Conseil d'État
Section du contentieux
10e chambre
**N° 406347**

# Mémoire ampliatif

**PRODUIT PAR**

**La Quadrature du Net**, association régie par la loi du 1er juillet 1901 dont le siège social est situé au 60 rue des Orteaux à Paris (75020), enregistrée en préfecture de police de Paris sous le numéro W751218406, prise en la personne de M. Benjamin Bayart, membre du conseil d'orientation stratégique de la Quadrature du Net, dûment habilité par délégation du président à agir en justice.
Tel. : 06 73 60 88 43
Mail : contact@laquadrature.net

**CONTRE**

**Le 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**

TABLE DES MATIÈRES

# I. FAITS ET PROCÉDURE

1 Par les présentes écritures, l'association requérante complète l'ensemble des moyens et des conclusions qu'elle a développés dans sa requête introductive dont elle entend conserver l'entier bénéfice.

2 Le 28 octobre 2016, a été publié le décret n° 2016-1460 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité (le décret attaqué) (prod. n° **1**). Sa publication a été précédée d'un avis n° 391080 rendu le 23 février par le Conseil d'État (prod. n° **5**) ainsi que d'un avis n° 2016-292 rendu par la Commission nationale de l'informatique et des libertés le 29 septembre 2016. Le décret attaqué vise à créer un traitement commun aux cartes nationales d'identité et aux passeports (pour lesquels des traitements sont prévus respectivement par le décret n° 55-1397 du 22 octobre 1955 et le décret n° 2005-1726 du 30 décembre 2005) au sein d'un nouveau traitement unique dénommé « titres électroniques sécurisés » (TES).

3 Le but poursuivi par la mise en œuvre du décret attaqué est de « simplifier les démarches des usagers et de fiabiliser les titres d'identité en luttant plus efficacement contre la fraude » [1] par la conservation de l'ensemble des données à caractère personnel concernant les demandeurs de ces titres, y compris des données biométriques.

4 Le décret attaqué dispose en son article 1er que le ministère de l'intérieur met en œuvre un traitement de données à caractère personnel pour procéder à l'établissement, à la délivrance, au renouvellement et à l'invalidation des cartes nationales d'identité et des passeports, ainsi que prévenir et détecter leur falsification et contrefaçon.

5 Il dispose en son article 2 que ce traitement comprend l'enregistrement de nombreuses informations obtenues auprès des demandeurs de titres, dont : l'image numérisée de leur visage et de leurs empreintes digitales, leurs noms, leur domicile, leur sexe, la couleur de leurs yeux, leur taille ainsi que l'identité et la nationalité de leurs parents. Ces données sont conservées pour une durée allant de dix à vingt ans en application de son article 9.

6 Pour leurs missions, aux termes des articles 3 et 4 du décret attaqué, peuvent accéder à ces informations : les agents chargés de la délivrance des

1. Communication du ministère de l'intérieur, "Le système des titres électroniques sécurisés", interieur.gouv.fr, consulté le 26 mars 2017.

passeports et des cartes nationales d'identité au sein des préfectures, des sous-préfectures, des ambassades, des consulats et du ministère de l'intérieur, ainsi que les agents ministériels chargés de l'application de la réglementation relative au passeport et à la carte nationale d'identité.

7 De même, pour leurs missions, peuvent accéder à ces informations (à l'exclusion de l'image numérisée des empreintes digitales) les agents et militaires qui, après avoir été individuellement désignés et dûment habilités par leur hiérarchie, sont chargés de la prévention et de la répression des atteintes aux intérêts fondamentaux de la Nation au sein de la police nationale, de la gendarmerie et des services spécialisés du renseignement.

8 Le 26 décembre 2016, La Quadrature du Net déposait une requête introductive d'instance au soutien d'un recours pour excès de pouvoir dirigé contre le décret n° 2016-1460.

9 Le décret attaqué s'inscrit dans un contexte technologique évolutif, loin d'être anodin. Plusieurs éléments constitutifs de ce contexte doivent d'emblée être rappelés.

10 Premièrement, les problématiques de sécurité informatique se sont fortement accentuées ces dernières années. Alors que pas une semaine ne se passe sans qu'il soit question d'attaques informatiques ou de menaces d'intrusions malveillantes [2], le fait de créer une base de données conservant les données biométriques relatives à la quasi-totalité de la population met en jeu de manière disproportionnée la sécurité collective.

11 Deuxièmement, les technologies biométriques se sont considérablement développées et répandues. Alors que les détecteurs d'empreintes digitales équipent de plus en plus de téléphones mobiles, la reconnaissance faciale connaît un très fort développement. Étant précisé que l'essor de ces technologies dans la vie commune s'accompagne nécessairement des risques de mésusage de ces données biométriques. [3]

12 À toutes fins utiles, il est précisé que le traitement institué par le décret attaqué prévoit non pas le stockage des données biométriques sur le support même du titre (p. ex. sur une puce électronique), mais la conservation de telles données au sein d'une (ou plusieurs) base(s) de données opérées par l'administration. De plus amples informations concernant le traitement faisant l'objet du décret attaqué sont disponibles sur le site du ministère de l'Intérieur et notamment dans le rapport d'audit de sécurité du système « titres électroniques sécurisés » de l'ANSSI et de la DINSIC (prod. n° **6**) [4] ou encore dans le communiqué du ministre de l'Intérieur en réponse au Conseil

2. Pour une illustration mettant en cause Interpol, d'ailleurs destinataire d'échanges avec le fichier créé par le décret attaqué, cf. AFP, *Fuite massive à Europol sur des enquêtes anti-terroristes*, Lexpress.fr, 30 novembre 2016.

3. Polloni (C.), *Pour pirater une empreinte digitale, cette photo suffit*, rue89.nouvelobs.com, 28 décembre 2014.

4. Communication du ministère de l'Intérieur, "Système TES : publication du rapport de l'Agence nationale de la sécurité des systèmes d'information et de la direction interministérielle du numérique et du système d'information et de communication de l'État", 17 janvier 2017, interieur.gouv.fr, consulté le 26 mars 2017.

national du numérique [5].

13 Le traitement du décret attaqué est donc radicalement différent des traitements envisagés par la règlementation européenne applicable en matière de passeports [6] ou en matière de permis de conduire [7]. Cette différence radicale porte tant sur les opérations constitutives du traitement (stockage local / conservation dans une base) que sur l'étendue des données dont dispose le responsable du traitement et ses destinataires pour les finalités du traitement, ainsi que sur l'analyse des risques auquel le traitement doit être soumis aux fins de sauvegarder les droits et libertés fondamentales — autant d'éléments déterminants du contrôle de proportionnalité en matière de protection des données à caractère personnel et de droit au respect de la vie privée.

5. Communiqué du ministère de l'Intérieur, "Fichier TES : Courrier de Bernard Cazeneuve au Président du Conseil national du numérique", 7 novembre 2016, interieur.gouv.fr, consulté le 26 mars 2017.

6. 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

7. Règlement (UE) n° 383/2012 de la Commission du 4 mai 2012 établissant les prescriptions techniques relatives aux permis de conduire munis d'un support de mémoire (microprocesseur)

## II. INTÉRÊT À AGIR

14 L'intérêt à agir de l'association requérante est certain en l'espèce. D'après l'article 3 de ses statuts (prod. n° **2**), La Quadrature du Net est une association constituée conformément à la loi du 1er juillet 1901 qui a pour objet :

> « - de mener une réflexion, des études, analyses, actions pour la défense des libertés individuelles sur internet et pour permettre aux citoyens de tirer tous les bénéfices de leur développement ;
> « - d'encourager l'autonomie des usagers et leur prise de contrôle sur les données les concernant ;
> « - de représenter ses membres dans ses relations : avec d'autres associations ou groupements similaires ou complémentaires, des entreprises, les pouvoirs publics et les instances communautaires et internationales, et dans ce cadre, d'être habilitée à traiter, notamment, d'aspects sociaux et réglementaires ou autres au nom de ses membres ;
> « - l'étude et la défense des intérêts sociaux, culturels, d'innovation et de développement humain des citoyens. Pour atteindre ce but, elle jouit de la capacité intégrale reconnue par la loi aux Associations et du pouvoir d'ester en justice. »

15 L'objet général de La Quadrature du Net est donc la défense des droits fondamentaux dans l'environnement numérique (non pas uniquement sur Internet), et notamment la liberté d'expression, la liberté de communication ainsi que le droit au respect de la vie privée et à la protection des données personnelles.

16 À ce titre, l'association intervient dans les débats français et européens relatifs à ces enjeux, notamment en développant des analyses juridiques, en proposant et en évaluant des amendements au cours des procédures législatives. Elle promeut également auprès des citoyens des outils leur permettant d'assurer un meilleur contrôle de leurs données numériques, à travers des informations diffusées sur Internet (à l'image du site controle-tes-donnees.net) et des ateliers de formation.

17 La Quadrature du Net a manifesté très tôt son opposition au décret attaqué [8]. Le 14 novembre 2016, l'association publiait un communiqué de presse de

8. Communiqué commun de l'Observatoire des Libertés et du Numérique (OLN), 14 novembre 2016, https://www.laquadrature.net/fr/oln-fichier-tes-danger-pour-libertes

l'Observatoire des libertés et du numérique, dont elle fait partie, dans lequel il était demandé au gouvernement l'abrogation du décret.

18 Par ailleurs, depuis plus de deux ans, avec l'association FDN et la Fédération FDN, La Quadrature du Net a engagé plusieurs actions contentieuses afin de défendre les droits au respect de la vie privée et à la protection des données personnelles devant le Conseil d'État et le Conseil constitutionnel, notamment contre les décrets d'application de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement (v. notamment la décision 2016-590 QPC du 21 octobre 2016).

## III. DISCUSSION – LÉGALITÉ EXTERNE

19 **À titre liminaire**, le décret attaqué doit être annulé en ce qu'il n'a pas été régulièrement soumis dans sa version finale à l'avis du Conseil d'État.

20 **En droit**, au titre de l'article 27 de la loi n° 78-17 du 6 janvier 1978, sont autorisés par décret en Conseil d'État les traitements mis en œuvre pour le compte de l'État qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes.

21 Le Conseil d'État ne peut être considéré comme ayant été consulté que si le projet dont il a été saisi est identique au décret finalement adopté (voir en ce sens, notamment, Conseil d'État, 16 oct. 1968, *Union nationale des grandes pharmacies de France*, n$^{os}$ 69186, 69206 et 70749, Rec. p. 488 ; Conseil d'État, 2 mai 1990, *Joannides*, n° 86662).

22 **En l'espèce**, il est constant que le décret attaqué est soumis aux conditions de l'article 27 de la loi n° 78-17 du 6 janvier 1978. Le Conseil d'État a été consulté par le Premier ministre le 12 janvier 2016 (soit plus de dix mois avant la publication du décret) et sa section de l'intérieur a rendu son avis le 23 février 2016 (prod. n° **5**). Cet avis décrit et analyse précisément le contenu du projet dont il a alors été saisi. Notamment, le Conseil d'État relève que, si ce projet était adopté en l'état, il prévoirait que :

- « les données biométriques et les données indiquant l'identité de la personne seraient conservées dans des bases différentes » ;
- « il serait impossible d'effectuer une recherche à partir des données biométriques, celles-ci n'étant accessibles qu'à partir des données d'identité » ;
- « seuls les agents chargés du traitement des demandes et de la délivrance des titres, individuellement habilités à cet effet, pourraient avoir accès aux données biométriques, ainsi que certains agents des services centraux du ministère de l'intérieur ou du ministère des affaires étrangères chargés de l'instruction des recours hiérarchiques contre les refus de titres ainsi que de la lutte contre l'usurpation d'identité et la production de faux documents » ;
- « l'accès s'effectuerait au moyen d'un code et d'une carte à puce individuelle permettant d'identifier l'agent » ;
- « le système conserverait la traçabilité de tous les accès et de l'usage qui en aurait été fait ».

23 Or, si de telles caractéristiques s'appliquaient en effet au projet de décret soumis pour avis en février 2016, il n'en va pas de même du décret attaqué, dans sa version publiée.

24 En cela, et comme il sera démontré *infra*, les modifications apportées au projet de décret ayant conduit à la version finale du décret attaqué, ne sont pas anodines. Au contraire, elles touchent à des caractéristiques déterminantes du traitement en cause et à des conditions substantielles que le Conseil d'État avait alors jugées nécessaires pour considérer « que les modalités techniques entourant l'accès aux données et leur usage garantiraient une utilisation du fichier conforme à son objectif » (p. 5 de l'avis). Ce qui n'est plus le cas aujourd'hui.

25 **En conclusion**, il en résulte nécessairement que le décret attaqué a été adopté au terme d'une **procédure irrégulière**, dès lors que la version du décret publiée au journal officiel ne correspond pas entièrement ou exactement à la version soumise pour avis à la Section de l'Intérieur du Conseil d'État.

26 De ce chef, déjà, son annulation est acquise.

# IV. DISCUSSION – LÉGALITÉ INTERNE

27 **En premier lieu,** si le Conseil d'État considère que le décret publié au journal officiel est un décret en Conseil d'État régulier au regard de l'article 27 de la loi n° 78-17, le Conseil d'État devrait reconnaître en tout état de cause que le décret publié est inconstitutionnel en ce qu'il méconnaît l'objectif d'accessibilité et d'intelligibilité du droit.

28 En effet, pour pouvoir se prononcer dans son avis précité (prod. n° **5**), le Conseil d'État a eu accès à des informations complémentaires sur les caractéristiques du traitement en cause (point 1 de l'avis). Or, certains éléments sur lesquels le Conseil d'État s'est prononcé (cf. notamment page 5 de l'avis) ne sont pas contenus dans le décret attaqué, ni publié au Journal Officiel. Ces éléments, qui ne sont toujours pas publics, sont seulement révélés indirectement et de manière parcellaire sur le site web du ministère de l'intérieur suite aux débats suscités par la publication du décret attaqué (cf. *infra*). Par conséquent, le décret prétend créer un traitement sans contenir l'ensemble des éléments nécessaires pour répondre à l'objectif d'accessibilité et d'intelligibilité et doit être annulé de ce seul fait.

29 **En second lieu,** le décret attaqué porte une atteinte disproportionnée au droit au respect de la vie privée ainsi qu'à la protection des données personnelles en ce qu'il manque de respecter les conditions imposées par :

- la loi n° 78-17 du 6 janvier 1978 telle qu'interprétée au regard de la décision du Conseil constitutionnel n° 2012-652 DC du 22 mars 2012 (cf. section 1 page suivante),
- l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales (la Convention) (cf. section 2 page 17) ainsi que par
- la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, lue à la lumière de la Charte des droits fondamentaux de l'Union européenne (la Charte) et telle qu'interprétée notamment par la Cour de justice de l'Union européenne dans son arrêt *Schwartz* du 17 octobre 2013 (cf. section 3 page 20).

# 1. Non-respect des exigences de proportionnalité imposées par le Conseil constitutionnel

30 Le décret attaqué n'est pas conforme aux exigences de proportionnalité imposées par la jurisprudence du Conseil constitutionnel (Conseil constit., 22 mars 2012, *Loi relative à la protection de l'identité*, 2012-652 DC), lesquelles s'appliquent *mutatis mutandis* au contrôle de proportionnalité de tout décret pris en application de la loi n° 78-17 du 6 janvier 1978.

31 **En droit**, le Conseil constitutionnel considère qu'un traitement de données personnelles dont la finalité est de « préserver l'intégrité des données nécessaires à la délivrance des titres d'identité et de voyage », étant « destiné à recueillir les données relatives à la **quasi-totalité de la population** » et qui contient des « **données biométriques** [...] susceptibles d'être rapprochées de traces physiques laissées involontairement par la personne ou collectées à son insu » doit respecter certaines exigences spécifiques de proportionnalité (Conseil constit., 22 mars 2012, *Loi relative à la protection de l'identité*, 2012-652 DC, § 9-10).

32 Ces exigences de proportionnalité interdisent notamment deux choses :

1. que « la consultation ou l'interrogation » des données traitées soient autorisées « non seulement aux fins de délivrance ou de renouvellement des titres d'identité et de voyage et de vérification de l'identité du possesseur d'un tel titre, mais également à **d'autres fins de police administrative ou judiciaire** » ;
2. que les « caractéristiques techniques » du traitement « **permettent son interrogation à d'autres fins que la vérification de l'identité** d'une personne ».

33 Ces deux exigences sont complémentaires. La première exigence porte sur les finalités et les destinataires des données du traitement, la seconde sur l'architecture du traitement et en particulier sur ses caractéristiques techniques. Dès lors, si un traitement concerné ne respecte pas l'une de ces exigences, il porterait « au droit au respect de la vie privée une atteinte qui ne peut être regardée comme proportionnée au but poursuivi » (Conseil constit., 22 mars 2012, *Loi relative à la protection de l'identité*, 2012-652 DC, § 11).

34 À cet égard, il faut souligner que ces exigences de respect de la vie privée s'appliquent *mutatis mutandis* au contrôle de proportionnalité d'un décret au regard de la loi n° 78-17 du 6 janvier 1978 concernant tout traitement de données soumis à cette loi.

35 En effet, le Conseil constitutionnel a défini ces exigences lors de sa censure de l'article 5 de la loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité, qu'il indiquait alors comme créant un traitement de données personnelles « dans les conditions prévues par la loi du 6 janvier 1978 » (Conseil constit., 22 mars 2012, *Loi relative à la protection de l'identité*, 2012-652 DC, § 2).

36 **En l'espèce,** le décret attaqué prévoit, en ses articles 1 et 2, la création d'un traitement de données personnelles relatif aux demandeurs de titres d'identité afin de « procéder à l'établissement, à la délivrance, au renouvellement et à l'invalidation » de ces titres « ainsi que prévenir et détecter leur falsification et contrefaçon ». Sa finalité est donc conforme à celle des traitements soumis aux exigences spécifiques de proportionnalité définies ci-avant.

37 Ensuite, le décret prévoit la création d'un traitement d'une vaste ampleur, destiné à traiter des données relatives à la **quasi-totalité de la population** de nationalité française. La constitution d'un fichier d'une telle ampleur n'a de précédent connu à ce jour que celui de la loi relative à la protection de l'identité adoptée par le Parlement en 2012 et censurée par le Conseil constitutionnel dans sa décision précitée.

38 De plus, les **données biométriques** contenues dans le traitement institué par le décret attaqué sont susceptibles d'être rapprochées de traces physiques laissées involontairement par la personne ou collectées à son insu. Il en va ainsi des empreintes digitales, mais aussi de la photographie de chaque personne, qui peut être rapprochée (par reconnaissance faciale et, notamment, de manière automatisée) d'images prises à son insu (tel que par des dispositifs de vidéo-surveillance).

39 Enfin, le traitement autorisé par le décret attaqué est évidemment soumis à la loi n° 78-17 du 6 janvier 1978.

40 **En conclusion**, le décret attaqué doit respecter la loi n° 78-17 du 6 janvier 1978 telle qu'interprétée par la Conseil constitutionnel dans sa décision de 2012, qui lui impose deux exigences spécifiques de proportionnalité. Pourtant, tel qu'il sera démontré ci-après, il n'en respecte aucune.

## 1.1. Autorisation de consultation à d'autres fins de police administrative ou judiciaire

41 En violation de la première exigence définie ci-avant, le décret attaqué autorise la consultation des **images numérisées du visage** des personnes concernées à **d'autres fins de police administrative ou judiciaire** que les simples fins de délivrance ou de renouvellement des titres d'identité et de voyage et de vérification de l'identité du possesseur d'un tel titre.

42 En effet, 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, ces finalités sont de l'ordre de la police tant administrative que judiciaire et sont clairement distinctes de celles liées à la délivrance de titres et à la vérification d'identité. Qui plus est, loin de se limiter à des questions de vérification d'identité, l'article 4 du décret attaqué poursuit une fin d'identification de personnes

autrement non-identifiées.

43 Ce même article 4 exclut les empreintes digitales des données auxquelles il confère un tel accès, mais n'en exclut aucunement les images de visages qui sont enregistrées dans le fichier. Or, l'image du visage est une donnée biométrique permettant l'identification des personnes concernées, notamment de manière automatisée et à leur insu par l'usage de technologies de reconnaissance faciale.

44 Or, le développement technologique de la reconnaissance faciale n'a rien de théorique mais implique des conséquences juridiques devant d'ores et déjà être considérées dans leur ensemble. Dès 2008, la commission des lois du Sénat produisait un rapport sur la vidéosurveillance [9] qui expliquait que :

> « En théorie, il serait **possible d'identifier une personne dans une foule**. Des expérimentations ont été lancées dans certains aéroports et gares britanniques, mais le taux d'erreur est très important. Si **l'ensemble des industriels travaillent sur cette technologie**, il est impossible de prédire à quel horizon une offre technique pourra être proposée à des utilisateurs. En revanche, il est probable que lorsqu'elle le sera, elle recevra des applications dans les gares internationales ou les aéroports. M. Frédéric Péchenard, directeur général de la police nationale, a d'ailleurs évoqué les réflexions actuelles sur la constitution d'un fichier « photos » sur le modèle du fichier national automatisé des empreintes génétiques (FNAEG) qui permettrait de reconstituer un visage et de le comparer avec des enregistrements sur une scène d'infraction. Un projet similaire a démarré au Royaume-Uni avant d'être interrompu pour des raisons éthiques et techniques, la crainte d'une partie de l'opinion étant que ce fichier puisse être interconnecté avec l'éventuel fichier national de la carte nationale d'identité. »

45 Depuis, les technologies de reconnaissance faciale se sont considérablement améliorées. La reconnaissance faciale tend désormais à être utilisée dans des champs nombreux et diversifiés tels que la médecine [10] ou encore les transactions bancaires en ligne [11].

9. Rapport d'information de MM. Jean-Patrick COURTOIS et Charles GAUTIER, fait au nom de la commission des lois n° 131 (2008-2009), 10 décembre 2008, http://www.senat.fr/notice-rapport/2008/r08-131-notice.html.

10. Aux fins de détecter certaines maladies génétiques notamment : Gabriele Porrometo, *La reconnaissance faciale parvient à détecter une maladie génétique rare*, Numerama.com, 24 mars 2017 http://www.numerama.com/sciences/243284-la-reconnaissance-faciale-parvient-a-detecter-une-maladie-genetique-rare.html.

11. Voir à ce sujet les applications de paiements s'appuyant sur la reconnaissance faciale, notamment : Aude Fredouelle, *Paiement : la reconnaissance faciale défie l'empreinte digitale*, Journaldunet.com, 28 avril 2016 http://www.journaldunet.com/economie/finance/1177505-paiement-la-reconnaissance-faciale-defie-l-empreinte-digitale/ ou encore Aude Fierla, *Mastercard lance le paiement par selfie*, Lefigaro.fr, 17 octobre 2016 http://www.lefigaro.fr/societes/2016/10/06/20005-20161006ARTFIG00006-mastercard-lance-le-paiement-par-selfie.php.

46 Ainsi, en 2017, plusieurs députés expliquent, dans une proposition de loi déposée à l'Assemblée nationale [12], que :

> « La vidéoprotection couplée à une technologie de reconnaissance faciale est de nature à offrir des gains significatifs en matière d'identification criminelle ou terroriste et d'analyse du renseignement, compte tenu des **récents progrès dans le domaine des algorithmes de reconnaissance faciale** et d'analyse vidéo en temps réel, comme un temps différé. »

47 Par ailleurs, cette proposition de loi, poursuivant l'effort engagé par une proposition précédente [13], démontre une volonté concrète et grandissante d'exploiter les images contenues dans les fichiers d'État à des fins de surveillance de la population. Le décret attaqué n'endigue nullement cette volonté mais, au contraire, y cède entièrement.

48 Pourtant, en 2016, la CNIL avait déjà parfaitement résumé la gravité de cette situation en expliquant que :

> « La reconnaissance faciale fait peser des risques importants sur les libertés individuelles : 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.
> « Par ailleurs, le contexte actuel est caractérisé par une multiplication du nombre des systèmes de vidéoprotection, permettant en théorie le **développement massif de la reconnaissance faciale**, avec des risques accrus en matière de protection des données et de vie privée. » (Délibération n° 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)

49 C'est ainsi que la CNIL considérait dès 2007, s'agissant d'une réforme du fichier TES concernant alors seulement les passeports, que :

> « le projet de décret devrait également faire mention de l'impossibilité pour les agents précités d'accéder à l'image numérisée du visage du titulaire. » (Délibération n° 2007-368 du 11 décembre 2007 portant avis sur un projet de décret en Conseil d'Etat modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques)

12. Proposition de loi de M. Éric CIOTTI et plusieurs de ses collègues d'orientation et de programmation pour la sécurité intérieure et la justice, n° 4582, déposée le 10 mars 2017, http://www.assemblee-nationale.fr/14/propositions/pion4582.asp.

13. Proposition de loi de M. Roger KAROUTCHI relative à la reconnaissance faciale dans les enquêtes terroristes, n°699, déposé au Sénat le 17 juin 2016, https://www.senat.fr/leg/ppl15-699.pdf.

50 **En conséquence,** le décret attaqué autorise à ce que des données biométriques qui ont été enregistrées au sujet de la quasi-totalité de la population soient exploitées pour d'autres fins de police administrative ou judiciaire que les simples fins de délivrance ou de renouvellement des titres d'identité et de voyage et de vérification de l'identité du possesseur d'un tel titre. Ce faisant, il viole la loi n° 78-17 et porte une atteinte manifestement injustifiée aux droits à la vie privée et à la protection des données personnelles de la quasi-totalité de la population.

## 1.2. Caractéristiques techniques du traitement permettent son interrogation à d'autres fins que la vérification de l'identité

51 **En droit**, par sa décision n° 2012-652 DC précitée, en faisant droit aux griefs avancés par les auteurs de la saisine, le Conseil constitutionnel s'est opposé à une architecture technique permettant l'identification des personnes à partir des données biométriques se trouvant dans une base centralisée. Le commentaire aux Cahiers relatif à la décision précitée fait clairement apparaître la disproportion d'un tel traitement en mettant notamment en avant d'autres modalités techniques permettant d'atteindre les objectifs de la loi d'alors, identiques à ceux du décret attaqué.

52 Dans son avis du 23 février 2016 sur le traitement informatique relatif aux cartes nationales d'identité et aux passeports, le Conseil d'État détaillait les caractéristiques techniques d'un fichier de nature à assurer qu'il ne puisse être interrogé qu'aux fins de vérification d'identité (point 5). Il a ainsi précisé que *« les modalités techniques entourant l'accès aux données et leur usage garantiraient une utilisation du fichier conforme à son objectif »* dans la mesure où *« il serait impossible d'effectuer une recherche à partir des données biométriques, celles-ci n'étant accessibles qu'à partir des données d'identité »*.

53 Or, **en l'espèce**, le traitement créé par le décret attaqué **ne rend pas impossible d'effectuer une recherche à partir des données biométriques**. En effet, les modalités techniques prévues par le décret attaqué ne présentent pas les garanties de nature à limiter l'interrogation de ce traitement aux seules fins de vérification de l'identité d'une personne.

54 Le décret se contente de préciser, à son article 2, que *« le traitement ne comporte pas de dispositif de recherche permettant l'identification à partir de l'image numérisée du visage ou de l'image numérisée des empreintes digitales enregistrées dans ce traitement »*, sans toutefois prévoir une quelconque caractéristique technique la rendant impossible — ni même raisonnablement plus difficile — ce qui, en raison de l'absence des garanties techniques déjà mentionnées, poserait un risque particulièrement grand d'utilisation non-autorisée à des fins d'identification.

55 À l'inverse, la création d'un traitement unique rend cette recherche possible. En effet, tout fichier liant des données biométriques à des données

d'identification permet systématiquement, par nature, l'identification des personnes y figurant à partir de ces seules données biométriques. Aucune « caractéristique technique » ne saurait effectivement prévenir une utilisation d'un tel fichier à des fins d'identification.

56 Les affirmations contraires du ministère de l'intérieur à cet égard ne résistent pas à l'analyse scientifique.

57 Ainsi que le précise l'INRIA dans sa note d'analyse du fichier TES (prod. n° **7**) :

> « Le ministère affirme que, s'il est "possible de remonter au deuxième compartiment, biométrique, à partir des données propres à la demande du titre, l'inverse est impossible. On ne peut accéder à l'identité à partir des données biométriques." Cette impossibilité serait non seulement juridique (le décret l'interdit), mais aussi technique. Le fichier TES offrirait donc des fonctions d'authentification ("vérification que la personne qui demande un titre est bien celle qu'elle prétend être au vu du contrôle de conformité des données biométriques que permet la base") mais serait mis en œuvre de manière à empêcher toute fonctionnalité d'identification (découverte de l'identité d'une personne à partir de données biométriques). Les explications sur cette mise en œuvre fournies par le ministère, notamment dans sa réponse au Conseil national du numérique, évoquent une conservation des données biométriques dans une base distincte et séparée de celle des demandes de titres, un lien "asymétrique" entre ces bases, et un blocage technique "garanti par une cryptographie spécifique et un lien unidirectionnel". Le rapport d'audit de l'ANSSI et la DINSIC affirme cependant que "le système TES peut techniquement être détourné à des fins d'identification" et recommande la prise en compte des "préconisations du Référentiel Général de Sécurité concernant les mécanismes cryptographiques mis en œuvre pour construire les liens unidirectionnels." Les éléments disponibles publiquement sont trop vagues pour permettre une véritable analyse technique. Cependant, certains scientifiques sont sceptiques sur la possibilité même de l'existence d'une solution technique offrant la fonctionnalité d'authentification tout en interdisant celle d'identification. » (page 3, notes de bas de page omises)

58 Autrement dit, le décret prévoit l'enregistrement et la conservation des données biométriques et des données d'identité dans une (ou plusieurs) base(s) de l'administration (articles 2 et 9 du décret attaqué). Quelque soit la mise en œuvre retenue pour ce traitement, cet enregistrement et cette conservation impliquent par leurs caractéristiques la possibilité technique d'une identification (découverte de l'identité d'une personne à partir de données biométriques). Ainsi, la mise en œuvre retenue ne saurait pallier les lacunes intrinsèques au décret attaqué.

59 En effet, l'INRIA démontre en quoi l'architecture retenue par le gouvernement ne pallie aucunement les insuffisances du décret :

> « Une protection contre l'identification est introduite [...] par l'utilisation de liens unidirectionnels, rendant plus difficile le passage d'une empreinte aux données d'état civil correspondantes. Cependant, **cette protection demeure très faible** car 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. **Il paraît difficile, voire impossible, de se protéger techniquement contre un tel risque à partir du moment où toutes les données sont contrôlées par une seule entité**. L'introduction de liens unidirectionnels complique l'identification, mais ne l'empêche pas de façon absolue. De même, le fait de ne stocker qu'un gabarit ou un condensat des empreintes ou des photos, comme il est parfois proposé, ne constitue qu'une faible protection contre ce risque, car il suffirait de comparer les condensats au lieu des empreintes afin de retrouver l'identité de la personne en question. Par ailleurs, **même sans reconstituer la base, il est possible de l'interroger pour vérifier certaines identités.** Il est aisé, par exemple lors d'une manifestation, d'effectuer une recherche à partir d'une liste de noms de "suspects" potentiels (opposants, syndicalistes, etc.). » (page 11, notes de bas de page omises)

60 La conclusion de l'INRIA mérite quelques explications supplémentaires.

### 1.2.1. Le lien à sens unique n'est pas efficace pour se prémunir contre l'utilisation du traitement à des fins d'identification

61 Quand une base de données est structurée à sens unique, comme c'est le cas en l'espèce[14] (depuis l'identité d'une personne, on peut retrouver les données biométriques, mais pas l'inverse), l'exercice qui consiste à construire le lien réciproque est un exercice qui ne pose aucune difficulté théorique, et qui peut être entièrement automatisé. La protection apportée par ce lien unique est donc une protection très faible, contre certains abus immédiats, mais absolument pas une *garantie* que l'usage de ces données ne pourra pas être détourné.

62 C'est d'ailleurs le constat fait par l'ANSSI dans son audit du fichier TES publié le 13 janvier 2017 (prod. n° **6**) :

> « Du point de vue des usages l'audit a constaté que le système TES peut techniquement être détourné à des fins d'identification, malgré le caractère unidirectionnel du lien informatique mis en œuvre pour relier les donnés d'identification alphanumérique

14. Article 2, II, du décret attaqué.

aux données biométriques. Cet usage illicite peut être atteint ne serait-ce que par reconstruction d'une base de données complète à partir du lien unidirectionnel existant ». (page 4)

63 On voit ici que le décret manque d'assurer la garantie d'une absence d'utilisation du fichier à des fins d'identification.

### 1.2.2. La conservation dans une base des données complètes n'est pas utile au regard des finalités

64 À partir des données brutes, en particulier de l'empreinte digitale, on peut sans difficulté technique majeure fabriquer un faux convaincant. Soit un faux qu'on puisse présenter à un lecteur biométrique (une empreinte digitale imprimée sur papier pour déverrouiller un téléphone, par exemple), soit un faux qu'on puisse laisser sur une scène de crime et que les techniques actuelles de police scientifique ne sauraient pas différencier d'un vrai. Si le fichier venait à être piraté, quand le fichier viendra a être piraté, et que les données en question auront fuité, beaucoup pourront produire de tels faux. La simple existence de ces données crée en cela un risque d'une dimension toute particulière.

65 Or, l'identification se fait en extrayant des données biométriques certaines informations structurelles (les points clefs pour une empreinte digitale, par exemple) et en comparant ces points clefs avec ceux stockés. La comparaison ne porte jamais sur les données biométriques brutes. Le stockage de ces données brutes n'apporte donc aucun avantage et représente un risque majeur pour la vie privée des personnes, ainsi que pour leur sécurité.

### 1.2.3. La conservation des données dans une base, même partielle, est peu utile

66 Le seul intérêt pratique de la conservation dans une base des données biométriques, même d'une conservation partielle, si l'on exclut la recherche depuis une donnée biométrique, est de pouvoir réémettre sans délai un duplicata du titre sécurisé sans devoir refaire le prélèvement des données (prise des empreintes, photographie, etc). Cet intérêt pratique n'emporte pas d'enjeu de sécurité publique, ou de sécurité des individus tel qu'il puisse être regardé comme proportionné avec le fait de créer un risque majeur.

67 Il est d'ailleurs à noter que dans l'audit précité, l'ANSSI relevait que :

> « La centralisation des données biométriques pour la carte nationale d'identité n'a pas actuellement un intérêt direct pour leur gestion. Leur utilisation se borne en effet au cas des requisition judiciaires. D'un point de vue de la gestion des titres, il est ainsi important de noter que l'existence dans TES d'un système de base de données conservant au niveau central les empreintes digitales collectées lors des demandes de ttres ne se justifie que pour faciliter les contrôles lors des renouvellements de titres.

De plus cela concerne uniquement les passeports puisqu'aucune fonctionnalité de ce type n'est à ce jour implémentée concernant la carte nationale d'identité » (p. 6).

68 Pour ces raisons tenant à ses finalités et ses caractéristiques techniques mêmes, le fichier TES faisant l'objet du décret attaqué porte une atteinte disproportionnée au droit à la protection des données à caractère personnel et au droit au respect de la vie privée.

69 **En conséquence,** le décret attaqué doit être considéré comme violant la loi Informatique et Libertés au regard des critères de proportionnalité établis par le Conseil constitutionnel et doit en cela être annulé.

70 **En outre,** le traitement automatisé prévu par le décret attaqué revêt un caractère disproportionné et illicite au regard de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (cf. section 2) ainsi que de plusieurs dispositions de la loi n° 78-17 du 6 janvier 1978 (cf. section 3 page 20).

## 2. Non-conformité du traitement à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales

71 **En droit**, l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (la Convention) dispose que :

> « 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
> « 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »

72 Dans son arrêt *Marper* du 4 décembre 2008, la Cour européenne des droits de l'homme (ci-après la Cour EDH) a jugé que :

> « le caractère général et indifférencié du pouvoir de conservation des empreintes digitales, échantillons biologiques et profils ADN des personnes soupçonnées d'avoir commis des infractions mais non condamnées, tel qu' il a été appliqué aux requérants en l'espèce, ne traduit pas un juste équilibre entre les intérêts publics et privés concurrents en jeu, et que l'Etat défendeur a outrepassé toute marge d'appréciation acceptable en la matière . Dès lors, la conservation litigieuse s'analyse en une atteinte disproportionnée au droit des

requérants au respect de leur vie privée et ne peut passer pour nécessaire dans une société démocratique. » (Cour EDH, g^de ch., 4 déc. 2008, *Marper c. R-U*, n^os 30562/04 et 30566/04, point 125)

73 Dans son arrêt du 18 avril 2013, *M. K c. France*, la Cour EDH a jugé, au sujet du fichier automatisé des empreintes digitales français (ci-après, le FAED) et au regard de l'article 8 de la Convention, que

> « [...] retenir l'argument tiré d'une prétendue garantie de protection contre les agissements des tiers susceptibles d'usurper une identité reviendrait, en pratique, à justifier **le fichage de l'intégralité de la population présente sur le sol français**, ce qui serait **assurément excessif et non pertinent**
>
> « De plus, à la première fonction du fichier qui est de faciliter la recherche et l'identification des auteurs de crimes et de délits, le texte en ajoute 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 délits. En visant également « les personnes, mises en cause dans une procédure pénale, dont l'identification s'avère nécessaire » (article 3, 2° du décret), il est susceptible d'englober de facto toutes les infractions, y compris les simples contraventions dans l'hypothèse où cela permettrait d'identifier des auteurs de crimes et de délits selon l'objet de l'article 1 du décret [...] ».
>
> (Cour EDH, 18 avr. 2013, *M. K c. France*, n° 19522/09, § 40 et 41)

74 Ainsi, la Cour s'opposait à un fichage de l'intégralité de la population française, notamment en ce qu'il était réalisé en vue de la poursuite de finalités indéterminées.

75 C'est la raison pour laquelle, par l'adoption du décret n° 2015-1580 du 2 décembre 2015 [15], le Gouvernement a été tenu de limiter les finalités du traitement institué ainsi que de les énoncer clairement à l'article 1^er du décret du 8 avril 1987 relatif au FAED.

76 Or, **en l'espèce**, le fichier TES a bien, en premier lieu, pour vocation de ficher l'ensemble de la population française. C'est un fait incontesté et sa vocation intrinsèque.

77 Aussi, le fichier a-t-il, en second lieu, des finalités indéterminées, et ce, à un double titre.

78 Une première indétermination réside dans le fait que le fichier institué a pour finalité affichée à l'article 1^er de lutter contre la fraude des titres documentaires mais que l'article 4 renvoie quant à lui à d'autre finalités.

79 Ainsi, selon l'article 4 du décret attaqué dispose que, « **pour les besoins de la prévention et de la répression des atteintes aux intérêts**

15. Décret n° 2015-1580 du 2 décembre modifiant le décret n° 87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur.

**fondamentaux de la Nation et des actes de terrorisme** », peuvent accéder au fichier une série d'agents de police, de militaires et d'agents des services spécialisés du renseignement. Contrairement à l'objectif d'ordre purement administratif affiché à l'article 1er du décret attaqué, à savoir la lutte contre la fraude documentaire, le fichier a donc des finalités judiciaires et administratives non clairement affichées visant à la prévention et à la répression des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme.

80 À cette première indétermination s'en ajoute une seconde : celle de savoir ce que sont les intérêts fondamentaux de la Nation ici en cause. A ce titre, il est à rappeler que les auteurs de la saisine ayant donné lieu à la décision du Conseil constitutionnel du 23 juillet 2015 n° 2015-713 DC, *Loi relative au renseignement*, avaient soulevé le caractère indéterminé des finalités énoncées à l'article L. 811-3 du code de sécurité intérieure (CSI), lequel se réfère lui aussi à la défense des intérêts fondamentaux de la Nation.

81 Pour rappel, les finalités de l'article L. 811-3 CSI se lisent comme suit :

> « Pour le seul exercice de leurs missions respectives, les services spécialisés de renseignement peuvent recourir aux techniques mentionnées au titre V du présent livre pour le recueil des renseignements relatifs à la défense et à la promotion des intérêts fondamentaux de la Nation suivants :
>
> 1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ;
> 2° Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ;
> 3° Les intérêts économiques, industriels et scientifiques majeurs de la France ;
> 4° La prévention du terrorisme ;
> 5° La prévention :
> a) Des atteintes à la forme républicaine des institutions ;
> b) Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ;
> c) Des violences collectives de nature à porter gravement atteinte à la paix publique ;
> 6° La prévention de la criminalité et de la délinquance organisées ;
> 7° La prévention de la prolifération des armes de destruction massive »

82 Dans sa décision du 23 juillet 2015, le Conseil constitutionnel avait jugé que cet article était compatible avec la Constitution, mais uniquement en ce que :

— l'usage des techniques de renseignement était limité à des seules fins administratives (considérant 9 de la décision du Conseil constitutionnel du 23 juillet 2015 précitée) et que
— les intérêts de la Nation concernés étaient limités à ceux énoncés aux

points 1 à 7 précités.

83 Qui plus est, ces intérêts de la Nation avaient dû être détaillés par le Conseil constitutionnel dans les termes suivants :

> « Considérant qu'en retenant, pour déterminer les finalités énumérées aux 1° à 4°, des définitions faisant référence à certains des intérêts mentionnés à l'article 410-1 du code pénal, le législateur a précisément circonscrit les finalités ainsi poursuivies et n'a pas retenu des critères en inadéquation avec l'objectif poursuivi par ces mesures de police administrative ; qu'il en va de même pour les finalités définies au a) du 5°, faisant référence aux incriminations pénales du chapitre II du titre Ier du livre IV du code pénal, de celles définies au b) du 5°, faisant référence aux dispositions de l'article L. 212-1 du code de la sécurité intérieure, de celles définies au c) du 5°, faisant référence aux incriminations pénales définies aux articles 431-1 à 431-10 du code pénal, de celles définies au 6°, faisant référence aux incriminations pénales énumérées à l'article 706-73 du code de procédure pénale et aux délits punis par l'article 414 du code des douanes commis en bande organisée et de celles définies au 7°, faisant référence aux incriminations pénales définies aux articles L. 2339-14 à L. 2339-18 du code de la défense ; »
> (Conseil constit., 23 juill. 2015, *Loi renseignement*, 2015-713 DC, considérant 10)

84 Or, force est de constater qu'en l'espèce :

- — une énumération limitative telle que celle figurant à l'article L. 811-3 CSI et des précisions telles que celles apportées par le Conseil constitutionnel font défaut et que
- — l'accès aux données biométriques stockées n'est en rien limité à des seules fins administratives puisque les autorités visées à l'article 4 du décret attaqué pourront accéder aux données biométriques conservées dans le fichier à la fois à des fins administratives et judiciaires.

85 **En conséquence,** le décret attaqué doit être jugé comme étant incompatible avec l'article 8 de la Convention EDH en ce qu'il a pour vocation de créer un fichier répertoriant les données biométriques de l'ensemble de la population en vue de l'accomplissement de finalités indéterminées.

## 3. Illicéité du traitement au regard de la loi n° 78-17 du 6 janvier 1978

86 Le traitement de données personnelles créé par le décret attaqué doit pour être licite se conformer aux dispositions pertinentes de la loi n° 78-17 du 6 janvier 1978. Il en va ainsi des dispositions relatives tant à la finalité, qu'au caractère proportionné aini qu'à la sécurité du traitement en cause.

## 3.1. Sur les finalités

87 **En droit,** un traitement de données à caractère personnel ne peut être licite au sens de l'article 6, 2° de la loi n° 78-17 du 6 janvier 1978 que si les données en cause sont « collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. »

88 **En l'espèce,** comme cela a été démontré *supra*, les finalités du traitement créé par le décret attaqué sont indéterminées à au moins deux égards : d'une part en ce qu'il poursuit des finalités autres que celles énoncées à l'article 1er et d'autre part en ce que ces autres finalités, énoncées à l'article 4, sont en elle-même extrêmement vagues.

89 **En conséquence,** le décret attaqué crée un traitement de données à caractère personnel dont les finalités sont indéterminées et doit de ce chef être annulé.

## 3.2. Sur le caractère adéquat

90 **En droit,** un traitement de données à caractère personnel ne peut être licite au sens de la loi n° 78-17 du 6 janvier 1978 que s'il porte sur des données à caractère personnel qui sont « **adéquates, pertinentes et non excessives** au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs » (art. 6, 3°).

91 Cette disposition transpose notamment l'article 6, paragraphe 1, c), de la directive 95/46, auquel l'article 6, 3° de la loi n° 78-17 du 6 janvier 1978 ne saurait être contraire (CJUE, 20 mai 2003, *Rundfunk*, C-465/00, C-138/01 et C-139/01, § 101) et devant être interprété au regard des articles 7, 8 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne (la Charte).

92 À ce jour, ces dispositions doivent aussi être lues à la lumière du règlement général sur la protection des données n° 2016/679 du 27 avril 2016 (ci-après, « RGDP »), quand bien même celui-ci ne serait pas encore entré en vigueur.

93 En effet, le RGDP est déjà pris en compte par les autorités nationales et doit l'être également dans le cadre du présent litige. C'est d'ailleurs le sens de l'action de la CNIL qui, anticipant l'entrée en vigueur du règlement précité, a revu sa doctrine en matière de traitement de données biométriques (cf. par exemple CNIL, *Biométrie : un nouveau cadre pour le contrôle d'accès biométrique sur les lieux de travail*, Cnil.fr, 27 septembre 2016). Cela vaut d'autant plus que le RGDP fournit une grille d'analyse utile pour examiner la licéité des traitements de données biométriques mis en œuvre par des États membres.

94 Ainsi, il convient de relever en premier lieu que le RGDP procède à la définition des données biométriques. Les données biométriques y sont définies à l'article 4, point 14, comme « les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques

physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques. »

95 Puis, en deuxième lieu, l'article 9 du RGDP énonce les conditions de validité d'un traitement de données biométriques dans les termes suivants :

> « Le traitement [...] des données biométriques aux fins d'identifier une personne physique de manière unique [n'est permis que s'il] est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée ; »

96 On retrouve ici le principe de proportionnalité que doivent respecter les autorités nationales lorsqu'elles mettent en œuvre des traitements de données personnelles tel que celui créé par le décret attaqué. Étant donné que l'identification des personnes dont il est question doit être entendue comme indiqué par le G29 :

> « L'identification d'une personne par le biais d'un système biométrique consiste généralement à comparer les données biométriques d'une personne (acquises au moment de l'identification) avec plusieurs modèles biométriques stockés dans une base de données (autrement dit, un processus de comparaison « un-à-plusieurs ») » (G29, Avis 3/2012 sur l'évolution des technologies biométriques, 27 avril 2012, p. 6).

97 Dans l'arrêt *Schwarz* du 17 octobre 2013, la Cour de justice a été amenée à apprécier la validité du règlement n° 2252/2004 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 [16].

98 Dans cette affaire, la juridiction de renvoi avait questionné la validité du règlement au regard du « *risque que, après le prélèvement des empreintes digitales en application de cette disposition, ces données de très haute qualité soient conservées, le cas échéant* ***d'une manière centralisée****, et utilisées à des fins autres que celles prévues par ce règlement* » (CJUE, 4e ch., 17 oct. 2013, *Schwarz*, C-291/12, § 58). En réponse à quoi la Cour de justice a considéré que :

> « [...] il importe de rappeler que l'article 1er, paragraphe 2, du règlement n° 2252/2004 ne prévoit la conservation des empreintes

16. 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 (JOUE L 385, p. 1), tel que modifié par le règlement (CE) n° 444/2009 du Parlement européen et du Conseil, du 6 mai 2009 (JOUE L 142, p. 1, et rectificatif JO L 188, p. 127).

digitales qu'au sein même du passeport, lequel demeure la possession exclusive de son titulaire.

« Ce règlement n'envisageant aucune autre forme ni aucun autre moyen de conservation de ces empreintes, il ne saurait être interprété, ainsi que le souligne le considérant 5 du règlement n° 444/2009, comme fournissant, en tant que tel, une base juridique à une éventuelle centralisation des données collectées sur son fondement [...].

« Dans ces conditions, les arguments évoqués par la juridiction de renvoi concernant **les risques liés à l'éventualité d'une telle centralisation** ne sont, en tout état de cause, pas de nature à affecter la validité dudit règlement et devraient, le cas échéant, être examinés à l'occasion d'un recours exercé, devant des juridictions compétentes, contre une législation prévoyant une base centralisée des empreintes digitales.

« Eu égard aux considérations qui précèdent, il convient de constater que l'article 1er, paragraphe 2, du règlement n° 2252/2004 n'implique pas un traitement des empreintes digitales qui irait au-delà de ce qui est nécessaire pour la réalisation du but tenant à la protection des passeports contre leur utilisation frauduleuse. »

(CJUE, 4e ch., 17 oct. 2013, *Schwarz*, C-291/12, § 59 à 63)

99 Dans ses conclusions, l'avocat général avait notamment souligné qu'il était essentiel, afin d'assurer le caractère proportionné de l'atteinte au droit à la protection des données personnelles, que l'image des empreintes ne soit stockée que sur le seul support, de sorte que le citoyen en est le seul détenteur et que l'État n'en conserve pas de copie (conclusions de l'avocat général Mengozzi présentées le 13 juin 2013, *Michael Schwarz contre Stadt Bochum*, C-291/12) :

> « Les données sont contenues dans le seul support de stockage sécurisé inséré dans le passeport, ce qui signifie que, en principe, le citoyen de l'Union est le seul détenteur de l'image de ses empreintes. Ledit règlement ne peut – *et c'est un élément essentiel* – servir de base juridique à la constitution par les États membres de bases de données stockant ces informations. [...] [J]'estime, au regard de l'ensemble des considérations qui précèdent et des précautions qui ont été prises, que le législateur a pris toutes les mesures nécessaires afin de garantir, dans toute la mesure du possible, le traitement loyal et licite des données personnelles requises pour la délivrance d'un passeport. Il est indéniable que, par son attitude mesurée, il a ainsi procédé à une pondération équilibrée des intérêts de l'Union en présence ».
>
> (points 56 et 58)

100 Au surplus, la CNIL rappelait dans sa délibération de 2007 précitée que :

> « le traitement, sous une forme **automatisée et centralisée**, de données telles que les empreintes digitales, compte tenu à la

fois des caractéristiques de l'élément d'identification physique retenu, des usages possibles de ces traitements et des **risques d'atteintes graves** à la vie privée et aux libertés individuelles en résultant ne peut être admis que dans la mesure où des exigences en matière de sécurité ou d'ordre public le justifient.

« Or, la CNIL observe que le traitement mis en œuvre conserve les mêmes finalités que celles énoncées aux termes de l'article 18 du décret du 30 décembre 2005 faciliter les procédures d'établissement, de délivrance, de renouvellement, de remplacement et de retrait des passeports ainsi que prévenir, détecter et réprimer leur falsification et leur contrefaçon.

« A cet égard, la commission considère que, si légitimes soient-elles, les finalités invoquées ne justifient pas la conservation, au plan national, de données biométriques telles que les empreintes digitales et que les traitements ainsi mis en œuvre seraient de nature à porter une atteinte excessive à la liberté individuelle. »

101 Enfin, il est à relever que le Conseil d'État néerlandais, et d'autres tribunaux avant lui ont-ils jugé dans plusieurs décisions concordantes que la conservation centralisée des données personnelles constituait un moyen inapproprié pour empêcher la fraude aux titres d'identité [17].

102 **En l'espèce,** le décret attaqué prévoit la centralisation au sein d'un traitement unique des informations collectées lors des demandes de passeports ou de cartes nationales d'identité.

103 Il crée un traitement :

— dont les finalités, énoncées en son article 1er, demeurent identiques à celles du décret de 2005 et
— mettant en place une conservation, au plan national, de données biométriques telles que les empreintes digitales et que les traitements, qui cette fois-ci concernent la quasi-totalité de la population.

104 En cela déjà, le traitement créé en l'espèce doit être jugé contraire à l'article 6 de la loi n° 78-17 du 6 janvier 1978 comme l'a considéré la CNIL dans sa délibération de 2007 précitée.

105 Au-delà, l'objectif poursuivi par le décret, « procéder à l'établissement, à la délivrance, au renouvellement et à l'invalidation » de ces titres « ainsi que prévenir et détecter leur falsification et contrefaçon » (article 1er du décret attaqué), aurait pu être poursuivi tout aussi efficacement en prévoyant la conservation des ces informations sur le seul titre d'identité, tout en faisant disparaître les risques liés à leur centralisation.

17. Traduction libre de "the Court deems centralised storage of fingerprints an 'inappropriate means' to prevent identity fraud with travel documents", Privacy First, *Dutch Council of State : mass storage of fingerprints in databases unlawful*, Privacyfirst.eu, 25 mai 2016 disponible sur le https://www.privacyfirst.eu/court-cases/653-dutch-council-of-state-storage-of-fingerprints-in-databases-unlawful.html et Privacy First, *Hague Court of Appeal : central storage of fingerprints unlawful*, Privacyfirst.eu, 18 février 2014 disponible sur le https://www.privacyfirst.eu/court-cases/611-hague-court-of-appeal-central-storage-of-fingerprints-unlawful.html.

106 En ce sens, dans son avis publié le 12 décembre 2016, le CNNum met en avant l'ensemble des moyens existants qui auraient pu être mis en place par le pouvoir réglementaire pour atteindre l'objectif légitime recherché sans porter une atteinte aussi importante à la protection de la vie privée et au respect des données personnelles de la quasi-totalité de la population française [18].

107 Parmi l'ensemble des méthodes pouvant être utilisées, il relève que :

> « La solution de cachet électronique visible « 2D - Doc » 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 pla cé 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. »
>
> (CNNum, avis du 12 décembre 2016, p. 10)

108 Plus encore, la note d'analyse de l'INRIA publié le 1er février 2017 (prod. n° **7**) fait clairement apparaître que le décret attaqué manque de définir les conditions permettant à la fois d'assurer de la manière la plus adéquate la réalisation de l'objectif énoncé à son article 1er et de se prémunir des risques causés par le traitement de données qu'il instaure.

109 Ainsi, l'architecture instaurée par le décret est celle qui parmi toutes les solutions pouvant être envisagées permet le moins d'assurer l'objectif énoncé à l'article 1erdu décret, à savoir la lutte contre la fraude documentaire (cf. p. 9, tableau 2, du rapport d'audit). L'INRIA fait bien apparaître ce fait en classant les différentes architectures possibles de A0, la solution proposée par le décret, jusqu'à A4, à savoir une architecture comportant "un fichier biométrique centralisé et des titres électroniques équipés d'une carte à puce stockant les données d'état civil et biométriques du détenteur" avec un "fichier centralisé des données d'état civil ne [comportant] aucun lien vers les données biométriques". (*ibid.*)

110 Alors que l'architecture A0 instituée par le décret obtient un score de 2,5/6 et se trouve être la solution la moins adéquate, l'architecture A4 obtient elle un score de 5,5/6.

111 Cette architecture dite A4 est aussi une des deux architectures présentant moins de risques que l'architecture retenue par le décret. En effet, tel qu'expliqué plus tôt, une centralisation implique systématiquement, par nature, le risque que ces données soient utilisées pour d'autres finalités que celles ayant justifié leur collecte initiale.

112 **En conséquence,** le décret attaqué crée un traitement de données à ca-

18. Voir l'annexe 2 de l'avis du CNNum sur le fichier TES du 12 décembre 2016, pp. 27 et s.

ractère personnel excessif et non-adéquat au regard de sa finalité.

113 Si un doute existait quant au caractère proportionné d'un tel traitement au regard du droit de l'Union européenne applicable en l'espèce, votre formation serait tenue de transmettre la **question préjudicielle** suivante à la Cour de justice de l'Union européenne :

> « L'article 6, paragraphe 1, c) de la directive 95/46, lu à la lumière des articles 7, 8 et 52, paragraphe 1, de la Charte doit-il être interprété en ce sens qu'ils permettent une conservation centralisée des empreintes digitales et des photos faciales de la quasi-totalité de la population ? »

## 3.3. Sur la sécurité

114 **En droit,** l'article 17, paragraphe 1, de la directive 95/46 précitée dispose que :

> « 1. Les États membres prévoient que le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite. »

115 L'article 34 de la loi n° 78-17 du 6 janvier 1978 transposant cet article dispose que :

> « Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »

116 À ce titre, il est connu de l'association requérante que selon un courant de jurisprudence : « un manquement à l'obligation de sécurité est, en lui-même, "sans incidence sur la légalité de l'acte par lequel le traitement a été autorisé" *(CE, 19 juill. 2010, n° 317182 et n° 334014, F. et C. : JurisData n° 2010-012219 ; JurisData n° 2010-012472 ; JCP G 2010, 822. – M.-C. de Monteclerc, Le Conseil d'État donne une leçon d'informatique et libertés à l'Éducation nationale : AJDA 2010, p. 1454, n° 26 ; Gaz. Pal. 5 août 2010, n° 217, p. 31, obs. P. Graveleau ; Dr. adm. 2010, comm. 146, note P. Raimbault ; LPA 22 mars 2011, n° 57, p. 3, note M.-C. Rouault).* » [19]

117 Néanmoins, cette jurisprudence a montré ses limites avec la création du fichier ici en cause et n'est surtout plus conforme aux exigences imposées par la Cour de justice au regard de l'article 8 de la Charte des droits

19. Lexis Nexis, Fasc. 274-40.

fondamentaux de l'Union européenne tel qu'interprété par la Cour de justice de l'Union européenne.

118 Au premier titre, il a bien été démontré dans le cas du traitement créé par le décret attaqué que le ministère de l'intérieur ne pouvait raisonnablement être laissé sans encadrement réglementaire. Ce n'est qu'à la suite du débat de société que ce décret a créé que le ministère de l'intérieur s'est senti tenu de faire expertiser le système mis en place. Mais depuis lors aucun changement n'a été effectué ou rien du moins ne peut garantir la sécurité du traitement, quand bien même il serait avéré que l'architecture choisie est des moins sûre.

119 Ensuite, il est à relever que la Cour de justice a invalidé la directive 2006/24 notamment en ce que

> « l'article 7 de la directive 2006/24 ne [prévoyait] pas de règles spécifiques et adaptées à la vaste quantité des données dont la conservation est imposée par cette directive, au caractère sensible de ces données ainsi qu'au risque d'accès illicite à celles-ci, règles qui seraient destinées notamment à régir de manière claire et stricte la protection et la sécurité des données en cause, afin de garantir leur pleine intégrité et confidentialité. En outre, il n'a pas non plus été prévu une obligation précise des États membres visant à établir de telles règles. »
>
> (CJUE, g^de^ ch., 8 avr. 2014, *Digital Rights Ireland*, C-293/12, C-594/12, point 62)

120 C'est donc au sein de l'acte législatif créant le traitement que les conditions techniques de sécurité doivent être définies « de manière claire et stricte ».

121 À cet égard, il convient de relever que le RGDP rend explicite le fait que la sécurité des données à caractère personnel est un principal fondamental pour tout traitement. En effet, le principe de sécurité est désormais consacré au même rang que les principes de finalité déterminée ou de caractère adéquat et non-excessif des données traitées. L'article 5, 1(f), du RGDP dispose ainsi que des données à caractère personnel, et *a fortiori* des données biométriques, doivent être :

> « traitées de façon à **garantir une sécurité appropriée** des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, **à l'aide de mesures techniques ou organisationnelles appropriées** (intégrité et confidentialité) ; »

122 **En l'espèce,** comme cela a été démontré *supra*, le décret attaqué a manqué d'instaurer les garanties nécessaires à la sécurité des données traitées puisque l'architecture mise en place de par son application est une de celles portant le plus de risques pour les données concernées.

123 Etant rappelé, à l'instar de ce que fait l'INRIA dans sa note d'analyse (prod. n° **7**), que les risques causés par une éventuelle intrusion dans le fichier

auraient des conséquences irréversibles et extrêmement dommageables pour l'ensemble des personnes concernées, soit la quasi-totalité de la population française.

124 **En conséquence,** le décret attaqué doit être annulé en ce qu'il manque de définir les conditions de sécurité permettant de garantir l'intégrité du traitement en cause.

125 Si un doute existait quant à la nécessité, au regard du droit de l'Union européenne applicable en l'espèce, de définir dans le décret attaqué les conditions de sécurité du traitement qu'il institue, votre formation serait tenue de transmettre la **question préjudicielle** suivante à la Cour de justice de l'Union européenne :

> « L'article 17, paragraphe 1, de la directive 95/46, lu à la lumière de l'article 8 de la Charte doit-il être interprété en ce sens qu'il oblige l'acte par lequel le traitement a été autorisé à définir les conditions de sécurité dudit traitement afin de garantir l'intégrité des données conservées ? »

**Par ces motifs,** et tous autres à produire, déduire, suppléer, au besoin même d'office, l'association exposante conclut à ce qu'il plaise au Conseil d'État de :

— ANNULER le 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 ;
— METTRE À LA CHARGE de l'État la somme de 1 024 € sur le fondement de l'article L. 761-1 du code de justice administrative.

*À titre subsidiaire*

— SAISIR la Cour de justice de l'Union européenne des questions préjudicielles suivantes (ou toute autre formulation qu'il voudra bien lui substituer) :

> « L'article 6, paragraphe 1, c), de la directive 95/46 lu à la lumière des articles 7, 8 et 52, paragraphe 1, de la Charte doit-il être interprété en ce sens qu'il permet une conservation centralisée des empreintes digitales et des photos faciales de la quasi-totalité de la population ? »
>
> « L'article 17, paragraphe 1, de la directive 95/46, lu à la lumière de l'article 8 de la Charte doit-il être interprété en ce sens qu'il oblige l'acte administratif par lequel le traitement a été autorisé à définir les conditions de sécurité dudit traitement afin de garantir l'intégrité des données conservées ? »

Le 27 mars 2017 à Paris,

Pour La Quadrature du Net

Benjamin BAYART

# PRODUCTIONS AU SOUTIEN DE LA REQUÊTE

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, *JORF n° 0254 du 30 octobre 2016*
2. Statuts de La Quadrature du Net
3. Extrait de compte rendu de la consultation du Bureau de La Quadrature du Net
4. Délégation habilitant M. Benjamin Bayart à agir aux fins du présent recours
5. Avis du Conseil d'État du 23 février 2016 sur le traitement informatique relatif aux cartes nationales d'identité et aux passeports, *conseil-etat.fr, 4 novembre 2016*
6. Audit du système « Titres électroniques sécurisés » du 13 janvier 2013 par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et la Direction Interministérielle des Systèmes d'Inforation et de Communication de l'État (DINSIC), *interieur.gouv.fr, 17 janvier 2017*
7. Note d'analyse de l'INRIA du 1er février 2017 intitulée « Titres électroniques sécurisés : la centralisation des données biométriques est-elle vraiment inévitable ? — Analyse comparative de quelques architectures » par Claude Castelluccia et Daniel Le Métayer, *inria.fr, 15 février 2017*

# TABLE DES DÉLIBÉRATIONS CNIL ET DES JURISPRUDENCES