PROJET non définitif, voir
https://exegetes.eu.org/consultation-tes/

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**

II Intérêt à agir **4**

III Discussion – Légalité externe **6**

IV Discussion – Légalité interne **8**

1 Non-respect des exigences de proportionnalité imposées par le Conseil constitutionnel 8

1.1 Caractère particulièrement sensible des données . . . 9

1.2 Vaste ampleur du traitement 9

1.3 Caractéristiques techniques du traitement 9

1.4 Fins de police administrative ou judiciaire 12

2 Caractère excessif et non-adéquat du traitement de données personnelles institué par le décret 13

Productions au soutien de la requête **17**

Table des jurisprudences **18**

I. FAITS ET PROCÉDURE

1 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). 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).

2 Le but poursuivi par la mise en œuvre du décret attaqué est de faciliter les traitements relatifs aux titres d'identité et de prévoir notamment la conservation de l'ensemble des données à caractère personnel concernant les demandeurs de ces titres, y compris des données biométriques.

3 Comme le relève le Conseil d'État dans son avis sur le décret attaqué, « la création d'un tel traitement de données informatique avait déjà été envisagée dans le cadre d'une proposition de loi d'origine sénatoriale qui devait aboutir à la loi du 27 mars 2012 relative à la protection de l'identité mais elle avait été censurée par une décision du 22 mars 2012 du Conseil constitutionnel. » L'article 5 soumis au contrôle du Conseil constitutionnel prévoyait :

> « la création, dans les conditions prévues par la loi du 6 janvier 1978 susvisée, d'un traitement de données à caractère personnel facilitant le recueil et la conservation des données requises pour la délivrance du passeport français et de la carte nationale d'identité, destiné à préserver l'intégrité de ces données ; que, parmi celles-ci, figurent les données contenues dans le composant électronique sécurisé de la carte nationale d'identité et du passeport dont la liste est fixée à l'article 2 de la loi, qui sont, outre l'état civil et le domicile du titulaire, sa taille, la couleur de ses yeux, deux empreintes digitales et sa photographie. »
>
> (Conseil constit., 22 mars 2012, *Loi relative à la protection de l'identité*, 2012-652 DC, considérant 2)

4 Par des motifs rappelés *infra*, cet article 5 de la loi de 2012 avait été censuré par le Conseil constitutionnel du fait qu'il portait une atteinte disproportionnée au droit au respect de la vie privée.

5 Le décret attaqué dispose à 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 mentionnées et des passeports, ainsi que prévenir et détecter leur falsification et contrefaçon.

6 Il dispose à 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.

7 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 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.

8 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.

9 Depuis la décision du Conseil constitutionnel de 2012, deux changements de circonstances majeurs doivent nécessairement être pris en compte.

10 Premièrement, les problématiques de sécurité informatique se sont fortement accentuées.

11 Alors que pas une semaine ne se passe sans qu'il soit question d'attaques informatiques ou de menaces d'intrusions malveillantes, [1] le fait de créer un traitement unique de données biométriques de la quasi-totalité de la population met en jeu de manière disproportionnée la sécurité collective.

12 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 qu'avec l'essor de ces technologies dans la vie commune s'accompagne nécessairement des risques de mésusage de ces données biométriques. [2]

1. 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

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

13 C'est pourquoi 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.

II. INTÉRÊT À AGIR

14 L'intérêt à agir de l'association requérante est certain en l'espèce.

15 D'après l'article 3 de ses statuts, 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. »

16 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.

17 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.

18 La Quadrature du Net a manifesté très tôt son opposition au décret attaqué [3].

3. 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

Le 14 novembre dernier, l'association publiait un communiqué de presse de l'Observatoire des libertés et du numérique, dont elle fait partie, dans lequel il était demandé au gouvernement l'abrogation du décret.

19 Par ailleurs, depuis 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

20 **Au préalable**, il convient de relever que le traitement TES a été créé par un acte réglementaire là où le législateur avait considéré en 2012 que la création d'un tel traitement relevait de son pouvoir. Aussi, l'article 5 de la loi de 2012 ayant été censuré, aucune base juridique ne peut être trouvée au décret attaqué dans cette loi. La seule base légale pouvant être trouvée dans le corpus législatif figure à l'article 27 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (« Loi Informatique & Libertés »).

21 Dans son avis, le Conseil d'État relevait à titre conclusif que :

> « S'agissant enfin du niveau hiérarchique de la norme requise, un tel fichier, dès lors qu'il respecterait, dans les conditions qui précèdent, les garanties fondamentales prévues notamment par l'article 6 de la loi du 6 janvier 1978, pourrait être créé par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés, ainsi que le prévoit l'article 27 de la même loi s'agissant des traitements contenant des données biométriques nécessaires à l'authentification des personnes. Toutefois, compte tenu de l'ampleur du fichier envisagé et de la sensibilité des données qu'il contiendrait, il n'est pas interdit au Gouvernement, s'il le croit opportun, d'emprunter la voie législative. »

22 **En droit**, au titre de l'article 27 de la loi Informatique & Libertés, sont autorisés par décret en Conseil d'État les traitements de données à caractère personnel 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.

23 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)

24 **En l'espèce**, il ne fait pas débat que le décret attaqué est soumis aux conditions de l'article 27 de la Loi Informatique & Libertés. 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 devenait un décret, 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 ».

25 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. Comme il sera démontré *infra* les modifications apportées au projet de décret et qui ont 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.

26 Il en résulte nécessairement que le décret attaqué a été adopté au terme d'une **procédure irrégulière**, dès lors que la version définitive du texte finalement publiée ne correspond pas à la version soumise pour avis à la Section de l'Intérieur du Conseil d'État.

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

IV. DISCUSSION – LÉGALITÉ INTERNE

28 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, d'une part, les conditions imposées par le Conseil constitutionnel dans sa décision n° 2012-652 DC du 22 mars 2012 (cf. section 1) et, d'autre part, celles imposées par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (« Loi Informatique & Libertés »), telle qu'interprétée notamment par la Cour de justice de l'Union européenne dans son arrêt *Schwartz* du 17 octobre 2013 (cf. section 2 page 13).

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

29 **En droit**, suivant la jurisprudence du Conseil constitutionnel, la création d'un traitement de données à caractère personnel facilitant le recueil et la conservation des données requises pour la délivrance de papiers d'identité porte une atteinte au droit au respect de la vie privée « 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, § 10-11) lorsque sont réunies les conditions suivantes :

1. les données traitées sont particulièrement sensibles, ce qui est le cas s'agissant de **données biométriques** susceptibles d'être rapprochées de traces physiques laissées involontairement par la personne ou collectées à son insu ;
2. le traitement est d'une vaste ampleur, ce qui est encore le cas s'agissant d'un traitement destiné à recueillir les données relatives à la **quasi-totalité de la population** de nationalité française ;
3. les caractéristiques techniques de ce traitement **permettent son interrogation à d'autres fins que la vérification de l'identité** d'une personne, et
4. la consultation ou l'interrogation de ce fichier sont 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**.

30 Si un traitement tel que celui qu'avait voulu créer le législateur en 2012 peut être créé par le pouvoir réglementaire, il faut alors considérer que lui aussi est soumis aux exigences énoncées par le Conseil constitutionnel. Toute interprétation contraire de la Loi Informatique & Libertés reviendrait à priver de garanties les exigences constitutionnelles fixées par l'article 34 de la Constitution, telles qu'interprétées par le Conseil constitutionnel dans sa décision précitée concernant un traitement analogue à celui du décret attaqué.

31 **En l'espèce,** le décret attaqué prévoit, à 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 ».

32 Pour les raisons développées ci-après, ce décret, bien que justifié par un motif d'intérêt général identique à celui poursuivi par le législateur en 2012, n'apporte pas les garanties de proportionnalité imposées par le Conseil constitutionnel dans sa décision de 2012. En effet, les quatre conditions alors réunies en 2012 le sont encore en l'espèce.

1.1. Caractère particulièrement sensible des données

33 Les **données biométriques** contenues dans ce fichier 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).

1.2. Vaste ampleur du traitement

34 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.

1.3. Caractéristiques techniques du traitement

35 Les caractéristiques techniques de ce traitement **permettent son interrogation à d'autres fins que la vérification de l'identité** d'une personne.

En effet, les modalités techniques prévues par le décret attaqué n'offrent pas les garanties de nature à limiter l'interrogation de ce traitement aux seules fins de vérification de l'identité d'une personne.

36 Dans son avis du 23 février 2016 sur le traitement informatique relatif aux cartes nationales d'identité et aux passeports, le Conseil d'État a détaillé les caractéristiques techniques d'un fichier de nature à assurer que celui-ci 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 :

- *« les données biométriques et les données indiquant l'identité de la personne seraient conservées dans des bases différentes »* ;
- *« l'accès s'effectuerait au moyen d'un code et d'une carte à puce individuelle permettant d'identifier l'agent »* afin de garantir que seuls les agents autorisés puissent interroger le fichier ;
- *« il serait impossible d'effectuer une recherche à partir des données biométriques, celles-ci n'étant accessibles qu'à partir des données d'identité »*.

37 Or, force est de constater que les caractéristiques techniques du traitement prévues par le décret attaqué n'apportent pas les garanties suffisantes, en ce que :

- les données biométriques et celles identifiant la personne ne sont pas conservées dans des bases différentes ;
- le fichier peut être interrogé ou consulté par d'autres moyens que par un code et une carte à puce individuelle remis à chaque agent.

38 Quant à l'impossibilité d'effectuer une recherche, 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 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.

39 Au contraire, à travers la création d'un traitement unique, cette recherche est rendue 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 telle utilisation de ce fichier — peu importe que certaines mesures puissent rendre une telle utilisation plus difficile.

40 [FIXME : point à développer ici suivant le commentaire du Conseil constitutionnel qui semble penser qu'un fichier avec "'lien faible" serait suffisant pour pallier les problèmes techniques]

1. Le lien à sens unique n'est pas efficace

41 Quand une base de données est structurée à sens unique, comme c'est le cas en l'espèce [4] (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.

2. Le stockage des données complètes n'est pas utile pour identifier

42 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 de gens pourront produire de tels faux. La simple existence de ces données crée un risque.

43 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, et pour leur sécurité.

3. Le stockage lui-même n'est pas utile à l'identification

44 L'objectif est de contrôler plusieurs points :

— que les donneés biométriques de l'individu correspondent à celles stockées sur la carte ;
— que cette carte est bien émise par les services de l'État.

45 Ce double objectif peut être atteint par l'utilisation d'une signature électronique sécurisée (par exemple prévue par le Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, par l'article 1367 du Code civil (anciennement 1316-4), et telle que détaillée par le décret 2001-272) qui apporte la preuve vérifiable que le titre a bien été émis par la puissance publique et n'a pas été modifié ultérieurement.

4. Le stockage des données, même partiel, est peu utile

46 Le seul intérêt pratique du stockage des données biométriques, même d'un stockage partiel, si l'on exclut la recherche depuis une donnée biométrique, et de pouvoir ré-émettre sans délai un duplicata du titre sécurisé sans devoir

4. Article 2, II, du décret attaqué.

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.

1.4. Fins de police administrative ou judiciaire

47 Le décret attaqué 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] » ; de sorte que, ainsi, le décret autorise la consultation ou l'interrogation de ce fichier 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.

48 Bien que les dispositions de l'article 4 prévoient d'en exclure l'accès aux images numérisées des empreintes digitales, il faut relever que ne sont nullement exclues les images numérisées du visage (lesquelles constituent également des données biométriques permettant l'identification des personnes concernées, notamment de manière automatisée par l'usage de technologies de reconnaissance faciale).

49 **En conséquence,** le décret attaqué prévoit la création d'un fichier comprenant des données biométriques relatives à la quasi-totalité de la population, sans toutefois empêcher que ce fichier ne soit utilisé à d'autres fins que la vérification d'identité mais, au contraire, en permettant que certaines données biométriques puissent, à des fins de police administrative et judiciaire, être utilisées afin de rattacher à des personnes identifiées des informations collectées à leur insu.

50 Dès lors, le décret attaqué ne respecte pas les garanties légales nécessaires pour assurer la proportionnalité exigée par la jurisprudence du Conseil constitutionnel, telle que précisée notamment par le Conseil d'État dans son avis. Il porte au contraire une atteinte manifeste aux droits à la vie privée et à la protection des données personnelles de la quasi-totalité de la population, tel que garantis par la Loi Informatique & Libertés.

51 En outre, le traitement automatisé prévu par le décret attaqué n'est pas licite au sens de l'article 6 de la Loi Informatique & Libertés.

2. Caractère excessif et non-adéquat du traitement de données personnelles institué par le décret

52 **En droit,** un traitement soumis à la Loi Informatique & Libertés, pour être licite, ne peut porter que 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°). Cette disposition transpose notamment l'article 6, paragraphe 1, c), de la directive 95/46, auquel l'article 6, 3° de la Loi Informatique & Libertés ne saurait être contraire (CJUE, 20 mai 2003, *Rundfunk*, C-465/00, C-138/01 et C-139/01, § 101).

53 L'interprétation des dispositions de la directive 95/46 et de l'article 8 de la Charte des droits fondamentaux de l'Union européenne faite par la Cour de justice à l'occasion de l'examen de la validité du règlement CE n° 2252/2004 [5] est éclairante. Ce règlement établit les normes de sécurité et les éléments biométriques des passeports et dispose que les données concernées sont conservées sur un support de stockage intégré dans le passeport et hautement sécurisé (article 1er, paragraphe 2). Dans cette affaire préjudicielle, la juridiction de renvoi questionne la validité du règlement eu égard au *« 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). La Cour de justice a considéré :

> « Cependant, il importe de rappeler que l'article 1er, paragraphe 2, du règlement n° 2252/2004 ne prévoit la conservation des empreintes 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 ou à l'utilisation de ces dernières à d'autres fins [...].
>
> « 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

5. 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) no 444/2009 du Parlement européen et du Conseil, du 6 mai 2009 (JOUE L 142, p. 1, et rectificatif JO L 188, p. 127).

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)

54 Si la Cour de justice a constaté que la collecte et le stockage des empreintes digitales n'allaient pas au-delà du nécessaire pour la réalisation du but tenant à la protection des passeports contre leur utilisation frauduleuse, *a contrario* la centralisation au sein d'une même base de données ou l'utilisation de cette base de données à d'autres fins ne saurait être limitée au strict nécessaire eu égard notamment aux **risques liés à une telle centralisation**.

55 **En l'espèce,** le décret attaqué prévoit de centraliser au sein d'un traitement unique les informations collectées lors des demandes de passeports ou de cartes nationales d'identité. L'objectif qu'il annonce ainsi poursuivre est 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 ».

56 Cet objectif aurait pu être poursuivi tout aussi efficacement en prévoyant la conservation des ces informations sur le seul titre d'identité, tout en faisant disparaître tout risques liées à leur centralisation.

57 Ainsi, 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 (cf. annexe 2 de l'avis du CNNum du 12 décembre 2016, pp. 27 et s.).

58 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)

59 En effet, tel qu'expliqué plus tôt, une telle centralisation implique systématiquement, par nature, le risque que ces données soient utilisées pour d'autres finalités que celles ayant justifié leur collecte initiale.

60 De plus, en application du règlement n° 2252/2004, les informations ainsi centralisées doivent déjà être conservées au sein des passeports. Au regard de l'objectif annoncé du décret attaqué, aucune circonstance ne saurait expliquer la nécessité d'en conserver une copie ailleurs.

61 **En conséquence,** la centralisation prévue par le décret attaqué constitue un traitement de données à caractère personnel excessif et non-adéquat au regard de sa finalité.

62 **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 euros sur le fondement de l'article L. 761-1 du code de justice administrative.

63 Avec toutes conséquences de droit.

Le FIXME (date limite fin 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, *http://www.conseil-etat.fr, 4 novembre 2016*

TABLE DES JURISPRUDENCES

CJUE, 20 mai 2003, *Österreichischer Rundfunk e. a.*, C-465/00, C-138/01 et C-139/01

CJUE, 4e ch., 17 oct. 2013, *Michael Schwarz c. Stadt Bochum*, C-291/12

Conseil constit., 22 mars 2012, *Loi relative à la protection de l'identité*, 2012-652 DC

Conseil d'État, 16 oct. 1968, *Union nationale des grandes pharmacies de France*, nos 69186, 69206 et 70749, Rec. p. 488

Conseil d'État, 2 mai 1990, *Joannides*, no 86662