Fichier TES : Le conseil d'Etat donne son feu vert au fichage biométrique de 67 millions de français.

Jean-Philippe Foegle

Édition électronique

URL : <http://journals.openedition.org/revdh/4879>

DOI : 10.4000/revdh.4879

ISSN : 2264-119X

Éditeur

Centre de recherches et d'études sur les droits fondamentaux

Référence électronique

Jean-Philippe Foegle, « Fichier TES : Le conseil d'Etat donne son feu vert au fichage biométrique de 67 millions de français. », *La Revue des droits de l'homme* [En ligne], Actualités Droits-Libertés, mis en ligne le 02 novembre 2018, consulté le 19 avril 2019. URL : <http://journals.openedition.org/revdh/4879> ; DOI : 10.4000/revdh.4879

Ce document a été généré automatiquement le 19 avril 2019.

Tous droits réservés

Fichier TES : Le conseil d'Etat donne son feu vert au fichage biométrique de 67 millions de français.

Jean-Philippe Foegle

- 1 Depuis les révélations d'Edward Snowden, les dispositifs de surveillance qualifiés – souvent abusivement – de dispositifs de surveillance dits “de masse” continuent paradoxalement à se multiplier, et ce à une vitesse de nature à faire pâlir d'envie ou de honte un lapin d'élevage.
- 2 . Au-delà de la diversité des mécanismes concourant à une telle surveillance des personnes physiques, ces dispositifs répondent à une logique opérative commune, qualifiée par Didier Bigo¹ de “grammaire du futur antérieur”, obéissant selon l'auteur à des matrices correspondant à quatre types distincts de programmes concourant à une surveillance dite “de masse”.
- 3 La première est celle de l'adjonction d'un “double numérique” à chaque personne à partir de ses traces numériques, ce qui correspond aux programmes que Margaret Hu² qualifie de programmes de type “Collect it all” qui visent à collecter un maximum de données pertinentes sur les individus. La seconde, liée à la première, a trait à la dépersonnalisation des données, afin de constituer des séries via des collectifs structurants celles-ci en fonction de critères jugés pertinents. La troisième, qui correspond aux programmes de type “Share it all” tels que le PNR font voyager ces données en les connectant à d'autres “doubles numériques” via l'interconnexion des bases de données pour regrouper, classer les individus en groupes supposés “à risque”. Enfin, l'usage des algorithmes – les programmes de type “Process it all” – permet de traiter les “doubles numériques” des individus ainsi classés et regroupés afin de calculer d'une manière – supposément – scientifique le risque que ceux-ci présentent pour la société.
- 4 Plus qu'une catégorie de surveillance à part entière, la surveillance “de masse” est donc avant tout un système constitué d'une constellation complexe de dispositifs techniques et juridiques, dont l'unité ne tient pas à un mode de fonctionnement unique et identifiable, mais à l'imaginaire technico-politique qui le sous-tend : celui d'une logique

précautionnaire poussée à ses extrémités et qui, ivre de l'infailibilité supposée de la technique, prétend pouvoir faire s'évaporer le risque avant que celui-ci n'advienne. Au détriment, dans toutes les hypothèses, des libertés individuelles.

*

- 5 Dans cet arsenal de surveillance aux multiples facettes, le traitement des données biométriques occupe une place particulière.
- 6 En raison de leur caractère hautement sensible, ces données se trouvent placées au cœur du droit à la protection de la vie privée-intimité en son sens le plus ancien³, de sorte que tout reflux de la protection des données personnelles en la matière ne peut que passer pour une atteinte particulièrement grave au fragile socle de protection de la vie privée. Définies par le G29 comme des données portant sur *«des propriétés biologiques, des aspects comportementaux, des caractéristiques physiologiques, des caractéristiques vivantes ou des actions reproductibles lorsque ces caractéristiques et/ou actions sont à la fois propres à cette personne physique et mesurables»*⁴ celles-ci ont pour particularité de rendre des caractéristiques physiques permanentes d'une personne «lisibles par une machine»⁵ et de permettre le profilage des individus en les plaçant dans des catégories prédéterminées, très souvent à leur insu.
- 7 Plus concrètement, les risques liés à l'explosion de l'usage de ces données sont nombreux et ont été soulignées tant par le contrôleur européen des données⁶ que par le G29⁷ et la CNIL⁸. Le droit a certes d'ores et déjà tenté d'encadrer le phénomène : au niveau de la « Grande Europe », le retentissant arrêt *Marper c. Royaume-Uni*⁹ a énoncé que le simple fait de conserver ou collecter ce type de données doit *« passer pour emporter des conséquences directes sur la vie privée de l'individu concerné, que ces données soient utilisées par la suite ou non »*.
- 8 En 2016, la CNIL avait elle aussi souligné les dangers liés à la collecte et au traitement de telles données en énonçant, s'agissant du stockage et du traitement de l'image faciale des personnes, que : *« (...) le visage est en effet une donnée pouvant être captée à l'insu des personnes, les progrès techniques rendant aujourd'hui encore plus facile de procéder à l'identification biométrique d'une personne à son insu, en comparant son visage avec une base de photographies, ou d'usurper l'identité d'une personne. »*¹⁰
- 9 Le risque est d'autant moins hypothétique que nombre d'états, dont la Chine, ont d'ores et déjà mis en place des systèmes de reconnaissance biométrique – faciale – à des fins de surveillance de masse.
- 10 *
- 11 L'affaire commentée concernait, précisément, la mise en place par l'Etat français d'une base de donnée biométrique, intitulée “Titres électroniques sécurisés” et instauré par le décret n° 2016-1480 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité

12

L'article 1 du décret prévoit que le traitement enregistre les données à caractère personnel des personnes souhaitant se voir délivrer, ou renouveler, un passeport ou une carte nationale d'identité aux fins de permettre l'instruction des demandes relatives à ces titres et de prévenir et détecter leur falsification et leur contrefaçon. Les données à caractère personnel enregistrées dans le traitement automatisé (**article 2 du décret**) sont

notamment, outre celles relatives à l'état civil du titulaire du passeport ou de la carte nationale d'identité, l'image numérisée du visage et celles des empreintes digitales qui peuvent être légalement recueillies. En outre, les **articles 3 et 4 du décret** listent quand à eux les catégories d'agents pouvant avoir accès aux données biométriques. Y figurent non seulement les agents chargés des missions de recherche et de contrôle de l'identité des personnes au sein des services de la police nationale, de la gendarmerie nationale et des douanes, mais également les agents chargés de la prévention et de la répression des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme.

- 13 La création de ce fichier, qui a rapidement suscité l'ire des associations de défense de la vie privée et notamment de la Quadrature du Net et des Exégètes Amateurs - qui ont d'emblée contesté le décret en produisant un recours particulièrement fouillé et complet - posait d'autant plus question que la France a été condamnée en 2013 par la CEDH pour le FAED (Fichier Automatisé des Empreintes Digitales) au motif que « La conservation des empreintes digitales par ce fichier s'analyse en une atteinte disproportionnée, ne peut passer pour nécessaire dans une société démocratique, et ne traduit pas un juste équilibre entre les intérêts publics et privés concurrents en jeu ». Pour parvenir à cette conclusion, la Cour avait notamment fait grief au fichier de ne pas avoir limité les finalités du traitement, en ne limitant le fichier en cause à une fonction de recherche et l'identification des auteurs de crimes et de délits, mais en y rajoutant une seconde, à savoir « *faciliter la poursuite, l'instruction et le jugement des affaires dont l'autorité judiciaire est saisie* » dont il n'est pas clairement indiqué qu'elle se limiterait aux crimes et délits¹¹.
- 14 L'enjeu principal de l'affaire tenait à la proportionnalité d'un traitement collectant en masse des données biométriques potentiellement sensibles et ce notamment au regard du principe de spécification de finalités limitées à un traitement de données - des données collectées pour un motif X ne peuvent être utilisées à une fin Y, différente du motif de collecte - prévu tant par la loi "Cnil" de 1978, que par la jurisprudence de la Cour de Justice de l'Union Européenne et la Cour Européenne des Droits de l'Homme. Au vu de l'arrêt *H.K contre France* sus-cité, notamment, un fichier d'une telle ampleur aurait constitué une atteinte disproportionnée au droit à la vie privée en l'absence de limitation des motifs de la collecte aux seules fins de lutte contre la fraude documentaire.
- 15 L'arrêt du Conseil d'Etat était d'autant plus attendu que l'arrêt *Willems* de la Cour de Justice de l'Union Européenne avait conduit cette dernière à refuser de garantir que les empreintes digitales rassemblées sur le fondement du règlement n° 2252/2004 (relatif aux passeports biométriques) de l'Union Européenne ne soient pas utilisées à des fins autres que la délivrance du passeport ou autre document de voyage biométrique, concluant à la non applicabilité de la Charte des Droits Fondamentaux de l'Union Européenne et laissant à la charge des états le soin de déterminer l'opportunité de constituer des bases de données biométriques¹².
- 16 Par un arrêt **décevant voire consternant**, le conseil d'Etat rejette l'ensemble de l'argumentation des requérants et se lave les mains du sort des données biométriques des citoyens, et ceci en dépit du fait que les Cours européennes avaient, précisément, renvoyé la balle aux juridictions nationales lorsqu'il s'agit de fixer des gardes-fous adéquats aux excès potentiels de la surveillance biométrique. En particulier, le conseil d'Etat juge d'une part que le traitement n'a pour finalité que de permettre l'instruction des demandes relatives à ces titres et de prévenir et détecter leur falsification et leur contrefaçon et qu'ainsi, les finalités ainsi poursuivies, qui excluent toute possibilité d'identifier une personne à partir de ses données biométriques, sont au nombre de celles qui justifient

qu'il puisse être porté atteinte au droit des individus au respect de leur vie privée. . Aussi, conformément à sa finalité d'authentification, l'accès à ce traitement ne peut se faire que par l'identité du porteur du titre d'identité, à l'exclusion, en raison des modalités mêmes de fonctionnement du traitement, de toute recherche à partir des données biométriques elles-mêmes.

- 17 En second lieu, les juges du Palais Royal énoncent si des agents chargés de la prévention et de la répression des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme ont également accès, sous certaines conditions, à ces données, l'article 4 du décret prévoit qu'ils ne peuvent pas accéder aux images numérisées des empreintes digitales. Ainsi, la consultation des empreintes digitales contenues dans le traitement informatisé ne peut selon le conseil d'Etat que servir qu'à confirmer que la personne présentant une demande de renouvellement d'un passeport ou d'une carte nationalité d'identité est bien celle à laquelle ce titre a été initialement délivré ou à s'assurer de l'absence de falsification des données contenues dans le composant électronique du passeport et, ainsi, que les finalités du traitement sont bien déterminées et limitées.
- 18 Douteux à de nombreux égards – et l'on renvoie sur ce point à nouveau au recours particulièrement fouillé et complet de la Quadrature du Net et des Exégètes Amateurs pour une analyse plus fouillée –, le jugement l'est notamment au regard du principe de détermination de finalités limitées à un traitement de données prévu par le droit européen.
- 19 Marquant la prise en compte de « l'exigence de prévisibilité des traitements de données »¹³, le principe de détermination de finalités limitées implique nécessairement que « la collecte des données à caractère personnel et ses modalités, ainsi que les finalités, doivent être décidées au préalable » tout traitement ultérieur incompatible avec les finalités prédéfinies étant interdit¹⁴. Dans son avis 03/2013¹⁵, le G29 avait précisément exprimé des inquiétudes quand au recul de principe de spécification des finalités du traitement et mis en place une grille de lecture permettant de sauvegarder les garanties liées à la détermination de ces finalités.
- 20 Soulignant que l'utilisation de données à des fins différentes de celles initialement prévues ne rend pas nécessairement cette utilisation illégale -sauf à interdire totalement tout usage à fin scientifique de ces données ou à faire du « big data » une coquille vide- le groupe avait néanmoins instauré une grille de lecture en 4 étapes permettant d'entourer de garanties ce type d'usages ultérieurs des données. Il s'agit en premier lieu, d'une part, d'examiner la relation entre les finalités poursuivies par la collecte initiale et la les finalités poursuivies par l'usage ultérieur des données, qui ne doivent pas a priori présenter un lien trop ténu et devraient contribuer aux mêmes buts¹⁶. D'autre part, il s'agit également d'examiner le contexte dans lequel la collecte de données est effectuée, et notamment le fait que la personne dont les données ont été collectées puisse ou non raisonnablement s'attendre à ce que ses données soient réutilisées par la suite. Dans ce cadre, comme le souligne le G29, plus la collecte est ciblée est spécifique, plus le titulaire des données doit pouvoir raisonnablement s'attendre à ce que ses données ne soient pas réutilisées.¹⁷En second lieu, il s'agit d'une part d'être attentif aux risques -notamment les risques de dissémination des données- que suscite la réutilisation des données, ce qui implique d'autre part que soit portée une attention particulière à la mise en sécurité des données.¹⁸
- 21 La Cour de Justice de l'Union Européenne a largement fait sienne ces exigences, en rappelant dans l'arrêt Schwartz de 2013 et en citant l'arrêt Marper¹⁹ de la Cour

Européenne des Droits de l'Homme, qu'en matière de collecte de données biométriques,, le législateur doit « s'assurer qu'il existe des garanties spécifiques visant à protéger ces données efficacement contre les traitements impropres et abusifs ». De manière plus pertinente encore au regard de l'arrêt Willems, la Cour avait souligné que le règlement en litige – qui concernait les passeports biométriques – ne pouvait d'aucune manière servir de base juridique à une éventuelle centralisation des données collectées sur son fondement ou à l'utilisation de ces dernières à d'autres fins que celles prévues par le règlement ;

- 22 Dans le cadre du système de la Convention Européenne des Droits de l'Homme, des garanties similaires ont été énoncées. Aux yeux des juges de Strasbourg, toute ingérence dans la vie privée des personnes doit être « prévue par la loi » au sens de l'article 8 de la convention, ce qui signifie que la collecte massive de données biométriques en vue de la constitution de bases de données de police doit s'accompagner, d'un minimum d'exigences concernant « la durée, le stockage, l'utilisation, l'accès des tiers, les procédures destinées à préserver l'intégrité et la confidentialité des données et les procédures de destruction de celles-ci, de manière à ce que les justiciables disposent de garanties suffisantes contre les risques d'abus et d'arbitraire »²⁰.
- 23 Ce bref aperçu de la jurisprudence européenne en la matière démontre qu'un traitement d'une ampleur telle que celui introduit par le fichier TES ne peut passer le cap du contrôle de conventionnalité qu'à la seule condition de prévoir des garanties visant à éviter que les données collectées ne soient utilisées à d'autres fins que la lutte contre la fraude documentaire, sauf à priver 67 millions de français de « garanties suffisantes contre les risques d'abus et d'arbitraire ».
- 24 Or, le décret prévoit à son article 4 que « les agents des services de la police nationale », « les militaires des unités de la gendarmerie nationale » et « les agents des services spécialisés du renseignement » peuvent, pour la « prévention et de répression des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme », « accéder aux données enregistrées dans » le fichier. Or, il s'agit là de finalités de police administrative et judiciaire qui non seulement ne sont pas clairement délimitées en raison du caractère vague la notion d' « intérêts fondamentaux de la Nation et des actes de terrorisme » mais qui, surtout, n'entretiennent que peu de rapport avec la finalité de lutte contre la fraude documentaire sur laquelle le fichier est fondé.
- 25 Certes, comme le souligne le conseil d'Etat, l'article 4 du décret prévoit que ces services ne peuvent pas accéder aux images numérisées des empreintes digitales. Ainsi, la consultation des empreintes digitales contenues dans le traitement informatisé ne peut servir qu'à confirmer que la personne présentant une demande de renouvellement d'un passeport ou d'une carte nationale d'identité est bien celle à laquelle ce titre a été initialement délivré ou à s'assurer de l'absence de falsification des données contenues dans le composant électronique du passeport.
- 26 Toutefois, comme l'a souligné l'INRIA en se fondant sur le rapport d'audit de l'ANSSI et la DINSIC , le système TES peut techniquement « être détourné à des fins d'identification », notamment parce que l'architecture technique du fichier ne prévoit aucune garantie qui ne puisse être détournée techniquement. En effet, « il suffirait d'interroger la base de données avec les noms des personnes susceptibles d'en faire partie (par exemple tous les citoyens français) pour reconstituer la base complète avec les liens bidirectionnels ». Ainsi, comme le souligne l'INRIA, il est impossible « de se protéger techniquement contre

un tel risque [d'abus] à partir du moment où toutes les données sont contrôlées par une seule entité”²¹

- 27 Ainsi, les effets cumulés des insuffisances de l'architecture technique du fichier, du caractère vague de la détermination des finalités du fichier et de l'ampleur de la collecte en cause exposent sans nul doute les citoyens aux *risques d'abus et d'arbitraire* que la jurisprudence européenne a précisément cherché à prévenir, de sorte qu'il ne fait guère de doute qu'en toute logique juridique, le fichier TES aurait dû être invalidé en raison de l'atteinte disproportionnée qu'il porte au droit à la vie privée des personnes.
- 28 La décision commentée affaiblit donc considérablement la protection dont bénéficient les citoyens contre les abus de la biométrie, ce qui, à l'heure où la « menace terroriste » et le « risque migratoire » justifient des entorses croissantes aux libertés publiques et où le risque d'une généralisation de la « biosurveillance » n'apparaît plus seulement hypothétique, ne peut susciter qu'amertume et déception.

*

- 29 Conseil d'Etat, 9e et 10e sous-sections réunies, 18 octobre 2018, M. H... G...et association Génération Libre, Req. n°404996

*

Les Lettres « Actualités Droits-Libertés » (ADL) du CREDOF (pour s'y abonner) sont accessibles sur le site de la Revue des Droits de l'Homme (RevDH) – Contact

NOTES

1. Didier Bigo, "Sécurité maximale et prévention ? La matrice du futur antérieur et ses grilles." In *Derrière les grilles. Sortons du tout-évaluation*, ed. Barbara Cassin, 111-138, Paris: Fayard, 2014
2. Margaret Hu, Taxonomy of the Snowden Disclosures (November 28, 2015). *Washington and Lee Law Review*, Vol. 72, 2015; *Washington & Lee Legal Studies Paper No.* 2016-5.
3. Il s'agit du "droit d'être laissé seul/à l'écart" (right to be left alone), expression mentionnée pour la première fois par les juges Brandeis et Warren dans un article de 1890, duquel l'on fait dater formellement l'idée de « droit à la vie privée ». V. Neil M. Richards, "The Puzzle of Brandeis, Privacy, and Speech", *Vanderbilt Law Review*, v.63, n.5, pp. 1295-1352.
4. V. G29, 20 juin 2007, Avis 4/2007 sur le concept de donnée à caractère personnel, WP 136
5. V. généralement, sur les risques suscités par ce type de techniques : Paul De Hert, Wim Schreurs et Evelien Brouwer. "„Machine-readable identity documents with biometric data in the EU–part IV “." *Keesing Journal of Documents & Identity*, 2007, n°24.

6. «Le recours à la biométrie dans les systèmes d'information n'est jamais anodin, surtout si le nombre d'individus concernés est très important. [E]n rendant possible la mesure des caractéristiques du corps humain par des machines et en permettant l'utilisation ultérieure de ces caractéristiques, la biométrie modifie définitivement la relation entre corps et identité. Même si les données biométriques ne sont pas accessibles à l'œil nu, des outils appropriés en permettent la lecture et l'utilisation, pour toujours et où que puisse se rendre la personne concernée.» V. Contrôleur européen des données, Avis du 23 mars 2005 sur la proposition de règlement du Parlement européen et du Conseil concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (JO C 181, p. 13)

7. V. G29, 4 octobre 2012, Avis 3/2005 sur l'application du règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, WP 112

8. V. par exemple, sur l'usage de la biométrie en lieu de travail: CNIL, Délibération n°2009-316 du 7 mai 2009 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail

9. Cour.EDH, Gr.Ch., 4 décembre 2008, S. et Marper c. Royaume Uni, Req. n° 30562/04 et 30566/04. V., sur cet arrêt : Sylvie Peyrou-Pistouley, « L'affaire Marper c/ Royaume-Uni : un arrêt fondateur pour la protection des données dans l'espace de liberté, sécurité, justice de l'Union européenne », RFDA 2009, p.94 ; Rocco Bellanova et Paul De Hert, « Le cas S. et Marper et les données personnelles : l'horloge de la stigmatisation stoppée par un arrêt européen », Cultures & Conflits [En ligne], 76 | hiver 2009, mis en ligne le 03 mai 2011,

10. Délibération no 2016-012 du 28 janvier 2016 portant avis sur un projet de décret portant modification d'un traitement automatisé de données à caractère personnel dénommé PARAFE

11. Cour EDH, 18 avr. 2013, M. K c. France, no 19522/09, § 40 et 41

12. CJUE, Quatrième chambre, 16 avril 2015, W.P Willems c. Burgemeester Van Nuth, aff. n° C-446/12 à C-449/12.

13. "L'exigence de prévisibilité a trouvé une expression particulière dans le droit de la protection des données qui impose que tout traitement de données soit lié à des fins déterminées, comme l'exige expressément l'article 8, paragraphe 2, de la charte ". V. Conclusions de l'avocat général Mme Juliane Kokott, 18 juillet 2007, Promusicae contre Telefónica de España SAU, Affaire C-275/06, §53

14. Conclusions de l'avocat général M. Niilo Jääskinen, 17 novembre 2011, Bonnier Audio AB contre Perfect Communication Sweden AB («ePhone»), Affaire C-461/10, §51

15. G29, 2 avril 2013, Opinion 03/2013 on purpose limitation, WP 203.

16. Idem, p.23

17. Idem, p.24

18. Idem, p.26

19. Cour.EDH, Gr.Ch., 4 décembre 2008, S. et Marper c. Royaume Uni, Req. n° 30562/04 et 30566/04, §103

20. Idem.

21. INRIA, 1er février 2017, « Titres électroniques sécurisés : la centralisation des données biométriques est-elle vraiment inévitable? — Analyse comparative de quelques architectures » par Claude Castelluccia et Daniel Le Métayer.

RÉSUMÉS

Par un arrêt du 18 octobre 2018, le conseil d'Etat a validé la création par l'Etat français d'une base de donnée biométrique, intitulée "Titres électroniques sécurisés" et instauré par le décret n° 2016-1480 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité. Celle-ci procède de facto à un fichage de l'ensemble des citoyens français puisqu'elle a pour but même de centraliser en une base unique l'ensemble des données biométriques (empreintes digitales et photographie du visage) des cartes d'identités sécurisées et des passeports. L'enjeu principal de l'affaire tenait à la proportionnalité d'un traitement collectant en masse des données biométriques potentiellement sensibles et ce notamment au regard du principe de spécification de finalités limitées à un traitement de données – des données collectées pour un motif X ne peuvent être utilisées à une fin Y, différente du motif de collecte – prévu tant par la loi "Cnil" de 1978, que par la jurisprudence de la Cour de Justice de l'Union Européenne et la Cour Européenne des Droits de l'Homme. Décevant, l'arrêt rejette l'ensemble de l'argumentation des requérants et prive ce faisant les citoyens de garanties contre les risques d'abus et d'arbitraire inhérents à la constitution de telles bases.

AUTEUR

JEAN-PHILIPPE FOEGLE

Doctorant en droit public (CREDOF - Université Paris Ouest Nanterre)