La création du fichier biométrique TES : la convergence de logiques au service du contrôle

François Pellegrini* André Vitalis†

Le décret du 28 octobre 2016 [1] qui crée le fichier TES (« Titres électroniques sécurisés ») centralisant des données biométriques sur la population française, motive cette création par des arguments purement gestionnaires. Il s'agit selon ses promoteurs de moderniser et de mieux sécuriser la délivrance des passeports et des cartes d'identité. Cet argumentaire administratif modernisateur masque cependant d'autres logiques qui ont toujours œuvré en faveur d'un recours aux techniques biométriques dans l'identification des individus : une logique politique de surveillance des populations favorable à la centralisation de ce type de données, une logique économique qui entend profiter du développement d'un nouveau marché, ainsi qu'une logique technicienne dont la motivation principale est de faire advenir ce qui est possible. C'est au confluent de ces logiques que se situe le fichier TES.

La centralisation de données extrêmement sensibles telles que les photographies d'identité et les empreintes digitales, à l'échelle de la population de tout un pays, comporte à l'évidence des dangers pour les droits et les libertés de l'individu. Le plus étonnant est de constater que ces dangers manifestes ont été délibérément ignorés. Depuis le vote d'une loi protectrice « Informatique et Libertés » en 1978, les garanties données aux citoyens face au traitement informatisé de leurs données ont été régulièrement amoindries, en particulier dans la sphère publique. Le décret créant le fichier TES marque le terme d'une évolution où une nouvelle gouvernance, sous prétexte d'efficacité, ne s'embarrasse plus de la question des libertés.

Une logique administrative de rationalisation

Jacques Ellul a analysé nos sociétés contemporaines comme des sociétés techniciennes qui privilégient, avant toute chose, la recherche d'efficacité [2]. En promouvant les technologies de l'information et de la communication, l'administration publique sert cette logique technicienne sans s'interroger sur les conséquences sociales ni sur les éventuels dégâts pour les libertés et les droits individuels, des modernisations qu'elle propose et réalise. Un expert en science administrative constate ainsi que la rationalité posée en termes de droit est tout à fait secondaire par rapport à la rationalité technique et économique que sert prioritairement l'administration moderne, qui y trouve la principale légitimation sociale de son action [3]. Alors que le premier type de rationalité fait de l'égalité et de la liberté ses fins ultimes, le second est préoccupé d'optimisation des ressources, de compétitivité commerciale, d'efficacité organisationnelle. En toutes occasions, il s'appuie sur une logique qui aborde sous le même angle tous les problèmes et tend à reléguer au second plan le respect des valeurs libérales et démocratiques.

Au nom d'un progrès dont ils sont convaincus d'être les serviteurs, des experts, sans qu'aucune demande explicite leur soit adressée, vont rechercher et proposer les solutions techniques les plus puissantes et novatrices. Comme le montre l'exemple des innovations de la statistique hollandaise pendant la dernière Guerre mondiale, cette logique technicienne peut conduire à d'énormes catastrophes dans les périodes de crise. Après la capitulation de la Hollande en 1940, un inspecteur des registres de la population, qui n'était pourtant pas nazi, mit son expertise et la passion de son art au service d'une meilleure identification des individus et particulièrement des individus juifs. Après avoir créé une carte d'identité infalsifiable, véritable chef d'œuvre de documentation, il mit au point un répertoire démographique général puis un répertoire alphabétique spécial des individus juifs, en recourant à la puissance de la mécanographie. Ces prouesses techniques servirent les responsables nazis dans leur politique d'extermination et conduisirent à la mort 73 % de la population juive vivant aux Pays-Bas [4].

Au début des années 1970, l'informatisation des fichiers de personnes est considérée comme une opération de modernisation technique nécessaire et bénéfique. Aucune limite n'est encore fixée aux savoirs-faire des informaticiens et les données personnelles les plus sensibles sont stockées et traitées par des moyens automatisés. Des experts en marge de l'administration traditionnelle vont concevoir un système SAFARI (« Système automatisé pour les fichiers administratifs et le répertoire des individus ») d'interconnexion des différents fichiers, en utilisant comme clé d'identification

*Professeur d'informatique, Université de Bordeaux, LaBRI & INRIA Bordeaux Sud-Ouest, 351 cours de la Libération, 33405 Talence, France. francois.pellegrini@labri.fr

†Professeur émérite de sciences de l'information et de la communication, Université Bordeaux Montaigne. andre.vitalis@msha.fr

1. Décret n° 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033318345 .

2. ELLUL, J., *La technique ou l'enjeu du siècle*, Armand Colin, Paris, 1954 ; *Le système technicien*, Calmann-Lévy, Paris, 1977 ; *Le bluff technologique*, Hachette, Paris, 1988.

3. D'ARCY, F., « Une idéologie en déclin : le droit », revue Actes, n° 4, 1974.

4. BLACK, E., *IBM et l'holocauste*, Robert Laffont, Paris, pp. 350–360, 2001.

un répertoire des individus tenu par l'INSEE. Cette opération, menée en l'absence de tout texte législatif et réglementaire, semble s'imposer par son seul caractère novateur [5]. Cependant, compte tenu des bouleversements considérables apportés dans la gestion des données personnelles, ce système va bientôt faire prendre conscience des menaces que l'informatisation fait peser sur les libertés individuelles. Il sera à l'origine du vote, en 1978, d'une loi « Informatique et Libertés » qui crée la Commission nationale de l'informatique et des libertés (CNIL) et donne de nouveaux droits aux personnes fichées.

La création du fichier TES participe de la même logique technicienne, que les responsables administratifs entendent mettre au service d'une meilleure productivité. Ce projet a été proposé par la Direction de la modernisation de l'action territoriale (DMAT) du ministère de l'Intérieur dans le cadre du programme PPNG (« Plan préfectures nouvelle génération ») dont le principal objectif est une rationalisation de l'action administrative visant à économiser des emplois. Le journaliste Jean-Marc Manach a minutieusement retracé les différentes étapes de cette opération [6]. Dans une annexe d'un projet de loi de finances, datée d'octobre 2015, il est estimé que la réduction des formalités et démarches accomplies aux guichets des préfectures doit permettre de supprimer 1 300 emplois. À cette même date, il est envisagé, toujours dans le cadre du PPNG, de regrouper dans le fichier TES, originellement mis en place pour les passeports biométriques (et que nous appellerons « TES-1 », pour le distinguer de son extension « TES-2 »), les données relatives à l'instruction et à la validation de la carte nationale d'identité. En novembre 2015, ce regroupement est validé, l'instruction des cartes d'identité cessant d'être effectuée à partir d'un Fichier national de gestion (FNG) jugé obsolète. Les empreintes digitales des titulaires, qui étaient auparavant conservées en préfecture sur des supports cartonnés, seront à l'avenir stockées nativement dans la base centrale TES-2. En décembre 2015, le programme PPNG est présenté en Conseil des ministres et le Conseil d'État est saisi pour avis. Dans les premiers mois de 2016, est élaborée une carte des 47 futures plateformes d'instruction des demandes et sont organisés des séminaires de formation des responsables et des agents. Les préfets sont chargés de l'installation de bornes biométriques dans un certain nombre de mairies et, après une expérimentation, il est prévu que le nouveau système de délivrance des cartes sera opérationnel dans tout le pays fin mars 2017. La suggestion du Conseil d'État du vote d'une loi n'a pas été retenue et, sollicitée le 20 juillet 2016, la CNIL rend son avis le 29 septembre, lorsque tout a déjà été défini et adopté, aussi bien la conception du nouveau système d'information que ses modalités d'application.

L'alliance des logiques politique et économique

La création du fichier TES-2, au delà des motifs gestionnaires à partir desquels elle est présentée et justifiée, comble d'autres attentes de nature politique et économique. Cette convergence de logiques gestionnaire, politique et économique n'est certainement pas étrangère à la réussite d'une opération d'une telle ampleur.

Une logique politique de surveillance n'est pas totalement absente du décret de création de TES-2, qui prévoit que de nombreux éléments du fichier seront partagés par les services de renseignement dans le cadre de la lutte contre le terrorisme. De manière plus significative, on peut constater que, depuis plus de trois décennies, le pouvoir politique a cherché à créer un fichier biométrique de toute la population. L'alternance politique et les réserves de la CNIL ont empêché cette création à l'occasion de projets d'informatisation de la carte d'identité en 1980 et en 1986. En 2005, un autre projet INES (« Identification nationale électronique sécurisée »), articulé autour de deux fichiers biométriques centralisés, est abandonné à la suite d'un débat organisé par le Forum des droits sur l'Internet. Une loi de 2012 sur la protection de l'identité semble enfin parvenir à l'objectif visé avant que le Conseil constitutionnel n'intervienne pour annuler la disposition créant un fichier biométrique de toute la population qui, selon lui, porte une atteinte au droit à la vie privée qui n'est pas proportionnée à la finalité déclarée.

Dans un contexte de mondialisation et de mobilité croissante des populations, les techniques biométriques présentent des avantages incontestables en matière d'identification [7]. Fondées sur des paramètres inchangeables et objectivés, n'ayant nul besoin d'une médiation sociale [8], elles facilitent l'authentification de l'identité et permettent de connecter entre eux les fichiers établis sur la même personne. On comprend dans ces conditions, qu'elles soient devenues le sésame d'un système d'identification au niveau mondial, particulièrement en matière de criminalité et de contrôle des flux migratoires. Après les attentats du 11 septembre 2001, au nom de la lutte contre un terrorisme qui se joue des frontières, les États-Unis vont promouvoir et imposer à leurs alliés leurs conceptions et leurs pratiques dans le contrôle des identités et des mouvements. Ils considèrent notamment que, couplée avec l'informatique, la biométrie constitue un identifiant sûr et universel. Après qu'ils ont exigé un passeport biométrique pour l'entrée sur leur territoire, l'Union européenne, dans un règlement de 2004, adopte elle aussi ce type de passeport. C'est en application de ce règlement que la France, en 2008, crée un passeport biométrique dont les données seront enregistrées au sein du fichier national TES-1.

Les entreprises françaises sont particulièrement présentes sur le marché de l'identification des personnes par des moyens électroniques, qui offre des possibilités considérables de développement. À l'époque des machines mécanogra-

5. VITALIS, A., *Informatique, pouvoir et libertés*, Economica, Paris, pp. 75–90, 1988.

6. MANACH, J.-M., « Comment (et pourquoi) Bernard Cazeneuve a décidé de ficher 60 millions de Français », *Libération*, 7 novembre 2016.

7. MATTELART, A. et VITALIS, A., *Le profilage des populations, Du livret ouvrier au cybercontrôle*, La Découverte, Paris, 2014.

8. PELLEGRINI, F. et VITALIS, A., « Identités biométrisées et contrôle social », rapport de recherche Inria n° RR-9046, mars 2017, https://hal.inria.fr/hal-01492431v2 .

phiques, un monopole sur ce type de marché a permis à IBM d'établir les bases de sa réussite et de son expansion mondiale. On comprend, dans ces conditions, l'intérêt que portent les entreprises aux nouvelles techniques d'identification. Cet intérêt est exprimé très clairement en 2004, dans un ouvrage du Groupement des industries de l'interconnexion, des composants et des sous-ensembles électroniques (GIXEL) qui voudrait le faire mieux partager : « La sécurité est très souvent vécue dans nos sociétés démocratiques comme une atteinte aux libertés individuelles. Il faut donc faire accepter par la population les technologies utilisées et parmi celles-ci la biométrie, la vidéosurveillance et les contrôles... Pour faire accepter les technologies de surveillance et de contrôle, il faudra probablement recourir à la persuasion et à la réglementation en démontrant l'apport de ces technologies à la sérénité des populations et en minimisant la gêne occasionnée » [9]. C'est ainsi que, pour familiariser les populations à l'usage de leurs empreintes biométriques, se sont peu à peu développés des usages non régaliens, tels que la mise en place de bornes électroniques dans les établissements scolaires et leurs cantines, l'authentification de l'usager d'un ordiphone par ses empreintes digitales ou celle des clients de banques par leur empreinte vocale.

Des libertés et des droits délibérément ignorés

L'enchaînement des événements à l'origine de la création de TES-2 ne peut que conduire à s'interroger sur la volonté de ses promoteurs d'échapper à tout contrôle de proportionnalité effectif en termes de libertés et de droits des individus. Cet évitement se matérialise à de nombreuses reprises : par le refus d'emprunter la voie parlementaire, pourtant conseillée tant par le Conseil d'État que par la CNIL ; par la saisine de cette dernière en bout de chaîne et après qu'un avis consultatif préalable a été demandé au Conseil d'État, à l'inverse de l'ordre habituel des saisines ; par le lotissement du marché de réalisation technique conduisant à ce qu'aucun des lots ne dépasse les 10 millions d'euros, somme au dessus de laquelle tout marché informatique doit être expertisé par la Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC).

Bien que le décret TES-2 ait fait l'objet d'un avis extrêmement réservé de la CNIL, le Conseil d'État, implicitement lié par son avis consultatif préalable rendu dans l'ignorance des arguments de celle-ci, valida le système TES-2. Il motiva cette décision par le fait que la seule finalité annoncée du fichier était l'authentification et que le ministère de l'Intérieur garantissait que des barrières techniques empêcheraient l'usage du fichier pour l'identification, en ne permettant pas de remonter d'une empreinte biométrique aux informations nominatives. Ces arguments sont inopérants. D'une part, les barrières techniques alléguées par le ministère de l'Intérieur peuvent être facilement contournées, car il est facile de reconstruire l'information de liaison entre les données biométriques et les identités [10] ; on peut s'en convaincre par le fait que réaliser une identification revient à effectuer une tentative d'authentification avec chacune des personnes de la base centralisée, avec l'espoir que l'une d'entre elles réussisse. D'autre part, le décret TES-2 mentionne explicitement la possibilité de réquisitions judiciaires, sans que la nature de celles-ci soit explicitée. À peine le ministre de l'Intérieur, lors de son audition devant la Commission des lois le 9 novembre 2016, a-t-il évoqué que le fichier TES-2 permettrait d'« extraire le dossier de demande du titre, y compris des données biométriques [...] d'auteurs d'attentats ou de catastrophes [...] », actant d'une finalité sécuritaire implicite, liée au souhait d'accélérer le travail des forces de police. Dans quelle mesure ces réquisitions peuvent-elles être étendues à un ensemble de suspects ? Puisqu'il est techniquement possible d'effectuer des identifications, un juge ne pourrait-il requérir de comparer les données biométriques du fichier avec celles issues d'une scène de crime ? Le décret TES-2 dispose également que les services de renseignement auront accès au fichier. Or, personne ne serait en mesure de contrôler l'usage par ces services d'une copie qu'ils en feraient pour leur propre usage. Toutes ces failles ont été confirmées, à mots à peine couverts, par l'audit du système TES-2 réalisé conjointement par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et la DINSIC [11], à la demande du gouvernement, en réponse à l'émoi suscité par la création du traitement TES-2 et aux nombreuses critiques dont il a fait l'objet.

Les risques de détournement de finalité par l'État d'un fichier biométrique centralisé ne sont malheureusement pas théoriques. Tel est le cas du FNAEG, fichier de police des empreintes génétiques initialement censé aider à l'identification des criminels sexuels récidivistes, et récemment transformé en fichier d'identification de la population. Ce détournement de finalité est le résultat de deux évolutions conjointes. D'une part, les « recherches en parentèle », qui étaient effectuées sur réquisitions judiciaires de façon sporadique et illégale depuis 2011, et ont été légalisées en juin 2016 [12], permettent de déterminer si une trace biologique correspond non plus seulement à une personne fichée, mais aussi à un parent d'une personne fichée. D'autre part, l'extension de la prise d'empreintes génétiques à une fraction toujours plus grande de la population, telle que par exemple les responsables d'atteintes aux biens, a mécaniquement étendu la portée des recherches, de sorte que toute personne puisse un jour être retrouvée à partir des empreintes de sa parentèle.

9. GIXEL (Groupement des industries de l'interconnexion, des composants et des sous-ensembles électroniques), Livre bleu, juillet 2004.
10. PELLEGRINI, F., « La biométrie des honnêtes gens, reloaded », blog personnel, novembre 2016, http://www.pellegrini.cc/2016/11/la-biometrie-des-honnetes-gens-reloaded/ .
11. POUPARD, G. et VERDIER, H., « Audit du système "Titres électroniques sécurisés" », janvier 2017, http://mobile.interieur.gouv.fr/content/download/100011/786238/file/rapport-commun-public-tes-13-01-20172.pdf .
12. Article 706-56-1-1 du code de procédure pénale, créé par l'article 80 de la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006071154&idArticle=LEGIARTI000032642502&dateTexte=20170423

Les risques manifestes de détournement du fichier TES-2, mis en lumière par les différentes analyses techniques [13], ont été balayés par le gouvernement, qui a indiqué que les préconisations de fond du rapport conjoint ANSSI-DINSIC ne seraient mises en œuvre que pour les versions ultérieures du système. Cette minoration des risques découle d'un « postulat démocratique », parfois explicitement exprimé, selon lequel l'État ne serait pas en mesure de se retourner contre la population [14] ; postulat que l'Histoire a souvent démenti [15].

Les barrières juridiques étant aisément réversibles, seules des barrières techniques peuvent offrir une protection effective contre les détournements de finalité des systèmes informatiques. La principale consiste en la définition d'architectures rendant impossible ces détournements [16], la mise en œuvre d'une architecture alternative à la base centralisée constituant également l'une des préconisations les plus fortes du rapport conjoint ANSSI-DINSIC.

C'est avec une motivation similaire que la CNIL a récemment reconsidéré sa doctrine sur la biométrie, afin d'encadrer le déferlement des usages commerciaux et domestiques de celle-ci [17]. Le fondement de cette doctrine est de privilégier les architectures techniques dans lesquelles les usagers restent maîtres de leurs données biométriques, les architectures centralisées devant être restreintes à des cas spécifiques (tels que les fichiers de police).

Au vu des risques avérés des architectures centralisées, tant en termes immédiats de sécurité (des fuites importantes de données biométriques ont déjà eu lieu dans d'autres pays, tels les États-Unis et Israël) que de détournements de finalité à moyen terme, il conviendrait d'appliquer cette doctrine à l'ensemble des données biométriques traitées par l'État et les différents opérateurs publics (on peut penser aux photographies des usagers collectées pour la délivrance des titres), ce que la CNIL ne peut encadrer efficacement depuis que son avis n'est plus que consultatif.

Un type de gouvernance façonné par des logiques de contrôle

Le fichier TES, par son ampleur et les menaces qu'il fait peser sur les libertés et le droit à la vie privée des individus, met pleinement en lumière une évolution régressive pour la démocratie [18]. Dans les années 1970, le pouvoir politique était intervenu pour poser des limites à une logique administrative et technicienne liberticide et pour donner de nouveaux droits aux personnes fichées. Aujourd'hui, ce même pouvoir ignore de manière délibérée les menaces pour les libertés, se bornant à consentir, face aux critiques qui lui sont adressées, quelques petits aménagements. Ainsi le gouvernement a-t-il consenti à ce que les empreintes digitales des personnes qui en feraient la demande ne soient pas incluses dans le fichier TES-2, mais toujours conservées sur supports cartonnés. Or, ce dispositif est doublement pervers : outre que la préservation des libertés n'est pas une option, et que l'État devrait la garantir pour tous les citoyens sans leur laisser le choix d'y renoncer, l'absence des empreintes des personnes dans le fichier TES-2 (qui n'est effective que pour les personnes n'ayant pas de passeport qui les ferait figurer dans TES-1) crée en creux un « fichier des récalcitrants » propice à tous les mésusages.

Dans ce type de gouvernance, les droits du citoyen sont sacrifiés pour des motifs d'économie ou de recherche d'une meilleure satisfaction du consommateur du service, sans qu'aucune réflexion de fond ne soit menée sur l'architecture technique mise en œuvre. Il est vrai que la révolution numérique a bouleversé les valeurs et les références traditionnelles [19]. Dans un contexte numérique mondialisé dans lequel de puissants monopoles privés violent régulièrement les droits des individus, en les fichant et en les profilant comme bon leur semblent, le pouvoir régalien peut toujours avoir la tentation de s'affranchir de règles qu'il estime néfastes à l'efficacité de son action. Un amoindrissement des libertés peut toujours se justifier par une augmentation de productivité, une offre de service plus pertinente et surtout par une sécurité mieux assurée. En cela, le choix d'une architecture centralisée n'est pas nécessairement un choix par défaut, mais peut être interprété comme le souhait de pouvoir disposer du contenu de ces fichiers si la situation l'exige. Comme dans le cas de la surveillance de masse, l'État place ainsi l'ensemble de la population dans un rôle d'ennemi potentiel. Le juriste Alain Supiot considère que, dans le monde réticulaire et sans verticalité façonné par les techniques d'information et de communication, les droits de l'Homme sont mis à mal par des calculs d'utilité [20]. Ainsi la dignité humaine ou le respect de la vie privée sont aujourd'hui mis en balance avec d'autres intérêts malgré le caractère intangible de la loi.

13. CASTELLUCIA, C. et LE MÉTAYER, D., « Note d'analyse – Titres électroniques sécurisés : la centralisation des données biométriques est-elle vraiment inévitable? Analyse comparative de quelques architectures », rapport de recherche Inria, février 2017, https://hal.inria.fr/hal-01467902 .

14. MANACH, J.-M., « Le "fichier des gens honnêtes", ce révélateur d'un mal français », *Slate.fr*, 1er mars 2017, https://www.slate.fr/story/138356/saga-generalisation-fichier-des-gens-honnetes .

15. HAFFNER, S., *Histoire d'un allemand – Souvenirs (1914–1933)*, in coll. Babel, n° 653, Actes Sud, Arles, septembre 2004.

16. ANTIGNAC, T. et LE MÉTAYER, D., « Privacy by Design : From Technologies to Architectures », in *Privacy Technologies and Policy : Second Annual Privacy Forum*, Athènes, 20–21 mai 2014, Springer International Publishing, pp. 1–17, DOI 10.1007/978-3-319-06749-0 1 ; PELLEGRINI, F., « La biométrie des honnêtes gens », blog personnel, novembre 2016, http://www.pellegrini.cc/2016/11/la-biometrie-des-honnetes-gens/ .

17. CNIL, « Biométrie : un nouveau cadre pour le contrôle d'accès biométrique sur les lieux de travail », 27 septembre 2016, https://www.cnil.fr/fr/biometrie-un-nouveau-cadre-pour-le-controle-dacces-biometrique-sur-les-lieux-de-travail ; « Biométrie dans les smartphones des particuliers : comment la loi informatique et libertés s'applique-t-elle ? », 8 mars 2017, https://www.cnil.fr/fr/biometrie-dans-les-smartphones-loi-informatique-et-libertes-exemption-ou-autorisation .

18. DE BERNARD, F., L'homme post-numérique – Face à la société de surveillance générale, Ed. Yves Michel, Gap, 2016.

19. VITALIS, A., *L'incertaine révolution numérique*, ISTE, Londres, 2016.

20. SUPIOT, A., *La gouvernance par les nombres*, Fayard, Paris, 2015.

La CNIL fut instituée en 1978 pour veiller à ce que l'informatisation des fichiers respecte le droit des personnes ; dès 2004, le législateur décida qu'elle ne pourrait plus s'opposer aux traitements mis en œuvre par l'État, étant désormais seulement habilitée à rendre des avis consultatifs dont il n'est tenu aucun compte. Le contre-pouvoir qu'elle constituait a été délibérément neutralisé par une génération qui, volontiers oublieuse des leçons de l'Histoire, ne jure que par l'efficacité du fichage. Quarante ans après, la majorité des interconnexions prévues par SAFARI est déjà mise en œuvre.