CNNum
Conseil National du Numérique

Avis du Conseil national du numérique sur le

fichier *TES*

décembre 2016

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Avis du Conseil national du numérique sur le fichier TES

Pour rendre son avis, le Conseil s'est appuyé sur les contributions recueillies sur la plateforme de consultation dédiée au sujet. Le Conseil a également mené une série d'auditions d'experts[1] et a rencontré des représentants du ministère de l'Intérieur et de l'Agence nationale des titres sécurisés (ANTS — établissement public administratif, placé sous tutelle du ministère de l'Intérieur).

Ce travail en amont a conduit le Conseil à réaliser des synthèses sur les solutions techniques alternatives reproduites en annexe 2 du présent avis et sur la consultation en ligne disponible sur le site tes.cnnumerique.fr :

- Centralisation et sécurité informatique[2] ;
- Prévention des utilisations détournées d'un fichier sensible, massif et centralisé[3] ;
- Gouvernance des choix technologiques de l'État[4].

[1] Voir la liste des personnes auditionnées en annexe 1
[2] https://tes.cnnumerique.fr/project/c2/synthesis/synthese-3
[3] https://tes.cnnumerique.fr/project/risques-prospectifs-et-detournements-de-finalites/synthesis/synthese-1
[4] https://tes.cnnumerique.fr/project/gouvernance-des-choix-technologiques-de-l-etat/synthesis/synthese

Contexte

Le 30 octobre, le Gouvernement a publié un décret prévoyant la création d'une base de données des « Titres électroniques sécurisés » (TES[5]). Ce décret annonce la fusion de la base TES existante relative aux passeports, qui concerne déjà près de 15 millions d'individus[6], et la base des cartes nationales d'identité, présentée avec un double objectif de lutte contre la fraude documentaire et de gestion simplifiée des titres[7]. Une telle base de données contiendrait notamment des données sur l'état civil des personnes, sur leurs signes physiques distinctifs ainsi que des données biométriques[8]. Elle devrait concerner à terme près de 60 millions de Français.

Dans un communiqué en date du 7 novembre 2016, le Conseil national du numérique a appelé le Gouvernement à suspendre la mise en œuvre de ce décret afin d'examiner des alternatives tenant compte de l'état de l'art technique et respectant les droits et libertés des citoyens[9]. Afin de contribuer à pallier l'absence de concertation sur ce sujet d'importance centrale, tant par la nature des données enregistrées que du nombre de personnes concernées, le Conseil a organisé un débat public au travers d'une plateforme de consultation en ligne (tes.cnnumerique.fr), afin de recueillir les avis et les expertises techniques et juridiques.

Depuis l'autosaisine du Conseil, le Gouvernement a ouvert un dialogue constructif avec le Parlement et la société civile et s'est engagé à « *impliquer de manière continue les organes d'expertise techniques, les autorités indépendantes et à rester à l'écoute des attentes de la société civile, notamment celles issues de la consultation engagée par le Conseil national du numérique, sur le sujet de l'identité numérique qui représente un enjeu majeur de modernisation et de protection pour nos concitoyens* »[10]. Des pistes d'évolution du dispositif ont par ailleurs été ouvertes : d'une part, en garantissant la possibilité pour tout individu de refuser le versement de ses empreintes ; d'autre part, en prévoyant une homologation de la sécurité du système et des procédures par l'Agence Nationale de la Sécurité des Systèmes

[5] Décret n° 2016-1460 du 28 octobre 2016
[6] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033318979&dateTexte=&categorieLien=id
[7] http://www.interieur.gouv.fr/Actualites/Le-fichier-des-titres-electroniques-securises
[8] Le fichier fusionné contiendra : le nom de famille, le nom d'usage, les prénoms, la date et le lieu de naissance, le sexe, la couleur des yeux, la taille, le domicile ou la résidence, les données relatives à la filiation (les noms, prénoms, dates et lieux de naissance de ses parents, leur nationalité), les données biométriques (image numérisée du visage et des empreintes digitales qui peuvent être légalement recueillies), l'image numérisée de la signature du demandeur de la carte nationale d'identité, l'adresse de messagerie électronique et les coordonnées téléphoniques du demandeur.
[9] https://cnnumerique.fr/cp_fichier_tes/
[10] http://proxy-pubminefi.diffusion.finances.gouv.fr/pub/document/18/21681.pdf

d’Information (ANSSI) et la Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC).

L’avis du Conseil vise à prolonger et opérationnaliser ces résolutions. La consultation qu’il a menée a en effet permis d’identifier des propositions intéressantes, tant du point de vue technique que procédural. Le Conseil est confiant sur le fait que le Gouvernement saura en tenir compte et que le dialogue avec la société civile continuera après cette première phase d’audit.

Synthèse

Le Conseil s’interroge sur la nécessité de stocker de manière centralisée des informations aussi sensibles. Sur la base des éléments mis à sa disposition ou rendus disponibles publiquement, il n'est pas en mesure de confirmer la nécessité de stocker de manière centralisée des données biométriques pour atteindre les finalités avancées. L’authentification biométrique ne constitue qu’un indicateur parmi d’autres s’agissant de l’instruction des demandes de titre d’identité ; par ailleurs les gains attendus en termes d’efficacité, de simplification et de lutte contre la fraude documentaire ne découlent pas, pour l’essentiel, de la fusion de ces deux bases. Au contraire, des risques considérables d’abus, de vol ou de détournement de finalité peuvent directement découler de la création de ce fichier.

Un travail d’anticipation détaillé reste à conduire. La base TES a été créée pour les passeports il y a plus de 8 ans. Son élargissement aux cartes d’identités mériterait une remise à plat pour tenir compte des nouveaux principes européens de protection de la vie privée, ainsi que des nouveaux standards technologiques de sécurisation des données biométriques. Si la sécurité du dispositif fait actuellement l’objet d’un audit de sécurité par l’ANSSI et la DINSIC, de nombreux contributeurs ont pointé l'existence d’alternatives au dispositif méritant d’être considérées par le Gouvernement. Ces dernières pourraient favoriser une meilleure maîtrise des risques liés aux cyberattaques tout en permettant d’atteindre les mêmes objectifs.

Plus largement, le cas TES est symptomatique d’une difficulté plus structurelle : l’État et ses organes doivent poursuivre leur adaptation afin de prendre les meilleures décisions technologiques possibles au regard, notamment, de leurs implications politiques, économiques et sociétales. **Au-delà des questions spécifiques au fichier TES, le Conseil conclut qu’il y a urgence à réformer la gouvernance des choix technologiques au sein de l'État dans le sens d'une transparence et d'une ouverture accrues.**

Recommandation N°1

Au regard de ces éléments, le Conseil ne peut que maintenir sa demande de suspendre l'application du décret et les expérimentations en cours. Cette suspension doit se prolonger au-delà de l'audit mené par la DINSIC et de l'ANSSI, jusqu'à la tenue d'un débat contradictoire public sur la base d'objectifs clairs et d'architectures techniques alternatives.

Pour ce faire :

1. **Le Conseil appelle le gouvernement à rendre publique une analyse justifiant le choix établi.** Cette analyse devrait inclure une quantification des avantages attendus de l'extension de la base TES dans le cadre du plan Préfectures Nouvelle Génération. Elle devrait justifier de l'utilité même de conserver des données biométriques pour atteindre les finalités avancées. Elle devrait enfin justifier que le choix de conserver ces données sous une forme centralisée offre les meilleures garanties en matière de libertés publiques au regard des règles européennes sur la protection des données et des risques de piratage.

2. Une fois ces éléments élaborés et discutés, et une fois publié le résultat de l'audit réalisé par l'ANSSI et la DINSIC justifiant notamment de l'impossibilité technique d'utiliser le dispositif à des fins d'identification, **le Conseil recommande que soit mise en œuvre une procédure de consultation de la communauté scientifique et technologique pour procéder à une analyse des solutions en présence, à une évaluation des risques et des coûts et à l'élaboration éclairée d'architectures adéquates.** Les conclusions de cette analyse devraient être présentées publiquement, en supprimant les éventuels éléments dont la publication serait susceptible de mettre en danger la sécurité du projet, afin qu'une parfaite transparence soit faite quant aux choix politiques et technologiques retenus.

3. **Suite à l'élaboration de ces deux analyses, de nouveaux avis conformes de la CNIL, de l'ANSSI et de la DINSIC devraient être demandés.**

Recommandation N°2

Le Conseil recommande par ailleurs d'initier un débat public avec les citoyens, les acteurs de la société civile, le secteur privé et le secteur public sur les sujets de l'identité administrative et de l'identité en ligne. L'objectif de ce débat est de porter une réflexion globale sur les facettes de l'identité à l'ère numérique (rôles respectifs et articulation entre FranceConnect, chaîne de traitement des passeports et de la CNI, identités numériques publiques et privées), qui prenne en compte la généralisation des smartphones et l'état de l'art en matière d'architectures (webservices, interfaces de programmation et informatique en nuage). Le Conseil appelle le gouvernement à encourager la recherche publique sur les sujets de l'identité numérique — encore peu soutenue en France — de la biométrie et des moyens de sa sécurisation.

Recommandation N°3

Le Conseil recommande enfin de poursuivre l'adaptation du modèle public de gouvernance des choix technologiques dans la mesure où ces décisions majeures vont se multiplier dans les prochaines années. Au-delà de la polémique, l'extension de la base TES apparaît comme le symptôme d'un processus décisionnel qui, en matière technologique, n'intègre pas suffisamment les exigences d'une vision politique de long terme.

À cette fin, le Conseil appelle le Gouvernement à :

1. **Édicter rapidement un cadre général constitué de normes et de bonnes pratiques communes aux administrations et s'appliquant à tout projet numérique susceptible d'avoir un impact significatif sur leurs publics**. Ce cadre pourrait prévoir que tout choix technologique important fasse préalablement l'objet d'une étude d'impact approfondie expliquant les choix effectués (sur le modèle de l'analyse d'impact relative à la protection des données imposée par le Règlement général pour la protection des données). Un tel cadre général pourrait être rendu à terme opposable par tous, mais une première étape pourrait consister à définir et mettre en œuvre des règles non-obligatoires (*soft law*).

2. **Étendre la logique d'État Plateforme en ouvrant le processus de décision publique**. L'instruction de tout projet technologique susceptible d'affecter significativement tout ou partie importante de la population devrait nécessairement être discutée, corrigée, amendée en s'appuyant non seulement sur les institutions de référence et les ministères concernés, mais aussi sur l'intelligence collective, les experts et les acteurs du monde académique.

3. **Renforcer le rôle de la CNIL, la DINSIC et l'ANSSI pour en faire des acteurs de premier plan dans cette transformation**.

Première partie

TES :
des risques importants pour des gains non démontrés

Le décret relatif à la base TES prévoit, en son article 1er, la création d'un traitement de données sensibles à caractère personnel commun aux passeports et aux cartes nationales d'identité. L'objectif de ce traitement est de permettre l'**authentification** des citoyens, c'est à dire de vérifier que la personne qui demande un titre est bien celle qu'elle prétend être. Le ministère de l'Intérieur insiste sur le fait que le traitement est conçu de manière à rendre impossible l'**identification,** c'est à dire de rechercher une identité à partir d'une trace biométrique en la comparant à une base de données biométriques. L'identification d'une personne par ses empreintes digitales est de ce fait particulièrement encadrée en droit français : elle ne peut être recherchée que dans des cas limitativement énumérés[11]. Il s'agit là d'un aspect crucial puisque c'est notamment cette possibilité d'identification qui avait conduit le Conseil constitutionnel à censurer le projet de carte nationale d'identité électronique en 2012[12].

Le fichier prévoit également d'autres finalités au traitement indiqué puisque les services de polices nationale et judiciaire, de gendarmerie et de renseignement peuvent accéder — aux termes de l'article 4 — aux données enregistrées dans le traitement prévu à l'article 1er, à l'exclusion de l'image numérisée des empreintes digitales « *pour les besoins exclusifs de leurs missions de prévention et de répression des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme* ».

Les données biométriques ne sont pas des données « *comme les autres* »

Un constat univoque ressort de la part des contributeurs et des experts auditionnés : **les données biométriques contenues dans le fichier TES sont par essence des données sensibles.** Attachées à une réalité biologique permanente, elles sont automatiquement reconnaissables, elles ne sont pas secrètes ni révocables et ont un caractère immuable. Elles accompagnent le plus souvent chaque individu de sa naissance à sa mort.

Malgré ce caractère sensible, les solutions d'authentification par biométrie se développent dans nos vies quotidiennes : utilisées aujourd'hui pour déverrouiller nos

[11] L'article 16-11 du Code civil précise ainsi que « *L'identification d'une personne par ses empreintes génétiques ne peut être recherchée que :*
1° Dans le cadre de mesures d'enquête ou d'instruction diligentées lors d'une procédure judiciaire ;
2° A des fins médicales ou de recherche scientifique ;
3° Aux fins d'établir, lorsqu'elle est inconnue, l'identité de personnes décédées ;
4° Dans les conditions prévues à l'article L. 2381-1 du code de la défense. (...) » https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070721&idArticle=LEGIARTI000006419307&dateTexte=&categorieLien=cidet

[12] Décision n° 2012-652 DC du 22 mars 2012, Loi relative à la protection de l'identité : http://www.conseil-constitutionnel.fr/decision/2012/2012-652-dc/decision-n-2012-652-dc-du-22-mars-2012.105165.html

téléphones grâce à nos empreintes digitales ou par reconnaissance faciale, elles pourront servir demain à ouvrir nos voitures ou à sécuriser nos transactions sur Internet. **À cet égard, une fuite des données biométriques d'une partie significative de la population française pourrait avoir des lourdes conséquences.** En effet, à l'inverse d'un mot de passe qu'il suffirait de modifier, nos empreintes ne pourraient plus être utilisées en cas de compromission.

Les exemples de tels incidents sont de plus en plus nombreux[13]. C'est d'ailleurs la raison pour laquelle tant la CNIL que la Cour de justice de l'Union européenne se montrent particulièrement attentives quant à la proportionnalité des traitements et des finalités pour la constitution de bases de données biométriques[14].

Les finalités invoquées du décret relatif au fichier TES ne semblent pas justifier la nécessité de conserver des données biométriques

L'élargissement de la base TES s'inscrit dans le cadre du plan Préfectures Nouvelle Génération (PNG). Cette réforme prévoit de simplifier et moderniser les modalités de délivrance des titres réglementaires afin de recentrer le travail des préfectures et des sous-préfectures sur ses quatre missions prioritaires : la gestion locale des crises, l'expertise juridique et le contrôle de légalité, la lutte contre la fraude documentaire et la coordination territoriale des politiques publiques.

Si le Conseil soutient cette volonté de modernisation, il ressort de ses premières analyses que le stockage de données biométriques dans la nouvelle base TES n'est pas un élément indispensable à la bonne conduite du plan Préfectures Nouvelle Génération. **L'authentification biométrique ne constitue en effet qu'un indicateur parmi d'autres s'agissant de l'instruction des demandes de titre d'identité**. Celle-ci passe notamment par la présentation d'un justificatif de domicile ainsi que d'un autre titre permettant de justifier de son identité (carte d'identité ou passeport valide ou périmé depuis moins de 5 ans, ou bien acte de naissance de moins de 3 mois complété par un justificatif de nationalité française si l'acte de naissance ne suffit pas à prouver la nationalité). Plus généralement, la biométrie ne devrait pas être considérée comme suffisante pour fournir un moyen d'authentification à part entière. Comme l'explique l'ANSSI dans son guide sur le contrôle des accès physiques[15], « *la biométrie est assimilable à une méthode d'identification (...). Elle peut donc se substituer au badge en tant que moyen d'identification, mais en aucun cas comme moyen d'authentification. Elle peut toutefois être utile pour authentifier le porteur, en*

[13] Comme le déclare, Josef Lorenzo Hall, technologue en chef au Centre for Democracy & Technology, *« le fait que le nombre d'empreintes digitales volées vient d'augmenter par un facteur de cinq est assez ahurissant ».*
[14] Voir *CJUE*, 4e Ch., 17 octobre *2013*, Michael Schwarz considérant 58 à 62 http://curia.europa.eu/juris/document/document.jsf?docid=143189&cid=146652 et l'avis de la CNIL sur le projet de décret https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033318979. Sur le principe de proportionnalité, voir aussi le Rapport d'information fait au nom de la commission des lois sur l'Usage de la biométrie en France et en Europe par MM. les Sénateurs François BONHOMME et Jean-Yves LECONTE : https://www.senat.fr/rap/r15-788/r15-7881.pdf
[15] https://www.ssi.gouv.fr/uploads/IMG/pdf/Securite_des_technologies_sans_contact_pour_le_controle_des_acces_physiques.pdf

association avec un badge stockant les éléments biométriques permettant la comparaison, dont le badge assure l'intégrité. Ce compromis reste d'une sécurité inférieure au mot de passe, qui peut être gardé secret, et qui est répudiable. »

Le stockage des données biométriques n'apparaît donc pas indispensable pour simplifier les démarches administratives des usagers. Cette simplification passe avant tout par la mise en place de procédures dématérialisées et simplifiées de prises de rendez-vous et de pré-remplissage des dossiers de demandes pour fluidifier les procédures.

S'agissant de l'objectif légitime de lutte contre la fraude documentaire, avancé pour justifier l'élargissement de la base TES aux cartes d'identités, le Conseil note que celle-ci est relativement peu élevée[16] et qu'il existe d'autres solutions pour prévenir l'enregistrement de données faussées ou frauduleuses[17]. **La solution de cachet électronique visible « 2D-Doc »[18] apparaît particulièrement pertinente de ce point de vue et pourrait constituer un premier pas rapide et peu coûteux à mettre en œuvre pour protéger les documents permettant de justifier d'une identité.** Cette solution est mise en place par l'Agence Nationale des Titres Sécurisés (établissement public administratif placé sous la tutelle du ministre de l'Intérieur) en collaboration avec des entités privées et publiques depuis 2012, suite notamment à la censure par le Conseil constitutionnel du projet de carte nationale d'identité électronique[19].

Enfin, il ressort des éléments soumis au Conseil que les arguments financiers avancés pour justifier la réforme méritent d'être relativisés. D'une part, le gain annoncé de 1300 emplois Équivalent Temps Plein annuel Travaillé (ETPT)[20] semble, selon les informations actuellement accessibles au Conseil, principalement lié à la délivrance des certificats d'immatriculation des véhicules et non à la gestion des passeports et des cartes d'identités. D'autre part, l'architecture choisie pour le dispositif TES est nécessairement coûteuse car sa sécurité repose en partie sur

[16] Selon les avocats Christophe Léguevaques et Jean-Marc Fedida, « *il y a une disproportion à ficher 100% de la population alors que la falsification des documents, comme la carte nationale d'identité et le passeport, concerne 15.000 documents, soit seulement 0.1% de la population* ». http://www.ouest-france.fr/societe/megafichier-tes-une-action-collective-reclame-son-annulation-4646928

[17] Voir le document annexé au projet de loi de finances 2016 précité : « *en ce qui concerne les titres sécurisés, les risques de falsification et de contrefaçon portent aujourd'hui davantage sur les justificatifs présentés à l'appui des demandes de titres que sur les titres eux-mêmes.* » https://www.senat.fr/fileadmin/Fichiers/Images/commission/finances/PLF_2016/NP_AGTE_2016.pdf

[18] Pour plus d'information sur ce sujet, se référer à la partie « 2.3. Cachet électronique visible » de la synthèse en annexe. Voir aussi le site de l'Agence nationale des titres sécurisés : https://ants.gouv.fr/Les-solutions/2D-Doc

[19] http://www.nextinpact.com/news/77394-des-qr-codes-pour-securiser-justificatifs-domicile-en-france.htm

[20] Voir la note de présentation de la mission "Administration générale et territoriale de l'État », examen par la commission des finances d'octobre 2015 pour le projet de finances pour 2016 réalisée par le Rapporteur Hervé Marseille qui explique que *«la modernisation des procédures de délivrance des titres et la lutte contre la fraude documentaire »* mobilisent *«29 % des effectifs totaux des préfectures »* et permettra de *«réduire les formalités et démarches accomplies aux guichets des préfectures»*. Objectif : *« libérer 2 000 ETPT de ces tâches inhérentes à la délivrance des titres et en redéployer 700 sur les autres missions prioritaires »*. Soit une suppression de 1 300 ETPT. Cette note affirme que « *ce désengagement est [...] manifeste s'agissant de la délivrance des certificats d'immatriculation des véhicules »*.

l'utilisation d'infrastructures physiques spécifiques (réseau dédié de plus de 2000 points d'accès et serveurs dédiés[21]).

Dès lors, le Conseil s'interroge sur la nécessité même de stocker ces informations sensibles. Il souhaite qu'une étude d'impact approfondie soit menée sur les éléments permettant de justifier la nécessité de conserver des données biométriques et de quantifier les avantages réellement tirés de l'extension de TES aux cartes d'identités.

Face aux risques technologiques, juridiques et démocratiques liés à la base TES, l'État doit se doter de moyens de résilience

Afin de servir de base à cette étude d'impact approfondie, le Conseil national du numérique a procédé à une première cartographie des risques liés à la constitution d'une base de données biométriques, en s'appuyant sur les contributions de la plateforme et sur les avis d'experts. Le Conseil précise que cette cartographie a pour unique objectif de préciser les points d'inquiétude et de vigilance de la communauté concernée. Du fait des limites liées à l'information disponible et au calendrier extrêmement rapide dans lequel ce travail a été mené, cette cartographie ne saurait aucunement se substituer à un travail d'analyse en profondeur à mener par les services du Gouvernement.

Une base centrale ne peut être totalement sécurisée

Quelles que soient les garanties juridiques et techniques apportées, la création d'un dispositif centralisé de cette taille n'est jamais totalement exempte de risques d'attaque, de vol et de détournement. **Les exemples étrangers sont à cet égard inquiétants et rappellent que le risque de fuite de données n'est jamais nul.** En 2015, aux États-Unis, des informations sur 21,5 millions d'Américains ont ainsi été dérobées, parmi lesquelles les empreintes digitales de 5,6 millions de fonctionnaires américains, dont des employés du Pentagone, du FBI ou de la NSA[22]. Au mois d'avril 2016, une faille de sécurité a entraîné une fuite massive de données relatives à 55 millions d'électeurs philippins[23], diffusées ensuite sur le site wehaveyourdata.com qui fournissait un moyen simple de chercher parmi ces données. Le même mois, c'est une base de données tirée du recensement et relative à la moitié de la population turque qui a été mise en ligne avec noms et adresses[24].

Les menaces ne sont pas uniquement externes : une partie des vulnérabilités de tout dispositif est lié aux usages internes ou de sous-traitance. Le facteur humain est en effet toujours un point faible en matière de cybersécurité. Ainsi, en 2009, un sous-traitant du gouvernement israélien avait copié un registre de la population contenant

[21] Voir à ce sujet la réponse de Bernard Cazeneuve au Président du Conseil national du numérique : http://www.interieur.gouv.fr/Actualites/Communiques/Fichier-TES-Courrier-de-Bernard-Cazeneuve-au-President-du-Conseil-national-du-numerique

[22] http://tempsreel.nouvelobs.com/tech/20150925.OBS6537/5-millions-d-empreintes-digitales-volees-la-faille-de-la-biometrie.html

[23] http://www.wired.co.uk/article/philippines-data-breach-comelec-searchable-website

[24] http://www.theregister.co.uk/2016/04/04/turkey_megaleak/

de nombreuses informations confidentielles sur 9 millions de citoyens : ce registre s'était retrouvé sur Internet[25].

La difficulté structurelle à sécuriser le dispositif TES a été signalée par de nombreux chercheurs auditionnés par le Conseil. Le Laboratoire Spécification et Vérification (LSV), laboratoire d'informatique de l'ENS Paris-Saclay et du CNRS, affirme même ne pas connaître « *de solution technique centralisée permettant de réaliser toutes les fonctionnalités prévues par le décret tout en garantissant la confidentialité des données des citoyens* »[26]. Ces craintes emportent un double risque d'image pour la France. À l'international d'une part, car la centralisation de données biométriques pourrait servir de brèche pour la mise en place de dispositifs similaires par d'autres États. D'autre part, ce projet fragilise la parole et les positions de la France, qui se trouve moins légitime à expliquer aux acteurs économiques ou à des États qu'il ne faut pas utiliser les données à caractère personnel des utilisateurs à leur insu.

Une extension ou un détournement des finalités ne peuvent être totalement exclus

De manière générale, les dernières années ont montré que la constitution de fichiers centralisés peut conduire à l'élargissement de leurs finalités initiales : ce fut le cas pour le système Eurodac des demandeurs d'asile, le fichier des demandeurs de visa ou encore le Système de traitement des infractions constatées (STIC). Compte tenu de la décision du Conseil constitutionnel de 2012, une extension des finalités de la base TES à des fins d'identification de tous les citoyens à partir de leurs données biométriques risquerait néanmoins d'être déclarée inconstitutionnelle[27].

Au regard de l'avis exprimé par la CNIL, le Conseil s'interroge sur la possibilité laissée par le décret d'utiliser un dispositif de reconnaissance faciale à partir de l'image numérisée de la photographie. Sur ce point, il importe de noter que les services de polices nationale et judiciaire, de gendarmerie et de renseignement peuvent d'ores et déjà accéder — aux termes de l'article 4 du décret — à l'image numérisée de la photographie enregistrée dans la base « *pour les besoins exclusifs de leurs missions de prévention et de répression des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme* ». La CNIL avait donc demandé à ce que le décret se fonde « *sur des dispositions juridiques plus explicites, permettant une information claire des citoyens sur les conditions d'utilisation des données biométriques collectées*. » La crainte d'une possible identification des individus couplée à des systèmes de vidéosurveillance est accentuée par le fait que l'optionalité du versement de l'image numérisée des empreintes digitales dans la base TES — proposée par le ministre de l'Intérieur — ne concerne pas la photographie. Dans tous les cas, comme le remarque François Pellegrini, Professeur en informatique et membre de la CNIL, l'optionalité du versement apparaît comme une faible garantie

[25] http://www.zdnet.com/article/israel-nabs-source-of-leak-of-9-million-personal-details/
[26] http://www.lsv.ens-cachan.fr/?l=fr
[27] Les sages ont considéré « l*a création d'un fichier d'identité biométrique portant sur la quasi-totalité de la population française et dont les caractéristiques rendent possible l'identification d'une personne à partir de ses empreintes digitales porte une atteinte inconstitutionnelle au droit au respect de la vie privée* ».

d'autant plus que *« la préservation des libertés n'est pas une option. C'est à l'État de la garantir pour tous les citoyens, sans laisser aux personnes le choix d'y renoncer. Il est facile d'imaginer que, une fois en préfecture, les demandeurs auront individuellement du mal à résister à la pression ambiante, d'autant qu'il leur sera indiqué que ceux qui les fourniront bénéficieront d'un « meilleur service » puisqu'ils n'auront plus de « paperasse » à présenter en cas de perte de leur titre d'identité.* [28] »

En outre, des usages détournés, hors de tout contrôle, ne peuvent être exclus pour de tels dispositifs. Rappelons à cet égard que l'absence d'encadrement était jusqu'à une époque récente caractéristique de l'activité des services de renseignement. Dès lors, penser que notre pays ferait exception revient à ignorer les leçons de l'histoire et des comparaisons internationales. Les reculs démocratiques et la montée des populismes, observés y compris en Europe et aux États-Unis, rendent déraisonnables ces paris sur l'avenir.

La garantie constitutionnelle est donc un garde-fou important, mais à l'heure du numérique, les garanties légales doivent s'accompagner de traductions techniques. Dans le cas du fichier TES, cette garantie technique se matérialise par la robustesse du lien unidirectionnel chiffré qui unit le compartiment de l'application contenant les éléments alphanumériques au compartiment contenant les données biométriques. L'analyse de l'ANSSI et de la DINSIC devrait notamment porter sur la robustesse de ce lien — afin qu'il puisse être techniquement inviolable dans le temps. Certains contributeurs émettent toutefois d'ores et déjà des doutes sur son caractère unidirectionnel, rappelant que, d'un point de vue théorique, l'identification d'un citoyen à partir de ses données biométriques pourrait être effectuée en déroulant un test d'authentification sur l'ensemble de la base nominative[29].

[28] Voir également la partie consacrée à la Résilience des sociétés humaines et faux papiers dans l'article de François Pellegrini, « La biométrie des honnêtes gens : penser le temps long » : http://www.pellegrini.cc/2016/11/la-biometrie-des-honnetes-gens-penser-le-temps-long/#more-76

[29] Voir la synthèse de la consultation "Prévention des utilisations détournées d'un fichier sensible, massif et centralisé" : https://tes.cnnumerique.fr/project/risques-prospectifs-et-detournements-de-finalites/synthesis/synthese-1 et l'article de François Pellegrini du 12 novembre, "La liberté n'est pas soluble dans la technique" qui explique que créer la table de correspondance inverse ne serait ni complexe, ni techniquement coûteuse à réaliser : http://www.pellegrini.cc/2016/11/la-biometrie-des-honnetes-gens-reloaded/

Deuxième partie

Un travail d’anticipation reste à mener

L'évolution rapide des technologies de l'information nécessite l'application d'un principe de précaution numérique. Ce principe n'est rien d'autre que le principe de précaution appliqué au cas de l'identité dans un monde numérisé. Dans le cas présent, ce principe impose de **ne pas faire de choix technique irrévocable dans la constitution d'une base qui, si dévoilée, ne pourrait pas être neutralisée** (en raison de son volume et de son importance dans le bon fonctionnement des services de l'État).

Des alternatives techniques méritent d'être considérées

Dans son avis sur le projet de décret[30], la CNIL souligne que « l*es risques spécifiques attachés au fichier envisagé, au regard tant de la nature des données enregistrées que du nombre de personnes concernées, imposent la plus grande prudence et obligent à n'envisager sa mise en œuvre que dans la stricte mesure où aucun autre dispositif, présentant moins de risques d'atteintes aux droits des intéressés, ne permet d'atteindre des résultats équivalents* ».

La sécurité du dispositif actuel repose notamment sur l'utilisation d'une cryptographie spécifique et d'un lien unidirectionnel entre données biométriques et données des demandes de titres[31]. Ces garanties importantes font actuellement l'objet d'un audit de sécurité par l'ANSSI et la DINSIC. Toutefois, de nombreux contributeurs à la consultation menée par le Conseil considèrent ces garanties insuffisantes et pointent l'existence d'alternatives au dispositif proposé, favorisant une meilleure maîtrise des risques liés aux cyberattaques tout en permettant d'atteindre les mêmes objectifs.

Le Conseil a donc souhaité creuser ces pistes afin de mettre à disposition une première analyse pour favoriser l'organisation d'un débat sur le sujet. Les pistes analysées peuvent être classées en trois catégories présentées ci-dessous et détaillées en annexe.

Architectures sans base de données centralisée

Selon plusieurs contributeurs, l'existence d'une base de données centrale n'est pas nécessaire pour atteindre les objectifs annoncés par le ministère de l'Intérieur, à savoir « *lutter contre la fraude documentaire* » et « *faire de la CNI un document sûr de l'identité de son porteur* ». Une solution comme le cachet électronique visible, déjà évoqué dans la partie précédente, pourrait ainsi être une première étape efficace pour atteindre, à faibles coûts, ces objectifs. À noter que des réflexions sont actuellement

[30] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033318979
[31] http://www.interieur.gouv.fr/Actualites/Communiques/Fichier-TES-Courrier-de-Bernard-Cazeneuve-au-President-du-Conseil-national-du-numerique

en cours pour faire évoluer ce standard et incorporer une fonctionnalité d'authentification biométrique[32].

La CNIL préconise[33], quant à elle, de faire évoluer la carte d'identité pour y inclure un support cryptographique contenant les données biométriques du détenteur. Les citoyens conserveraient de cette manière la maîtrise de leurs données, réduisant les risques d'une utilisation à leur insu. S'il est vrai que cette solution nécessite un investissement spécifique, cet investissement pourrait être compensé par la possibilité de supprimer les coûts d'un réseau spécifiquement dédié au dispositif TES. Elle serait en outre fortement créatrice de valeur : selon certains contributeurs, une telle solution pourrait par exemple fournir une base essentielle permettant le développement de signatures électroniques ou de mécanismes d'authentification propices à la simplification des démarches administratives.

Renforcer la confiance dans la bonne utilisation de la base de données

La justification principale de la constitution d'une base de données biométriques est de permettre un contrôle plus efficace dans les cas où la personne souhaitant refaire son document d'identité ne dispose pas d'autre moyen de prouver son identité. Le Conseil s'est donc intéressé aux architectures techniques qui, même dans le cas où la base serait diffusée, révèlent le moins d'informations personnelles possible sur les utilisateurs.

Plus généralement, il est possible de renforcer la confiance dans la bonne utilisation du système en distribuant des responsabilités à un ensemble d'acteurs. Plusieurs contributeurs ont ainsi proposé la mise en place d'une architecture à clés multiples, tout accès à la base nécessitant ensuite l'accord d'un nombre minimal de ces acteurs[34].

Formats sécurisés pour le stockage de données biométriques

Au-delà des solutions décrites précédemment concernant l'architecture du système, le Conseil s'est intéressé aux formats de stockage des données biométriques. La recherche — privée et publique — est en effet active sur les sujets d'identité, de biométrie et de sécurisation.

La CNIL a ainsi recommandé de procéder à l'enregistrement des seuls gabarits et non de la photographie des empreintes digitales. D'autres possibilités existent mais sont encore du domaine de la recherche, telles que le BioHashing qui consiste à stocker les informations biométriques sous une forme transformée par une fonction non-inversible garantissant l'impossibilité de reconstruire les données brutes originelles. On parle alors de « biométrie révocable », puisque, dans le cas où les données

[32] Pour plus d'explications sur ce point, voir notamment la contribution de Nathalie Launay à la consultation du Conseil : https://tes.cnnumerique.fr/projects/risques-prospectifs-et-detournements-de-finalites/consultation/consultation-2/opinions/les-solutions-proposez-vos-solutions/identification-authentification-quelles-sont-les-alternatives-a-puce-ou-sans-envisageables-pour-repondre-au-besoin-tout-en-etant-conforme-aux-reglements-et-standards-internationaux

[33] https://www.cnil.fr/fr/fichier-tes-audition-de-la-presidente-de-la-cnil-au-senat

[34] En pratique, il s'agirait par exemple de distribuer une partie des clés aux services de police, une partie à la CNIL, une partie à la justice et une partie à l'utilisateur en opt-in.

biométriques seraient compromises, il est possible de changer de fonction transformatrice.

De nouveaux principes règlementaires

Outre l'existence d'alternatives techniques, la mise en œuvre du nouveau décret TES intervient parallèlement à l'implémentation du Règlement général pour la protection des données (RGPD)[35] qui a récemment intégré deux principes réglementaires majeurs au cœur de la doctrine européenne :

- le principe de « privacy by design[36] » qui impose aux organisations de prendre en compte les exigences relatives à la protection des données personnelles dès la conception des produits, services et systèmes exploitant des données à caractère personnel ;

- le principe d'une évaluation d'impact (« Data protection Impact Assessment ») préalablement à la mise en place de toute activité pouvant avoir des conséquences importantes en matière de protection de données personnelles. Cette étude doit aussi prévoir les mesures pour diminuer l'impact des dommages potentiels à la protection des données personnelles[37].

Sur ce sujet de la protection des données à caractère personnel, le Conseil recommande donc au Gouvernement de s'inspirer de ces deux principes et d'instaurer plus généralement un principe de frugalité du stockage des données à caractère personnel des citoyens : a-t-on réellement besoin de stocker ces données sous une forme centralisée ? Qui dans l'État doit se poser cette question ? Une telle étude d'impact a d'ailleurs été demandée par la CNIL dans son avis du 29 septembre 2016[38].

Une suspension nécessaire

Depuis l'autosaisine du Conseil, le Gouvernement s'est engagé à suspendre le déploiement du dispositif sur l'ensemble du territoire jusqu'à l'homologation par l'ANSSI et la DINSIC par un avis conforme sur la sécurité du système et des procédures[39]. Le rapport d'audit est attendu pour mi-janvier et le ministre de l'Intérieur s'est engagé à en rendre publique une version expurgée des éléments les plus sensibles. Si le Conseil accueille favorablement le lancement de cet audit, il regrette le mandat restrictif et le délai trop court accordé aux deux administrations pour conduire l'analyse nécessaire des architectures alternatives.

[35] http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679
[36] Protection de la vie privée dès la conception
[37] Voir l'article 35 du règlement
[38] « *La Commission réitère que les enjeux soulevés par la mise en œuvre d'un traitement comportant des données particulièrement sensibles relatives à près de 60 millions de français auraient mérité une véritable étude d'impact et l'organisation d'un débat parlementaire.* »
[39] http://proxy-pubminefi.diffusion.finances.gouv.fr/pub/document/18/21681.pdf

La base centralisée de données biométriques utilisée pour délivrer les passeports biométriques a été créée il y a plus de 8 ans[40]. Il est nécessaire de rappeler que la constitution d'une telle base n'était requise ni par l'Organisation de l'Aviation Civile Internationale[41] (OACI) ni par le règlement européen relatif à l'intégration d'éléments biométriques dans les passeports et les documents de voyage[42]. ***A minima*, son élargissement aux cartes d'identités mérite une véritable analyse contradictoire menée de manière transparente pour tenir compte de l'état de l'art technique et des bonnes pratiques réglementaires.**

Dans ce contexte, le Conseil estime qu'il est indispensable de suspendre l'application du décret TES ainsi que les expérimentations en cours dans les Yvelines et en Bretagne jusqu'à ce qu'une comparaison précise de l'ensemble des architectures possibles, mesurant les bénéfices, les coûts et les risques des systèmes complets, soit rendue disponible, publiquement débattue avec des experts indépendants et devant l'opinion, et discutée au parlement. Ce travail de réflexion doit aussi porter sur la base actuellement utilisée pour les passeports.

Ouvrir de nouveau le sujet de l'identité en ligne

Au-delà de la question du fichier TES et compte tenu de l'application prochaine du règlement eIDAS, il est urgent d'ouvrir une réflexion publique et globale sur la question de l'identité à l'heure du numérique.

Les sujets de l'identité numérique et de sa sécurisation sont sur le devant de la scène européenne avec le règlement eIDAS. Ce règlement impose dès 2018 aux États membres la reconnaissance mutuelle des schémas d'identité numérique : chaque État membre sera obligé de reconnaître les moyens d'identification numérique des autres États membres s'ils respectent un niveau minimal de garanties spécifiques. Le règlement normalise trois niveaux de sécurité (faible, substantiel, élevé). La France a engagé des travaux, dans le cadre de sa feuille de route de l'identité numérique, pour proposer un schéma d'identité numérique qui présente des garanties suffisantes. À ce jour, les fournisseurs d'identité agrégés par FranceConnect ne permettent d'atteindre que le niveau minimal (niveau 1) alors qu'une authentification électronique à plusieurs facteurs[43] pourrait permettre d'atteindre les niveaux 2 et 3. Au-delà des problèmes d'image pour la France de ne pas notifier un schéma d'identité numérique de niveau suffisant à l'UE, le non-respect d'eIDAS pourrait être source de problèmes pour les entreprises françaises[44].

[40] À la suite d'un décret du 30 avril 2008
[41] L'OACI est une organisation internationale qui dépend des Nations unies. Son rôle est de participer à l'élaboration des normes qui permettent la standardisation du transport aéronautique international.
[42] http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=URISERV%3Al14154
[43] L'authentification biométrique, sous une forme non-centralisée, pourrait être l'un de ces facteurs.
[44] Par exemple, afin de répondre à une procédure d'appels d'offres dématérialisée dans un autre pays, une entreprise pourrait être obligée de se constituer une identité numérique reconnue dans le pays, ce qui passerait potentiellement par la création d'une structure juridique dans un État membre respectant la normalisation eIDAS.

En outre, l'article 136 de la loi pour une République numérique spécifie que l'Agence nationale de sécurité des systèmes d'information (ANSSI) va établir un cahier des charges pour un moyen d'identification électronique fiable permettant l'accès à des services en ligne ainsi qu'à un coffre-fort électronique. Dès lors, le Conseil s'interroge sur le calendrier suivi : n'aurait-il pas fallu faire de la remise de ces éléments un préalable à la publication du décret du 28 octobre et à la refonte de la chaîne de l'identité ?

Les sujets de l'identité administrative et de l'identité numériques sont traités séparément en France depuis plus de 10 ans. Néanmoins, la question de leur relation est appelée à prendre de l'ampleur dans les prochaines années. À court terme, il s'agit d'assurer le plus haut niveau d'interopérabilité prévue par la législation européenne et de tirer pleinement partie des avancées et des réflexions de la recherche ; à long-terme, il est question de penser un modèle pour notre société numérique. Il semble en particulier nécessaire de développer une réflexion sur les impacts profonds à long terme sur notre société d'une généralisation des procédures d'authentification pour accéder à tout service - public ou privé, en France ou à l'étranger. Il s'agit d'un chantier multidisciplinaire de grande ampleur et essentiel à la construction de notre pays, qui ne peut être éludé par des prises de décisions partielles et bornées à des besoins opérationnels immédiats, et doit nous amener à nous poser au préalable des questions structurantes sur les visions sociale, politique, philosophique et économique de l'identité ?

Troisième partie

Tout choix technologique révèle un choix de société

La constitution d'une base de données visant à recenser près de 60 millions de Français ne peut s'analyser comme une décision administrative ou un simple aménagement technique ; il s'agit ni plus ni moins d'un choix de société.

La controverse entourant l'élargissement du fichier TES est révélatrice d'une difficulté structurelle : l'État et ses organes doivent poursuivre leur adaptation pour prendre les meilleures décisions technologiques possibles au regard, notamment, de leurs implications politiques, économiques et sociétales. Bien que le problème soit identifié depuis plus d'une décennie, les dernières années ne semblent pas avoir permis d'avancer suffisamment en ce sens. Plusieurs illustrations en témoignent : l'accord-cadre passé entre Microsoft et le Ministère de la Défense[45] qui questionne l'indépendance stratégique de la France ; le partenariat, annoncé par surprise en novembre 2015, qui lie cette même société et le Ministère de l'Éducation nationale ; ou plus récemment, le dévoilement de l'algorithme de sélection d'Admission Post Bac (APB)[46]. Ces choix sont régulièrement vidés de leur sens politique, voire relégués au rang de simples choix techniques, alors même qu'ils tracent les contours de la société numérique de demain et devraient à ce titre être porteurs d'une vision stratégique.

TES : un contre-exemple symptomatique

L'affaire du fichier TES apparaît donc comme le symptôme d'un processus décisionnel qui, en matière technologique, n'intègre pas suffisamment les exigences d'une vision politique de long terme. La question de la proportionnalité (la constitution d'un fichier centralisé d'une telle ampleur est-elle le seul moyen de parvenir aux objectifs ?) comme celle de l'anticipation des risques (quelles garanties techniques et juridiques exceptionnelles peut-on apporter ?) n'ont pas été traitées avec la profondeur et la transparence nécessaire aux différentes étapes de la prise de décision. Paradoxalement, l'Agence nationale de sécurité des systèmes d'information (ANSSI) créée en 2009 et la Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC), créée en 2014, visaient précisément à mieux configurer cette gouvernance technologique et à pallier cette absence de vision stratégique de long terme. Or il semble que ni l'une ni l'autre n'ont été saisies de manière approfondie en amont de la publication du décret, alors même que ces deux institutions sont fortement concernées par le sujet de l'identité numérique : l'ANSSI travaille depuis plusieurs mois à l'implémentation du règlement « eIDAS » tandis que la DINSIC anime un écosystème très actif autour de FranceConnect.

[45] Signé en 2009 et renouvelé en 2013 pour 4 ans
[46] L'Education nationale a dévoilé cet algorithme dans une forme partielle, quasiment illisible et à rebours du mouvement en faveur de l'open data porté par la loi pour une République numérique

À l'inverse, si la CNIL a bien été consultée (le recueil de son avis motivé est obligatoire pour les traitements mis en œuvre pour le compte de l'État qui portent sur des données biométriques), cette dernière n'a eu que 9 jours[47] pour se prononcer sur ce fichier aux implications conséquentes pour la protection des données des ressortissants français. Par ailleurs, cette saisine est intervenue très tardivement, dans la mesure où l'avis du Conseil d'État est daté du 23 février 2016, soit 7 mois plus tôt, et que le dispositif semble avoir été finalisé depuis plus longtemps encore[48]. Cette situation conduit de nombreux contributeurs à la consultation menée par le Conseil à regretter la réduction des prérogatives de la CNIL suite à la réforme du 6 août 2004 et à s'interroger sur l'importance accordée par le Gouvernement aux avis et délibérations de la CNIL. Le ministre de l'Intérieur a par la suite décidé de la saisine *a posteriori* de l'ANSSI et de la DINSIC pour les charger d'auditer publiquement le dispositif et de rendre un avis conforme. Cette démarche — positive — doit être saluée mais plus encore : elle doit faire école.

Faire évoluer la prise de décision publique

Au-delà de cette polémique, la crise révèle la nécessité de poursuivre l'adaptation du modèle public de gouvernance des choix technologiques dans la mesure où ces décisions majeures vont se multiplier dans les prochaines années. À mesure de la numérisation de la société, de la place croissante des algorithmes dans l'aide à la décision publique, de la constitution de nouvelles bases de données[49], ces débats sont appelés à devenir récurrents.

La prise de décision publique en matière numérique devrait ainsi évoluer :

1. **Vers plus d'ouverture.** Tout projet technologique susceptible d'affecter significativement tout ou partie importante de la population devrait nécessairement faire l'objet d'une concertation et d'une étude d'impact proportionnées aux enjeux. Les solutions techniques devraient en ce sens pouvoir être discutées, corrigées, amendées en s'appuyant sur l'intelligence collective et l'opinion experte : il est nécessaire d'associer plus en amont le secteur privé, le monde de la recherche ainsi que la société civile. **En conformité avec l'engagement de la France pour le Partenariat pour un gouvernement ouvert (PGO), cette ouverture à l'extérieur apparaît particulièrement nécessaire.**

2. **Vers une plus grande réflexivité.** Il s'agit là d'un point essentiel, qui consiste, pour la personne publique, à s'interroger sur les implications politiques, économiques, sociales et sociétales des choix technologiques qu'elle est amenée à prendre. Le déploiement technique d'un projet ne peut se permettre de perdre de vue la perspective générale, le tableau d'ensemble. Le développement du

[47] Le projet de décret ayant été transmis à la CNIL le 20 septembre 2016, celle-ci a rendu sa délibération le 29.
[48] Source : Comment (et pourquoi) Bernard Cazeneuve a décidé de ficher 60 millions de Français http://www.liberation.fr/france/2016/11/07/comment-et-pourquoi-bernard-cazeneuve-a-decide-de-ficher-60-millions-de-francais_1526551
[49] Pour rappel la France, pays centralisé de 66 millions d'habitants, dispose d'une des plus grandes bases médico-administrative du monde

numérique appelle une transformation culturelle de l'administration. Comme l'a déclaré le Président François Hollande à l'occasion de l'ouverture du PGO[50], le numérique engendre la possibilité qu' « *une nouvelle démocratie puisse émerger : une démocratie où l'État, l'administration et les collectivités territoriales s'ouvrent à toutes les initiatives, associent tous les talents qui souhaitent apporter leur concours, que l'innovation soit partout présente.* »

3. C'est pourquoi il est nécessaire de **renforcer le rôle de la CNIL, la DINSIC et de l'ANSSI pour en faire des acteurs de premier plan dans cette transformation**. Plus généralement, il est nécessaire d'infuser une éthique technique au sein de l'État, afin d'inciter les agents publics à réaliser un pas de côté, à prendre du recul sur leurs choix technologiques pour s'interroger sur les conséquences de long-terme des projets qu'ils conduisent.

4. **En s'appropriant l'exigence d'innovation dans son fonctionnement.** À la manière de toutes les grandes organisations, l'État est confronté à la question de sa propre transformation numérique. Elle suppose que pour mener ces grands chantiers numériques, l'État s'éloigne du mode projet pour adopter une posture d'innovation : plus d'agilité, de mise en réseau, de collaboration.

Sur cette base, le Conseil recommande d'édicter un cadre général de gouvernance ouverte, constitué de normes et de bonnes pratiques communes aux administrations et s'appliquant à tout projet numérique susceptible d'avoir un impact significatif sur son public. Il pourrait prévoir que les choix technologiques importants fassent l'objet d'une étude d'impact approfondie, expliquant les choix effectués. Afin que cette analyse tienne compte de l'état technologique, l'instruction devrait être menée de la manière la plus ouverte possible, associant chacun des ministères concernés, les institutions de référence, les experts et les acteurs du monde académique.

L'objectif serait de fixer de manière transparente et de réévaluer régulièrement des principes directeurs. De ce fait, le cadre général devrait idéalement être opposable par tous, dans les plus brefs délais. Toutefois, une première étape à court terme pourrait consister à définir et mettre en place des règles non-obligatoires (*soft law*). Dans le cas présent, l'existence de telles règles aurait pu par exemple fournir des arguments supplémentaires au Conseil d'État et à la CNIL pour appeler le Gouvernement à une véritable étude d'impact et à l'organisation d'un débat parlementaire.

[50] http://www.elysee.fr/videos/discours-du-president-a-l-occasion-de-l-ouverture-du-pgo/

Annexes

Annexe 1
Liste des personnes auditionnées

Association Aeternam
- Damien Maitrot, Chief Technology Officer & Founder
- David Robert, Président & fondateur

Benjamin André, CEO et Président de Cozy Cloud

Alexandre Archambault, Avocat

Xavier Brunetière, Directeur de l'Agence nationale des titres sécurisés (ANTS)

Chaire Valeurs et Politiques des Informations Personnelles (CVPIP) - Institut Mines-Télécom
- Pierre-Antoine Chardel, Professeur de philosophie sociale et d'éthique à Télécom Ecole de Management, co-fondateur de la Chaire ;
- Armen Khatchatourov, Ingénieur de recherche - Télécom Ecole de Management

Chercheurs de l'École nationale supérieure d'ingénieurs
- Rima Belguechi,
- Vincent Alimi,
- Estelle Cherrier,
- Patrick Lacharme,
- Christophe Rosenberger

Orr Dunkelman, Associate professor at the Computer Science Department of the University of Haifa

Institut national de recherche en informatique et en automatique - Inria
- Claude Castelluccia, Directeur de Recherche, Responsable de l'équipe-projet Privatics
- Gérard Le Lann, Directeur de recherche émérite
- Philippe Pucheral, Responsable de l'équipe-projet SMIS

Nathalie Launay, Consultante indépendante

Ministère de l'Intérieur :
- Arnaud Mazier, Adjoint au chef de la mission de gouvernance ministérielle des systèmes d'information et de communication (MGM SIC)
- Jean-Luc Nevache, Directeur de cabinet du ministre Bruno Le Roux
- Vincent Niebel, DSI adjoint

- Patrick Strzoda, Directeur de cabinet du ministre Bernard Cazeneuve

OCTO technologies

- Édouard Devouge, Senior Consultant, Cloud Architect & DevOps Evangelist,
- Benoît Lafontaine, One Technical Leader
- Maxime Uszpolewicz, Manager Service Public

Annexe 2
Synthèse des alternatives techniques

Plusieurs contributions à la consultation publique menée par le Conseil pointent l'existence d'alternatives techniques plus protectrices que la constitution d'une base de données biométriques centralisée. Ce document présente les pistes évoquées lors des auditions menées par le CNNum. Cette synthèse ne se veut pas exhaustive et le Conseil n'entend pas prendre parti en faveur de l'une ou de l'autre. Son seul but est de montrer que la recherche — publique et privée — est aujourd'hui très active sur ces sujets d'identité, de biométrie et de sécurisation.

1. Considérations générales

La phase d'authentification est souvent considérée comme le lien le plus faible dans la sécurité des transactions électroniques. Actuellement, l'authentification par identifiant/mot de passe reste la méthode d'authentification la plus utilisée même si la moins sécurisée, mais les solutions biométriques se développent (lecteurs biométriques sur les smartphones, systèmes d'authentification aux frontières comme PARAFE…)

L'utilisation de la biométrie est prometteuse pour plusieurs raisons :

- le fort lien entre l'utilisateur et son identité (pas de perte de mot de passe) ;
- la facilité d'usage (les capteurs sont faciles à déployer) ;
- les empreintes biométriques, ainsi que certaines caractéristiques faciales (écartement des yeux, arêtes du nez, commissures des lèvres…) sont très discriminantes (elles sont, dans la plupart des cas, propres et uniques à chaque utilisateur).

  Cela n'exclut pas de forts risques liés à la protection des données biométriques :
- le caractère fortement discriminant permet le suivi et la traçabilité de l'activité des utilisateurs ;
- ces données donnent des informations sensibles sur l'utilisateur (origine ethnique, santé, etc.) ;
- les données biométriques ne sont pas secrètes ;
- les données biométriques ne sont pas révocables ;
- il reste des problèmes de faux-positifs.

Constituer une base de données biométriques est donc dangereux vis-à-vis de la protection de la vie privée, même si cette base est gérée par une partie de confiance. La CNIL a ainsi recommandé de procéder à l'enregistrement des seuls gabarits et non de la photographie des empreintes digitales, même si certains travaux récents s'intéressant à retrouver les empreintes à partir de gabarits pourraient remettre en cause cette protection. Scinder et distribuer la base en plusieurs sous-parties permet

de renforcer la protection du système, mais le calcul d'appartenance à la base devient rapidement trop complexe. De plus, si une partie significative des sous-parties est récupérée, on peut reconstruire la base complète. Il est donc nécessaire de rechercher des méthodes plus génériques pour protéger les données biométriques.

2. Architectures sans base de données centralisée

2.1. Solutions décentralisées

Procéder à l'authentification biométrique d'un passeport (contrôle aux frontières par exemple) ne nécessite pas de constituer une base de données biométrique de la population. Une comparaison des empreintes en dehors du passeport est effectuée entre des données biométriques stockées dans le document[51] et un gabarit extrait d'une nouvelle capture saisie au moment du contrôle. La comparaison des données stockées avec les nouvelles données saisies est alors effectuée sur un système sous le contrôle de l'autorité régalienne du pays[52]. Un contrôle à distance de la validité du passeport peut par ailleurs être fait, comme c'est le cas pour les cartes de paiement. Il n'implique pas de communiquer le secret (code) sur le réseau, ni de le conserver de manière centralisée.

En lieu et place de TES, la CNIL préconise, quant à elle, de faire évoluer la carte d'identité pour y inclure un support cryptographique contenant les données biométriques du détenteur avec une solution améliorée par rapport à celle utilisée pour les passeports : une solution « *match on card* », grâce à laquelle les données ne sont jamais extraites de la puce ou du document, propriété de l'utilisateur et sous son contrôle exclusif (voir le paragraphe 2.2 - Renforcer la sécurité grâce au "match on document").

S'il est vrai que cette solution nécessite un investissement potentiellement coûteux, elle serait aussi fortement créatrice de valeur : selon certains contributeurs, une telle solution pourrait en effet fournir une base essentielle en vue de la construction d'un schéma d'identification numérique pour accéder aux services en ligne (publics et privés). L'identité numérique est d'ailleurs l'un des 5 domaines de l'appel à projets thématique « Sécurité des personnes et des biens, des infrastructures et des réseaux » lancé par la BPI dans le cadre de l'action « Projets industriels d'avenir » (PIAVE) du Programme d'investissements d'avenir.

L'ANTS est en train de développer la solution Alicem pour utiliser les passeports biométriques avec les mobiles des utilisateurs en utilisant uniquement la reconnaissance faciale pour vérifier que la personne demandeuse est bien le détenteur du passeport. Il est d'ailleurs mentionné dans le rapport du sénat « *l'application*

[51] Ces données sont extraites selon le protocole Extended Access Control (EAC), qui permet de vérifier l'autorisation d'un pays tiers à y accéder. Ceci nécessite la mise en place d'échanges bilatéraux et/ou le bon fonctionnement du "Single Point of Contact" (SPOC)

[52] Cette comparaison peut être effectuée localement, ou avec un service centralisé distant (source : http://frontex.europa.eu/assets/Publications/Research/Best_Practice_Technical_Guidelines_for_Automated_Border_Control_Systems.pdf, paragraphe 5.2.2.1)

ALICEM ne générerait aucune base de données. À terme, ALICEM pourrait également fonctionner à partir des titres de séjour ou d'une carte d'identité électronique. »

L'approche de cloud personnel avec des données certifiées se présente également comme une alternative à la centralisation : à titre d'exemple, des chercheurs français développent ainsi actuellement un serveur personnel sécurisé permettant à l'individu d'exercer un contrôle sur ses données personnelles tout en préservant durabilité, disponibilité et partage[53].

2.2. Renforcer la sécurité grâce au "match on document"

La puce des passeports ne permettant pas de faire des calculs du type *Match on Card* (calcul de comparaison fait par la puce du document qui stocke les données) que ce soit pour des empreintes ou pour de la reconnaissance faciale, la comparaison décrite dans le paragraphe précédent entre les données stockées dans le document et les données extraites d'une nouvelle capture est effectuée sous le contrôle de l'autorité régalienne du pays visité sur la borne de contrôle, en local ou sur un serveur distant.

Il est toutefois possible d'augmenter la sécurité en utilisant :

- soit du « Match on Card » comme décrit par la CNIL dans sa communication sur TES ;
- soit un concept plus général de "match on document" (calcul de comparaison par une application exécutée sur un dispositif sous le contrôle de l'utilisateur[54] avec des données stockées sur un support physique propriété et sous le contrôle exclusif de l'utilisateur.
  Ces procédés satisfont le besoin de contrôle exclusif de ses données biométriques (faciales ou empreintes) répondant ainsi au besoin de protection des données personnelles retranscrit par la CNIL pour le droit français mais aussi pour le futur RGDP, ainsi qu'au besoin eIDAS niveau 2 (substantiel).

2.3. Cachet électronique visible

Un objectif affiché par le ministre de l'Intérieur est de faire face au besoin de sécurisation de l'identité du citoyen et de lutter contre l'usurpation de l'identité et le *look alike*[55]. Mais pour lutter efficacement contre de telles fraudes documentaires, une première étape devrait être de protéger les documents permettant de justifier d'une identité (appelés *breeder documents* : justificatif de domicile, acte de naissance, etc.)

Pour atteindre cet objectif, l'ANTS a déjà mis en place une spécification le 2D DOC (https://ants.gouv.fr/Les-solutions/2D-Doc). Cette spécification repose sur le principe de vérification explicite d'un cachet électronique visible qui est un nouveau standard en cours d'élaboration au sein de l'Afnor et qui intègre le cas d'usage régalien 2D

[53] http://www.lemonde.fr/acces-restreint/sciences/article/2016/11/28/62720c29a55460323461839b414747e3_5039719_1650684.html
[54] par exemple l'environnement TEE du mobile device, voir mieux via une puce, telle que sa SIM consumer centric ou la SDcard de son mobile
[55] Cette méthode consiste à usurper l'identité d'une personne en l'imitant physiquement

DOC ANTS. Il s'agit d'une solution à base d'un code à barres sécurisé et verrouillé par une signature électronique qui garantit l'intégrité, l'origine et la validité des données.

Ce mode ne permet toutefois pas de vérifier que le document appartient bien à la personne qui prétend être son détenteur. Ce standard pourrait donc utilement évoluer en incorporant une vérification de données biométriques. Pour cela, il faut recourir à de la vérification implicite dont le principe est de comparer des données biométriques capturées avec des données stockées de façon sécurisée dans le code-barre. La vérification est alors effectuée non pas avec les données stockées en brut dans le code-barre, mais après un calcul intermédiaire avec des données auxiliaires dont le résultat est ensuite comparé avec des données signées et cryptées. Ceci permet ainsi d'éviter tout stockage de données biométriques brutes ou en clair, tout en permettant une vérification de l'authentification biométrique.

2.4. Blockchain

Suite à une première étape d'authentification locale comme décrite dans les paragraphes précédents, l'usage d'un ISAEN[56] en lieu et place d'un ou de plusieurs certificats de validité de la donnée (avec une durée de vie limitée, et accessibles ou stockés sur un support cryptographique) pourrait être approprié tout en garantissant le parfait respect des principes de la GDPR que ce soit pour des services publics et privés.

Cette solution blockchain ISAEN ne stocke en effet par principe aucune donnée privée. La blockchain est uniquement utilisée comme un registre décentralisé des actes de notarisation (de consentement, de validation des identités, etc.). Les certificats délivrés par les tiers de confiance sont mis à jour en temps réel, permettant de satisfaire à la fois les droits des citoyens (consentement explicite, droit de modification ou de suppression…), les devoirs des fournisseurs d'identité, des fournisseurs de service et des fournisseurs de solutions de traitement des données (portabilité, auditabilité), mais aussi la fiabilité des identités et la valeur probante des transactions.

3. Protéger les données biométriques

Au-delà des solutions décrites précédemment, le fait que l'État dispose d'une base de données biométriques des citoyens permet un contrôle plus efficace dans les cas où la personne souhaitant refaire son document d'identité ne dispose pas d'un autre document permettant une authentification biométrique[57]. L'objectif de cette partie est de s'intéresser aux architectures de base de données biométriques qui, même dans le cas où la base serait diffusée, révèlent le moins d'information personnelle possible sur les utilisateurs.

[56] Identifiant anonymisé d'une blockchain pour une "self sovereign identity" tel qu'en cours d'élaboration dans un groupe de travail de normalisation européen CEN workshop84 : http://www.cen.eu/work/areas/ICT/Pages/WS-IS%C3%86N.aspx

[57] Deux cas peuvent notamment apparaître : lors d'une première demande, ou bien lors de la réédition d'une carte perdue ou volée.

3.1. Base de données biométriques anonymisées

Disposer d'une base de données biométriques anonymisées permet de vérifier l'unicité de la demande, c'est à dire si la personne souhaitant refaire son document d'identité a déjà fait une demande par le passé.

Afin de permettre la réédition de cartes perdues ou volées, il peut toutefois s'avérer nécessaire d'inclure dans la base des informations non-anonymes. C'est le cas pour la base TES, qui permet à partir de données d'état civil de retrouver les informations biométriques. Comme expliqué précédemment, une telle base est très sensible et doit donc être sécurisée. En outre, il ne suffit pas de protéger le lien entre informations nominatives et informations biométriques (même un lien faible est un lien qui se casse).

3.2. Biométrie chiffrée

Une première possibilité est de recourir à de la biométrie chiffrée, c'est-à-dire de chiffrer les informations biométriques contenues dans la base de telle sorte que le déchiffrement n'est pas nécessaire pour procéder à une authentification. En cryptographie, ce type de chiffrement est appelé "chiffrement homomorphe".

Un tel système est complexe à construire car il faut conserver une *intra-user variability* (2 photos différentes de la même empreinte doivent être reconnues comme appartenant à la même personne). Il existe un champ de recherche important sur la création de *Template protection scheme* permettant de contourner ce problème.

3.3. Biométrie révocable

Afin de se protéger contre une éventuelle fuite de données, une autre solution consiste à utiliser des données biométriques révocables. Le principe est de ne pas stocker dans la base de données les informations biométriques brutes, mais d'utiliser des données biométriques transformées par une fonction non-inversible. Personne ne peut alors retrouver les données originelles, et, si le système est compromis, il suffit de changer de fonction transformatrice.

Un exemple de données biométriques révocables est le BioHashing qui combine les données biométriques à une sorte de mot de passe appelé *seed* (nombre pseudo-aléatoire que l'utilisateur doit stocker).

3.4. Stockage sous forme de réseau de neurones

Une autre piste à explorer est celle du stockage de données biométriques via un réseau de neurones. Ce type d'algorithme statistique s'inspire du fonctionnement des neurones biologiques pour modéliser un problème. Or, contrairement aux méthodes traditionnelles de résolution informatique qui nécessitent la construction d'un

programme pas à pas, l'une des caractéristiques des réseaux de neurones artificiels est de fonctionner par apprentissage inductif, en modélisant le problème à partir d'observations.

De cette manière, il pourrait ainsi être possible de construire un algorithme pouvant répondre à la question "ce nom et cette empreinte vont-ils ensemble ?" sans qu'il n'y ait besoin de base de stockage de chaque empreinte.

3.5. Gestion des clés de chiffrement

D'autres contributeurs ont proposé la mise en place d'une architecture à clé multiple (par exemple de type partage de clé secrète de Shamir). Cette solution consiste à renforcer la confiance dans la bonne utilisation du système en distribuant des responsabilités à un ensemble d'acteurs (appelés *blinding entities*) : en pratique, il s'agirait par exemple de distribuer une partie des clés aux services de police, une partie à la CNIL, une partie à la justice et une partie à l'utilisateur en opt-in[58].

L'objectif est de s'assurer que les requêtes sensibles dans la base soient doublement protégées (légalement et techniquement) :

- L'accès à la base est protégé par une clé, et chaque *blinding entity* ne dispose que d'une partie de cette clé ;
- Pour effectuer une requête sur la base (ajout d'une nouvelle personne, authentification, etc.), il faut disposer de la clé en entier et donc convaincre un nombre minimal de *blinding entity*.
- Les informations permettant de remonter à l'identité des citoyens ne sont révélées qu'en cas de duplicata : là aussi il faut donc disposer de la clé en entier et donc convaincre un nombre minimal de *blinding entity*.
  D'autres solutions peuvent être envisagées, dans lesquelles le support serait porteur d'une information cryptographique qui ne nécessiterait pas le recours à des dispositifs technologiquement coûteux. Par exemple, le dos du titre d'identité peut être utilisé pour stocker un motif binaire imprimé (à la façon d'un « QR-code » de grande taille) constituant la clé de déchiffrement de l'information stockée en base centrale. Cette clé pourrait alors être l'unique moyen de débloquer les données stockées en base, l'ensemble constituant ainsi un dispositif biométrique à la main de l'usager, selon les préconisations nouvelles de la CNIL.

3.6. Construire un système auditable et traçable

Quelles que soient les garanties prévues, un détournement de finalité n'est pas totalement à exclure. L'expérience montre que la plupart des vulnérabilités sont liées à des contrôles des usages internes : le système doit donc être auditable et traçable.

Pour ce faire, chaque consultation doit être associée à un numéro d'identifiant qui puisse être tracé, comme pour les interceptions administratives. Ceci permettrait de voir si des usages détournés sont ponctuels et isolés ou répétés et d'identifier les

[58] Une solution opt-in correspondrait davantage au besoin de sécurité sollicité par les citoyens qu'une solution opt out

détournements de finalités (« réquisitions de confort »). Une telle disposition est prévue à l'article 9 du décret : « *Les consultations, créations, modifications ou suppressions de données font l'objet d'un enregistrement comprenant l'identification de leur auteur ainsi que la date, l'heure et la nature de l'opération. Ces informations sont conservées pendant cinq ans à compter de l'enregistrement* ».

Pour ce faire, l'usage et le déploiement de la carte agent RGS** prescrit par l'ANSSI doit être renforcé, non seulement pour les agents d'état de ministères centralisés mais aussi pour les agents et élus des organismes territoriaux et locaux. En effet, s'il s'avérait que l'enrôlement des données biométriques et la délivrance des titres régaliens continuaient d'être délégués aux communes, l'usage d'une carte d'agent ne peut être que requis. Il pourrait également être pertinent que la carte d'agent soit un moyen d'authentification utilisé pour l'usage de "France connect agent" en lieu et place du login/mot de passe, non seulement pour des raisons de sécurité nationale sur l'ensemble de notre territoire, mais aussi pour le respect de la vie privée et éviter les risques de détournements.

Annexe 3
Exemple d'États ayant recours à la carte d'identité biométrique

	Collecte d'empreinte	Base de données	Date de lancement
Allemagne	Facultative	Non	2010
Espagne	Obligatoire	Oui	2006
Italie	Obligatoire	Non	-
Royaume Uni	Non	Non	-
Belgique	Non	Non	2005
Pays-Bas	Obligatoire	Oui	2014
Portugal	Obligatoire	Non	2007
Suède	Non	Non	-
Finlande	Non	Non	-
Lituanie	Oui	Oui	2009

Source : Rapport fait au nom de la commission des lois du Sénat par MM. les Sénateurs François BONHOMME et Jean-Yves LECONTE : https://www.senat.fr/rap/r15-788/r15-7881.pdf

www.cnnumerique.fr/fichier-tes-avis

Conseil national du numérique
Bâtiment Atrium
5 place des Vins-de-France
75573 Paris Cedex 12
info@cnnumerique.fr - @CNNum
01 53 44 21 27

CONTACT PRESSE
Yann Bonnet, Secrétaire Général
presse@cnnumerique.fr
01 53 44 21 27