

Marie Alauzen. L'État plateforme et l'identification numérique des usagers Le processus de conception de FranceConnect. *Réseaux*, La Découverte, 2019, n° 213 (1), pp.211-239. doi:10.3917/res.213.0211.

The final version of the review article can be retrieved on: www.cairn.info/revue-reseaux-2019-1-page-211.htm

L'État plateforme et l'identification numérique des usagers

Le processus de conception de FranceConnect

Marie ALAUZEN

FranceConnect est un bouton de connexion aux services publics inséré, depuis 2015, sur plusieurs centaines de sites administratifs¹. Ce bouton, qui pourrait paraître anodin, constitue pourtant la première réalisation d'un projet de modernisation de l'État appelé « l'État plateforme », et s'inscrit dans la lignée des dispositifs administratifs qui ont fait de la figure de l'utilisateur le destinataire privilégié de la modernisation de l'État (Weller, 1998 ; Gélédan, 2016). FranceConnect a été pensé comme un investissement technologique destiné à réduire le « fardeau administratif » des citoyens. Techniquement, il est le résultat d'une politique de simplification visant à éviter aux usagers de créer de nouveaux comptes et préremplir les formulaires avec des données déjà enregistrées par les administrations.

Pour prendre la mesure de cette innovation informatique et administrative, il est utile de la replacer dans les études sur la production étatique de l'identité (ou régime de véridiction de l'identité) qui ont exploré les technologies d'inscription des personnes, les savoirs administratifs, policiers et les outils nécessaires au gouvernement de ceux que l'on nomme désormais les individus. En France, cette histoire de l'individu a été remarquablement étudiée par Gérard Noiriel (1988), Pierre Piazza (2004) et Vincent Denis (2008 ; Denis et Ilse, 2010). Registre d'état civil, livret anthropométrique, passeport ou carte nationale : tous ces instruments de gouvernement de l'identité ont provoqué des controverses et des suspicions quant aux effets de subjectivation et aux potentialités de surveillance et de contrôle, non pas de quelques individus suspectés, mais de la population entière. Ces controverses sur l'identification étatique ont été d'autant plus fortes lorsque les dispositifs étaient portés par le développement de l'informatique et ont permis de circuler dans le trop-plein d'informations (Denis et Lacour, 2016).

En proposant une reconnaissance accélérée des individus et en facilitant, au nom d'une certaine modernité technique, l'échange de leurs données, FranceConnect peut sembler, à bien des égards, une innovation inquiétante. Cette inquiétude, propre aux études des technologies d'identification, nous engage à considérer scrupuleusement le projet de modernisation mentionné plus haut, l'État plateforme. Celui-ci désigne un programme d'investissement dans les systèmes d'information des administrations françaises en même temps qu'une théorie de l'État en actes. Il a été porté, publiquement à partir de 2015, par le Secrétariat général pour la modernisation de

¹ Je remercie chaleureusement Vincent-Arnaud Chappe, Jérôme Denis, Quentin Dufour, Fabian Muniesa, Florence Paterson, David Pontille, Alexandre Violle et les relecteurs de la revue pour leurs commentaires. Merci également à Thomas Menant et à Jocelyn Lelong. La thèse défendue et les défauts restants me sont imputables sans réserve.

l'action publique (SGMAP), le service du Premier ministre en charge, de 2012 à 2017, de l'activité coordonnée de réforme de l'État. Cette stratégie de plateforme poursuit les politiques de développement de l'administration électronique (Truche, Faugère et Flichy, 2002 ; Dagiral, 2007) et d'ouverture des données publiques (Denis et Goëta 2017). Elle s'est matérialisée dans des choix d'interopérabilité, de mutualisation d'infrastructures informatiques, ainsi que dans une quête d'alignement sur les industries numériques de plateforme (Facebook, GitHub, Google)². D'ailleurs, de manière très explicite, FranceConnect emprunte son nom, son design et ses fonctions à Facebook Connect, le bouton d'identification à un site tiers via le réseau social Facebook.

L'article analyse en profondeur ce nouvel outil d'identification des usagers des services publics en ligne et s'efforce de caractériser l'État qui apparaît dans cette entreprise de modernisation. Il ne se concentre ni sur l'usage, ni sur une quelconque réception controversée, ni encore sur l'efficacité du dispositif, mais sur le travail de conception mené en amont. L'anthropologie des techniques (Akrich, 1989 ; Bijker et Law, 1992 ; Bijker, Hughes et Pinch, 1993) a arpenté les coulisses, la genèse et la consolidation progressive des innovations pour montrer que les problèmes techniques sont éminemment politiques et que rien n'est jamais joué d'avance. Cette perspective a par exemple donné lieu à des travaux en sociologie des données qui explorent la production des algorithmes et le lourd travail de l'information (Cardon, 2015 ; Denis, 2018). En nous interrogeant sur la façon dont cette technologie d'identification a été envisagée et en retraçant les problèmes auxquels se sont confrontés ses concepteurs, nous verrons advenir deux qualités spécifiques de l'État plateforme. Cette analyse nous met sur la piste de la sociologie des épreuves d'État (Linhardt et Moreau de Bellaing, 2005 ; Linhardt et Muniesa, 2011 ; Linhardt, 2018). Cette branche pragmatiste de la sociologie de l'État se distingue par le souci de ne jamais prendre l'État comme une donnée, et nous enjoint à porter une attention extrême aux épreuves, ces événements mettant en question la réalité d'une entité. En tant qu'opérateur de la modernisation de l'État, le SGMAP devient alors un site particulièrement propice pour explorer les accomplissements bureaucratiques et technologiques de l'État français.

Nous étudierons d'abord le projet de faire de l'État une plateforme ; ou plus précisément, pourquoi le SGMAP s'est saisi des technologies dites plateforme. Nous examinerons, à partir d'une lettre de mission du Premier ministre, comment le projet d'identification étatique s'est orienté vers le développement des usages de l'administration en ligne. La technologie OpenID Connect, qui semblait être plébiscitée par les usages, s'est imposée et a rejoint la préoccupation pour la souveraineté numérique, récemment importée dans la modernisation de l'État. Dans un second temps, nous insisterons sur les choix technologiques propres aux deux fonctions du bouton FranceConnect : identifier les usagers et échanger des informations administratives. Nous verrons que les concepteurs de FranceConnect ont créé une application frugale en données personnelles (caractérisant l'utilisateur par un état civil minimal) et dirigée par des enjeux d'accessibilité, de confort, de traçabilité et le caractère opposable des échanges. Cet État plateforme en train d'advenir dans ces épreuves de conception est articulé autour de deux qualités essentielles : la souveraineté numérique et l'ergonomie des services publics.

² Pour comprendre la spécificité des infrastructures participatives et organisationnelles dans le cas de Google et Facebook, on se reportera à Plantin et al. (2016).

Une ethnographie de la conception administrative et informatique

L'article s'appuie sur une enquête ethnographique approfondie du SGMAP. J'ai été recrutée en octobre 2014 pour y rédiger une thèse sur la modernisation numérique de l'État français. J'ai été présente, dans les bureaux parisiens, entre deux et trois jours par semaine, d'octobre 2014 à novembre 2016, puis plus sporadiquement jusqu'en septembre 2017. Dans ce cadre, j'ai réalisé des observations ethnographiques du développement de FranceConnect (durant environ 60 demi-journées) et mené des entretiens informels avec les participants (n = 40), consignés dans des carnets de terrain. Ces matériaux m'ont fourni une riche compréhension de la trajectoire de ce projet de modernisation. Afin de multiplier les points de vue et de comprendre les problèmes quotidiens et les tâtonnements, j'ai récolté des documents internes au service : emails, présentations, documentation technique, notes, études. Ce corpus m'a non seulement permis de reconstituer la chronologie (y compris d'événements auxquels je n'ai pas pu assister), mais surtout de documenter les débats, les états d'âme, les changements de position ainsi que le lexique et les technologies impliquées. Mon dossier d'archives numériques de FranceConnect rassemble, outre ma collecte, les archives personnelles d'un membre du projet. Enfin, pour accéder à une version plus stabilisée et officielle du bouton, j'ai enregistré, en continu depuis l'automne 2014, un corpus d'informations publiques (rapports, textes de loi, documents stratégiques, communiqués, revue de presse web).

Les agents chargés par le SGMAP de la conception et du développement de FranceConnect (ci-après les concepteurs) ont formé un collectif professionnel hybride de sept personnes et de quelques soutiens ponctuels. Juristes spécialisés en droit du numérique, ingénieurs informaticiens ou cadres de l'administration ; ils ont pour point commun d'être quasi exclusivement des hommes, issus de grandes écoles ou de formations universitaires sélectives, de ne pas être fonctionnaires et d'être mobilisés sur le programme d'État plateforme. Avant de constituer l'équipe, la plupart ont travaillé sur d'autres projets du SGMAP, en tant que chargé de mission, juriste, architecte de système d'information, ou responsable de la sécurité informatique. Les développeurs étaient des prestataires d'une entreprise de services informatiques agiles ; seniors ou juniors, ils ont travaillé durant plusieurs mois sur le plateau technique mis à disposition par l'administration, participé aux réunions et aux tests au même titre que les agents du SGMAP. Certains avaient développé une connaissance spécifique de l'écologie ministérielle au cours de leur trajectoire professionnelle et étaient aguerris aux protocoles utilisés par FranceConnect (OAuth 2.0, OpenID Connect). Au fil des mois, ils ont acquis des savoir-faire pour suivre l'évolution technique, administrative et juridique du projet, intéresser des partenaires (dans et hors des administrations) et négocier avec la hiérarchie. Cette dynamique collective a été essentielle au succès du bouton, qui affiche trois ans après son lancement, à l'été 2018, « 6 millions de Franceconnectés »³.

³ FranceConnect.fr, consulté le 10/09/18.

Des technologies de plateforme à la souveraineté numérique

Pour comprendre ce qu'est FranceConnect, il nous faut remonter à la création du SGMAP, à la fin de l'année 2013, où l'on apprend que la modernisation des services publics s'est problématisée autour des usages et du rétablissement de la confiance dans l'administration. Nous analyserons alors comment la notion d'État plateforme, importée des États-Unis à la même période par Nicolas Colin et Henri Verdier, a progressivement pris sens dans cette nouvelle écologie de la modernisation. Enfin, à partir du moment où l'État plateforme est devenu un programme d'action officiel, nous insisterons sur les effets politiques de cette stratégie dans la discrète diplomatie menée contre le droit américain, les grandes entreprises de services, et grâce à un alignement sur de récentes normes européennes sur l'identité numérique.

Inventer une identification alternative

En janvier 2013, le Premier ministre Jean-Marc Ayrault a envoyé une lettre de mission au SGMAP, nouvellement créé. La lettre mandatait le service pour concevoir, dans le cadre de ses fonctions de modernisation de l'action publique, une solution d'identification numérique alternative de la carte d'identité électronique et commune à l'ensemble des services publics en ligne. « *Le défi c'était de ne pas refaire la carte d'identité électronique, mais de penser, à partir des besoins des usagers, une solution numérique accessible au grand public et suffisamment sécurisée et bien foutue pour que toutes les administrations, à commencer par la commune de moins de 10 000 habitants, s'en saisissent* »,⁴ m'a expliqué le chef de projet lors de notre première rencontre.

La lettre a heurté les agents du ministère de l'Intérieur pour qui l'identification, numérique ou non, a fait partie de leurs prérogatives. En effet, depuis la fin du XIX^e siècle, l'Intérieur s'est constitué un domaine réservé autour « des papiers » et s'est efforcé de lisser l'hétérogénéité des technologies d'identification, avant de parvenir à imposer, sous le régime de Vichy, le « *bienheureux bout de carton* » de la carte nationale d'identité (Piazza, 2004, p. 162-270). Fort de ce monopole historique et de l'expertise accumulée lors de la rédaction de la loi relative à la protection de l'identité (censurée l'année précédente par le Conseil constitutionnel⁵), le ministère a réclamé le transfert du dossier. Mais le Premier ministre, convaincu de l'intérêt de séparer les domaines de l'identification administrative et policière⁶, a confirmé l'attribution au SGMAP. Le calcul du gouvernement a été, d'une part, de mener une politique de modernisation de l'État en rupture avec la Révision générale des politiques publiques (Bezes, 2010 ; Gélédan, 2012). Le programme de Modernisation de l'action publique (graduellement éclipsé par le projet d'État plateforme) devait moins se traduire par une réorganisation à marche forcée ou une quête d'économies budgétaires, que par des investissements technologiques et la simplification des services proposés aux usagers (Gélédan, 2016). D'autre part, toujours en réaction à la politique menée sous le précédent mandat, le gouvernement a cherché à se prémunir de la tentation sécuritaire propre à l'Intérieur (fichier national, biométrie, puce électronique), qui a régulièrement

⁴ Notes de terrain, 13/10/14.

⁵ Conseil constitutionnel, Décision n°2012-652 DC du 22 mars 2012, Loi relative à la protection de l'identité.

⁶ La quête d'une alternative était d'autant plus évidente que parmi les députés qui avaient saisi le Conseil constitutionnel le 7 mars 2012, on retrouvera neuf ministres et secrétaires d'État du premier gouvernement socialiste dont Marylise Lebranchu, ministre de tutelle du SGMAP, et Jean-Marc Ayrault.

susité des controverses et amoindri la confiance dans l'administration (Crettiez, 2006).

Deux équipes ont proposé de répondre à la commande politique. Les méthodes de conception préconisées partageaient une grande vigilance pour l'acceptation sociale et l'utilité pratique de la technologie d'identification. La mission d'Appui au développement de l'administration numérique (ci-après l'équipe A) est partie du principe que l'identité administrative sur internet ne faisait pas forcément sens pour des internautes habitués à utiliser des pseudonymes, manœuvrer entre plusieurs adresses et mettre à jour continuellement leurs profils sur les réseaux sociaux. Ils ont conseillé la réalisation d'études sur les usages de l'identité en ligne et la convocation d'instances de participation afin que les usagers conçoivent la future technologie d'identification administrative. Le service Architecture et urbanisation des systèmes d'information (ci-après l'équipe B) a programmé une étude de marché et rencontré d'autres acteurs, administrations ou entreprises, qui utilisaient l'identification numérique de très larges publics (banques, transports en commun, sociétés de téléphonie). Parmi toutes les solutions recensées, la technologie OpenID Connect leur a semblé la moins chère et la plus solidement ancrée dans les usages.

De quoi s'agit-il ? OpenID Connect (plus connu des internautes sous la formule « créer un nouveau compte ou se connecter avec Facebook, Google ou Twitter ») est un système d'authentification libre et décentralisé arrimé à la délégation d'autorisation OAuth 2.0, permettant aux internautes de s'authentifier auprès de plusieurs sites sans avoir à retenir un identifiant et un mot de passe pour chacun d'entre eux. Le protocole, créé en 2005 par Brad Fitzpatrick, un développeur américain de logiciels libres, est venu apporter une solution sécurisée et générique au problème de la multiplication des identités qui agaçait les internautes et les gestionnaires des sites internet. Depuis, il s'est amplifié et agrège des contributions des grands industriels : Microsoft à partir de 2007, Yahoo!, IBM et surtout Google en 2008 et Facebook l'année suivante. En 2010, Facebook a cessé de contribuer au protocole commun pour lancer Facebook Connect, sa version propre. Le bouton « se connecter avec Facebook » remporte un immense succès auprès des sites partenaires, car Facebook transfère de nombreuses informations sur le profil des personnes identifiées (Tchuenté, Baptiste-Jessel et Canut, 2011). Ces informations permettent aux sites de mieux cibler leur politique commerciale et, éventuellement, d'acheter à Facebook des emplacements publicitaires pour les utilisateurs ayant un profil similaire aux personnes identifiées (Cardon, 2015)⁷.

En résumé, l'équipe A a soumis une ouverture de la technologie d'identification administrative, là où l'équipe B a proposé de s'aligner sur OpenID Connect, un standard gratuit et largement éprouvé par les internautes. Dès le mois d'avril 2013, l'agenda gouvernemental est venu sommer le SGMAP de présenter « *la doctrine de la France en matière d'identité numérique* »⁸. La popularité et le caractère aisément reproductible du bouton (en raison de l'ouverture du code

⁷ De l'autre côté, deux expérimentations (Egelman, 2013 ; Robinson et Bonneau, 2014) ont montré que plus de 88 % des utilisateurs de Facebook cliquent quotidiennement sur ce bouton, par commodité, et parce qu'ils accordent leur confiance au site sur lequel ils naviguent. Leur compréhension du système de délégation et des conséquences sur leurs données personnelles s'avère relativement limitée.

⁸ Chef de projet, entretien, 09/06/16.

d'OpenID Connect) ont définitivement fait basculer l'arbitrage en faveur de l'équipe B.

Toutefois (et de manière paradoxale puisque les concepteurs se sont orientés vers le protocole libre OpenID Connect), la renommée du bouton Facebook Connect était telle que nommer, par analogie, le projet d'identification étatique « FranceConnect », « *c'est plus simple pour les ministres qui ne comprennent rien au numérique, et pour le grand public qui l'utilise déjà. On leur dit : « c'est comme Facebook, mais c'est l'État », l'idée c'est la confiance* »⁹. Cette analogie qui n'était initialement que temporaire et pédagogique est restée : à partir du mois de septembre 2014, le nom est déposé¹⁰, le projet communiqué au grand public¹¹ et, dans les administrations, FranceConnect est présenté comme la première pierre d'une nouvelle stratégie de l'État, la stratégie de plateforme.

La stratégie d'État plateforme

La notion d'État plateforme s'est implantée dans la modernisation de l'État par l'intermédiaire d'Henri Verdier. Dans *L'Âge de la Multitude* (2012), Nicolas Colin et Henri Verdier, respectivement inspecteur des finances en disponibilité et directeur du pôle de compétitivité numérique Cap digital, se sont intéressés aux métamorphoses de la valeur engendrées par les grandes industries de services numériques. Ils défendaient une vision de l'entrepreneuriat comme capitalisation des ressources produites par « la Multitude » (qui regroupe les administrations, la société civile et les entreprises) et la formation d'infrastructures de valorisation, appelées plateformes. Suivant la stratégie *Government as a Platform* initialement promue par un entrepreneur de la Silicon Valley (O'Reilly, 2010) et réinvestie par l'administration Obama en 2012¹², ils estimaient que l'État français doit adapter ses activités de régulation et de services à cette nouvelle économie et se faire, lui aussi, plateforme – notamment en ouvrant les données publiques et en concevant des API¹³.

Fort de ses prises de position publiques et de son expertise, en janvier 2013, Henri Verdier a été nommé directeur de la mission d'ouverture des données, Étalab, rattachée au SGMAP. La mission s'est agrandie et Henri Verdier est rapidement devenu une personnalité influente au sein du SGMAP : il fournissait un éclairage technique aux secrétaires généraux et aux cabinets qui se succédaient, participait au recrutement de nombreux développeurs et ses idées suscitaient l'enthousiasme des agents. Parmi elles, la notion d'État plateforme a pris de l'ampleur. Moins d'un an après son arrivée, elle était inscrite par les ingénieurs de la direction

⁹ Directeur technique, notes de terrain, 18/12/14.

¹⁰ Institut national de la propriété intellectuelle, Dépôt de la marque FranceConnect, n° national 145118624, 17/09/14.

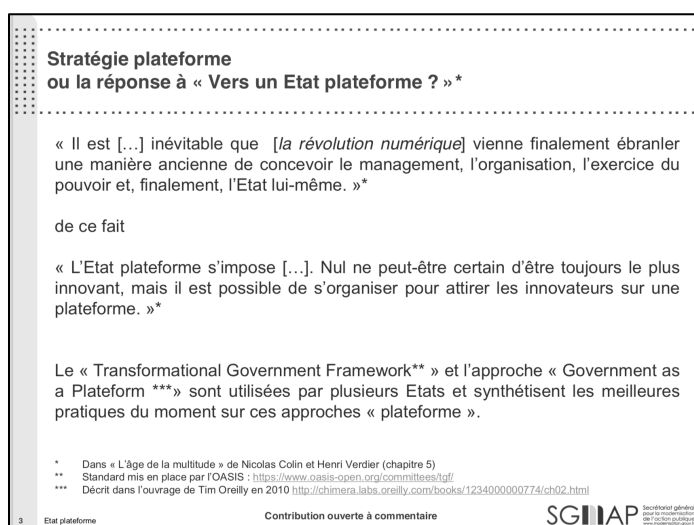
¹¹ Cabinet du secrétaire d'État chargé de la Réforme de l'État et de la Simplification Thierry Mandon, dossier de presse, « visite du plateau de développement de FranceConnect », 02/10/14.

¹² Maison blanche, « Digital government. Building a 21st Century Platform to Better Serve the American People », livre blanc, 23/05/12.

¹³ Une *Application Programming Interface* (API) désigne une solution informatique prête à l'emploi qui permet à des applications de communiquer, via un langage de programmation, et d'échanger mutuellement des services sans avoir à se soucier du fonctionnement de l'autre application. Les API sont utilisées pour fournir un même service, par exemple l'authentification, à un très grand nombre de sites ; Open ID Connect, Facebook Connect et FranceConnect sont des API.

interministérielle du Système d'information et de communication de l'État (l'une des deux directions du SGMAP) au cœur du document stratégique sur la modernisation des services en ligne (figure 1). Plus précisément, le document a été pensé comme une réponse aux défis pour l'État listé dans le cinquième chapitre de *L'Âge de la Multitude* ; et FranceConnect (qui n'existait alors que dans des supports qui circulaient dans les réunions administratives et à l'état de prototype) a été annoncé comme la première réalisation de l'État plateforme. « *On a fait le choix de commencer par l'identité de l'utilisateur et créer son écosystème d'échange des données. On est convaincu que pour tout il faut partir de l'utilisateur. Et, FranceConnect c'est ça, l'interface de la multitude des usagers avec la plateforme, c'est-à-dire toutes vos administrations* », a expliqué un ingénieur du projet lors d'une rencontre avec les directions des systèmes d'information des ministères¹⁴.

Figure 1. L'importation de la stratégie de plateforme



Source : SGMAP, L'État plateforme & Identité numérique ou comment concevoir les services publics numériques autrement, synthèse du 12/11/2014, p. 3

Cette vision de l'État à moderniser sur le modèle des industries numériques a essuyé peu de critiques. La seule mise en cause publique de la modernisation par le rattrapage technologique est venue de Dominique Boullier, professeur de sociologie à Sciences Po. Dans un billet intitulé « L'Âge de la Prédation » et publié le 7 octobre 2012 sur *InternetActu.net*, il écrivait une certaine vision du rattrapage technologique, la sous-problématisation des monopoles établis par les entreprises de la Silicon Valley et alertait sur le projet, sous-jacent, d'un État prédateur de données et obnubilé par l'innovation¹⁵. Cette critique a sporadiquement été récupérée à l'intérieur du SGMAP, comme ici, lorsqu'un développeur revient sur le choix technologique de FranceConnect : « *on a eu peur de se faire ubériser, d'être moins étatique parce que des acteurs privés font de l'identification massive, mais en fait on a manqué d'imagination [...] on n'a pas assez critiqué ce que ça veut dire pour un État souverain de faire comme Facebook et Google* »¹⁶. Le développeur pointait un « manque d'imagination » dans le fait de prendre les technologies des plateformes pour modèle de la

¹⁴ Notes de terrain, 11/12/14.

¹⁵ Voir aussi la réponse d'Henri Verdier sur son blog, « Boullier contre la Multitude » : henriverdier.com/2012/09/sciences-po-contre-lage-de-la-multitude.html, (consulté le 26/11/2018).

¹⁶ Notes de terrain, 26/04/16.

modernisation de l'État, car, s'il était évident que la France n'a rien à voir ni avec Facebook ni avec aucune des grandes plateformes de services numériques, le SGMAP a performé, par la conception d'une telle application, une certaine version de l'État identifiant et façonné la relation aux usagers.

L'alignement comme opération diplomatique

Le SGMAP était préoccupé par les acteurs qui ont fait de l'accessibilité et de la commodité de leurs services un moyen de se rendre indispensables dans le quotidien de centaines de millions d'internautes. Dans cette politique de l'*user-friendliness* et du confort, les questions de l'identification et de la collecte de données personnelles sont régulièrement revenues dans les débats ; par exemple ici lors d'une discussion de couloirs, « *Aujourd'hui on se rend compte que même si toi tu fais super attention à tes données, que tu as un [téléphone mobile] 33 10 ou que tu changes de carte SIM chaque semaine, il suffit que des gens enregistrent ton numéro sous le même nom dans leur Android ou dans leur iPhone pour que Google et Apple sachent qui tu es. C'est un problème personnel, mais aussi un challenge pour l'État* »¹⁷. Ces entreprises ont très souvent été mentionnées au cours du terrain ; et, sans contradiction avec le fait de servir de direction à l'État plateforme, elles ont été constituées en figure ennemie.

La notion d'ennemi désigne moins celui que l'on veut supprimer par la guerre, qu'une ligne de politisation, un moyen de repérer les risques et un principe unificateur pour l'exercice de la souveraineté (Monod, 2007). Or, pierre angulaire de ce nouvel exercice de souveraineté de l'État, appelé souveraineté numérique, FranceConnect a participé à une opération diplomatique à l'encontre des plateformes. C'est du moins ce qu'a expliqué Henri Verdier en prenant la parole lors d'une démonstration de FranceConnect devant une partie du SGMAP, réunie en séminaire. Il y fait part de sa crainte de voir les plateformes promues comme infrastructure technique du service public. Plusieurs initiatives seraient déjà en cours : le très controversé projet Internet.org visant à apporter aux habitants des pays du Sud une version allégée d'internet, largement axée sur Facebook ; ou, plus proche de nous, le partenariat entre Google et la Bibliothèque nationale de France sur la numérisation des archives. Selon lui, la menace la plus inquiétante pour la modernisation des services publics dont le SGMAP était en charge tenait dans la possibilité que des administrations installent, par commodité, Facebook Connect (ou d'autres boutons de connexion) pour réaliser plus aisément certaines démarches, démarches qui peuvent sembler anodines parce qu'elles ne réclament pas un niveau d'authentification élevé (acheter une carte de transports), mais pour lesquelles l'entreprise récupère des données administratives. La situation était réputée « urgente », car des projets dans ce sens auraient déjà vu le jour au Royaume-Uni.

Pour que tout le monde comprenne, il aurait fallu commencer par dire l'urgence dans laquelle nous nous trouvions. Dans certains pays européens, plusieurs sites de services publics ont installé le bouton Facebook. Ça veut dire que les citoyens utilisent Facebook pour se connecter à l'Administration, au site des impôts, vous imaginez ? Facebook sert de carte d'identité et récupère toutes les données sur les échanges.

¹⁷ Chef de produit, notes de terrain, 18/06/15.

En France, il était urgent d'éviter ça et de rétablir la souveraineté numérique. FranceConnect est d'abord un acte souverain¹⁸.

La souveraineté numérique est un concept qui circule dans les administrations depuis les années 2000 et justifie certaines opérations du droit. Le plus souvent, elle se réfère à la souveraineté à la fois comme territoire (matériellement contrôlé par l'État) et comme juridiction (sur laquelle il exerce pleinement justice). C'est, par exemple, au nom de la souveraineté numérique que l'État mène des investigations sur les réseaux et punit l'usurpation d'identité en ligne. En tant que future application d'identification étatique, FranceConnect projetait d'être une médiation de la souveraineté numérique – au même titre que les cyberenquêteurs de la police et de la gendarmerie – et de structurer la position de l'État sur l'identité numérique.

Toutefois, la souveraineté numérique en question différait de celle qui anime cette cybersécurité policière. Les agents du SGMAP (et plus particulièrement ceux de la direction interministérielle du Système d'information et de communication de l'État) ont largement insisté sur le fait que les échanges administratifs, y compris dans leurs dimensions les plus ordinaires, devaient rester sous le contrôle de l'État. Les données devaient donc être stockées sur le sol français, archivées un certain nombre d'années (pour être opposables) dans des serveurs étatiques et protégées de toutes formes d'intrusion. Cette dimension éminemment territoriale et matérielle s'appelle la « couche physique » des infrastructures numériques (câbles terrestres ou sous-marins, satellites, centres de données). Mais le défi n'a pas seulement été de veiller sur cette couche physique, il fallait également protéger la « couche logicielle ».

Cette seconde dimension du cahier des charges de la souveraineté numérique ne va pas sans poser de problèmes pratiques aux agents du SGMAP qui avaient pour ambition de concevoir la modernisation des services publics à partir des besoins des usagers et des pratiques ordinaires. « *On aimerait bien utiliser du Google ou du Facebook, parce que c'est plus pratique, et que tout le monde le fait, mais c'est une question de protection des données des usagers... Et des données de l'administration* ¹⁹ ». Le Référentiel général de sécurité²⁰, le cadre réglementaire de la sécurité informatique de l'État (rédigé par l'Agence nationale de sécurité des systèmes d'information et le SGMAP), interdisait l'utilisation, dans l'activité administrative, d'applications développées par des entreprises soumises au *Patriot Act*²¹, et encourage les administrations à développer leurs propres outils à partir de logiciels libres. En conséquence, le code source de FranceConnect (alors en cours stabilisation à partir des protocoles OAuth 2.0 et OpenID Connect) ne pouvait pas être hébergé sur GitHub (seuls des cas d'usage, une version de test et de la documentation ont été déposés sur cette plateforme).

¹⁸ Notes de terrain, 21/01/15.

¹⁹ Chargée de mission web, notes de terrain, 15/12/14.

²⁰ Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

²¹ Cette loi à effet extraterritorial autorise le renseignement américain à exiger la communication de toute information détenue par une entreprise américaine, que ses serveurs soient ou non localisés aux États-Unis. Les fuites du programme PRISM orchestrées par Edward Snowden ont montré que cette modalité du *Patriot Act* (la section 215) était systématiquement requise. L'administration américaine envoyait des requêtes pénales concernant de très vastes segments de population, en dehors de la procédure prévue à cet effet (Landau, 2013).

L'extension, physique et logicielle, du domaine de la souveraineté a produit une mesure de protection vis-à-vis d'un ennemi dédoublé entre les industries de plateformes (Facebook, GitHub, Google) et le *Patriot Act* américain ; et FranceConnect a donc été une discrète action diplomatique de l'État français. Or, comme toute diplomatie, cette action ne s'est pas passée d'alliés : le SGMAP avait intégré les standards d'identification requis par le règlement e-IDAS, adopté par le Parlement européen et le Conseil à l'été 2014, peu avant le début du développement²². Aussi, contrairement à ce que pouvait initialement laisser penser l'adoption de la stratégie de plateforme, l'État n'a pas adopté « sans imagination » des standards dominants ; mais a fait exister une nouvelle version de la souveraineté. Cette souveraineté de l'État, européenne, attentive aux données et aux infrastructures numériques, constituait la réaction, partielle et située, du SGMAP à une vaste épreuve diplomatique qui se jouait sur internet.

Concevoir une ergonomie pour les services publics

Nous savons désormais en quoi a consisté le projet FranceConnect et à quels problèmes pratiques et diplomatiques de l'État cette application était supposée répondre. Il nous reste encore à entrer dans ces plis fonctionnels et étudier les choix de conception : d'abord concernant l'identification, puis l'échange de données. Nous y verrons émerger une deuxième caractéristique de l'État modernisé, non plus souverain en direction d'un ennemi extérieur, mais ergonomique et soucieux de l'accessibilité du service public par les usagers.

Identifier les usagers

Pour commencer arrêtons-nous sur quelques principes de fonctionnement des protocoles OpenID Connect et OAuth 2.0 choisis par les concepteurs pour faire le « Facebook français ». OpenID Connect offre un « accès universel aux administrations en ligne » (figure 2) – à bien distinguer d'un identifiant universel, interdit par la loi Informatique et liberté du 6 janvier 1978 et éternel objet de controverses (Crettiez, 2006 ; Ceyhan, Piazza, 2011). Autrement dit, le protocole a instauré une architecture décentralisée des identités numériques. Cela signifie qu'un usager qui se rendrait sur un site pour effectuer une démarche se verrait offrir le choix entre utiliser un compte local (dans l'exemple ci-dessous, le compte de l'Assurance retraite), ou se connecter avec FranceConnect.

²² Règlement 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.

Figure 2. Interface de connexion à de l'Assurance retraite



Source : www.lassuranceretraite.fr, capture d'écran, 26/11/2018.

Les concepteurs ont insisté auprès de toutes les administrations rencontrées : l'utilisation de FranceConnect doit rester facultative²³, elle est « *un raccourci, non une voie unique* »²⁴. Ils employaient la métaphore du raccourci dans le sens où, l'utilisateur peut se connecter via un compte préexistant (chez l'un des trois « fournisseurs d'identité » : impots.gouv.fr, ameli.fr, idn.laposte.fr) et s'économiser le temps de création d'une identité numérique par site. Une fois l'identifiant et le mot de passe validés, l'utilisateur est reconnu par le « fournisseur d'identité » qui transmet une clé de fédération au site sur lequel l'utilisateur effectue sa démarche. Cette clé contient l'« identité pivot » et permet au site de reconnaître l'utilisateur ; elle équivaut à la présentation d'un document officiel dans une situation de face-à-face. Voyons cette opération de reconnaissance plus en détail afin de comprendre de quel régime de vérification de l'identité il s'agit.

Les données échangées grâce à cette clé (envoyée par le fournisseur d'identité au site du fournisseur de service) se présentent comme un assemblage standardisé de cinq éléments : prénoms, nom, sexe, date, ville et département (ou pays) de naissance²⁵ ; soit des informations d'état civil. Pourquoi, avec une telle technologie, revenir à l'état civil (qui plus est, à un état civil simplifié) ? Les données de l'identité pivot ont été sélectionnées pour deux raisons. La première est synoptique. Au cours du premier mois de développement, l'équipe a fait l'hypothèse que toutes les administrations enregistreraient au moins ces cinq informations, présentes sur les documents que les particuliers fournissent pour demander un service. Elles étaient réputées être « le plus petit dénominateur commun » entre des bases de données structurées pour répondre à des usages administratifs divers (le traitement d'une plainte, l'instruction d'un dossier de départ en retraite, ou la délivrance d'un permis de conduire). Lors des premiers « open labs » (les réunions entre les concepteurs et les ministères ou les opérateurs intéressés par l'installation de FranceConnect) à l'automne 2014, l'hypothèse a été confirmée : ces données permettraient d'authentifier près de

²³ Arrêté du 24 juillet 2015 portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication d'un téléservice dénommé « FranceConnect », art. 2, 3.

²⁴ Notes de terrain, 02/03/15.

²⁵ Arrêté du 24 juillet 2015, art. 3, 1.

90 % des personnes enregistrées dans les bases. Toutefois, un rapide coup d'œil dans les bases leur a donné un aperçu de l'immense hétérogénéité de l'enregistrement étatique de l'identité (y compris sur cinq données). Premièrement, ils ont constaté la diversité des standards de saisie. Deuxièmement, outre les standards locaux, tel ministère ne tenait pas compte des accents, tel autre enregistrait systématiquement les trois prénoms, tel opérateur ne connaissait que le nom de naissance des femmes mariées ; de sorte qu'une même personne qui renouvelait sa carte d'identité n'était, au plan scriptural, pas la même que celle qui déclarait la naissance d'un enfant. Sans compter que, troisièmement, les bases de données elles-mêmes n'étaient jamais « propres » : la saisie n'était pas cohérente sur toutes les lignes et n'était pas à jour si les personnes n'ont pas signalé un changement de situation. Aussi, afin de ne pas désorganiser les applications professionnelles reliées à ces bases, ils ont demandé aux administrations intéressées par FranceConnect de copier leurs bases de données et de réaliser, sur cette copie, une série d'opérations de standardisation des informations d'identité suivant le format d'écriture d'OpenID Connect (par exemple pour les dates de naissance : année-mois-jour).

La seconde raison qui a présidé au choix de l'identification des citoyens par l'État civil tenait de l'économie morale de l'information administrative. Du point de vue strictement algorithmique, il serait possible d'identifier une personne avec moins de cinq données. Par exemple, grâce aux données mobiles, quatre repères spatio-temporels suffiraient à identifier 95 % de la population étasunienne (Montjoye et al., 2013). Mais, si de nombreux acteurs collectent et traitent les *big data* (à des fins commerciales ou sécuritaires), ce n'est pas le cas des opérateurs du service public, soumis au droit de l'Informatique et des libertés. D'ailleurs, même si elles venaient à être collectées, ces informations n'auraient que très peu de sens pour réaliser des démarches en ligne, car elles ne permettent pas de remplir un formulaire administratif. Le raisonnement est le même pour les données biométriques et les traces de navigation : certes, ces données rendent possible la reconnaissance d'une personne à peu de frais (quelques points sur un iris ou un pouce), mais elles ne prennent pas place dans les réseaux tenus de l'instruction administrative qu'a cherché à moderniser FranceConnect.

En conséquence, l'État plateforme qu'ont dessiné les concepteurs de FranceConnect a démultiplié une version ordinaire de l'identification dans l'environnement administratif. Même écrites au format d'OpenID Connect, prénoms, nom, date et lieu de naissance restent des données rudimentaires d'état civil. Toutes les autres informations (filiation, conjoint, nationalité, taille, couleur des yeux, nom marital, signature, etc.) n'ont pas été enregistrées. L'affirmation, dans des choix techniques tels le format et la qualité des données, d'un régime de vérification des individus très minimal a fait exister un État identifiant simple, rassurant (au regard du droit et des usages), ou plus exactement ergonomique en ce sens qu'il est orienté vers une amélioration des conditions du « travail administratif » des usagers des services en ligne (Dujarier, 2008 ; Denis, 2018). Nous allons maintenant appréhender le rapport différencié aux données personnelles, en comparant FranceConnect avec la technologie qui sert de référence (autant que de repoussoir) au projet, Facebook Connect. Nous continuerons également d'explorer les fonctions de l'application en nous penchant sur les modalités de l'échange de données.

Échanger des données administratives

Sur le réseau social Facebook, l'identité personnelle dépasse les seules informations renseignées et le couple identifiant et mot de passe. Elle est le produit d'une présentation de soi continue et très contrôlée (Turkle, 2011, p. 182-186). En revanche, pour Facebook, l'identité prend forme dans le « graphe social », un tissu d'agrégats de données, accumulées, classées et exploitées pour agencer les actualités et vendre des espaces publicitaires (Cardon, 2015, p. 35). Comme pour le reste des services gratuits proposés par la plateforme, la commodité de Facebook Connect a un coût caché (Egelman, 2013 ; Robinson et Bonneau, 2014) : récolter plus de données sur le comportement des usagers sur les sites qui installent le bouton et vendre du ciblage et des emplacements publicitaires (sur Facebook). Dans ce régime de connaissance par profil, le site « *enregistre bien les comportements, mais sans vraiment connaître les individus* » (Cardon, 2015, p. 23). Autrement dit, « *les personnes ont tendance à disparaître derrière les traces* » (Cardon, 2015, p. 37).

Par contraste avec les *big data* nécessaires à l'actualisation du graphe social, avec une technologie pourtant similaire, FranceConnect a établi un tout autre rapport à l'identification et aux données. Dans un premier temps, FranceConnect transfère l'identité pivot puis organise, à la demande de l'utilisateur, des échanges de données, ponctuels et cryptographiés, entre administrations. L'échange est réalisé lorsque l'utilisateur fournit les pièces requises par la procédure. Il peut alors choisir entre demander à FranceConnect de transférer les pièces justificatives d'une administration à l'autre (figure 3), ou transmettre cette information par des moyens traditionnels (courrier, guichet). Contrairement aux démarches physiques dans lesquelles les usagers copient des documents originaux (l'avis d'imposition) et obligent les agents instructeurs à « *plonger dans l'écrit* » pour localiser la donnée nécessaire au passage du service (Denis, 2018, p. 138), FranceConnect rend possible l'échange d'une donnée située (la seule ligne du revenu fiscal de référence plutôt que les quatre pages de l'avis d'imposition). L'un des points d'intérêt de cette technologie frugale en données personnelles est, selon ses concepteurs, que « *l'administration apprend à consommer de la donnée correctement* »²⁶. En effet, au cours des projets de modernisation antérieurs, les agents ont constaté non seulement l'hétérogénéité des pièces requises pour réaliser une même démarche, d'un guichet à l'autre, mais surtout la surconsommation de pièces par rapport à ce qui est techniquement requis pour l'instruction. « *Rien que pour renouveler une carte d'identité, c'est hallucinant tout ce qu'on demande d'inutile, et je ne parle même pas de Neuilly ni du guichet des étrangers dans n'importe quelle préfecture...* »²⁷. La standardisation via FranceConnect revêt ici des enjeux d'égalité devant le droit.

²⁶ Juriste, notes de terrain, 13/10/14.

²⁷ *Ibid.*

Figure 3. Autorisation d'échanger une donnée, SGMAP, 2017



Source : DINSIC, test FranceConnect, capture d'écran, 10/08/2017.

L'échange de données dans FranceConnect permettrait donc de simplifier le travail administratif des usagers, de limiter les fluctuations et solidifier des dossiers pour lesquels il manque souvent un justificatif ou persiste une erreur de remplissage et, en retour, d'optimiser le temps d'instruction des agents²⁸. Comme pour les données de l'identité pivot, cette simplification n'a pas nécessité d'interconnexion de bases de données professionnelles. Les concepteurs et les administrations intéressées par FranceConnect ont progressivement isolé et standardisé une copie des données repérées pour leur caractère récurrent dans les formulaires administratifs (attestation de domicile, revenu fiscal de référence, quotient familial, attestation de sécurité sociale). D'ailleurs, sans ce ciblage des données, les concepteurs se seraient heurtés aux règles du droit de l'informatique : l'accès et l'interconnexion non contrôlés de systèmes d'information sont interdits. De plus, contrairement à ce que font les plateformes, le système reste décentralisé. Il n'y a pas de serveur unique, l'équipe a scrupuleusement laissé les données dans chacune des administrations participant aux échanges.

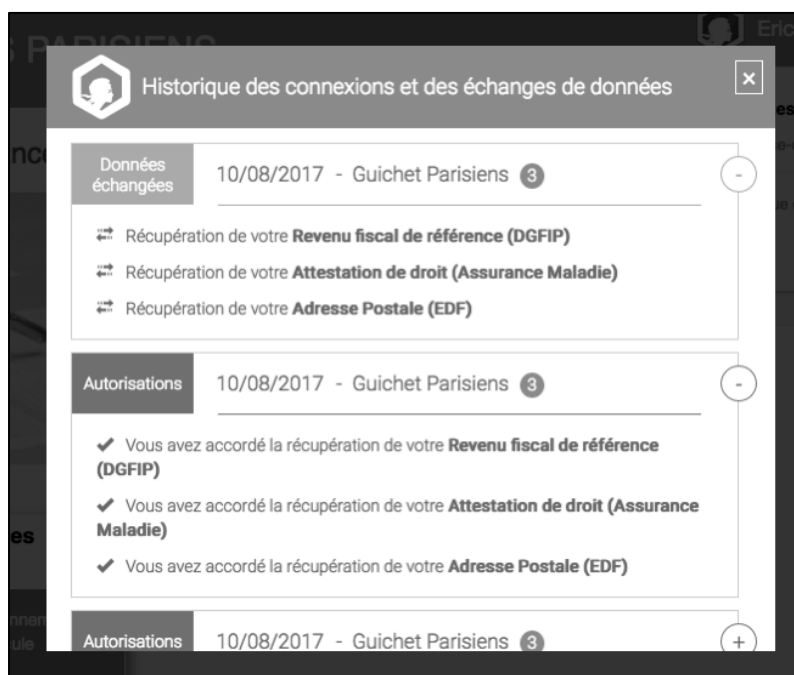
Les concepteurs ont donc bâti une architecture proche de la lettre du droit et frugale en données, dans laquelle la circulation est orientée vers la délivrance d'un service à l'utilisateur. Pour ce faire, FranceConnect a intégré un certain nombre de critiques juridiques, sociales et morales concernant la surveillance technologique ; autant adressées à l'identification étatique (Ceyhan, 2004 ; Lyon, 2009 ; Ceyhan et Piazza, 2011), qu'aux applications des plateformes comme Facebook Connect (Robinson et Bonneau, 2014, Egleman, 2013 ; Miculan et Urban, 2011). D'abord, personne n'est jamais contraint d'utiliser FranceConnect : on peut à tout moment réaliser la même démarche par d'autres moyens. Ensuite, contrairement au régime d'autorisation de Facebook Connect dans lequel le fournisseur de service et la plateforme récupèrent des informations, les données de FranceConnect transitent dans un circuit fermé, actionné à la demande expresse de l'utilisateur (figure 3). En un sens, les concepteurs ont fait du caractère facultatif et minimaliste de FranceConnect une ressource pour favoriser la confiance des usagers.

Dans cette lignée d'opérations pour susciter la confiance et se conformer à la législation,

²⁸ On l'a vu, FranceConnect a été conçu à destination des usagers (actuels et potentiels) des services publics en ligne. Au-delà d'un idéal d'automatisation peu explicité dans le projet d'État plateforme, les conséquences pratiques sur le travail des agents instructeurs ont peu été anticipées.

lors des discussions avec la CNIL²⁹, au printemps et à l'été 2016, FranceConnect s'est vue amplifier d'un registre de traçabilité (figure 4). Le registre permet d'appréhender l'ensemble des connexions et des échanges de données autorisés. Cette « mémoire pour le futur » (Torny, 2003) s'est appuyée sur des pratiques d'écriture déjà standardisées sur un grand nombre de sites et d'applications (l'historique des connexions) et assure par ce formalisme la production *a priori* de preuves en cas de problèmes futurs – une contestation, voire un contentieux. Toutefois, à la différence de la traçabilité en vigueur ailleurs, seuls les usagers (et le juge le cas échéant) accèdent à l'historique complet des échanges. Les administrations impliquées dans FranceConnect reçoivent des clés de chiffrement demandant de fournir une identité pivot ou une donnée (de manière cryptée), mais ne connaissent pas le motif de la demande (la procédure initiée) ni le destinataire (« guichet des Parisiens », figure 4). L'utilisateur, placé au centre du dispositif, est en mesure d'exercer une vigilance active sur ses données personnelles, même longtemps après la délivrance du service.

Figure 4. Registre de traçabilité de l'utilisateur



Source : DINSIC, test FranceConnect, capture d'écran, 10/08/2017.

L'État qui a émergé de cette plateforme d'identification et d'échange de données personnelles se distingue donc par un souci des conditions informatiques de la délivrance du service public. Nous nommerons ce souci, à la fois juridique et pratique, liant des problématiques de commodité d'usage, de confort, de confiance et de transparence des opérations administratives, souci ergonomique de l'État. La qualification ergonomique vient souligner la finalité de cette

²⁹ CNIL, Délibération n° 2015-254 du 16 juillet 2015 portant avis sur un projet d'arrêté portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication d'un téléservice dénommé « FranceConnect ».

forme singulière de modernisation de l'État mentionnée plus haut : améliorer les conditions du travail administratif des usagers des services publics – en l'espèce le remplissage de formulaires et la justification de demandes adressées aux différentes administrations. Souverain et ergonomique voici donc les deux caractéristiques de l'État plateforme qui ont émergé des choix de conception de FranceConnect et sur lesquels il nous faut maintenant conclure.

Conclusion

L'État qui a pris forme dans cette entreprise de modernisation de l'identification n'est évidemment pas tout l'État : on crée toujours des comptes, présente toujours sa carte d'identité et la police continue d'exercer ses activités de surveillance. FranceConnect tient pourtant lieu d'instance d'explicitation, d'épreuve d'État (Linhardt, 2018), en ce sens que l'application offre un accès privilégié à un aspect du mode d'existence de l'État contemporain. En s'appuyant sur le concept stratégique de plateforme, en rassemblant le droit autour de la souveraineté numérique, en mobilisant des protocoles libres et en reconstruisant des bases de données minimisées et des registres de traçabilité qui donnent des prises aux usagers, l'État s'est manifesté sous une forme située, théorisée par les acteurs du SGMAP sous le nom d'État plateforme. Cette forme historiquement ancrée tient à la fois de l'ergonomie (avec une attention à l'intelligibilité des interfaces, mais aussi à l'accessibilité, la traçabilité et la confiance, dans le but de simplifier le travail administratif) et de la souveraineté (en se prémunissant des collectes massives de données, en concevant sa propre API et en faisant exister une juridiction européenne et nationale sur internet).

D'aucuns seront tentés de requalifier FranceConnect d'instrumentation de l'action publique (Halpern, Lascoumes et Le Galès, 2014). Or, l'intérêt de rentrer dans les sries de la conception est bien de voir, aux côtés des acteurs, que rien n'est gagné d'avance et n'a pu être déduit d'un quelconque document stratégique sur la modernisation de l'État. C'est en répondant à des problèmes qui ont pu sembler purement techniques, à propos de l'identification des usagers et de l'échange des données administratives, que les concepteurs ont façonné cette réalité de l'État plateforme.

Il reste maintenant à signaler l'extrême fragilité, institutionnelle et technique, de cette manifestation de l'État. À peine le bouton FranceConnect installé, les activités de ceux que nous avons appelés les concepteurs évoluent vers la maintenance. Les accomplissements autour de l'ergonomie et de la souveraineté sont intégrés et devenus moins sensibles. De nouvelles épreuves apparaissent : la transmission du savoir-faire, la responsabilité en cas de bug, la mise à jour des protocoles, l'intégration d'entreprises privées, induisant à chaque fois des réaménagements plus ou moins profonds. En outre, depuis le 22 novembre 2017, le SGMAP n'existe plus. Il a été divisé en deux administrations, l'une rattachée au secrétariat d'État au Numérique et l'autre au ministère des Finances. La première poursuit officiellement le programme d'État plateforme, tandis que la deuxième est en charge de la transformation de l'action publique. L'État plateforme semble devenu un mot d'ordre parmi d'autres. Les priorités sont désormais redistribuées en faveur du développement de l'intelligence artificielle, de l'économie comportementale et de la mutualisation des infrastructures informatiques ; soit autant de pistes d'enquêtes et de nouvelles épreuves pour tracer d'autres modes d'existence de l'État.

Références

- Akrich M. (1989), « La construction d'un système socio-technique. Esquisse pour une anthropologie des techniques », *Anthropologie et Sociétés*, vol.13, n°2, pp. 31-54.
- Bezes P. (2010), « Morphologie de la RGPP. Une mise en perspective historique et comparative », *Revue française d'administration publique*, vol. 136, n°4, pp. 775-802.
- Bijker W., Hughes T., Pinch T. (eds.) (1993), *The Social Construction of Technological Systems. New Directions in the Sociology and History of Technology*, Cambridge (Ma), MIT Press.
- Bijker W., Law J. (eds.) (1992), *Shaping Technology / Building Society*, Cambridge (Ma), MIT Press.
- Cardon D. (2015), *À quoi rêvent les algorithmes ? Nos vies à l'heure des big data*. Paris, Le Seuil.
- Ceyhan A. (2004), « Sécurité, frontières et surveillance aux États-Unis après le 11 septembre 2001 », *Cultures & Conflits*, vol. 53, n°1, pp. 113-145.
- Ceyhan A., Piazza P. (eds.) (2011), *L'identification biométrique : champs, acteurs, enjeux et controverses*, Paris, Éditions de la MSH.
- Crettiez X. (ed.) (2006), *Du papier à la biométrie : identifier les individus*, Paris, Presses de Sciences Po.
- Dagiral É. (2007), « La construction socio-technique de l'administration électronique. Les usagers et les usages de l'administration fiscale », *Thèse de sociologie*, École nationale des ponts et chaussées.
- Denis J., Goëta S. (2017), « Rawification and the careful generation of Open Government Data », *Social Studies of Science*, vol. 47, n°5, pp. 604-629.
- Denis J. (2018), *Le Travail invisible des données. Éléments pour une sociologie des infrastructures scripturales*, Paris, Presses des mines.
- Denis V. (2008), *Une histoire de l'identité : France, 1715-1815*, Seyssel, Champ Vallon.
- Denis V., Ilsen A. (2010), *Histoire de l'identification des personnes*, Paris, La Découverte.
- Denis V., Lacour P.-Y. (2016), « La logistique des savoirs. Surabondance d'informations et technologies de papier au XVIII^e s. », *Genèses*, vol. 102, n°1, pp. 107-122.
- Dujarier M.-A. (2008), *Le Travail du consommateur*, Paris, La Découverte.
- Egelman S. (2013), « My profile is my Password, Verify Me !: the Privacy/Convenience Tradeoff of Facebook Connect », in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, New York (NY), ACM Press, pp. 2369-2378.
- Gélédan F. (2012), « Le management au secours des services publics ? Modernisation de l'État et régimes de domination à l'heure de la Révision générale des politiques publiques (RGPP), 2007-2012 », *Siècles* [En ligne], n°35-36, URL : <https://journals.openedition.org/siecles/1436>, (consulté le 26/11/2018).
- Gélédan F. (2016), « Spectres du Léviathan. L'État à l'épreuve de la simplification administrative », *Revue française d'administration publique*, vol. 1, n°15, pp. 33-48.
- Halpern C., Lascoumes P., Le Galès P. (eds.) (2014), *L'Instrumentation de l'action publique : Controverses, résistance, effets*, Paris, Presses de Sciences Po.
- Landau S. (2013), « Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations », *IEEE Security & Privacy*, vol. 11, n°4, pp. 54-63.
- Linhardt D. (2018), « L'État de société. Considérations sur la méthode », in B. Karsenti et D. Linhardt (eds.), *État et société politique. Approches sociologiques et philosophiques*, Paris, Éditions de l'ÉHESS (Raisons pratiques, vol. 27), pp. 63-81.
- Linhardt D., Moreau de Bellaing C. (2005), « Légitime violence ? Enquête sur la réalité de l'État démocratique », *Revue française de science politique*, vol. 55, n°2, pp. 269-298.
- Linhardt D., Muniesa F. (2011), « Du Ministère à l'agence. Enquête sur un processus d'altération politique », *Politix*, vol. 95, n°3, pp. 73-102.

- Lyon D. (2009), *Identifying Citizens: ID Cards as Surveillance*, Cambridge (Ma), Polity Press.
- Miculan M., Urban C. (2011), « Formal Analysis of Facebook Connect Single Sign-On Authentication Protocol », in *SOFSEM*, vol. 11, n°1, pp. 22-28.
- Monod J.-C. (2007), *Penser l'ennemi, affronter l'exception. Réflexions critiques sur l'actualité de Carl Schmitt*, Paris, La découverte.
- Montoye (de) Y.-A, Hidalgo C. A., Verleysen M., Blondel V. D. (2013), « Unique in the Crowd: The Privacy Bounds of Human Mobility », *Nature. Scientific reports*, vol. 3, n°1, pp. 1376.
- Noiriel G. (1988), *Le Creuset français : histoire de l'immigration (19^e-20^e siècles)*, Paris, Seuil.
- O'Reilly T. (2010), « Government as a Platform », *Innovations*, vol. 6, n°1, pp. 13-40.
- Piazza P. (2004), *Histoire de la carte nationale d'identité*, Paris, Odile Jacob.
- Plantin J.-C., Lagoze C., Edwards P., Sandvig C. (2016), « Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook », *New Media & Society*, vol. 20, n°1, pp. 293-310.
- Robinson N., Bonneau J. (2014), « Cognitive Disconnect: Understanding Facebook Connect Login Permissions », in *Proceedings of the second ACM conference on Online social networks*, ACM, pp. 247-258.
- Tchente D., Baptiste-Jessel N., Canut M.-F. (2011), « Accès à l'information dans les réseaux sociaux », *Hermès*, vol. 59, n°1, pp. 59-64.
- Torny D. (2003), « Une mémoire pour le futur. La traçabilité comme allocateur de responsabilité », in P. Pédrot (ed.), *Traçabilité et responsabilité*, Paris, Économica, pp. 72-87.
- Truche P., Faugère J.-P., Flichy P. (2002), « Administration électronique et protection des données personnelles », livre blanc remis au ministre de la Fonction publique, La documentation française.
- Turkle S. (2011), *Alone together. Why We Expect More from Technology and Less from Each Other*, New-York, Basic Books.
- Verdier H., Colin N. (2012), *L'Âge de la Multitude. Entreprendre et gouverner après la révolution numérique*, Paris, Armand Colin.
- Weller J.-M. (1998), « La modernisation des services publics par l'utilisateur : une revue de la littérature (1986-1996) », *Sociologie du travail*, vol. 40, n°3, pp. 365-392.

Marie Alauzen est doctorante au Centre de sociologie de l'innovation, de Mines ParisTech, marie.alauzen@mines-paristech.fr. Sa thèse porte sur la modernisation de l'État et notamment le programme d'État plateforme visant à reconfigurer les administrations autour des mots d'ordre de la simplification, de l'amélioration du confort des usagers ou encore de l'embellissement informatique de l'État.