Les tressautements du "devenir interface" de notre relation à l'État : Controverse sur l'expérimentation d'Alicem

Marie Alauzen

Les tressautements du devenir interface de notre relation à l'État
Controverse sur l'expérimentation d'ALICEM

Marie Alauzen[1]

> « Si la population française consent à recourir à la reconnaissance faciale dans son quotidien de consommateur, pratique contribuant à la désensibiliser selon certains sociologues, elle n'est pas prête à en accepter l'exploitation par les forces de l'ordre à n'importe quelle condition. La société française, traumatisée par le régime de Vichy et son système d'enregistrement d'identité, conserve dans son ADN collectif des marqueurs de rejet du fichage étatique[2]. »

L'histoire de la monopolisation de l'identification par les États est tissée d'une telle multiplicité de controverses, de mouvements de résistance au contrôle social et de tensions pour institutionnaliser techniques et fichiers d'identité (About, Ilsen, Lonergan, 2013 ; Breckenridge, 2014 ; Caplan, Torpey, 2001 ; Ceylan, Piazza, 2011 ; Crettiez, Piazza, 2010 ; Higgs, 2003 ; Noiriel, 2007), que l'on peut la considérer comme l'un des cas typiques de controverse qui ne refroidit jamais (Callon, 1986 ; Barthe, Linhardt, 2009 ; Chateauraynaud, Debaz, 2017). SAFARI, EDVIGE, INÉS, FNAEG, TAJ, TÉS ou plus récemment SIDÉP : au cours des cinquante dernières années, en France, les observateurs, spécialistes de l'identification ou professionnels concernés, ont souligné la centralité des dynamiques conflictuelles et l'inventivité administrative pour réduire l'identification à de la pure information, la dépolitiser ou, au contraire, pour problématiser la constitution de tels fichiers et intégrer, comme en témoigne la note de la Gendarmerie en exergue, des éléments de la critique.

Avec, d'un côté, des techniques biométriques de reconnaissance faciale et digitale ou de traçage numérique plus ancrées dans l'analyse des comportements que les précédentes techniques d'identification et, de l'autre, la performance accrue des systèmes de classement de l'information normalisés par le marché de la sécurité et par les industries de plateformes, on assiste depuis le tournant des années 2010 à un phénomène inédit. L'usage par les États de technologies d'identification et d'authentification pose

---

[1] Cette étude a été réalisée dans le cadre de deux contrats de recherche avec la Chaire identité numérique responsable de Télécom Paris entre janvier 2019 et juillet 2020. Une version préalable de l'article a été discutée par Florent Castagnino, Martin Drago et Jonathan Keller dont les questions et les commentaires m'ont permis de clarifier des points décisifs. Je remercie les relecteurs de la revue de leurs remarques bénéfiques. Les propos défendus et les éventuelles erreurs m'appartiennent.

[2] Centre de recherche de l'École des officiers de la Gendarmerie nationale, « Reconnaissance faciale et contrôles préventifs sur la voie publique, l'enjeu de l'acceptabilité », note nº 43, septembre 2019, p. 1.

régulièrement un problème[1] ; c'est le « rejet du fichage étatique » qui réactive la controverse historique et n'a pas échappé au Centre de recherche de l'École des officiers de la Gendarmerie nationale. Or, dans leur vie quotidienne, nombreux sont ceux qui recourent à ces technologies pour des raisons de commodité. Pour ne prendre que l'exemple des technologies biométriques qui cristallisent, sans doute plus que toutes autres, la critique (Ceylan, Piazza, 2011) : pour déverrouiller un téléphone ou accéder à un espace de travail sécurisé, elles se superposent désormais aux badges et aux mots de passe. Ce paradoxe d'une sensibilité politique accrue à l'identification étatique et d'une commodification des usages privés a été identifié par les administrations et c'est sur le terrain de la mise en forme du problème de la reconnaissance à distance des personnes par l'État et de ses conséquences politiques, en France, que nous mène cet article.

Au début des années 2010, deux événements ont encadré les technologies de reconnaissance des personnes physiques : la censure partielle de la loi pour la protection de l'identité par le Conseil constitutionnel le 6 mars 2012[2], mettant un terme au projet INÉS conférant de nouvelles fonctionnalités à la carte nationale d'identité électronique (Lacouette-Fougère, 2011 ; Piazza, 2006), et l'entrée en vigueur du règlement européen sur l'identification électronique et les services de confiance du 23 juin 2014 (EIDAS)[3], instituant des niveaux d'identification. Ces deux textes ont reconfiguré l'équipement juridique et clarifié les conditions de la reconnaissance à distance des populations par l'État. Ce principe d'une reconnaissance entièrement à distance, sans la médiation d'un agent régissant, à un bout ou l'un autre de la chaîne, l'épreuve documentaire de la présentation des papiers ou authentifiant le geste de la signature, témoigne d'une transformation majeure du rapport entre l'État garant dans le passé, le présent et l'avenir des identités civiles et les usagers des services publics.

Loin de la simple extraction des écrits authentiques et des documents d'identité de leur enveloppe de cellulose (Fraenkel, Pontille, 2003), la reconnaissance par l'État des personnes à distance actualise la possibilité, sous-tendue par la dématérialisation des procédures administratives, d'un *devenir interface* de notre relation à l'État. Cette expression ne désigne nullement un équipement neutre de la relation administrative, mais la

[1] L'authentification désigne à l'origine une écriture sur soi : une signature, un sceau, un cachet qui fait que le scripteur considère l'écrit en surplomb, comme le résultant de sa volonté (Fraenkel, Pontille, 2003). En informatique, elle renvoie à une procédure de singularisation de l'identité d'une utilisatrice qui accède à un système ou un réseau (*login*) ; là où l'identification désigne la même action de singularisation effectuée par un tiers pour s'assurer de l'identité de l'utilisatrice. Dans de nombreuses technologies, dont celle examinée ici, ces deux régimes d'action se confondent : l'État créé un dispositif d'identification au moyen duquel les personnes s'authentifient ; autrement dit, il s'agit d'une coproduction de l'identité numérique.

[2] Conseil constitutionnel, décision de non-conformité partielle n° 2012-652 DC du 22 mars 2012 sur la loi relative à la protection de l'identité.

[3] Règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.

possibilité d'une atténuation du mode de présence bureaucratique de l'État en société, qui emporte avec elle une mutation de la culture matérielle (remplissage de formulaires, constitution de dossiers personnels, signature, stockage de données…), induite par les interactions entre les personnes et les machines, en même temps que des reconfigurations du risque (fuite de données, piratage, surveillance…) et des ajustements discrets des acteurs impliqués (industriels ou hackers, en plus des agents identificateurs et des personnes identifiées). Or, contrairement à d'autres facettes de la modernisation contemporaine de l'État (dont la réduction du nombre de fonctionnaires ou le recours aux consultants), cette propension n'est jamais explicitée ni objet d'un débat public ; de sorte qu'il est difficile d'en saisir les effets, au-delà des interpellations sur le creusement de la fracture numérique et de l'expansion d'une surveillance généralisée. Elle façonne pourtant le rapport à l'État de catégories de la population familières avec les technologies numériques et capables, par exemple, de valider leur déclaration de revenus en quelques clics, puis d'être prélevées sur leur compte bancaire et ne plus se soucier d'un acte aussi symbolique que l'acquittement de l'impôt sur le revenu, jusqu'à n'exister, elles aussi, plus que sous la forme d'information dans les logiciels des administrations (Grommé, Ruppert, 2020).

Partant de ces nouveaux montages du droit et de possibilités technologiques renouvelées, les administrations ont produit différents dispositifs de reconnaissance à distance. Outre les systèmes d'identifiant personnel couplé à un mot de passe conçus pour une procédure donnée, à partir de la rentrée 2014, l'administration de mission responsable de la réforme de l'État a élaboré l'application FranceConnect. Conçue sur le modèle des boutons « se connecter avec Facebook, Google, LinkedIn, etc. », elle a fait de la simplicité et de l'ergonomie de connexion non pas à un, mais à l'ensemble des services publics un enjeu politique central, constitutif du projet d'État plateforme (Alauzen, 2019). À partir de 2016, le ministère de l'Intérieur a quant à lui mis au point l'expérimentation de l'application d'« Authentification en ligne certifiée sur mobile » (ALICEM), dans le but de fournir, par l'intermédiaire de FranceConnect, une identité numérique plus sécurisée, sans objet technique certifié ni agent assermenté. L'application, installée sur le téléphone portable, requiert que son utilisatrice compare elle-même son visage avec l'image enregistrée sur la puce de son titre biométrique pour accéder aux services publics. Cette mise au travail, qui parie sur l'équipement mobile, la familiarité avec l'authentification par reconnaissance faciale, la fiabilité de la collecte de données par ce même terminal mobile et la performance d'un algorithme de comparaison d'images localisé au ministère de l'Intérieur, porte en elle un profond bouleversement du rapport à l'État. Elle constitue à la fois une « épreuve de composition de l'État », soit une situation dans laquelle la réalité de ce qu'est l'État à un moment et en un lieu donnés s'explicite (Linhardt, 2009), et façonne, en retour, un type de sujet politique (Akrich, 1992). Or, contrairement à l'application FranceConnect qui s'est imposée par les usages ou à de nombreuses technologies administratives participant discrètement de ce devenir interface de la relation à l'État, l'épreuve en question a été une épreuve de force ; car l'introduction de

l'agencement des citoyens-utilisateurs reliés à l'État par leur mobile a ravivé la chaleur de la controverse sur l'identification étatique, politisant peut-être pour la première fois les contours de cette métamorphose par les technologies numériques.

Que nous apprend ce nouvel agencement controversé ? Quels glissements politiques entraîne cette technologie d'identification relevant de l'expérimentation et d'une sensibilité à la critique ? Le cas permet d'estimer la consistance du devenir interface précédemment évoqué, en mettant en lumière des changements dans les relations politiques et administratives liant une entité « État » à certains membres de la société : personnes identifiées, dont des testeurs, acteurs des services publics, y compris à titre dérogatoire — dont les *white hats*, mais aussi industries offrant des technologies numériques. Je m'appuierai sur les méthodes et les descripteurs de la sociologie des sciences et des techniques (Bijker *et al.*, 1987 ; Callon, 1986 ; Latour, 1985) et enchâsserai le récit de la controverse dans les développements de la sociologie de l'État et de la sociologie de l'action publique en prise avec les questions technologiques (Barthe, 2006 ; Chateauraynaud, Torny, 1999 ; Hecht, 2014 ; Laurent, 2022). J'explorerai d'abord la stabilisation de l'agencement technologique qui est l'objet de la controverse, en dépliant la configuration de l'État identifiant et de l'utilisatrice identifiée dans et par cette technologie. Puis, je considérerai sa déstabilisation dans le temps de l'alerte lancée contre l'application, la mobilisation des pouvoirs publics et la multiplication des arènes de la controverse ; soit trois séquences au cours desquelles l'agencement proposé par ALICEM est éprouvé et donne à voir des visions conflictuelles des relations entre l'État identifiant, cette technologie mobile et les personnes identifiées. Enfin, je dégagerai deux caractéristiques sur le devenir interface de notre relation à l'État susceptibles de compléter les comptes rendus existants sur la surveillance et la fracture numérique. Il s'agit de la mise en exergue d'une politique du mode expérimental de gouvernement et de la préoccupation de l'État de se signaler auprès des acteurs du marché.

Mon enquête s'appuie sur la collecte et le traitement de trois types de données. Premièrement, l'étude des documents publiés dans les médias (presse écrite et en ligne, télévision, radio, réseaux sociaux), entre mars 2016 et mars 2020, dessine l'arène médiatique de la controverse. Cette arène constitue un poste d'observation privilégié des effets sociaux des signaux d'alerte. Plus largement, son analyse facilite le suivi des trajectoires argumentatives des concepteurs et des opposants et offre un accès aux enjeux de moralité, de justice et d'identité collective soulevés par cet objet contesté. Deuxièmement, l'enquête plonge dans la littérature institutionnelle et les documents d'expertise produits par les acteurs de la controverse (réglementation, rapports publics, notes administratives, dossier contentieux), pour appréhender la technicité juridique et informatique de l'application. Ces sources permettent de déchiffrer les ambitions inscrites dans la technologie et les modalités d'étatisation des utilisateurs d'ALICEM. Enfin, j'ai complété l'examen des sources documentaires d'entretiens avec des concepteurs, des évaluateurs et des promoteurs de l'application (n=7) et de séquences d'observations des

espaces de débat : les consultations du Conseil national du numérique [CNNUM] menées à l'automne 2019, les auditions de la mission commune identité numérique de l'Assemblée nationale conduites de novembre 2019 à juin 2020, ainsi que quelques événements, administratifs ou militants, dédiés à l'identité numérique. Ces matériaux me permettent de donner une plus juste consistance à la mutation inscrite dans l'application, pondérant les déclarations d'intention par les difficultés pratiques et tenant compte de la réflexivité des agents publics et des groupes mobilisés.

Nouvel agencement de l'identification numérique : description socio-technique de l'application ALICEM

Afin d'éclairer les termes de la mobilisation contre l'application ALICEM, j'examinerai d'abord le contexte institutionnel et juridique dans lequel l'application a été problématisée — au sens que lui confère Michel Callon de l'effort pour rendre quelque chose indispensable (Callon, 1986) — par l'Agence nationale des titres sécurisés (ANTS) du ministère de l'Intérieur, avant de considérer, dans son fonctionnement technique, la configuration de l'identité numérique générée par la collecte des données personnelles lors de l'activation de l'application. Dans la lignée ouverte par la sociologie des sciences et des techniques, nous nous intéresserons donc à la manière dont un objet technique définit les actants et les relations entre les actants, pré-inscrivant ainsi des rôles, une géographie de la responsabilité et un ordre politique et moral (Akrich, 1992 ; Bijker *et al.*, 1987).

Problématisation d'un État européanisé garant des identités numériques

« C'est génétique, depuis [la censure partielle du Conseil constitutionnel en] 2012, l'Intérieur n'a jamais cessé de développer des solutions d'identité numérique, ALICEM entre autres[1] », lança un agent au cours d'un séminaire consacré à l'identité numérique organisé par la Commission nationale de l'informatique et des libertés (CNIL). ALICEM, mentionnée par cet agent au détour d'une métaphore biologisante sur l'action du ministère qui a établi un monopole historique sur l'identification des personnes physiques (Piazza, 2004), est une application pour téléphone mobile dont le prototype a, en effet, été conçu durant de longues années par le département de l'innovation de l'ANTS rattachée au ministère de l'Intérieur. Elle a été mise au point à partir de décembre 2016 par le prestataire de services numériques Gemalto, devenu, au printemps 2019, Thales Digital. L'application doit permettre à tout particulier qui décide de l'utiliser de prouver son identité sur internet « de manière sécurisée ».

Le droit européen qui s'impose depuis 2014 aux développements de telles applications associe la notion au niveau de sécurité élevée au sens du règlement EIDAS, c'est-à-dire du

[1] Notes de terrain, séminaire interne de la CNIL, 27 février 2020.

recours à un moyen d'identification des utilisateurs des services en ligne certifié par l'État (en l'espèce, par l'Agence nationale de sécurité des systèmes d'information [ANSSI]), puis notifié à la Commission européenne pour une reconnaissance par l'ensemble des États membres (Encadré 1). L'authentification de la personne suppose, à défaut d'une signature en présence d'un agent assermenté, la comparaison d'une ou plusieurs caractéristiques physiques auprès d'une source faisant autorité (soit, dans la plupart des cas, un document officiel d'identité).

Encadré 1 : le règlement EIDAS, ou le dessein de produire l'Europe et les sujets européens par les objets techniques

Le Parlement européen et le Conseil de l'Union européenne ont adopté, le 23 juillet 2014, le règlement nº 910/2014/UE sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement EIDAS. L'adoption de ce règlement fait suite à un relatif constat d'échec de la directive 1999/93/CE sur la signature électronique (Blanchette, 2006 ; Fraenkel, Pontille, 2003). Le règlement a été publié au *Journal officiel de l'Union européenne* le 28 août 2014 et est entré en vigueur le 17 septembre 2014. Il est applicable depuis le 1er juillet 2016 pour la majeure partie de ses dispositions, et, depuis février 2020, la Commission communique sur de prochaines révisions de ses dispositions : la création d'un « portefeuille d'identités » et d'un cadre réglementaire plus étroit. Au cours de la période de conception d'ALICEM, trois niveaux de garantie étaient prévus par le règlement :

– Faible : l'objectif est de réduire le risque d'utilisation abusive ou d'altération de l'identité, par exemple, en demandant à l'utilisateur de renseigner un mot de passe ;

– Substantiel : l'objectif est de réduire substantiellement le risque d'utilisation abusive ou d'altération de l'identité, en ajoutant un second facteur d'authentification au mot de passe préalablement saisi, par exemple, un code temporaire envoyé par SMS ;

– Élevé : l'objectif est d'empêcher l'utilisation abusive ou l'altération de l'identité ; par exemple, en ajoutant aux deux niveaux précédents, la présentation d'un titre officiel d'identité.

Les exigences applicables aux niveaux de garantie de l'identification électronique prévus par le règlement sont détaillées dans le règlement d'exécution nº 2015/1502 du 8 septembre 2015. Ces niveaux sont accordés par des organismes nationaux de certification, en fonction du respect de spécifications, de normes et de procédures. Si le règlement est un cas typique de production de l'Europe et des sujets européens par les objets techniques (Grommé, Ruppert, 2020 ; Laurent, 2022 ; Pelizza, 2020), l'européanisation de l'identité numérique n'empêche pas une certaine flexibilité interprétative des États membres ; de sorte que l'accord sur des protocoles, des standards et des usages derrière ces trois niveaux varie amplement d'un certificateur national à

l'autre. En France, l'ANSSI qui fournit une expertise juridique et technique sur l'application du règlement et délivre les niveaux aux concepteurs, publics ou privés, de solutions d'identification est réputée être parmi les certificateurs les plus exigeants.

Dans le règlement, les États membres n'ont pas l'obligation de déclarer de solution d'identification, quel qu'en soit le niveau. En revanche, la reconnaissance mutuelle des moyens d'identification électronique est devenue obligatoire le 29 septembre 2018. Ce qui revient à inciter les États qui enregistrent les technologies de leurs voisins à harmoniser leurs procédures et créer, à leur tour, par un processus de gouvernementalisation proprement européen, des solutions d'identification électronique (Laurent, 2022).

Au moment de l'enquête, il n'existe pas, en France, de solution électronique de niveau élevé. Seules des technologies de niveau substantiel ont été stabilisées dans les services à distance, notamment parmi les fournisseurs d'identité de l'application FranceConnect. Or, « la France n'est pas obligée de faire sa solution d'identité numérique [de niveau élevé], mais elle a tout intérêt à le faire. Elle est la seule à ne pas encore avoir notifié à la Commission européenne[1] », répétaient les agents du ministère de l'Intérieur, mobilisant la rhétorique du retard technologique et de la nécessaire harmonisation européenne. À la nuance près que cette problématisation de l'urgence de l'identification numérique européanisée s'est fondue dans un argumentaire de la souveraineté numérique, qui assimilait les plateformes numériques à l'ennemi dont il fallait protéger la population : « si l'État ne sort pas rapidement une solution d'identité numérique, les GAFAM [Google, Apple, Facebook, Amazon, Microsoft] s'en chargeront[2] ».

Problématisé à partir de l'urgence perçue par le ministère de l'Intérieur de concevoir une solution d'identification sécurisée, additionnée à l'impératif d'harmonisation européenne et aux enjeux de souveraineté numérique, un processus d'irréversibilisation était en cours (Barthe, 2006 ; Chateauraynaud, Debaz, 2017). La technologie ALICEM dans laquelle s'inscrivait cette problématique n'était pas discutable : elle devait être mise à disposition du public français et européen d'ici le 1er janvier 2020. Regardons plus avant les spécificités de cette application et l'identité numérique qu'elle coproduit avec ses futurs utilisateurs.

Configuration du sujet politique en utilisateur de mobile

Croisant les écrits sur l'identification des personnes et sur la configuration socio-technique des usagers, les études sur les systèmes d'identification ont montré la dimension coproduite et performative des technologies qui transforment les in-dividus en des identités lisibles, par l'intermédiaire d'une longue chaîne de traduction (Pelizza, 2020, 2021 ; Roa, 2018 ; Van der Ploeg, 2003). Pour décrypter le processus de co-production

[1] Entretien avec un cadre du ministère de l'Intérieur, 25 novembre 2019.
[2] Notes de terrain, chargé de mission à la Direction interministérielle du numérique, 19 juin 2019.

par lequel l'utilisatrice d'un téléphone mobile se mue en une identité numérique sécurisée, il faut repartir du script contenu dans le cadre réglementaire.

Suivant le décret n° 2019-452 du 13 mai 2019 autorisant la création d'un moyen d'identification électronique dénommé ALICEM, l'application pour générer une identité numérique a été mise au point pour les systèmes d'exploitation Android mobiles non débridés. Ce paramétrage exclut les populations qui seraient équipées d'autres systèmes d'exploitation que celui de Google (par exemple, celui d'Apple dont l'écriture du système est inaccessible), ou auraient débridé leur téléphone mobile, c'est-à-dire disposeraient de tous les droits d'administration de ce dernier (l'accès complet aux fichiers et couches du système d'exploitation, pour supprimer des applications du système, lancer des applications exigeant des droits d'administrateur ou remplacer le système d'exploitation du mobile). La seconde condition d'utilisation de l'application est qu'ALICEM n'est accessible qu'aux détenteurs de titres biométriques, soit les personnes en possession d'un titre de séjour, d'un passeport ou d'une carte d'identité délivrée après le 30 mars 2017. Le cumul de ces deux conditions fait qu'indépendamment des dimensions d'accès et d'usage inhérentes à la fracture numérique (Pasquier, 2018 ; Rallet, Rochelandet, 2004), en France, seule une faible portion de la population peut effectivement entrer dans le réseau socio-technique d'ALICEM. « Tout au plus six millions aujourd'hui, c'est presque que symbolique, mais pas avant 2025 pour tous les Français[1] », a estimé un agent de la direction interministériel du numérique (DINUM).

Pour créer une identité numérique ALICEM, l'utilisatrice remplissant les deux conditions télécharge l'application sur son téléphone et doit se créer un compte personnel. De manière habituelle dans les protocoles d'authentification en ligne, elle renseigne une adresse électronique, un numéro de téléphone et saisit un mot de passe. De manière moins habituelle, elle scanne ensuite grâce à la caméra de son téléphone devenue lecteur *Near Field Communication* (NFC) la zone de lecture optique du titre d'identité biométrique, pour que l'application se fasse la « porte-parole » des données contenues dans la puce embarquée (Callon, 1986 ; Pelizza, 2021). Cette opération de lecture de titre à partir d'un téléphone mobile constitue un cas très atypique de « mise au travail » de l'utilisatrice. En effet, si scannant eux-mêmes les produits, les clients contribuent, à l'efficacité productive des entreprises de services, de McDonald à la grande distribution (Tiffon, 2013), et que les usagers des services publics réalisent depuis longtemps des tâches de saisie et de coordination (Dagiral, 2007 ; Mesnel, 2016), une telle coproduction est inattendue dans une procédure d'enrôlement requérant une authentification sûre et certaine, assurée jusqu'alors par un officier d'état civil ou un agent habilité à procéder à un contrôle d'identité et équipé d'un lecteur optique réglementé.

Les six-sept données récupérées par le terminal mobile sur la puce correspondent à celles enregistrées par l'ANTS sur le fichier des titres électroniques sécurisés (TÉS) lors de la

[1] Notes de terrain, participant invité à la semaine de l'innovation publique, 27 novembre 2019.

création du document national d'identité[1]. Elles sont alphanumériques (noms, prénoms, sexe, date et lieu de naissance, nationalité, adresse postale, etc.) et biométriques (taille et couleur des yeux, photographie du visage[2]). Ces données sont, par la suite, stockées dans le téléphone jusqu'à la suppression du compte de l'utilisatrice. « Ce n'est pas la dématérialisation du titre, mais un coffre-fort, une extraction du titre[3] », précise un agent du ministère justifiant le choix d'une architecture décentralisée. L'application envoie ensuite ces données dans la base Docvérif du ministère de l'Intérieur pour contrôler que l'information encodée dans la zone de lecture optique corresponde à un titre d'identité valide.

Pour s'assurer que le titre scanné appartient à l'utilisatrice du téléphone, la mise au travail continue et consacre un renversement du paradigme de l'authentification (Blanchette, 2006 ; Pontille et Fraenkel, 2003). L'utilisatrice doit réaliser deux opérations d'authentification par reconnaissance faciale, traduisant ainsi sa chair en images : une capture dynamique et une capture statique[4]. L'application utilise ensuite un algorithme pour estimer la correspondance entre des repères sur les photos de son visage extraites de la vidéo et celles enregistrées sur le titre encodé dans le fichier TÉS. Une fois l'authentification de l'utilisatrice réussie par alignement des repères, la vidéo et la photo du visage sont supprimées. Jusqu'alors, les données biométriques (image de l'empreinte digitale ou palmaire, de l'iris ou du visage) ne bénéficiaient pas du statut juridique de signe de validation, car elles pouvaient avoir été capturées à l'insu de la personne (Fraenkel, 1992, p. 250-252 ; Fraenkel, Pontille, 2003, p. 101-102). Dans cette procédure banalisée, en particulier par le dispositif de déverrouillage FaceID d'Apple, une telle mise à disposition du visage est considérée comme une opération librement consentie, porteuse des garanties nécessaires à l'authenticité de la procédure. Du fait des réserves de la CNIL[5], des solutions alternatives à l'authentification par reconnaissance faciale seraient toutefois en cours d'élaboration : authentification du porteur de titre lors d'un face à face avec un agent public, dans un service public ou en visioconférence, et par l'activation d'un code barre (*QR code*) ont été envisagés par l'ANTS.

---

[1] Se reporter au décret n° 2016-1 460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité.

[2] Le fichier TÉS contient également un relevé numérisé des empreintes digitales qui n'est pas transféré à l'application. Voir les articles 5 et 6 du décret n° 2019-452 du 13 mai 2019.

[3] Entretien avec un cadre du ministère de l'Intérieur, 21 novembre 2019.

[4] La première est une vidéo prise en temps réel : l'utilisatrice doit cligner des yeux, remuer la tête, visage face à la caméra ; la seconde est une photographie en plan fixe (*selfie*). Sur les implications de disponibilité et de lisibilité des corps par les machines, on se reportera à Van der Ploeg, 2003.

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

Pour l'ensemble de cette manipulation qui étend la chaîne d'actants de la reconnaissance étatique des personnes (Pelizza, 2021 ; Roa, 2018), l'ANTS et l'utilisatrice par l'intermédiaire de l'application mobile, façonnent une identité numérique composée de trente-deux données personnelles[1], aptes à « parler » pour l'ensemble du corps de l'individu. Une fois le compte créé et prêt à s'interfacer avec les fournisseurs de services publics numériques pour le compte de l'utilisatrice, elle peut se connecter aux services requérant une identification élevée en saisissant un code personnel à six chiffres. Elle n'a plus besoin de réitérer la mise en route. Son identité numérique devient alors un « mobile immuable » (Latour, 1985), réputé certifié par l'État français et pouvant circuler sans se transformer dans une zone technologique européenne (puisqu'elle ambitionne d'être interopérable avec les systèmes d'information d'administrations et d'entreprises européennes à l'issue de la notification à la Commission).

Pourtant, ALICEM qui aspirait à amorcer un nouveau mode de relation à l'État pour certains utilisateurs de téléphone mobile n'a finalement jamais été certifiée comme identité numérique de niveau substantiel ni de niveau élevé par l'ANSSI. Elle est restée une identité faible comme celles proposées par de nombreux services publics ou privés. Par ailleurs, selon la DINUM, il n'existe pas en France de démarches réclamant une identité numérique élevée. Cela pourrait être le cas, dans les prochaines années, de la signature électronique de certains actes (les actes notariés ou la souscription d'un contrat), de la procuration, voire du vote en ligne, assuraient les responsables du ministère de l'Intérieur, qui restaient discrets sur les usages envisagés alors qu'apparaissaient les premières contestations visant à infléchir la fatalité et à recomposer la linéarité du temps du déploiement d'ALICEM. Il nous faut donc aller au-delà de la description de l'identification stabilisée dans un tel mode d'emploi et considérer ce qui advient du devenir interface dans les tressautements de l'agencement technologique.

Déstabilisation de l'agencement : alicem serait-elle une application dangereuse ?

Des alertes sur l'application ALICEM sont apparues avant même sa certification et sa mise à disposition du public, dès le lendemain de la publication, au *Journal officiel*, du décret autorisant l'application. Elles ont autant mis en cause les choix politiques, que juridiques ou techniques sur lesquels reposait l'application. Cette opposition à la figure de l'irréversibilité de l'avènement de cette technologie a précipité la réaction des pouvoirs publics et démultiplié les arènes de la controverse, l'orientant vers une problématique non plus d'identification des utilisateurs des services publics, mais d'acceptation de la reconnaissance faciale et, partant, d'un mode de relation numérique et expérimental à l'État.

[1] Soit, en plus des données précitées sur l'identification de la personne et du titre qu'elle détient, les données relatives à l'historique des transactions associées au compte ALICEM qui s'accumuleront au fil des connexions (*logs*) et l'identifiant unique du service de notification.

Double mise en cause et inscription dans des séries de mobilisations

L'application conçue par l'ANTS est apparue au grand public à partir de la publication du décret de création, le 13 mai 2019[1]. Elle n'a toutefois été médiatisée qu'à l'été 2019 et ce défavorablement, avec les signaux d'alerte lancés par l'association de défense des libertés numériques, La Quadrature du net, et par l'expert en sécurité informatique, Baptiste Robert. Ces deux événements ont participé à l'élaboration d'un « contre-discours » visant à déconstruire la problématisation mise en avant par le ministère de l'Intérieur par l'activation d'une mémoire du risque (Chateauraynaud, Torny, 1999).

Le dépôt, le 15 juillet 2019, d'une requête introductive d'instance devant le Conseil d'État par La Quadrature du net lança l'alarme contre ALICEM. L'argumentation juridique que La Quadrature du net a opposée à l'ANTS s'est, en grande partie[2], appuyée sur les considérations critiques de la CNIL dans l'avis du 18 octobre 2018 publié en même temps que le décret. Ce faisant, les lanceurs d'alerte ont fait de la publication de cet avis le premier signal d'une affaire dont la publication et la contestation du décret n'auraient été que des rebondissements. Les situations dans lesquelles les alertes prennent appui sur des indices ou sur des faits établis antérieurement sont courantes dans les affaires et les controverses. Elles ont pour principal effet de recomposer la linéarité du temps et de stabiliser des prises pour l'action politique de contestataires, qui cherchent à ouvrir l'espace des possibles (Chateauraynaud, Torny, 1999, p. 63-68).

Rapidement après l'introduction du recours, les premiers médias généralistes relayaient les arguments de La Quadrature du net mettant en cause l'application : *Le Monde, Le Figaro.fr*, *France Inter*, *La Croix*, *Le Canard enchaîné*. Citant des extraits d'entretiens avec les membres de l'association ou de leur communiqué de presse, les journalistes se fondent sur le raisonnement juridique et politique des lanceurs d'alerte, en partie standardisé pour favoriser leur décodage et leur reprise médiatique. Les arguments sur l'absence d'alternative à la reconnaissance faciale pour enrôler les utilisateurs opérant un basculement dans l'ère du soupçon généralisé, transformant le contrat de confiance dans l'État, ouvrant la voie à des initiatives comparables à celles de la Chine sécuritaire ont alors ravivé la controverse historique sur l'identification étatique. L'une des spécificités de l'argumentation contre ALICEM reprise avec force dans les médias était la dénonciation d'une « expérimentation à ciel ouvert » de la reconnaissance faciale de la population, à peine masquée par le prétexte de l'accès sécurisé aux services publics.

[1] Avant la publication du décret, seule la presse spécialisée sur les questions administratives (*La lettre A, Acteurs publics*) ou numériques (*L'Usine nouvelle*), un rapport d'information du Sénat de 2016 et le rapport d'activité de l'ANTS en 2018 avaient fait état du développement de l'application.

[2] Du moins dans la version initiale de la requête. Dans le mémoire en réplique envoyé au Conseil d'État en janvier 2020, La Quadrature du net a ajouté un argumentaire sur l'économie du traitement des trente-deux données qui composent l'identité numérique d'ALICEM.

Pour les membres de La Quadrature du net, ALICEM n'était nullement la première application du genre. Elle s'inscrivait dans une série de contentieux que l'association a menée contre l'expansion des usages de la biométrie. L'argumentaire juridique de l'association avait déjà été partiellement structuré par les recours déposés devant les juridictions nationales et européennes contre le fichier des antécédents judiciaires, commun à la police et à la gendarmerie nationales, permettant de faire de la reconnaissance faciale à partir de photographies de personnes mises en cause lors d'une enquête, ainsi que contre le fichier TÉS centralisant les informations biométriques et alphanumériques des détenteurs de carte nationale d'identité et de passeport. Le recours contre ALICEM participait aussi de « Technopolice », une campagne de communication organisée depuis le début de l'année 2019 avec une centaine de collectifs[1] pour mobiliser contre les technologies urbaines sécuritaires (portiques de sécurité, caméras-piétons, capteurs de nuisances sonores, vidéosurveillance de l'espace public et des écoles, drones, caméras thermiques, etc.) à l'aide d'une rhétorique et d'une esthétique orwelliennes. Les militants préparaient par ce recours une « mobilisation générale des esprits critiques » pour la rentrée 2019, en particulier devant les lycées de Marseille et de Nice à l'entrée desquels la région avait installé des portiques biométriques pour « fluidifier l'accès des élèves ».

La critique juridique d'ALICEM (adressée initialement par la CNIL et prolongée par La Quadrature du net) portait sur l'interprétation du Règlement général pour la protection des données (RGPD) en matière d'exercice du consentement[2]. Dans son avis du 18 octobre 2018, la CNIL soulevait en effet « des interrogations » quant à l'expression libre, spécifique, éclairée et univoque du consentement (article 4-11 du RGPD), qui ne saurait se réduire à un simple clic sur une interface mobile au démarrage de l'application, et ce, d'autant plus lorsque la création de l'identité numérique ALICEM est conditionnée à cette seule procédure. Cette interpellation rejoint une discussion juridique et philosophique

[1] Parmi les signataires du manifeste fondateur de Technopolice, réglage d'organismes hétérogènes montés en réseau, on comptait alors des associations de défense des libertés numériques (La Quadrature du net, Bits of Freedom), dont un certain nombre de libristes (Framasoft, #Nog00gle, Initiatives pirates, RevLibre, Hoga, Ubunteam), des collectifs libertaires (l'Union communiste libertaire, la Fédération anarchiste), des syndicats professionnels (SUD Intérieur, le Syndicat des avocats de France, le Syndicat de la magistrature, la Confédération nationale du travail du 31, l'Union syndicale solidaire), des associations locales (Halte au contrôle numérique à Saint-Étienne, l'Association pour la démocratie à Nice, Tous citoyens !), des mouvements de protection des droits de l'homme (le Comité justice et libertés pour tous, la Ligue des droits de l'Homme, ESS et société, le Mouvement Utopia), des militants de la transparence de la vie publique (Citoyennes lobbyistes d'intérêts communs, le Réseau Ritimo) et même une maison d'édition (La Volte qui publie, entre autres, des dystopies).

[2] Il y a dans l'article 9 du RGPD deux possibilités de collecter les données à caractère personnel de type « sensibles » que sont les données biométriques : le motif d'intérêt public important ou le consentement éclairé de l'utilisatrice. Le premier motif est réservé aux usagers policiers. Dans le décret ALICEM qui vise explicitement la connexion aux services numériques, la base légale invoquée est celle du consentement.

émergeant en Europe sur la place prise par le dispositif du consentement forcé par le design des interfaces depuis l'entrée en vigueur du RGPD (Khatchatourov, 2019).

Même si le cadre du RGPD est récent (il s'applique depuis mai 2018), la CNIL avait elle aussi inscrit son avis dans une longue série d'échanges avec le ministère de l'Intérieur sur l'usage des données biométriques. La profondeur historique de ces échanges est visible dans les rapports d'activité de la Commission et dans de nombreux communiqués pressant le législateur de s'emparer du sujet et d'organiser un débat démocratique. Elle a rappelé cette position dans une note publique, qui convoqua, en plein déferlement médiatique de l'automne 2019 au sujet d'ALICEM, des arguments de droit sur la protection des données sensibles, mais aussi d'opportunité, à rebours de l'économie de la promesse sur laquelle reposait la reconnaissance faciale. La note faisait état de limites statistiques de la correspondance des gabarits (faux positifs et négatifs), de biais algorithmiques, du coût pour la dépense publique, de la fascination technologique, mais aussi, d'un choix de société transformé par l'enregistrement d'images et d'un changement du paradigme de surveillance étatique par la captation sans contact, mettant potentiellement fin à l'anonymat dans l'espace public[1]. Cette dimension sérielle et éminemment politique du débat se manifestait jusque dans les couloirs de la CNIL, où la critique des agents s'affichait dans des dessins et des slogans (Figure 1).

Figure 1 Dessin dans les couloirs de la CNIL du caricaturiste Xavier Gorce produit lors d'une conférence sur les *civic techs* en décembre 2019.
Photo prise en février 2020.

Le second signal d'alerte contre l'application ALICEM a été envoyé à la fin de l'été 2019 par Baptiste Robert, alias le compte Twitter Elliot Alderson. Celui qui se décrit comme un « hacker français » s'était fait connaître quelques mois auparavant en mettant au jour

[1] CNIL, « Reconnaissance faciale : pour un débat à la hauteur des enjeux », note publique, 15 novembre 2019.

des failles dans le système d'identification biométrique indien, Aadhaar (Nair, 2019 ; Rao, 2018 ; Singh, 2019), en partie mis au point par Idemia, une filiale du groupe Safran ; puis, en identifiant des vulnérabilités dans la messagerie sécurisée de l'État français, Tchap. À compter du 22 août 2019, le hacker amorça une série de dénonciations en opérant un rapprochement entre ALICEM et Aadhaar et en multipliant les mises en cause de l'application, dont il prétendait localiser les failles, interpelant ses responsables (le prestataire Gemalto à la Figure 2). Le report de failles de sécurité consiste à révéler que l'on a localisé un problème, sans en dévoiler publiquement l'emplacement, afin d'éviter que des personnes mal intentionnées ne l'exploitent ; tout en négociant, pour soi, une récompense pécuniaire (Auray, Kaminsky, 2007). Cette version quasi publique et collaborative de l'analyse de risques et du report de vulnérabilités s'est institutionnalisée dans le monde de la sécurité informatique ; elle est désignée par le terme de *white hat*.

Figure 2 Premier tweet d'une séquence d'accusations portées à partir de la démonstration de l'application à laquelle Elliot Alderson aurait accédé, captures d'écran à l'appui. Twitter, le 23 septembre 2019 à 09 : 52.

Premièrement, avec d'autres experts du domaine[1], Elliot Alderson contestait la fiabilité du système technique et l'a inscrit dans la lignée du très controversé Aadhaar (« *The French*

[1] En particulier Watchguard, Varonis, « Application ALICEM - Sécurité et privacy deux enjeux difficiles à maitriser », *Global Security Mag*, 25 octobre 2019 qui blâment l'authentification monofacteur, le code personnel à six chiffres pour activer l'application une fois l'identité numérique créée, qui peut être facilement récolté par une campagne d'hameçonnage ou en regardant au-dessus de l'épaule de l'utilisatrice.

Aadhaar » à la Figure 2). En spécialiste des failles dans les terminaux mobiles, il condamnait fermement le choix d'une application mobile pour collecter des données personnelles sensibles, arguant que les garanties de sécurité sont réputées assez faibles sur un téléphone. Par exemple, lorsque les données sortent du terminal pour vérifier la concordance du titre photographié avec une entité de la base Docvérif ou pour rapprocher les images faciales récoltées avec celles du détenteur du titre par l'algorithme du ministère, elles peuvent aisément être interceptées[1]. Il avance que de tels détournements pour revendre les données biométriques seraient désormais courants en Inde. Deuxièmement, Elliot Alderson a mis en doute la capacité de l'État français à concevoir de tels systèmes techniques. Celui-ci se serait fait flouer par son prestataire, qui aurait repris un projet néerlandais, Utopia, dont la technologie initiale utilisait des standards désormais obsolètes et faillibles[2] et, de manière générale, aurait manqué de vigilance. Dans les couloirs des administrations centrales, cette critique du manque de contre-expertise était régulièrement formulée à l'encontre de l'ANTS : « ils ne comprennent rien […], les presta font ce qu'ils veulent[3] ». Troisièmement, Elliot Alderson a attaqué l'idée selon laquelle ALICEM serait utilisée par des utilisateurs volontaires et consentants en rappelant qu'en Inde, Aadhaar était initialement présenté de manière similaire et a progressivement été imposé par des mesures indirectes (Nair, 2019 ; Singh, 2019). L'histoire de l'identification des personnes a en effet déjà souligné cette tendance des technologies à s'étendre, non seulement géographiquement (Breckridge, 2014), mais aussi au-delà des sous-catégories de population et des usages pour lesquelles elles ont initialement été conçues (Caplan, Torpey, 2001 ; Noiriel, 2007).

Les couches argumentatives des deux lanceurs d'alerte, La Quadrature du net et Baptiste Robert/Elliot Alderson, formulées dans plusieurs arènes (juridique du Conseil d'État, politique de la rue et médiatique des réseaux sociaux), ont été assemblées par une journaliste de l'agence de presse américaine Bloomberg, dans une virulente dépêche publiée le 3 octobre 2019[4]. Caractéristique d'un art de l'amplification, la dépêche a été reçue comme une véritable détonation : le jour même, l'information était relayée par des dizaines de médias étrangers, elle était citée près de 100 fois par les médias nationaux et régionaux, contraignant les responsables de l'application à prendre part à ce qui était en

[1] Il existe plusieurs techniques visant à intercepter de telles données, notamment lorsque l'utilisatrice est connectée en wifi : la création d'une réplique de réseau public, l'attaque dite de l'homme du milieu interceptant les communications entre deux parties, le détournement de session, l'installation d'un analyseur de paquets capturant les paquets du flux de données qui transitent sur un réseau ou le simple fait de regarder au-dessus de l'épaule de celle qui saisit ses données.

[2] Apache Tomcat 9.0.M9, une version de 2016 qui comportait de nombreuses failles de sécurité.

[3] Notes de terrain, agent public et ancien consultant auprès de l'ANTS, 9 mars 2020.

[4] Fouquet H., « France Set to Roll Out Nationwide Facial Recognition ID Program », *Bloomberg.com*, 3 octobre 2019.

train de devenir une controverse. « On peut dire que Bloomberg, nous a fait beaucoup de mal[1] », grinçait un responsable du ministère de l'Intérieur.

Tentative de neutralisation

La réaction des pouvoirs publics dans l'arène médiatique peut être résumée en trois séquences constitutives d'un régime de neutralisation de la controverse : discréditer la critique, rassurer le public et invoquer le caractère expérimental de l'application. Se situant dans un espace de vérité préconstitué et indiscutable, les responsables publics ont considéré le conflit émergeant autour d'ALICEM comme une pathologie sociale qu'il s'agissait de soigner en rééduquant le public. Refusant de prendre au sérieux les critiques, en particulier techniques et juridiques, ils ont psychologisé la contestation de l'application, la déplaçant ainsi vers l'enjeu d'acceptation sociale des technologies biométriques. Comme pour d'autres controverses au long cours dont celle de l'enfouissement des déchets nucléaires, « la reformulation en termes d'acceptabilité sociale n'est rien d'autre que le point d'aboutissement d'un processus de rehiérarchisation entre deux modes de problématisation : à une problématique technique […] s'est peu à peu substituée une autre forme de problématisation, principalement tournée vers le "public", sa "peur viscérale" du nucléaire en général et des résidus radioactifs en particulier » (Barthe, 2006, p. 66).

Discréditer d'abord. Gilles Babinet, le vice-président du CNNUM, a jugé l'information de Bloomberg reprise dans le *Telegraph* comme étant une « belle pièce de désinformation[2] ». Le secrétaire d'État au Numérique, Cédric O, interrogé par *Le Monde* le 14 octobre 2019 a évoqué des « fantasmes » et de l'impératif de ne « pas se laisser emporter par une vision dystopique ni utopique de la reconnaissance faciale »[3], Jérôme Létier, le directeur de l'ANTS, a parlé de « contre-vérités[4] » et déploré « l'agitation du spectre de la reconnaissance faciale[5] ».

Ces deux derniers acteurs, promoteurs de l'application dans l'espace public, se sont aussi donné pour mission de rassurer l'opinion et ont mis en scène une posture gouvernementale à la fois prudente et déterminée.

> Si ALICEM se généralise, nous veillerons à ce qu'il y ait des alternatives à la reconnaissance faciale. Mais nous avons le temps pour cela […]

[1] Entretien avec un cadre du ministère de l'Intérieur, 21 novembre 2019.
[2] Gilles Babinet @Babgi, tweet du 5 octobre 2019, 12 : 59.
[3] Utersinger M., « Cédric O : "Expérimenter la reconnaissance faciale est nécessaire pour que nos industriels", *Le Monde*, 14 octobre 2019.
[4] Rees M., « Jérôme Letier (ANTS) : "Il y a des contrevérités qui circulent sur ALICEM" », *NextImpact.com*, 18 octobre 2019.
[5] « "Si ALICEM se généralise, il y aura des alternatives à la reconnaissance faciale", assure Jérôme Létier, du ministère de l'Intérieur », *L'Usine nouvelle*, 15 octobre 2019.

> Nous avons bien sûr consulté le Conseil d'État qui a validé notre projet au préalable. Là, il est saisi au contentieux ; nous avons donc présenté nos éléments de défense et nous attendons sa décision. Mais nous sommes très confiants. Notre projet respecte la lettre et l'esprit du RGPD. Nous avons veillé à ce que seules les données nécessaires soient utilisées et que celles sensibles restent sous la maîtrise de l'utilisateur[1].

Discréditer la posture vigilante et les alertes en les traitant au mieux comme des malentendus au pire comme des manifestations d'un délire paranoïaque, avant de rassurer l'opinion sur les intentions et les procédures en cours constituent des opérations de stabilisation classiques dans les controverses (Barthe, 2006 ; Chateauraynaud, Torny, 1999). Ce qui l'est moins est la manière dont les acteurs publics — le secrétaire d'État au Numérique, Cédric O, en particulier — ont endossé une posture expérimentale sur l'acceptation sociale, participant à réorienter la controverse sur cette application de connexion aux services publics en ligne en direction des usages généraux de la reconnaissance faciale et du type de relations que cette dernière établit entre l'État et les citoyens. Reprenant l'attaque contre un cadre juridique réputé lourd et inadapté à l'innovation scientifique et technique, ce dernier a déclaré au journal *Le Monde*, « la technologie est en avance sur la régulation […] expérimenter est également nécessaire pour que nos industriels progressent[2] ».

L'expérimentation de la reconnaissance faciale en direction de laquelle pointait Cédric O était autant parée de vertus pacificatrices, qu'elle était louée comme un horizon d'accomplissement du progrès porté par les industries nationales auquel les citoyens étaient enjoints à prendre part en livrant leurs images faciales. Un tel recours à l'expérimentation liant l'État, les industries numériques nationales et les corps des citoyens était dans l'air du temps : il avait été suggéré, quelques semaines auparavant, par une note de l'Office parlementaire d'évaluation des choix scientifiques et techniques (OPECST)[3], une instance de l'Assemblée nationale conçue pour traiter des controverses et largement orientée vers leur dépolitisation et leur clôture (Barthe, Borraz, 2011), ainsi que par la Gendarmerie nationale dans le document précité[4].

---

[1] Ibidem.

[2] Utersinger M., « Cédric O : Expérimenter, art. cit. ».

[3] OPECST, « La reconnaissance faciale », note n° 11, juillet 2019, p. 1.

[4] Centre de recherche de l'École des officiers de la Gendarmerie nationale, « Reconnaissance faciale, cité », p. 4.

Nouvelles arènes et reproblématisation de l'acceptation sociale de la reconnaissance faciale

Avec la réponse gouvernementale faisant fi des contestations juridiques et techniques et la proposition d'expérimenter plus amplement la reconnaissance faciale, la controverse sur l'application ALICEM s'est transformée. De nouvelles arènes dédiées à la négociation se sont ouvertes, dépassant le cas d'ALICEM. Le CNNUM mandaté le 9 juillet 2019 par le gouvernement pour organiser une consultation publique « des acteurs impliqués » dans le but de « comprendre la perception », d'« anticiper au mieux les besoins » et de « garantir l'appropriation collective de l'identité numérique »[1] a commencé à réunir le premier de ses sept ateliers le 9 novembre à Montpellier. Une mission commune de l'Assemblée nationale sur l'identité numérique nommée le 30 octobre 2019 a entrepris une série d'auditions d'experts à partir du 20 novembre 2019, puis a procédé à une consultation citoyenne en ligne à compter du 9 mars 2020. Enfin, le 19 février 2020, l'ANTS a annoncé, en complément des méthodes probabilistes d'analyse de risque de l'ANSSI, le lancement d'un *bounty bug*, une « chasse » rémunérant les experts en sécurité informatique (*white hats*) à la hauteur des vulnérabilités qu'ils rapportaient à l'organisateur.

En liant la sollicitation d'expertises diverses (de juristes, de philosophes, de *white hats*, d'associations, d'entreprises, de représentants d'État européens, etc.), à des procédures de consultation du public, le gouvernement a déployé une forme d'« objectivité politique », visant à mettre à distance la conflictualité de la controverse pour mieux la trancher (Laurent, 2022 ; Barthe, Linhardt, 2009 ; Chateauraynaud, Torny, 1999). Mais la méthode n'a pas suffi à emporter une pleine adhésion sur le cas de l'application ALICEM. Non seulement les lanceurs d'alerte continuaient à s'agacer dans des tweets et des communiqués excitant l'arène médiatique, mais, ralliant sensiblement leurs arguments, les agents de certaines des administrations concernées fustigeaient, eux aussi, cette reproblématisation appuyée sur une idée dépolitisée du consensus : « Vu de l'ANSSI, l'enjeu du *bug bounty* est essentiellement de la communication, car notre travail n'est pas celui d'un après-midi ; l'évaluation d'ALICEM a commencé il y a plusieurs mois et n'est pas terminée[2] », « On doit absolument lancer une conférence de citoyens sur le sujet. On veut un vrai débat démocratique, c'est pas possible ce qu'il se passe en ce moment[3] ».

Il est remarquable qu'en dépit de la construction de cette démarche d'objectivité, la certitude de l'irréversibilité technologique d'ALICEM n'ait en rien été ébranlée chez ses concepteurs et promoteurs et, adoptant une approche purement mentaliste du problème, elle se soit matérialisée, dès le cadrage de la discussion, dans ces nouvelles arènes de négociation. Au fil des semaines, la fatalité semblait même nettement explicitée, assumée

[1] Lettre de saisine du CNNUM, 9 juillet 2019.

[2] Entretien avec un cadre de l'ANSSI, 27 mars 2020.

[3] Notes de terrain, semaine de l'innovation publique, cadre spécialisée dans la consultation du public, 21 novembre 2019.

et durcie. L'irréversibilité portait désormais autant sur le rôle de facilitation et de sécurisation des transactions proposé par la biométrie dans les relations à l'État, que sur l'intérêt propre d'ALICEM. La validité juridique du consentement, les risques de fuite de données, de dysfonctionnements de la technologie ou de détournements de finalité étaient exclus du débat, comme s'ils étaient « techniquement solubles », que les critiques qui s'étaient efforcées de bâtir un contre-discours et de rendre discutable cette technologie étaient de dangereux extrémistes venus d'un sombre passé (des « prophètes de malheur », dépourvus d'éléments tangibles dans le lexique de Chateauraynaud, Torny, 1999).

À l'automne 2019, ce formatage des débats se retrouvait autant au CNNUM où un représentant du ministère de l'Intérieur martelait aux organisateurs « on est déjà biométrisés par l'État », que dans les auditions de la mission commune identité numérique où la rapporteuse insistait sur l'impératif de « partir de la réalité dans laquelle on est aujourd'hui ».

> Quand vous arrivez à l'aéroport, quand vous demandez votre visa, vous êtes enrôlés biométriquement, on vous demande vos dix doigts plus la photo. En France, pour faire le passeport on vous demande les dix doigts. Finalement, on est déjà biométrisés par l'État, ce qui fait que quand on arrive à l'hôtel [en Chine] et qu'on vous dit : « on vous prend en photo, ce sera l'accès à votre chambre », la reco faciale on n'est plus à ça près […] Je ne dis pas que la société [française] est prête pour ça, loin de là […] Mais à chaque fois que je vois des polémiques dans la presse, j'ai quand même un doute […] sur la représentativité de ces discours militants qui font peur [au grand public][1].
>
> Christine Hennion, rapporteuse de la mission — [aux associations de défenses des libertés numériques qui détaillaient leur opposition] J'ai lu vos documents… (rire nerveux) Par contre, j'ai vraiment du mal à comprendre. Aujourd'hui on a dépassé ce monde-là, j'ai l'impression qu'il faut partir de la réalité dans laquelle on est aujourd'hui. Aujourd'hui, on a des gens qui demandent à avoir de la vidéoprotection, on a des gens qui sont tous les jours sur internet, qui se prennent en photo avec leur portable pour accéder à leur compte. Est-ce que c'est vraiment le bon angle d'attaque de dire : « on refuse tout et voilà ça n'existera pas » ? Est-ce qu'on vit sur une petite planète ? Ou est-ce qu'il n'y a pas plus de risques à avoir cette attitude […] ? J'ai

[1] Notes de terrain, cadre du ministère de l'Intérieur, débat des experts du CNNUM, 18 décembre 2019.

> l'impression que vous êtes dans une position extrêmement catégorique et extrême qui ne va pas forcément amener les bonnes solutions[1].

Il se dégage de l'observation de ces nouvelles arènes l'idée que l'on pourrait clore la controverse, rassurer le public par des débats et de l'expérimentation, sans changer autrement qu'en réparant en un après-midi de *bounty bug* les modalités légales et techniques de l'application ALICEM. Un seul futur serait possible suivant cette approche mentaliste des critiques et la société française devrait raisonnablement l'accepter. Cette mise en politique critiquée d'ALICEM témoigne d'une manière de traiter la question de l'acceptation sociale de l'application par le déplacement du débat vers la généralisation de la reconnaissance faciale de la population par l'État.

Toutefois, en juin 2020, la mission commune identité numérique de l'Assemblée nationale a annoncé la fin de l'expérimentation d'ALICEM et le lancement d'une nouvelle identité numérique européenne, dont l'application aurait finalement servi de « préfiguration ». Le projet de la Commission présenté un an plus tard contient en effet trois directions : rendre obligatoire au moins une identité numérique interopérable par État membre, créer un portefeuille d'identités numériques téléchargeables sur mobile et permettre à cette identité numérique européenne d'ouvrir l'accès aux services publics, mais aussi privés (transports, énergie, finances, santé, etc.). Aussi, le devenir interface de la relation entre cet État européanisé et amplifié technologiquement et des utilisateurs de téléphone mobile semble promis à une nouvelle extension avec ce « portefeuille » dont « la version bêta » prend, au moment de la finalisation de l'écriture du présent article, le nom de France Identités. Mais, si les développements de l'application controversée ont officiellement cessé et que ses enseignements — y compris le rejet de la reconnaissance faciale — ont été retraduits en une préfiguration pour le projet d'identification des personnes suivant, il n'en reste pas moins que deux caractéristiques d'ALICEM méritent d'être dégagées afin d'accroître notre compréhension du phénomène de devenir interface et de lire d'un œil avisé les évolutions qui pourraient venir avec France Identités.

En deçà de la controverse, appréhender le devenir interface

Même si ALICEM a supposé un arrangement technologique inédit, nous savons que, pour les acteurs concernés, l'application trouve des précédents qui fondent tant les pratiques de vigilance des lanceurs d'alerte (fichiers biométriques, technologies urbaines sécuritaires, Aadhaar), que celles des concepteurs (INÉS, FranceConnect). Pour conserver une capacité d'étonnement face au cas, ne pas trop vite refermer sa trajectoire dans un enchevêtrement des technologies de surveillance dans la vie démocratique ou de creusement de la fracture numérique et, dans le même temps, en tirer des apprentissages collectifs, ALICEM doit aussi être lue comme un moment charnière de l'histoire des

[1] Christine Hennion, députée LREM, rapporteuse de la mission, auditions de la mission commune identité numérique de l'Assemblé nationale, 4 février 2020.

relations entre la société politique et l'État moderne. Afin de démêler ce que reconfigure cet agencement d'un État technologique, européen et des utilisateurs d'une application mobile, je reviens sur deux éléments en filigrane du récit : la signification disputée du genre expérimental et le signal envoyé au marché, enjeux remarquables du devenir interface de notre relation à l'État, utiles pour saisir les tressautements de l'identification étatique des personnes.

Fonctions politiques de l'expérimentation

ALICEM se présentait comme relevant d'une expérimentation : les documents officiels évoquaient alternativement une « application en cours d'expérimentation », une « préfiguration », un « test » ou un « prototype ». De manière contre-intuitive, c'est même en juin 2019, après la parution du décret, qu'a démarré cette expérimentation sur un millier d'utilisateurs volontaires, dénommés *friends and family*, et essentiellement recrutés dans les rangs du ministère de l'Intérieur. Ni les finalités de la revendication de l'incomplétude et du caractère « en chantier » du dispositif ni le contenu de l'expérimentation n'ont été justifiés par l'ANTS, malgré l'intensification de la controverse. La mise en avant de ce vocabulaire pourrait être tout autant une manière de se revendiquer de l'informatique agile, devenue à partir de 2014 le mot d'ordre de la conduite des projets informatiques de l'État, qu'une précaution de l'ANTS pour se prémunir, après le coup d'arrêt porté au projet INÉS (Lacouette-Fougère, 2011 ; Piazza, 2006), d'une critique trop acerbe en mettant en avant l'ouverture à d'éventuelles orientations réflexives. Quoi qu'il en soit, le maintien en expérimentation peut être lu comme une anticipation stratégique visant la défense de l'application, soit un mode d'action désormais courant dans la communication publique, une manière de « climatiser » les controverses au long cours (Barthe, Linhardt, 2009), sinon une posture vigilante supposée plus conforme aux attentes des citoyens du XXIe siècle que la prévision (Chateauraynaud, Torny, 1999).

Toutefois, parce qu'ils ont développé les formes de vigilance précédemment exposées, les lanceurs d'alerte ont interrogé, tout au long de la controverse, la véracité et le sérieux de l'expérimentation : « Et d'ailleurs ces expérimentations, elles durent combien de temps, elles sont faites par qui ? Contrôlées par qui ? » s'est enquis Baptiste Robert[1]. Ou encore : « le débat que propose le gouvernement sur la reconnaissance faciale pour faciliter les "expérimentations" est faussé : la technologie est d'ores et déjà largement déployée en France[2] », s'exaspérait La Quadrature du net. D'autres acteurs de la société civile présents aux auditions à l'Assemblée nationale ont questionné la finalité de l'expérimentation : l'ANTS va-t-elle réformer ou supprimer ALICEM si l'expérimentation n'était pas concluante ? Peut-on la généraliser pour certaines démarches administratives ? Faut-il

[1] Baptiste Robert @Eliot Alderson, tweet du 26 décembre 2019.

[2] La Quadrature du net, « Reconnaissance faciale : le bal des irresponsables », communiqué de presse, 22 novembre 2019.

autoriser plus largement la reconnaissance faciale ? Parmi eux, nombreux sont ceux qui s'indignaient de la finalité invoquée par les promoteurs d'ALICEM, « le progrès d'industriels français brimés par le RGPD » et la tentative de recourir à un « état d'exception », une suspension des cadres de l'État de droit dans lequel les citoyens se trouvent réduits à des testeurs configurés pour les besoins du marché[1]. Autrement dit, au cours de cette controverse, l'expérimentation comme mode de gouvernement des populations et des choses et sa spécificité en matière de technologies numériques qui alertent nombre de sociologues de sciences et des techniques (en particulier Marres, 2020) sont devenues les objets d'interrogations collectives.

Et, les capacités réflexives ne se situaient pas seulement du côté des opposants au projet : les acteurs des administrations n'étaient nullement dupes des fonctions stratégiques de l'expérimentation. Les administrations enclines à expérimenter pour introduire et évaluer des dispositifs d'action publique (par exemple, Laurent *et al.*, 2021 ; Leprêtre, 2019) sont en effet en mesure de distinguer les bonnes des mauvaises pratiques expérimentales. « Dans les discussions avec le cabinet de [Cédric] O, il est très clair que l'expérimentation vise à rendre les choses acceptables, précipiter l'usage, faire prendre la mesure de la praticité et forcer le consentement. Ça en dit long sur le rapport des membres du gouvernement aux libertés publiques…[2] », a déploré un expérimentateur dans un ministère. Plus encore, forts de leur position d'évaluateurs, les agents de l'ANSSI s'accordent a posteriori pour dire que l'expérimentation qui a eu lieu avec l'application ALICEM, sans jamais les murs du laboratoire n'aient été explicitement délimités par ses concepteurs, était triple : technologique, politique et sociale. Technologiquement, l'ANTS aurait testé la correspondance entre le visage d'une personne se photographiant dans le présent avec un dispositif non réglementé (son téléphone), et les mesures de son propre visage enregistrées dans le passé sur une puce, il y a parfois dix ans de cela, après vérification par un agent d'état civil et d'après une photographie normée. « D'habitude [lorsqu'on se passe d'agent habilité, c'est qu'] on lit les puces des passeports pour passer un portique, c'est le dispositif PARAFES [passage automatisé rapide aux frontières extérieures de l'espace Schengen] des aéroports[3], on est alors dans un environnement très contrôlé[4] », explique un spécialiste pour souligner l'incertitude de cette situation de co-production de l'identité numérique. Politiquement, l'ANTS aurait expérimenté la dématérialisation de la relation administrative, qui, à partir d'un titre officiel scanné par un mobile, peut se passer de relations directes, même pour les démarches les plus sensibles ou symboliques du rapport entre le citoyen et l'État, comme pourrait l'être le vote. « On

[1] Siry G., Faure O., Comarmond (de) F., Jamey-Fournier B., « Reconnaissance faciale : nos droits et nos libertés ne sont pas à vendre ! », *Libération*, 6 janvier 2020.
[2] Notes de terrain, cadre d'un ministère responsable de plusieurs expérimentations, 9 mars 2020.
[3] Le dispositif PARAFES créé par décret le 3 août 2007 est un héritier du projet expérimental PÉGASE d'identification biométrique lancé en juin 2005 par Air France au terminal 2F de l'aéroport Roissy-Charles-de-Gaulle.
[4] Entretien avec un cadre de l'ANSSI, 27 mars 2020.

est là sur l'expérimentation d'un changement de société, avec une relation de proximité avec certains services administratifs qui se transforme en une relation informatisée[1] », un projet de société qui se retrouve d'ores et déjà dans de nombreux pays, dont l'Inde à laquelle se référait l'un des lanceurs d'alerte (Nair, 2019). Enfin, socialement, l'ANTS aurait testé avec ALICEM et l'ouverture des arènes de négociation qui en ont découlé, l'acceptation de la reconnaissance faciale de la population par l'État, soit la reconfiguration psychologisante de la critique précédemment évoquée.

La controverse autour de l'application ALICEM présente donc l'intérêt d'attirer l'attention sur un niveau de réflexivité dans la production des politiques publiques, une aptitude à distinguer les modalités et les fonctions de l'expérimentation, rendant ainsi visible une forme de politisation suscitée par le devenir interface de notre relation à l'État, irréductible aux enjeux de surveillance ou d'inégalités d'accès. En effet, le phénomène critique ne portait pas seulement sur l'application de reconnaissance à distance (son design incluant ou excluant telle ou telle catégorie d'utilisateurs, la biométrie, ses effets politiques, etc.), mais aussi sur le mode de gouvernement stratégique inhérent à l'introduction d'une telle technologie. Aussi, plutôt que de considérer la technologie comme étant suffisamment ouverte pour accueillir les critiques ou faire valoir un protocole expérimental qui aurait supposé la formulation d'hypothèses, la construction d'un contre-factuel, d'outils de mesure et de traçabilité comme cela se fait par ailleurs, l'expérimentalisme politique en question était perçu comme un rejet du « vrai débat démocratique » et une pensée de la rectification des conduites et des opinions individuelles. Les implications démocratiques de cette vision disputée de l'expérimentation dépassent le seul cas d'ALICEM et ont fait de cette controverse, pour une partie des observateurs, acteurs des administrations et opposants, l'occasion de porter la discussion sur les modes de relation à l'État dans les sociétés technologisées.

Signalement de l'État auprès du marché

L'autre trait saillant du cas au sujet du devenir interface de notre relation à l'État est le souci des concepteurs, des promoteurs, mais aussi des opposants pour les liens qu'une telle application stabilise avec le marché. En conséquence, ALICEM n'est en aucun cas un face-à-face médié par une technologie mobile entre une utilisatrice et l'État, mais un tissu de relations plus vaste ouvrant sur des acteurs soutenus par des politiques industrielles.

En effet, tout au long de la controverse, la place des industriels français et du marché de l'identité numérique en particulier a été une préoccupation majeure des acteurs étatiques. Leur préoccupation se déclinait autour de la notion de « souveraineté numérique », qui désignait, dans ce contexte, un souci pour l'État de revendiquer le territoire numérique dans lequel évoluait sa population, à l'heure où ce dernier était en grande partie contrôlé par des plateformes de droit américain (Google, Facebook, Amazon…), en même temps

[1] Ibidem.

qu'une inquiétude pour la compétitivité des industries nationales (Safran, Thales, Atos, Dassault, Imprimerie nationale…). Le premier volet de ce signalement de la souveraineté numérique, qui a déjà largement façonné l'ergonomie du bouton FranceConnect et du programme d'État plateforme (Alauzen, 2019), a été formulé de manière exemplaire par le secrétaire d'État au Numérique, Cédric O, auditionné à l'Assemblée nationale.

> Alors que se développent des systèmes d'identification privés, émanant notamment de grandes entreprises américaines comme Facebook Connect ou Google Connect, la question qui est au cœur de nos décisions est celle de savoir qui va gérer les identités. Qui détiendra l'identité demain ? Ceux qui fourniront l'identité seront-ils les GAFA — Google, Apple, Facebook, Amazon —, des services privés, agréés par l'État ou uniquement l'État ? On pourrait considérer que, tout bien pesé, l'identité numérique n'est pas une bonne chose pour diverses raisons. Mais cela reviendrait à laisser le champ libre à des acteurs qui ne nous ont pas attendus pour la développer[1].

Le secrétaire d'État mettait en scène la figure d'un État hanté par la crainte du dépassement technologique, de l'obsolescence, et la souveraine nécessité d'envoyer promptement, en retissant des liens numériques avec la population, un signal aux acteurs du marché : « nous pensons qu'il faut d'abord conquérir les usages en déployant les services le plus vite possible. Une banque ou un opérateur de santé ne doit pas avoir à se demander s'il va recourir à la solution de l'État ou à une solution d'une entreprise privée, américaine par exemple[2] ». Ces propos sur la présence de l'État pour les acteurs du marché, qui peuvent être lus dans la continuité de l'expérimentalisme politique précédemment évoqué et comme une tentative de clore le débat en invoquant l'irréversible, n'ont pas manqué d'interpeler la critique : l'énonciateur met en équivalence des dispositifs d'identification, sans considération des technologies, des usages ou des règles juridiques les régissant. Ils indiquent surtout une priorité : rassurer les acteurs du marché (banques, opérateurs de santé et toutes les entités nécessitant pour leurs transactions commerciales une vérification de l'identité des personnes) quant à la revendication du monopole documentaire, qui ne passe pas, dès lors que les opérations ont lieu en ligne, entre les mains des GAFAM. Cette revendication supposait alors de faire exister un réseau socio-technique reliant l'État souverain, des industries nationales fournissant des services technologiques et placées sous sa protection, à une population individualisée par des technologies d'identification — un réseau ayant porté, à titre expérimental, le nom d'ALICEM.

[1] Cédric O, secrétaire d'État chargé du Numérique, audition de la mission commune identité numérique de l'Assemblée nationale, 18 février 2020.
[2] Ibidem.

Dans cette version dramatisée de la souveraineté numérique, la préoccupation pour le marché se matérialisait également, à la direction générale des entreprises du ministère de l'Économie et des Finances, dans des politiques de filières et d'organisation de « champions nationaux de l'identité numérique » héritées de la seconde moitié du XX^{e} siècle (Hecht, 2014). Plus précisément, l'organisation parallèle au développement d'ALICEM d'une politique industrielle numérique souligne que certains grands groupes français faisaient pleinement partie de la stratégie de rayonnement de la France (Safran, Thales, Atos, Dassault, Imprimerie nationale…). Or, c'est pour favoriser leur compétitivité sur les marchés internationaux que l'expérimentation à partir d'une population traduite en données avait été rendue possible par les pouvoirs publics (Grommé, Ruppert, 2021 ; Pelizza, 2021 ; Marres, 2020) — ce qui n'est pas sans rappeler certaines politiques insulaires de développement de services numériques (sur le cas de Singapour, voir Laurent *et al.*, 2021).

> On voit aussi que les acteurs privés sont en état d'attente par rapport à l'État. Ça conditionne leur prise d'initiative […] Ils n'arrêtent pas de venir nous voir. Les startups viennent beaucoup […] On les renvoie à l'Imprimerie nationale [IN]. Toute perspective de contribution ne peut que passer par l'IN group [qui produit les titres d'identité]. On les invite à intégrer des technologies, mais c'est elle qui fait les choix, pas nous. L'IN est dans une logique de rachat systématique des startups, ce qui va très bien aux startups, et dans une logique de monopole que l'on voit très clairement : Thales rachète Gemalto, IN group rachète des startups dès qu'elles arrivent sur le marché. On n'est pas sur un marché typique, mais régi par le régalien. On ne peut pas réfléchir comme sur les autres marchés[1].

À côté de l'épineuse question de la domination des GAFAM, le marché de l'identification était décrit par les responsables administratifs comme un oligopole réactif aux innovations et fortement conditionné par les décisions de l'État. Cet état de vigilance fait partie de « la promesse d'une offre publique confiante dans le respect des libertés publiques […] Apple n'a pas l'ANSSI sur le dos. Nous on est soumis au droit européen et français. On sait coller au droit [2]», s'enorgueillissait même ce même haut fonctionnaire. Toutefois, la situation de proximité des acteurs politiques et administratifs avec les grands industriels du secteur a aussi fait le lit de la critique : elle a nourri des accusations de capture du régulateur et de conflit d'intérêts. « Le passage de Cédric O chez Safran pose ouvertement la question du conflit d'intérêts, je ne suis pas le premier à le dire[3] », s'est indigné un expert entendu par la mission d'information identité numérique de l'Assemblée nationale en marge de son audition.

---

[1] Entretien avec un cadre du ministère de l'Intérieur, 25 novembre 2019.
[2] Ibidem.
[3] Notes de terrain, expert auditionné par l'Assemblée nationale, 20 février 2020.

En d'autres termes, la controverse sur ALICEM a rendu visibles les contours d'une relation d'identification des personnes physiques imaginée, bien au-delà de la délivrance ordinaire des services publics. Elle suppose l'alliance de fournisseurs de services commerciaux, de champions industriels et une ligne de politisation contre les industries de plateformes américaines ; soit tout un pan du devenir interface de notre relation à l'État, masqué par le monopole documentaire et des justifications relatives à la souveraineté numérique, qui ne faisait, jusqu'ici, pas l'objet d'un débat public.

- -

La séquence précipitée par l'application ALICEM présente plusieurs points d'intérêt sur lesquels il convient de conclure. Du point de vue de la socio-histoire de l'identification, ALICEM a opéré une contraction du temps. Elle constitue une phase chaude d'une controverse séculaire sur l'identification des personnes par l'État, d'ores et déjà augmentée de nouvelles excroissances. Elle montre à la fois la continuité de problématiques bien identifiées (Breckenridge, 2014 ; Caplan, Torpey, 2001 ; Crettiez, Piazza, 2010 ; Higgs, 2003 ; Noiriel, 2007) — dont le souci de véridiction de l'identité personnelle, les tensions sur le périmètre des populations identifiables ou la biométrisation de l'identité administrative — et met en lumière certaines recompositions propres à la période contemporaine : la gouvernementalisation des États par l'harmonisation du marché européen de l'identification électronique, la préférence pour l'expérimentation sur la planification, le choix de soutenir un écosystème industriel national ou encore la crainte des plateformes ; le tout justifié par le terme commode de « souveraineté numérique ».

Du point de vue de la sociologie des controverses, ce cas montre une tentative d'atténuation de la conflictualité, au cours de laquelle l'État a employé une forme souple d'expérimentation. Cette manière de neutraliser la chaleur de l'histoire longue des rapports à l'État ne reprend pas tout à fait le répertoire de la réversibilisation des choix techniques qui a participé à faire émerger un « autre mode d'agir politique » (Barthe, 2006 ; Barthe, Linhardt, 2009 ; Laurent *et al.*, 2021) ; elle génère désormais des contestations, tant internes qu'externes. L'emploi de l'expérimentation indiquait ici des velléités mentalistes de rectifier des comportements individuels, plutôt que de reprendre la critique pour réformer une technologie contestée — alors même que cette dernière, faite de code informatique, dispose de plus de flexibilité technologique que bien d'autres objets techniques (l'aménagement urbain, les infrastructures de réseaux ou encore les déchets nucléaires). Elle est donc, et peut-être pour la première fois, devenue l'objet d'un débat public.

Enfin, pour la sociologie de l'État, ALICEM constitue l'une des premières mises en débat de cette « nouvelle citoyenneté » moquée dans les couloirs de la CNIL (Figure 1) et à laquelle nous sommes régulièrement renvoyés, et cela singulièrement depuis la mise en place du passeport sanitaire. Ce n'est pas seulement l'inégalité dans l'accès aux services publics ou la biométrisation et la surveillance des populations dont nous avons aperçu une

tentative de discussion par le public. Il s'agit là de l'expression d'une profonde rénovation des liens politiques, sous-tendue dans la possibilité de se passer du contact humain dans le face-à-face avec l'État, sinon d'étendre de manière telle les chaînes de traduction qu'elles ne permettent de connaître et de n'être reconnu que dans un rapport scriptural et désincarné, qui offre une place de choix à certains acteurs industriels et suppose une constante disponibilité au test.

Bibliographie

ABOUT, I., BROWN, J., LONERGAN, G. (eds.) (2013), *Identification and Registration Practices in Transnational Perspective: People, Papers and Practices*, Basingstoke, Palgrave Macmillan.

AKRICH, M. (1992), « The De-Scription of Technical Objects », dans BIJKER, W. E., LAW, J., *Shaping Technology/Building Society. Studies in Sociotechnical Change*, Cambridge (MA), MIT Press, p. 205-224.

ALAUZEN, M. (2019), « L'État plateforme et l'identification numérique des usagers : le processus de conception de FranceConnect », *Réseaux*, vol. 1, nº 213, p. 211-239.

AURAY, N. KAMINSKY, D. (2007), « The Professionalisation Paths of Hackers in IT Security: The Sociology of a Divided Identity », *Annales des télécommunications*, vol. 62, nº 11-12, p. 1312-1326.

BARTHE, Y. (2006), *Le Pouvoir d'indécision. La mise en politique des déchets nucléaires*, Paris, Economica.

BARTHE, Y., BORRAZ, O. (2011), « Les controverses sociotechniques au prisme du Parlement », *Quaderni*, nº 75, p. 63-71.

BARTHE, Y., LINHARDT, D. (2009), « L'expérimentation : un autre agir politique », *Working paper du CSI*, nº 13, en ligne, https://halshs.archives-ouvertes.fr/halshs-00352411/document.

BIJKER, W. E., HUGHES, T. P., PINCH, T. (1987). *The Social Cconstruction of Technological Systems. New Direction in the Sociology and History of Technology.* Cambridge (MA), MIT Press.

BLANCHETTE, J. -F. (2006), « The Digital Signature Dilemma », *Annales des télécommunications*, vol. 61, nº 7-8, p. 908-923.

BRECKENRIDGE, K. (2014), *The Biometric State: The Promise and Peril of Digital Government in the New South Africa*, Cambridge, Cambridge University Press.

CALLON, M. (1986), « Éléments pour une sociologie de la traduction : la domestication des coquilles Saint-Jacques et des marins-pêcheurs dans la baie de Saint-Brieuc », *L'Année sociologique*, vol. 36, nº 3, p. 169-208.

CAPLAN, J., TORPEY, J. (eds.) (2001), *Documenting Individual Identity: The Development of State Practices in the Modern World*, Princeton (NJ), Princeton University Press.

CEYLAN, A., PIAZZA, P. (dir.) (2011), *L'Identification biométrique : champs, acteurs, enjeux et controverses*, Paris, Éditions de la Maison des sciences de l'homme.

CHATEAURAYNAUD, F., TORNY, D. (1999), *Les Sombres Précurseurs. Une sociologie de l'alerte et du risque*, Paris, Éditions de l'ÉHESS.

CHATEAURAYNAUD, F., DEBAZ, J. (2017), *Au bord de l'irréversible. Sociologie pragmatique des transformations,* Paris, Éditions Pétra.

CRETTIEZ, X., PIAZZA, P. (dir.) (2010), *Du papier à la biométrie : identifier les individus*, Paris, Presses de Sciences Po.

DAGIRAL, É. (2007), « La construction sociotechnique de l'administration électronique. Les usagers et les usages de l'administration fiscale », *Thèse pour le doctorat en sociologie,* École nationale des Ponts et Chaussées.

FRAENKEL, B., (1992), *La Signature. Genèse d'un signe*, Paris, Gallimard.

FRAENKEL, B., PONTILLE, D. (2003), « L'écrit juridique à l'épreuve de la signature électronique, approche pragmatique », *Langage et société*, vol. 104, nº 2, p. 83-122.

GROMMÉ, F., RUPPERT, E. (2020), « Population Geometries of Europe: The Topologies of Data Cubes and Grids », *Science, Technology, & Human Values*, vol. 45, nº 2, p. 235-261.

HECHT, G. (2014), *Le Rayonnement de la France. Énergie nucléaire et identité nationale en France après la Seconde Guerre mondiale*, Paris, Éditions Amsterdam.

HIGGS, E. (2003), *The Information State in England: The Central Collection of Information on Citizens since 1500*, Basingstoke, Palgrave Macmillan Education.

KHATCHATOUROV, A. (2019), *Les Identités numériques en tension : entre autonomie et contrôle*, Londres, ISTE Editions.

LACOUETTE-FOUGÈRE, C. (2011), « Le projet INÉS aboutira-t-il ? La carte nationale d'identité électronique en France : une solution à la recherche de problèmes », dans CEYLAN, A. PIAZZA, P. (dir.), *L'Identification biométrique : champs, acteurs, enjeux et controverses*, Paris, Éditions de la Maison des sciences de l'homme, p. 198-215.

LATOUR, B. (1985), « Les "Vues" de l'Esprit. Une introduction à l'anthropologie des sciences et des techniques », *Culture et technique*, nº 14, p. 4-30.

LAURENT, B. (2022), *European Objects. The Troubled Dreams of Harmonization,* Cambridge (MA), MIT Press.

LAURENT, B., DOGANOVA, L., GASULL, C., MUNIESA, F. (2021), « The Test Bed Island: Tech Business Experimentalism and Exception in Singapore », *Science as Culture*, vol. 30, p. 367-390.

LEPRÊTRE, N. (2019), « Innover dans la ville par l'expérimentation : Les démonstrateurs urbains comme instrument de gouvernement à distance de politiques énergétiques territorialisées », *Gouvernement et action publique*, vol. 8, nº 3, p. 9-33.

LINHARDT, D. (2009), « L'État et ses épreuves : éléments d'une sociologie des agencements étatiques », *Clio@Themis,* nº 1, en ligne, http://cliothemis.com/L-Etat-et-ses-epreuves.

MARRES, N. (2020), « What if Nothing Happens? Street Trials of Intelligent Cars as Experiments in Participation », dans MAASEN, S., DICKEL, S., SCHNEIDER, C.,

TechnoScienceSociety. Technological Reconfigurations of Science and Society, Cham, Springer, p. 111-130.

MESNEL, B. (2017), « Les agriculteurs face à la paperasse. *Policy feedback* et bureaucratisation de la politique agricole commune », *Gouvernement et action publique,* vol. 1, nº 1, p. 33-60.

NAIR, V. (2019), « Governing India in Cybertime: Start-up Cultures, Biometric IDs, and the Temporalized State », *South Asia: Journal of South Asian Studies*, vol. 42, nº 3, p. 519-36.

NOIRIEL, G. (dir.) (2007), *L'Identification. Genèse d'un travail d'État*, Paris, Belin.

PASQUIER, D. (2018), *L'internet des familles modestes. Enquête dans la France rurale,* Paris, Presses des Mines.

PELIZZA, A. (2020), « Processing Alterity, Enacting Europe: Migrant Registration and Identification as Co-Construction of Individuals and Polities », *Science, Technology, & Human Values*, vol. 45, nº 2, p. 262-288.

PELIZZA, A. (2021), « Identification as Translation: The Art of Choosing the Right Spokespersons at the Securitized Border », *Social Studies of Science*, vol. 51, nº 4, p. 487-511.

PIAZZA, P. (2004), *Histoire de la carte nationale d'identité,* Paris, Odile Jacob.

PIAZZA, P. (2006), « Les résistances au projet INÉS », *Cultures & Conflits*, nº 64, p. 65-75.

RALLET, A., ROCHELANDET, F. (2004), « La fracture numérique : une faille sans fondement ? », *Réseaux*, vol. 22, nº 127-128, p. 19-54.

RAO, U. (2018), « Biometric Bodies, or How to Make Fingerprinting Technology Work in India », *Body & Society*, vol. 24, nº 3, p. 68–94.

SINGH, R. (2019), « Give me a Database and I will Raise the Nation-State », *South Asia: Journal of South Asian Studies*, vol. 42, nº 3, p. 501-518.

TIFFON, G. (2018), *La Mise au travail des clients,* Paris, Économica.

VAN DER PLOEG, I. (2003), « Biometrics and the Body as Information », Lyon D. (dir), *Surveillance as social sorting: Privacy, risk and Automated discrimination*, Londres et New-York, Routledge, p. 57-73.

Résumé : Comment s'assurer de l'identité d'une personne dans les services à distance ? L'article analyse la controverse sur la réponse française à la problématisation de l'authentification à distance dans ALICEM, une application mobile conçue par l'Agence nationale des titres sécurisés du ministère de l'Intérieur pour doter les utilisateurs des services publics d'une identité numérique sécurisée. Il décrit les raisons qui ont mené ce ministère à mettre au point cette application ainsi que les choix techniques et politiques formulés dans la technologie, avant de retracer la mise en cause et les réponses gouvernementales pour tenter d'endiguer la critique. L'étude tire de cette controverse deux enseignements sur les reconfigurations contemporaines de la relation entre un État technologique européen et les utilisateurs des services publics (nommées « devenir interface ») : la diffusion contestée d'une modalité d'action expérimentale et le souci de signaler la présence de l'État sur le marché.

Mots clés : biométrie, controverse, expérimentation politique, reconnaissance à distance, souveraineté numérique

Frictions linked to the citizen's relationship to the state "becoming interface". Controversy over the ALICEM experiment

Abstract: How can a person's identity be verified in remote governmental services? The article presents an analysis of controversy over the French response to this problem of remote identification, ALICEM, a mobile application designed by the French Ministry of the Interior's National Agency for Identity Documents to provide public services users with a secure digital identity. It describes the reasons that led the Ministry to design this application and the technical and political choices embedded in the technology, before identifying the issues involved and the government's responses in an attempt to stem the critiques of its actions. The analysis presented two insights regarding the contemporary reconfigurations of the relationship between the technological state and digital users (named here "becoming an interface"): the contested diffusion of an experimental mode of action and a choice made to signal the presence of the state to the market.

Keywords: biometrics, controversy, digital sovereignty, political experiment, remote recognition