQUE ?

Si l'on souhaite donner un sens citoyen à l'identité numérique, elle doit s'inscrire dans le parcours du citoyen. Il y a des moments clés pour créer une identité numérique : naissance, entrée à l'école, Journée défense et citoyenneté (JDC), inscription sur les listes électorales, etc. Il faut imaginer une attribution souple, qui prenne en compte les besoins d'identification du citoyen, tout en le préservant d'un recueil trop précoce de ses données. Il doit mesurer l'utilité citoyenne du dispositif.

À ce titre, de vifs débats ont eu lieu récemment en France autour de la majorité numérique, dans le cadre de la transposition au niveau national du Règlement général sur la protection des données (RGPD)[20]. La loi française fixe désormais à 15 ans l'âge à partir duquel un mineur peut consentir seul au traitement de ses données. En dessous de cet âge, le consentement de ses parents sera nécessaire. Par la définition de cet âge limite, le législateur souhaitait harmoniser la loi française qui fixait notamment déjà à 15 ans la majorité sexuelle. Le règlement européen autorisait les États membres à définir un seuil entre 13 et 16 ans, 13 ans correspondant en particulier à l'âge minimum requis sur les principales plateformes sociales pour se créer un compte.

Quel que soit le dispositif choisi, l'attribution doit s'inscrire de manière cohérente dans le parcours du citoyen. Mais cette identité doit également trouver une manière naturelle de s'incarner auprès de ses usagers, ce qui correspond à un double enjeu d'appropriation et de sécurité.

20 « Données personnelles : rendre ces droits effectifs », Renaissance Numérique, *Digital Society*, mai 2018.

INCARNER L'IDENTITÉ NUMÉRIQUE

L'identité numérique s'incarne principalement par un identifiant unique (à la suite d'une identification de la personne) et un mot de passe sécurisé (authentification en ligne), qui nous indiquent les informations personnelles requises pour accéder aux services proposés sur les sites que nous visitons. Mais certaines opérations qui nécessitent une vérification de sécurité supérieure, conformément à la classification du règlement eIDAS, peuvent demander d'avoir recours à un objet possédé pour valider l'authentification.

Les pays européens qui ont adopté l'identité numérique lui ont prêté des supports différents : clé USB, smartphone, carte d'identité électronique. Ces supports peuvent être fondés sur des normes ou standards nationaux et internationaux ou sur des technologies propriétaires, qui en garantissent la conformité avec un cahier des charges national, européen ou international. Une solution d'identité numérique faisant référence à un même standard permettrait d'offrir une interopérabilité entre ces services partout dans le monde[21].

L'ÉTAT, GARANT DE L'IDENTITÉ NUMÉRIQUE ?

L'État pourrait sembler le mieux placé pour assurer la confiance dans les objectifs poursuivis. L'identification de ses citoyens relève de ses prérogatives régaliennes. C'est par exemple le ministère de l'Intérieur qui définit les conditions de résidence et d'appartenance du citoyen dans l'espace national, et par extension européen. Mais il ne faut pas oublier, d'une part, les coûts de mise en œuvre d'un tel dispositif et la rapidité d'exécution nécessaire à son adoption et, d'autre part, la défiance que les Français entretiennent vis-à-vis de leurs institutions[22] avec le risque d'une centralisation excessive des données, en particulier pour les usages du secteur privé. L'État doit ici pleinement jouer sa fonction d'État plateforme, c'est-à-dire non pas un État qui centralise, mais qui structure, fédère, ouvre, sécurise les dispositifs d'identité numérique. Il en va d'un enjeu d'acceptabilité pour les citoyens.

21 « Identité Numérique : la révolution invisible », Pascal Agosti, *Usine Digitale*, le 5 octobre 2018.

22 À ce titre, il est toujours intéressant d'observer le classement sur l'indice de perception de la corruption de Transparency international. La France était 23ème en 2017, et 11ème au niveau européen.

Certains pays ont fait le choix de fragmenter les supports de l'identité numérique, en en confiant la mission à différents opérateurs mandatés par la puissance publique, de sorte à éviter la constitution d'une base centrale d'informations sur les citoyens, potentiellement exhaustive. Cette base présenterait par ailleurs des risques de sécurité et de souveraineté pour l'État.

Un tel fichier existe pourtant déjà, il s'agit du fichier TES (Titre électronique sécurisé), que Bernard Cazeneuve, alors ministre de l'Intérieur, avait fait adopter par décret[23] en novembre 2016 et qui avait déclenché un tollé auprès de l'opinion publique. Il s'agit de la réunion de deux fichiers existants : celui des demandes de renouvellement de cartes d'identité avec celui déjà utilisé pour les passeports depuis 2008[24]. Le gouvernement s'était néanmoins défendu de vouloir utiliser un tel fichier pour authentifier les personnes sur des services tiers, une disposition qui aurait ravivé l'ire du Conseil constitutionnel. Ce dernier avait en effet en partie basé son argumentaire de censure du projet de loi « protection de l'identité » en 2012, sur le manque de clarté autour de l'utilisation des informations rassemblées dans ce type de « méga fichier » par des acteurs tiers, notamment à des fins d'authentification.

Par ailleurs, la puissance publique n'apparaît pas suffisamment équipée pour déployer cette identité, au moment où ses agents voient leurs habitudes transformées et leurs effectifs se réduire. Le Plan Préfectures Nouvelle Génération[25] (PPNG), qui vise à réaliser des économies d'échelle dans l'organisation territoriale, a ainsi recentré l'activité des préfectures et sous-préfectures sur quatre missions : la gestion des crises, la lutte contre la fraude documentaire, l'expertise juridique et le contrôle de légalité, et la coordination territoriale des politiques publiques. Des dispositions qui accentuent la fermeture des guichets administratifs sur le territoire.

23 Décret n° 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité.

24 « Qu'est-ce que le système TES ? », interieur.gouv.fr, le 17 janvier 2017.

25 Voir à ce sujet la présentation du Plan Préfectures Nouvelle Génération sur le site du ministère de l'Intérieur : https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Plan-Prefectures-Nouvelle-Generation

LE RÔLE DE L'ÉTAT DANS LE DÉPLOIEMENT DE L'IDENTITÉ NUMÉRIQUE

Si la (co)conception et sa garantie doivent lui appartenir, l'essaimage de l'identité numérique ne repose pas qu'entre les mains de la puissance publique. L'État se positionne donc plus en définisseur du cahier des charges et garant du respect des procédures qui encadreront le dispositif d'identité numérique. Les supports d'identité mentionnés plus haut peuvent être émis par des opérateurs privés ou qui assurent une mission de service public. Le maillage territorial de leur activité reste pour chacun le premier atout de leur positionnement, qu'il s'agisse des banques, des opérateurs télécoms ou du service postal. L'identité numérique peut également être portée par des fédérations de métiers comme les notaires et les professions réglementées ou la confédération des buralistes. Néanmoins, il n'est pas évident que chacun de ces acteurs ait un intérêt à jouer un rôle dans ce déploiement.

En Belgique, banques et opérateurs télécoms se sont fédérés pour lancer le programme *Itsme*, qui permet de s'identifier sur Internet avec un identifiant unique (sites marchands, banques, services publics). Ce programme faisait suite à l'échec de la mise en œuvre de la carte nationale d'identité électronique, qui a pâti d'une faible utilisation du fait d'un usage trop contraignant. Elle obligeait en effet chaque citoyen à s'équiper d'un lecteur payant pour pouvoir l'utiliser en ligne. Le programme *Itsme* initié par le consortium Belgian mobile ID[26] (trois opérateurs de téléphonie et réseaux mobiles et quatre banques), avec la coopération des administrations publiques, visait ainsi à offrir un parcours d'identification numérique plus adapté

Dans plusieurs pays européens, les services des postes jouent également un rôle important dans le déploiement et l'adoption de parcours d'identification numérique. Au Danemark, l'initiative postale *e-Boks*, intégrée à *Digital Post*, la plateforme de poste électronique sécurisée de la poste danoise, constitue aujourd'hui un usage phare du *NemID* (bientôt *MitID*), l'identité numérique danoise, avec près de 4,3 millions d'utilisateurs en 2017[27]. De même en Suisse, est utilisée la *Swiss Post Box*, la boîte à lettre électronique sécurisée, accessible avec *SwissID*.

26 https://www.belgianmobileid.be/fr

27 https://joinup.ec.europa.eu/document/denmark-improves-user-experience-its-digital-post-solution-skat-nemid

Pour le citoyen, le meilleur choix est celui de l'opérateur qui inspire le plus de confiance et de transparence dans sa relation. C'est également le dispositif qui viendra le plus naturellement rejoindre ses usages existants, où qui offrira des interfaces de proximité familières. L'investissement technique est à la portée de beaucoup d'entreprises. Il reste en revanche important de bien identifier l'intérêt économique des acteurs qui souhaitent la porter, et les garanties qu'ils offriront vis-à-vis de la protection des données qu'ils manipuleront.

L'APPROPRIATION EST AUSSI UN ENJEU D'INCLUSION

L'identité numérique se trouve également au confluent de problématiques préexistantes relatives à l'inclusion numérique. Son effet est ambivalent sur ces problématiques : si elle peut éloigner du service public à cause d'une expérience trop aride de l'interface, voire d'un non accès à cette dernière, elle peut aussi gommer certains stigmates de l'exclusion sociale, associés à la démarche au guichet[28]. Son effet incitatif supposé sera notamment à vérifier au moyen d'indicateurs de non-recours au droit et de perception des prestations sociales. L'obstacle réside souvent d'ailleurs moins dans le support numérique, que dans la relation aride et anxiogène avec l'administration, qu'elle soit dématérialisée ou non.

La complexité des expériences de navigation sur les sites web des institutions publiques complexifie les démarches administratives pour beaucoup de Français.

> *« Ce sont la brutalité des courriers et la difficulté de faire le lien avec un agent par téléphone qui accentue l'exclusion et éloigne du numérique »*
>
> Dominique Pasquier
> Sociologue[29]

Un constat valable pour l'ensemble de la population, mais qui accentue l'exclusion des ménages modestes.

28 Voir le rapport sur la dématérialisation de la prime d'activité de la Direction générale de la cohésion sociale en 2017.

29 *L'Internet des familles modestes. Enquête dans la France rurale*, Dominique Pasquier, Presses des Mines, 2018.

L'IDENTITÉ NUMÉRIQUE POUR LUTTER CONTRE L'ILLECTRONISME ?

Le concept d'illectronisme[30] définit le blocage de certains usagers à utiliser un support informatique. À titre d'exemple, l'utilisation du mail comme canal de communication privilégié avec l'administration peut être source de rupture dans la relation avec cette dernière. La plupart des ménages que Dominique Pasquier a pu observer au cours de son enquête éprouvent des difficultés à intégrer l'adresse mail dans leurs usages quotidiens, ce qui crée une barrière dans leur relation avec l'administration[31]. Il ne s'agit pas à proprement parler d'un problème d'équipement : 75 % des Français disposent d'un smartphone, 78 % d'un ordinateur[32]. « Elles (les familles modestes) ont beaucoup plus de facilité à utiliser les applications bancaires sur leur téléphone qu'à naviguer sur certains sites administratifs sur un ordinateur. Certaines personnes consultent leurs comptes en banque au quotidien à raison de plusieurs fois par jour ». Par son ambition de simplification des usages, l'identité numérique pourrait-elle être un facteur d'e-inclusion ? Ce point est soulevé par les associations de solidarité qui accompagnent les populations les plus en difficultés dans leurs démarches administratives et témoignent de la complexité de la gestion des mots de passe pour leurs bénéficiaires, et par ricochet leurs bénévoles, à l'instar de la Croix Rouge. Pour les bénéficiaires les moins enclins à utiliser des supports informatisés, la création de plusieurs comptes sur des services en ligne (administratifs ou autres) peut vite s'avérer anxiogène. Face à cela, les bénévoles qui les accompagnent se retrouvent dans des situations souvent très inconfortables, en particulier vis-à-vis des enjeux de protection des données : c'est à eux qu'échoit le rôle d'aide-mémoire pour l'ensemble des identifiants nécessaires à la réalisation des démarches en ligne.

Néanmoins, l'identité numérique demeure un outil qui dépend de la stratégie qui l'entoure, dans sa conception et sa diffusion. Sans une réflexion plus globale sur le parcours utilisateur des services en ligne et une politique volontariste d'accompagnement au déploiement et à l'appropriation de ce dispositif, ces attentes resteront à l'état d'un vœu pieux.

30 « L'illectronisme» en France », CSA / Syndicat de la presse sociale, le 25 juin 2018.

31 « L'Internet des familles modestes : les usages sont-ils les mêmes du haut au bas de l'échelle sociale ? », interview de Dominique Pasquier par Hubert Guillaud, InternetActu.net, le 21 septembre 2018.

32 « Baromètre du numérique 2018 », Agence du Numérique, Autorité de Régulation des Communications Électroniques et des Postes (ARCEP) et Conseil Général de l'Economie, de l'Industrie, de l'Energie et des Technologies (CGE), décembre 2018.

DE L'IMPORTANCE DE LA MÉDIATION

Quand on interroge les Français sur leur degré d'inquiétude par rapport aux démarches administratives en ligne, ils sont 39 % à se dire inquiets, dont 68 % parmi les non-diplômés[33]. Même parmi les plus jeunes et les plus diplômés, plus d'une personne sur cinq s'estime inquiète quant à la généralisation de ces démarches.

À chaque typologie d'usager correspond des freins différents, et à chaque usage des contraintes spécifiques. Aussi, pour accompagner le déploiement de l'identité numérique, il convient de développer des ressources pédagogiques à même d'épouser la granularité des situations et des publics. En complémentarité avec les démarches de sensibilisation en ligne et par voie médiatique, l'accompagnement « en présentiel » s'avère ici déterminant. C'est la logique qui a conduit au développement des 1150 Maisons de services au public (MSAP) recensées en 2017. Ces structures hybrides s'appuient sur des partenariats avec des opérateurs de service public (Caisse d'allocations familiales, Pôle emploi, etc.), afin d'assurer la présence et la qualité des services de proximité dans les territoires. Ces structures mettent l'accent sur l'accompagnement des publics par des agents d'accueil, formés auprès des administrations partenaires. À ce titre, le projet de réforme de la justice actuellement en débat au Parlement fait l'objet de vives critiques, notamment du côté des avocats et des juges. Le 19 novembre dernier, le Défenseur des droits, Jacques Toubon, a ainsi dénoncé *« des atteintes à l'accès au droit des justiciables »*, notamment des *« plus fragiles »*.[34] Il alerte sur « les difficultés d'une dématérialisation sans phase transitoire et la nécessité d'un accompagnement numérique des usagers ». En cela, il rappelle le nombre conséquent de saisines reçues à l'occasion du déploiement du Plan Préfecture Nouvelle Génération.

33 « E-administration : la double peine des personnes en difficulté », CRÉDOC, avril 2017.

34 « Réforme de la justice : le Défenseur des droits dénonce des atteintes à l'accès au droit des justiciables », Défenseur des droits, Communiqué de presse, le 19 novembre 2018.

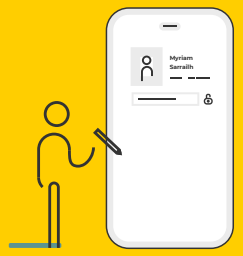
CONSOLIDER LA RELATION NUMÉRIQUE AVEC LE CITOYEN DANS LA DURÉE

Le choix du support, des opérateurs et la définition d'un projet qui résonne auprès de tous seront déterminants pour l'adoption du dispositif. Ces choix permettront en outre de poser les bases d'une relation numérique nouvelle avec les usagers-citoyens, qui sera amenée à évoluer dans la durée, tout comme les fonctionnalités du parcours d'identification numérique. Ces nouvelles fonctionnalités devront être développées sur la base d'une observation fine des usages qui évolueront au fur et à mesure, en même temps que l'appropriation de l'identité numérique et des choix politiques nouveaux.

Pour l'observer, le dispositif pourra ouvrir des espaces de dialogue, par exemple avec des comités d'utilisateurs. Il pourra également s'appuyer sur l'analyse des flux de données générées par ces derniers, afin de prioriser les projets d'évolution au regard de leur pertinence en termes d'usages. En ce sens, la confiance et l'appropriation passent aussi par la compréhension de la valeur générée par ces flux de données, pour le citoyen et pour l'État.

PARTIE 3

LES DONNÉES D'IDENTITÉ NUMÉRIQUE, UN DOUBLE ENJEU DE MAÎTRISE POUR L'ÉTAT ET LE CITOYEN



Aujourd'hui, nos données personnelles font l'objet de débats entre des acteurs qui les exploitent à des fins commerciales ou publiques et des autorités indépendantes qui visent à réglementer leurs conditions de captation et d'exploitation afin d'en assurer leur protection.

> « *La technologie n'étant pas neutre, elle fournit des éléments d'identité qui ne sont pas toujours contrôlés. Par ailleurs, plus on se connecte sur des dispositifs hétérogènes d'identification, plus ils se recoupent quand ils deviennent massifs. Ce qui amène à une concentration d'informations relatives à l'identité des usagers.* »
>
> Etienne Drouard
> Avocat

Aujourd'hui, quand on additionne les usages des utilisateurs en ligne, on s'aperçoit que le recoupement des informations qu'ils génèrent ouvre un boulevard pour tracer l'ensemble de leurs activités. À ce titre, il est important que l'État s'autorise à concurrencer sur ce terrain les acteurs privés dans leur captation, leur flux et leur protection.

LES DONNÉES D'IDENTITÉ NUMÉRIQUE, UNE MANNE CONSIDÉRABLE

Pour les acteurs marchands, le recoupement des données récoltées auprès des usagers leur permet d'adresser des publicités, des recommandations personnalisées, et de pratiquer de la discrimination par les prix en récupérant des informations sur leurs habitudes : historique de navigation, géolocalisation, fréquence de connexion, historique d'achats en ligne, etc. L'analyse de ces données fournit des avantages concurrentiels considérables pour les acteurs qui y ont accès. Elle nous enferme également dans des parcours d'usages, des algorithmes et des bulles filtrantes. Un parcours d'identification numérique porté par l'État peut-il en ce sens nous redonner la maîtrise et le contrôle de nos données ?

UN CADRE JURIDIQUE RELATIF AUX DONNÉES À CARACTÈRE PERSONNEL

Les données d'identité numérique relèvent des données à caractère personnel. Leur protection ne fait donc pas exception au cadre juridique standard sur la protection des données personnelles et de la vie privée. Ce régime juridique s'est renforcé depuis l'entrée en vigueur du Règlement général sur la protection des données (RGPD) en mai dernier. Il repose sur deux piliers :

- Le respect de la vie privée : il s'agit d'un droit défensif, qui garantit des recours contre toute atteinte à la vie privée. Il est assuré au niveau international, européen et français.[35]

- Le respect des données personnelles : encadré par le RGPD, il est quant à lui préventif. Il s'appuie notamment sur le principe de « *Privacy by Design* », qui impose aux organisations de prendre en compte des exigences relatives à la protection des données personnelles dès la conception des produits, services et systèmes exploitant des données à caractère personnel. Il renforce également le principe de minimisation des données : seules les données personnelles nécessaires à la finalité du service doivent être traitées.

Ce cadre invite ainsi les concepteurs des dispositifs d'identité numérique à gérer les données qui en sont issues avec frugalité. À ce titre, l'arrêté relatif au fonctionnement de FranceConnect délimite précisément les données qui sont concernées[36], les acteurs qui en sont destinataires et les modalités de conservation de ces données[37].

35 Par l'article 12 de la Déclaration universelle des droits de l'Homme de 1948, l'article 8 de la Convention européenne des droits de l'Homme, et l'article 9 du Code civil français, issu de la loi du 17 juillet 1970.

36 Voir le Tableau 2 p 37.

37 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.

TABLEAU 2 : LES DONNÉES D'IDENTITÉ NUMÉRIQUE À CARACTÈRE PERSONNEL - EXEMPLE DE FRANCECONNECT[38]

Catégories de données	Données
Données obligatoires pour la gestion de l'identification de l'utilisateur	• le sexe • le nom de famille • le(s) prénom(s) • la date et le lieu de naissance • l'adresse de courrier électronique • le cas échéant, le numéro d'inscription de l'entreprise ou de son établissement au répertoire des entreprises et de leurs établissements (SIREN ou SIRET) • les clés de fédération ou « alias » générés par le système à la connexion de l'utilisateur • un alias technique unique propre au système obtenu par le hachage irréversible de tout ou partie des données à caractère personnel mentionnées
Données facultatives pour la gestion de l'identification de l'utilisateur	• le nom d'usage • le numéro de téléphone fixe • le numéro de téléphone portable • l'adresse de courrier électronique • l'adresse postale
Données pour la gestion de la traçabilité des accès de l'utilisateur	• l'adresse IP • les dates et heures de connexion au service FranceConnect • les jetons issus du mécanisme d'échange d'informations permettant de vérifier la bonne information de l'utilisateur et, le cas échéant, le recueil de son consentement

38 Liste définie par l'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.

RÉFLÉCHIR AUX INTERFACES DE GESTION DES DONNÉES

Le cadre juridique autour des données d'identité numérique se décline en des traitements distincts :

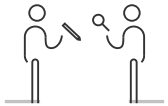
- l'identification relève du traitement de toutes les données relatives à l'identité d'un individu, qui se déclinent en de nombreux attributs d'identité (du registre d'état civil au numéro de sécurité sociale) ;
- le consentement relève du mécanisme par lequel l'individu va consentir l'accès à ses données et ses attributs d'identité à un fournisseur de service qui les lui réclamera ;
- le flux des données personnelles relève de la manière dont ces données, ainsi que les données d'usages, vont circuler, être utilisées et associées.

En droit, la maîtrise de ces données sera donc aux mains du citoyen, qui pilotera la manière dont elles pourront être recoupées, en ouvrir ou en révoquer l'accès. Concrètement, les solutions généralement déployées pour ce pilotage à l'échelle européenne font appel au modèle du *dashboard,* du « tableau de bord », qui permet de piloter les accès qui sont accordés à chaque fournisseur de service dès lors que l'on se connecte via un dispositif d'identification numérique.

Techniquement, un fournisseur de service (un site web) va interroger le fournisseur d'identité, qui attendra la validation de l'usager avant de transmettre au fournisseur de service les attributs d'identité exigés pour l'accès au service. Ces mesures permettent d'utiliser des données partagées, tout en limitant leur diffusion et de garder le contrôle sur leur utilisation par des tiers.

LA « SELF-DATA »

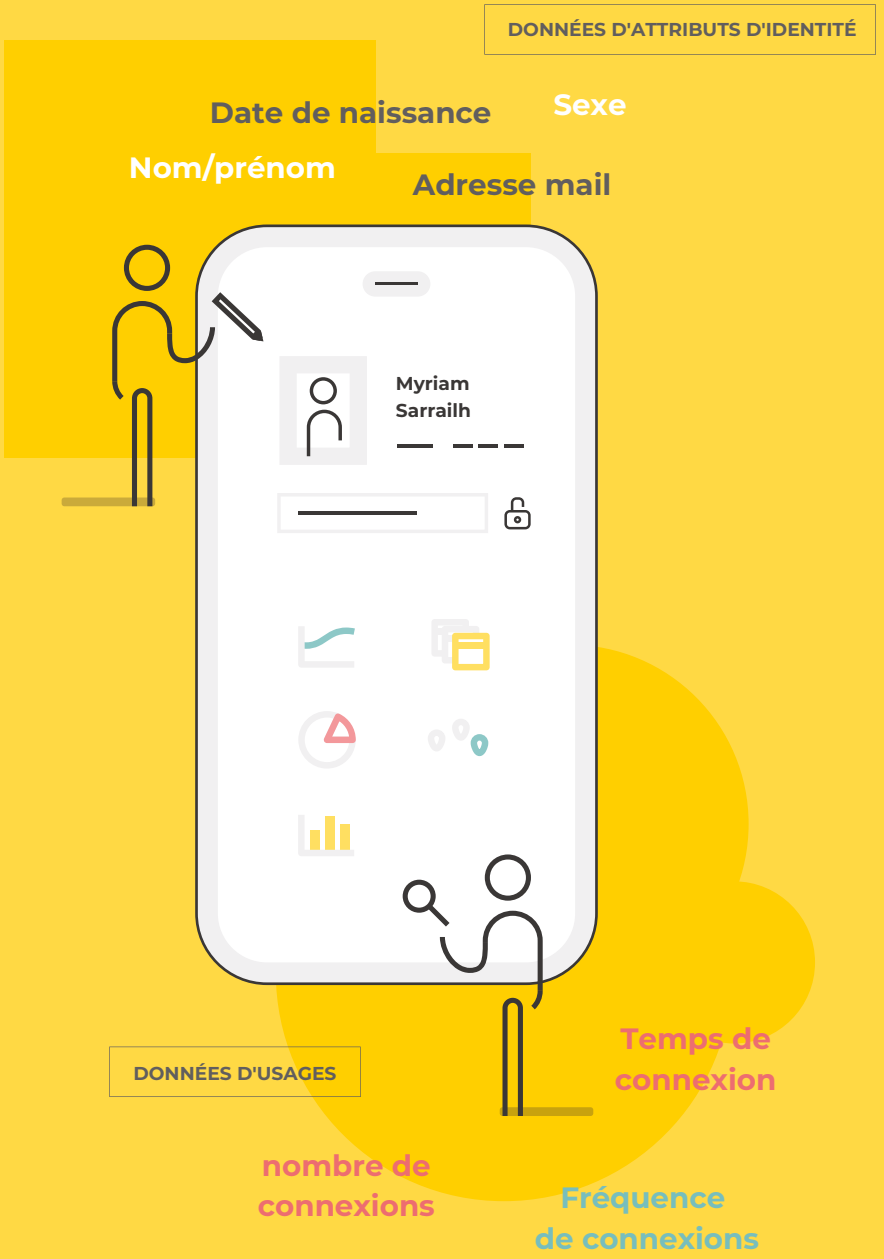
La démarche MesInfos, menée par la Fondation Internet Nouvelle Génération (Fing), explore la « *Self Data* », qu'elle définit comme « *la production, l'exploitation et le partage de données personnelles par les individus, sous leur contrôle et à leurs propres fins* » et recense les initiatives du même type à travers le monde : *Mydata* en Finlande, *Midata* en Angleterre, *Smart Disclosure* aux États-Unis, *VRM* (*Vendor RelationShip Management*), *Cloud Personnel*, *Quantified Self*, *PDS* (*Personal Data Store*), *PIMS* (*Personal Information Management System*), *Customer Commons*, etc. Ce type d'interfaces sert à la fois d'outil de pilotage et de personnalisation des services offerts par le dispositif d'identité numérique. Elles constituent en même temps une ressource pédagogique pour véhiculer une bonne compréhension des enjeux autour des données, parce qu'elles donnent des arguments et du pouvoir à l'utilisateur pour arbitrer la diffusion de ses données et préserver leur intégrité contextuelle.



ENJEUX DE MAÎTRISE DES DONNÉES

Au-delà de la maîtrise de la donnée personnelle par le citoyen, le parcours d'identification numérique s'inscrit dans un existant dans lequel l'État, et l'administration de manière plus générale, n'a pas toujours accès à des données qui lui seraient utiles pour la gestion et l'amélioration des services publics, et qui sont générées par ses citoyens sur son territoire. Les acteurs qui opèrent en France et qui ne sont pas sous mission de service public ne partagent pas leurs données, où uniquement dans le cadre de partenariats spécifiques établis avec les administrations, sous des conditions qui les mettent souvent en situation de force dans les négociations. La gestion de la mobilité en ville par la donnée a par exemple explosé depuis plusieurs années, avec des acteurs comme Uber ou Waze. Il s'agirait ainsi pour l'État et les collectivités territoriales de renforcer leur souveraineté en sécurisant les données tirées de l'identité numérique de leurs citoyens. Il s'agirait également potentiellement de renforcer leur capacité d'action, en permettant aux citoyens de leur partager leurs données, sous réserve de leur protection et anonymat, dans une logique de contribution à l'amélioration des services publics. En termes d'évaluation des politiques publiques et pour le champ de la recherche, ces données représentent une manne intéressante à analyser et ouvrent le développement d'outils plus efficaces que les méthodes de panels ou d'échantillons classiques généralement développés. Elles pourraient permettre d'améliorer des politiques publiques par une lecture plus fine des enjeux grâce aux données. Toutefois, ces usages invitent à définir un tiers de confiance, à même de garantir leur anonymisation et les bonnes conditions de leur réutilisation.

Le citoyen, maître de ses données d'identité numérique



HUIT PRÉREQUIS POUR UNE POLITIQUE D'IDENTITÉ NUMÉRIQUE AU SERVICE DE TOUS LES CITOYENS

Qu'il s'agisse de ses caractéristiques techniques ou des modalités de son déploiement, le développement du parcours d'identification numérique sécurisé relève avant tout d'un arbitrage politique de la part de l'État. En témoigne son histoire discontinue en France, avec les gouvernements successifs (et leurs échecs). Or, le débat actuel fait encore peu de cas des usages citoyens, des attentes, des défis de son adoption. Au-delà même de ces usages, il peine à porter des objectifs, des priorités, un sens à cette politique publique qui pourra résonner auprès des citoyens. Tous les citoyens ne feront pas usage demain de l'identité numérique. Mais il faut s'assurer qu'ils n'en soient pas écartés et qu'ils y trouvent un intérêt. En cela, cette politique est fortement imbriquée à celle de la dématérialisation des services publics. Dans un contexte de fracture importante, sociale, territoriale, numérique, alors que cette politique vise l'amélioration des services publics, elle ne doit pas résulter en l'ajout de nouveaux irritants. Partant de là, l'État doit tenir compte de huit prérequis à sa mise en œuvre :

UNIVERSALITÉ

Tous les citoyens français doivent pouvoir disposer d'une identité numérique quels que soient leur lieu de résidence, le type de papier d'identité dont ils disposent, le système d'exploitation de leur smartphone. Par extension, cela inclut les résidents en lien avec l'administration.

ACCESSIBILITÉ

L'administration doit rendre progressivement toutes ses démarches qui nécessitent l'identification physique d'un citoyen, réalisables en ligne au moyen d'une identité numérique de niveau substantiel (ou élevé).

INCITATION

L'État doit fortement encourager les premiers usages de l'identité numérique afin de mettre en place des habitudes, par des dispositifs d'incitation sur des usages existants, comme il l'a fait pour les impôts, et demain pour de nouveaux usages (cf. santé ou justice).

SIMPLIFICATION

Le parcours d'identification numérique doit partir des démarches administratives les plus irritantes, pour que la simplification permise par l'authentification en ligne soit pleinement vécue par le citoyen.

ANTICIPATION

L'État doit dès à présent anticiper les futurs plans d'accompagnement au déploiement de cet outil, par une politique ciblée auprès des populations, en particulier des publics les plus éloignés du numérique. Par exemple, une liste des lieux facilement identifiables pour assurer la prise en main de cet outil par son expérimentation, doit être établie.

ACCULTURATION

L'administration doit évoluer vers une culture de la simplicité, tant par la formation et l'accompagnement de ses agents que dans l'architecture même de ses services (physiques et en ligne).

AGILITÉ

Une logique d'agilité doit prévaloir dans la conception de l'outil. À l'instar des services, l'outil devra évoluer avec son adoption par les citoyens.

MAÎTRISE

La maîtrise des données d'identité numérique par les citoyens doit être appréhendée au-delà même de leur sécurisation, dans la conception d'outils d'appropriation, tels que des tableaux de bord. S'ils le souhaitent, les citoyens doivent pouvoir partager leurs données anonymisées, dans une logique contributive pour l'amélioration des politiques publiques.

POUR EN SAVOIR PLUS

- **« Données personnelles : rendre ces droits effectifs »**, Renaissance Numérique, mai 2018.
- **« L'identité numérique en France – situation, enjeux et propositions »**, Guy de Felcourt, David Naccache et André Viau, Centre des hautes études du ministère de l'Intérieur, décembre 2017.
- **« Démocratie : le réenchantement numérique ? »**, Renaissance Numérique, mars 2017.
- **« Danemark : une stratégie numérique pour contribuer à l'inclusion »**, Institut de la gestion publique et du développement économique, ministère de l'Économie et des Finances, Note réactive n° 86, septembre 2016.
- **« Les enjeux de l'identité numérique »**, Claire Levallois-Barth, Chaire *Valeurs et Politiques des informations personnelles*, Institut des Mines-Télécom, novembre 2013.

REMERCIEMENTS

Nous remercions pour leur contribution les différents acteurs qui ont participé aux auditions, à savoir :

- **John Billard**, Vice-président de l'Association des maires ruraux de France
- **Sylvie Billard**, Responsable du Schéma Directeur du Numérique, Ministère de la Justice
- **Candice Dauge**, Directrice du programme Identité Numérique, Groupe La Poste
- **Étienne Drouard**, Avocat
- **Valéria Faure-Muntian**, Députée de La Loire
- **Hervé Groléas**, Directeur Innovation numérique et Systèmes d'information, Grand Lyon
- **Daniel Kaplan**, Conseiller scientifique, FING
- **Soisic Rivoalan**, Chargée de mission inclusion bancaire et inclusion numérique, La Croix Rouge
- **Amal Taleb**, Directrice adjointe des Affaires publiques, SAP France
- **Cédric Verpeaux**, Responsable des programmes d'investissement innovants et territoriaux, Caisse des dépôts et consignations

DIRECTEURS DE LA RÉDACTION

Henri Isaac, Président de Renaissance Numérique

Philippe Régnard, Directeur des Affaires publiques, Branche numérique du Groupe La Poste

COORDINATION

Jennyfer Chrétien, Déléguée générale de Renaissance Numérique

RAPPORTEUR

Pierre-Olivier Cazenave, Vice-président du Social Media Club France

RENAISSANCE
numerique

À PROPOS DE RENAISSANCE NUMÉRIQUE

Renaissance Numérique est le principal think tank français indépendant dédié aux enjeux de transformation numérique de la société. Réunissant des universitaires, des associations, des grandes entreprises, des start-ups et des écoles, il vise à élaborer des propositions opérationnelles pour accompagner les acteurs publics, les citoyens et les acteurs économiques dans la promotion d'une société numérique inclusive.

Renaissance Numérique
22 bis rue des Taillandiers - 75011 Paris
www.renaissancenumerique.org

Janvier 2019