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

Mémoire en réplique

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 son président M. Benjamin Bayart, dûment habilité à agir en justice ;
Tél. : 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. RAPPEL DE LA 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).

2 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, suivi le 27 mars 2017 du dépôt d'un mémoire complémentaire.

3 Le 18 août 2017, le ministère de l'Intérieur communiquait son mémoire en défense, en réponse aux arguments de la requérante et des autres parties requérantes ou intervenantes.

II. DISCUSSION

4 La réponse du gouvernement ne remet pas en cause l'argumentation précédemment articulée par la requérante, dont elle souhaite expressément conserver l'entier bénéfice. Néanmoins, cette réponse appelle plusieurs précisions techniques opportunes qui sont exposées au travers des observations suivantes.

1. Intérêt à agir

5 Selon le ministre de l'Intérieur, le décret attaqué ne se rapporte ni à Internet, ni au développement des nouvelles technologies, contrairement à l'objet social de La Quadrature du net.

6 Sur ce point, l'association requérante renvoie à ses précédentes écritures.

7 Partant, l'association requérante bénéficie d'un intérêt à agir certain contre le décret litigieux.

2. Légalité externe

2.1. Sur la régularité de la procédure

8 Le ministre de l'Intérieur écarte le moyen selon lequel le projet de décret soumis à avis du Conseil d'État serait différent de celui qui a été adopté. Il affirme en ce sens que l'avis auquel il convient de se référer aurait été délibéré en séance du 29 septembre 2016, dont il prétend joindre une copie qui démontrerait l'identité des deux textes.

9 La réponse du ministère ne convainc pas, et ce, à deux égards.

10 D'une part, il n'existe aucune preuve de l'existence d'un tel avis, qui ne correspond pas à ce qui est invoqué par le Conseil d'État lui-même (cf. section 2.1.1 page suivante). D'autre part, si cet avis existe bel et bien, son élaboration n'a pu respecter les conditions d'adoption d'un décret en Conseil d'État et rend de ce fait la procédure irrégulière (*cf.* section 2.1.2 page suivante).

2.1.1. Sur l'inexistence de cet avis

11 **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'authentication ou au contrôle de l'identité des personnes.

12 **En l'espèce**, le ministre de l'Intérieur déclare dans sa réponse qu'un tel avis a été délibéré par la section de l'intérieur du Conseil d'État, lors de la séance du 29 septembre 2016.

13 Cependant, cette prétention est infirmée par les propres déclarations du Conseil d'État.

14 En effet, le 4 novembre 2016, était publié sur le site de l'institution un avis accompagné du sous-titre « *Le Gouvernement a décidé de rendre public l'avis du Conseil d'État sur le traitement informatique relatif aux cartes nationales d'identité et aux passeports* » [1]. Il s'agit de celui précité en date du 23 février 2016, et aucune référence n'est faite quant à un autre avis rendu par le Conseil d'État qui serait daté du 29 septembre 2016.

15 À l'inverse de cet avis du 23 février, l'avis du 29 septembre 2016 n'a pas été rendu public. Contrairement à ce qu'affirme le gouvernement, il n'en joint pas la minute dans sa réponse. Le document transmis n'est en réalité qu'une copie du projet de décret, certes identique au décret adopté, mais non assorti de délibérations ou commentaires, dont il n'existe — dès lors — aucune trace.

16 Dans l'hypothèse où cet avis aurait été réellement délibéré, il est demandé au Conseil d'État de le communiquer aux parties et intervenants, pour la bonne poursuite de la procédure, conformément aux règles garantissant le procès équitable.

17 Un refus ne pourrait être interprété que comme un indice corroborant l'inexistence de cet avis, qui renverrait à utiliser l'avis rendu le 23 février, tel qu'il a été soutenu dans le mémoire complémentaire des exposantes (*cf* p.6 du mémoire complémentaire de la requérante).

18 En définitive, si l'avis n'existe pas, les arguments soulevés par la requérante dans son précédent mémoire quant à la légalité interne demeurent pertinents.

2.1.2. Sur le caractère irrégulier de l'avis

19 **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'authentication ou au contrôle de l'identité des personnes.

20 En vertu de cette même disposition, ce décret doit être pris **après avis**

1. http ://www.conseil-etat.fr/Decisions-Avis-Publications/Avis/Selection-des-avis-faisant-l-objet-d-une-communication-particuliere/Traitement-informatique-relatif-aux-cartes-nationales-d-identite-et-aux-passeports

motivé et publié de la Commission nationale de l'informatique et des libertés.

21 Afin de présenter l'ensemble des règles, principes et méthodes qui doivent être observés lors de la préparation de textes normatifs (lois, ordonnances, décrets, arrêtés), le Conseil d'État et le Secrétariat général du gouvernement ont conçu un guide de légistique [2], selon lequel il est précisé que le Conseil d'État doit être saisi **après les autres organismes** dont la consultation est requise ou souhaitée ; il ne peut statuer qu'au vu des avis rendus par les organismes dont la consultation est obligatoire (Guide de légistique, 2.4.2).

22 En outre, le défaut de consultation du Conseil d'État dans le cadre d'une telle procédure *"entraîne l'illégalité des actes administratifs dont le projet devait lui être obligatoirement soumis"* (CE, 17 juillet 2013, Syndicat national des professionnels de santé au travail, n°358109). Il en est de même lorsque la consultation est incomplète et **tardive** (CE, Ass., 9 juin 1978, *SCI Boulevard Arago*, n° 02403, Rec. p. 237).

23 **En l'espèce**, dans sa réponse, le ministre de l'Intérieur déclare qu'un tel avis a été délibéré par la section de l'intérieur du Conseil d'État lors de la séance du 29 septembre 2016.

24 Or, le 29 septembre 2016 correspond également à la date où la Commission nationale de l'informatique et des libertés a rendu sa délibération n° 2016-292 portant avis sur le projet de décret autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité (saisine n° 1979541), c'est-à-dire le décret attaqué.

25 Compte-tenu de la proximité chronologique de ces avis, deux hypothèses sont possibles.

26 Soit la section de l'intérieur n'a pas pu connaitre de cette délibération de la CNIL sous sa forme définitive, et son avis est donc nécessairement incomplet.

27 Soit la section de l'intérieur a pu prendre connaissance de cette délibération et aurait donc rendu son avis le même jour – cette supposition étant, néanmoins, difficilement concevable.

28 En effet, la célérité d'une telle procédure ne peut que donner lieu à un examen non exhaustif des recommandations de la CNIL, et ne satisferait donc pas à la nécessité de bonne confection et qualité de la loi.

29 Lorsque le Conseil d'État est consulté, de manière facultative ou obligatoire, un rapporteur est d'abord chargé de préparer un avis sur le projet de texte, lequel est ensuite examiné en section. Ces deux étapes auraient donc été réalisées dans la même journée, ce qui parait peu concevable au regard de l'ampleur d'un tel travail.

30 De même, dans son rapport public de l'année 2011, le Conseil d'État regrettait la dégradation des conditions dans lesquelles il était saisi, notamment quant à la brièveté des délais :

2. https ://www.legifrance.gouv.fr/Droit-francais/Guide-de-legistique

> « De tels délais ne permettent pas d'effectuer les recherches et vérifications approfondies qu'exige l'examen des textes, notamment au regard des normes constitutionnelles, de celles de l'Union Européenne ou des engagements internationaux, ni de procéder dans des conditions satisfaisantes aux échanges nécessaires avec les représentants du Gouvernement. »

31 Si cette critique visait l'adoption des lois de finance, le même raisonnement s'applique à toute autre norme dont la confection implique un examen par le Conseil d'État, *a fortiori* lorsqu'il s'agit de libertés individuelles nécessitant une protection particulière.

32 De manière plus concrète, une telle hypothèse ne correspond pas à la pratique habituelle du Conseil d'État lorsque celui-ci fait état d'un délai d'examen se situant entre un et deux mois (d'après les statistiques publiées chaque année dans le rapport public du Conseil d'État quant aux délais moyens d'adoption des décrets réglementaires par les sections administratives).

33 L'avis du Conseil d'État n'a ainsi pu tenir compte de la délibération de la CNIL de manière effective.

34 Ce point conforte la requérante lorsqu'elle soutient que le décret attaqué a été adopté au terme d'une procédure irrégulière. Or, ce vice de procédure doit être regardée comme «susceptible d'exercer une influence sur le sens de la décision ou [de] priv[er] les intéressés d'une garantie» (*cf.* CE, Ass., 23 décembre 2011, *Danthony*, req. n°335033, Rec. p. 649) et doit donc emporter l'annulation de l'acte litigieux.

35 En effet, l'avis prononcé par la CNIL émane d'une autorité experte et indépendante, et permet de souligner les éventuelles ingérences dans le droit à la protection des droits et libertés fondamentaux des citoyens.

36 À cet égard, déjà, l'annulation doit être prononcée.

3. Légalité interne

37 À titre liminaire, il convient de rappeler, **en droit**, « *que l'ingérence dans l'exercice du droit de toute personne au respect de sa vie privée que constituent la collecte, la conservation et le traitement, par une autorité publique, d'informations personnelles nominatives, ne peut être légalement autorisée que si elle répond à des finalités légitimes et que le choix, la collecte et le traitement des données sont effectués de manière adéquate et proportionnée au regard de ces finalités* » (CE, Ass., 26 octobre 2011, *Association pour la promotion de l'image et autres*, req. n°317827, Rec. p.506).

38 Or, la mesure attaquée ne saurait remplir de telles exigences.

39 La mise en place du fichier TES dans les modalités décrites par le décret attaqué ne saurait être regardée comme nécessaire et adéquate, et ne s'avère pas davantage proportionnée.

3.1. Sur la centralisation du fichier

40 D'emblée, il convient de constater que le caractère centralisé du fichier n'est nullement nécessaire.

41 Tel qu'il a été relevé lors des écritures précédentes (mémoire complémentaire, § 98 ss.), la centralisation de fichiers est unanimement déconseillée par les acteurs industriels comme institutionnels. C'est d'autant plus exact que d'autres architectures techniques auraient pu être retenues afin de remplir l'objectif visé par le fichier TES.

42 En ce qui concerne les réserves des acteurs institutionnels, la requérante les a déjà soulignées (voir les rapports de l'ANSSI et de l'INRIA déjà produits, mémoire complémentaire p. 14 et 15).

43 Il n'est pas inutile de se pencher sur les avis publiés à l'échelle internationale. En 2004 déjà, le G29 [3] publiait dans son "Opinion sur le Règlement 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" le passage suivant :

> « Il y a un risque que la mise en place d'une base de donnée centralisée contenant les données personnelles, et particulièrement les données biométriques, de tous les citoyens (européens) se fasse en violation du principe basique de proportionnalité. Toute base de donnée centralisée augmenterait les risques d'emplois abusifs ou détournés.» [4]

44 Cet avis est loin d'être isolé. Par exemple, le Commissariat à la protection de la vie privée du Canada a publié une recommandation sur ce sujet en 2011, affirmant que :

> « Dans la mesure du possible, plutôt que d'être stockés dans une base de données centrale, les renseignements biométriques devraient toujours être stockés localement, soit dans des ordinateurs personnels ou des dispositifs de sécurité, tels que des cartes à puce, qui sont en la possession des utilisateurs ultimes. Le stockage dans une base centrale augmente le risque de voir des données perdues ou encore comparées de façon inappropriée entre divers systèmes. Le stockage local, par contre, permet aux personnes d'exercer un meilleur contrôle de leurs renseignements personnels» [5].

3. Groupe de travail Article 29 sur la protection des données, organe consultatif européen indépendant sur la protection des données et de la vie privée rassemblant les autorités nationales indépendantes chargées de la protection des données personnelles.

4. passage librement traduit par nos soins, rapport accessible en ligne sur https://www.bfdi.bund.de/SharedDocs/Publikationen/EU/Art29Gruppe/WP112_en.pdf?___blob=publicationFile&v=1

5. Source en ligne : <https ://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/ renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/gd_bio_201102/>.

45 Signalons, en outre, les craintes de fuite de données, qui sont loin d'être infondées. En 2015, une brèche majeure à l'Office of Personnel Management des États-Unis a eu pour conséquence un vol de données concernant 21,5 millions de personnes employées sous contrat avec le gouvernement fédéral américain. Les données contenaient également les jeux d'empreintes de 5,6 millions d'employés, parmi lesquels des employés diplomatique et des agents sous couverture [6].

46 Dans un article commentant la faille, le spécialiste en sécurité informatique fréquemment invité du Congrès américain en tant qu'expert, Bruce Schneier, conclut ainsi :

> « Nous devrions être sceptiques de toute tentative de stocker [les données biométriques] en masse, que ce soit par des gouvernements ou des entreprises. Nous avons besoin de nos donnés biométriques pour nous authentifier, et nous ne pouvons pas nous permettre de nous les faire prendre par des hackers. ». [7]

47 Bruce Schneier est un spécialiste en sécurité de renommée internationale, membre du conseil d'administration de la principale organisation américaine de défense des droits fondamentaux sur Internet, l'Electronic Frontier Foundation, conseiller spécial pour IBM Security et auteur de plusieurs algorithme de chiffrement utilisés dans l'industrie.

48 En l'espèce, le rapport de l'ANSSI et de la DINSIC faisant état de plusieurs "vulnérabilités de gravité variable" découvertes durant le test d'intrusion réalisé au cours de l'audit (*3.5 Test d'intrusion*, p. 9 du rapport de l'ANSSI du 13 janvier 2017 précité par la requérante, pièce-jointe n° 6 du mémoire complémentaire) ne peut que renforcer les craintes d'une possible intrusion.

49 Pour contenir les risques en cas de faille menant à une fuite de données, le décret attaqué prévoit que les données biométriques soient stockées de manière chiffrée. Il est important de souligner qu'une telle mesure ne permet au mieux que de temporiser les conséquences d'une faille, en retardant l'exploitation des données.

50 En effet, toute méthode de chiffrement cryptographique, même bien implémentée, doit être considérée comme ayant une durée de vie utile limitée dans le temps (appelée "algorithm security lifetime" ou ASL [8]). Cette limitation importante est une conséquence normale des progrès constants aussi bien

6. Voir « Millions of US government workers hit by data breach » publié sur BBC News, le 5 juin 2015.

7. Traduction libre de "*We should be skeptical of any attempts to store [biometrics] data en masse, whether by governments or by corporations. We need our biometrics for authentication, and we can't afford to lose them to hackers.*" Accessible en ligne : https://www.schneier.com/blog/archives/2015/10/stealing_finger.html.

8. ASL. Définition disponible en ligne sur le site du *National Institute of Standards and Technology*, ou *NIST* (qu'on pourrait traduire par « Institut national des normes et de la technologie »), une agence du département du Commerce des États-Unis. Son but est de promouvoir l'économie en développant des technologies, la métrologie et des standards de concert avec l'industrie. Cette agence a pris la suite en 1988 du National Bureau of Standards fondé en 1901 avec substantiellement les mêmes missions. Définition disponible en ligne https://csrc.nist.gov/Glossary/?term=2884.

en termes de performances du matériel informatique (qui rend possible des attaques auparavant jugées trop coûteuses car trop longues) que dans le domaine de la cryptographie (de nouvelles techniques sont découvertes pour affaiblir les méthodes de chiffrement et en faciliter l'attaque).

51 À titre illustratif, l'ENISA, l'Agence Européenne chargée de la sécurité des réseaux et de l'information (aussi qualifiée d'"Agence Européenne de cyber-sécurité"), a proposé dans son rapport de 2014 intitulé "*Algorithms, key size and parameters report*" ("Rapport sur les algorithmes, les tailles de clés et paramètres") [9] une fourchette de dix à cinquante ans pour la durée de vie utile des algorithmes de chiffrement modernes.

52 Dans la majorité des cas où le chiffrement est utilisé pour le stockage de données sensibles, telles que les mots de passe ou les données bancaires, une telle garantie est suffisante. En cas de fuite de données, elle laisse aux utilisateurs qui en sont informés un temps amplement suffisant permettant d'entreprendre les démarches pour rendre obsolètes les données compromises.

53 Cependant, une différence majeure concernant les données biométriques par rapport à d'autres types de données sensibles est *qu'elles ne peuvent jamais être modifiées*. En effet, s'il est facile de changer un mot de passe et s'il est possible de changer de numéro de compte bancaire, il est en revanche impossible de changer d'empreintes digitales. Il est donc impossible à un individu dont les données biométriques ont été compromises d'entreprendre une quelconque démarche pour se prémunir de leur exploitation, si ce n'est de renoncer autant que possible à leur usage.

54 Il apparaît donc que, même en utilisant des techniques de cryptographie modernes, la création d'une base de données biométriques centralisée et à grande échelle est une source de risques graves pour les individus concernés.

55 En faisant l'hypothèse très optimiste que l'algorithme de chiffrement retenu ait une durée de vie utile (ASL) élevée, par exemple de quarante ans, et qu'il est mis en œuvre sans la moindre erreur, une faille de sécurité amenant à une fuite de données aurait pour conséquence qu'une part importante des individus concernés devra s'attendre à ce que leurs données biométriques soient compromises dans les décennies qui suivent, et donc de leur vivant. [10]

56 Concernant le domaine industriel, la démocratisation de l'usage des données biométriques pour les dispositifs type smartphones s'est accompagnée d'un soin tout particulier à garantir que le stockage de ces données se fasse *exclusivement* au niveau de l'appareil.

9. Rapport disponible en ligne https://www.enisa.europa.eu/publications/algorithms-key-sizes-and-parameters-report/.

10. On considère ici une durée de vie théorique de l'algorithme de chiffrement, supposant une mise en œuvre parfaite. La durée de vie effective de la technique peut être drastiquement diminuée suite à la moindre erreur dans son implémentation ou son utilisation. Par exemple une simple faiblesse dans la qualité du générateur de nombres aléatoires utilisé au moment du chiffrement des données réduit considérablement l'ASL. Une simple erreur de paramétrage, dans le cas d'un stockage centralisé des données, se répercute sur l'ensemble de la base. À l'opposé, la même erreur de paramétrage sur un système décentralisé n'a d'effet que sur les données des personnes utilisant ce système affaibli.

57 C'est ainsi que *Google* impose aux fabricants désirant bénéficier de la certification Android des conditions strictes concernant le traitement des données biométriques. En effet, le traitement de ces données doit être entièrement réalisé sur le dispositif lui-même, dans un environnement sécurisé isolé du reste de l'appareil. Aucun système extérieur à cet environnement ne doit pouvoir lire les données biométriques, même s'il dispose d'un accès privilégié à l'appareil. [11]

58 Une telle démarche n'est pas isolée, puisque *Apple* fournit des garanties similaires.

59 Concernant les dispositifs de type iPhone, les données biométriques sont traitées au sein d'une "enclave sécurisée", interne à l'appareil, sans que les données soient centralisées. Concernant le traitement d'une empreinte digitale, *Apple* précise notamment que :

> "*elle ne peut être accédée par le système d'exploitation de l'appareil ou par aucune application tournant dessus. Elle n'est* ***jamais stockée sur les serveurs d'Apple, elle n'est jamais sauvegardée dans iCloud, ou nulle par ailleurs****, et elle ne peut pas être utilisée pour établir des correspondances vers d'autres bases d'empreintes*". [12]

60 Il convient donc de constater que, dans le domaine de la téléphonie mobile, le standard de sécurité pour les données biométriques des utilisateurs consiste en un stockage directement sur le dispositif afin de privilégier la sécurité de l'utilisateur. Celui-ci suit une logique de décentralisation afin d'éviter les risques auxquels seraient exposées ces données en cas de faille d'un dispositif centralisé.

61 Devant ces alternatives, qui poursuivent aussi efficacement le même objectif tout en réduisant drastiquement les risques d'atteinte à la vie privée, il ne peut qu'être conclu que la centralisation, au sein d'un fichier, de données d'une sensibilité telle que celle des données biométriques ne saurait être regardé comme nécessaire.

62 À cet égard, déjà, l'annulation du décret est acquise.

3.2. Sur les risques techniques de dévoiement du fichier

63 Le ministre de l'Intérieur prétend qu'il serait impossible d'identifier une personne à partir de ses seules données biométriques grâce à la séparation des bases de données et à la nature du lien unidirectionnel permettant de basculer de l'une vers l'autre. Il ajoute que les interconnexions de fichiers sont très limitées (Interpol, Schengen).

11. Source en ligne : https://source.android.com/security/authentication/fingerprint-hal#implementation_guidelines.

12. Traduction libre de : "It can't be accessed by the OS on your device or by any applications running on it. It's never stored on Apple servers, it's never backed up to iCloud or anywhere else, and it can't be used to match against other fingerprint databases." Source en ligne : https://support.apple.com/en-us/HT204587.

64 Afin de démontrer qu'il a satisfait aux exigences de l'article 34 de la loi du 6 janvier 1978, imposant de prendre toutes précautions utiles pour préserver la sécurité des données, le ministère de l'intérieur fait état de l'audit de sécurité réalisé par l'ANSSI et la DINSIC, remis le 16 janvier 2017. Celui-ci conclut que le système TES serait « compatible avec la sensibilité des données qu'il contient », et formule des recommandations que le ministère de l'intérieur affirme avoir mis en œuvre, lui permettant de définir une stratégie de sécurisation afin de lutter contre deux types de risques, le « risque interne », c'est-à-dire le détournement de finalités du traitement du fichier (développé ci-dessous) et le « risque externe » concernant le risque de piratage et d'intrusion malveillante (déjà traité p. 25, §110, du mémoire complémentaire de la requérante).

65 Le ministre soutient dans sa réplique (p. 31 de la réplique du ministre de l'intérieur) que la robustesse du lien unidirectionnel, assurant que le fichier ne soit utilisé qu'à des fins d'authentification et non d'identification, constitue une garantie fiable et suffisante.

66 Or, il n'en est rien.

67 Ces mécanismes de sécurité constituent l'élément central de l'irrégularité des mesures prévues par le décret mettant en place le fichier. Ils ne concernent pas uniquement l'article 34 de la loi de 1978 mais, plus largement, la base légale du traitement autorisé par le décret attaqué. Ces mécanismes nécessitent, à cet égard, davantage de développements et d'analyse.

68 **Le gouvernement soutient** que la conservation dans des bases différentes reliées entre elles par un lien chiffré et unidirectionnel empêcherait d'identifier des personnes à partir de l'image numérisée de leur visage ou de leurs empreintes digitales, garantissant l'impossibilité d'effectuer une recherche à partir de données biométriques à des fins d'identification d'une trace relevée à l'insu ou non d'une personne.

69 La prévention de ce risque aurait été renforcée par le renforcement du chiffrement du lien unidirectionnel et la mise en place de mécanismes de "défense en profondeur" contre un tel détournement, au moyen d'un chiffrement renforcé des données biométriques et des autres données sensibles.

70 De telles conclusions ne sauraient convaincre.

71 En effet, afin de saisir la fragilité du système proposé par le décret, il est utile d'effectuer une comparaison de son fonctionnement avec celui d'un annuaire téléphonique dont la conception est similaire.

72 **En pratique**, un annuaire permet à partir du nom d'une personne de retrouver son numéro de téléphone, mais ne permet pas facilement de trouver le nom d'une personne à partir d'un numéro donné. Il serait cependant abusif de prétendre que cette relation unidirectionnelle entre le nom d'une personne et son numéro constituerait une garantie contre l'utilisation d'un annuaire pour retrouver à quel individu appartient un numéro spécifique. En effet, il suffit à une personne de parcourir l'annuaire à partir de la première page, jusqu'à trouver l'entrée contenant la personne à laquelle est associée le numéro donné. Il est même aisé de construire un annuaire

inversé, simplement en parcourant tout l'annuaire et en créant sa version miroir.

73 Dans l'hypothèse d'un annuaire sous format papier, une telle démarche apparaît difficile à mettre en œuvre par la lenteur qu'elle suppose. Néanmoins, dès lors que que le support devient numérique, cette méthode de recherche, ou de construction d'un annuaire inversé, peut être automatisée donnant un accès simplifié aux informations stockées dans une base de données.

74 En effet, **concernant le fichier TES**, un tel procédé pourrait être effectué par un ensemble d'attaques dites par recherche exhaustive - aussi appelées attaques par force brute, dont le principe fondamental est d'énumérer toutes les valeurs possibles afin de trouver celle qui correspond à ce qui est recherché.

75 Un utilisateur disposant d'un accès au système sera en mesure d'utiliser ce type de mécanismes pour exploiter la connexion entre les deux bases de données, de telles attaques pouvant être étalées discrètement sur plusieurs années.

76 En effet, l'exploitation de tels mécanismes peut se faire soit de manière active, en effectuant des requêtes avec pour seul objectif d'acquérir les données supplémentaires, soit de façon passive, en collectant au fil du temps et en recoupant les résultats des requêtes initialement effectuées pour des raisons légitimes. Dans ce second cas, l'exploitation de la vulnérabilité est indétectable, car indifférenciable d'un usage licite du système.

77 De cette manière, par une modification non pas du fichier lui-même mais de son utilisation, il est possible de reconstruire une version partielle, voire complète, d'une base de données permettant l'identification de personnes par données biométriques.

78 Il convient de préciser que le principe d'une telle manipulation est d'une extrême simplicité, au point qu'il n'est pas rare de rencontrer un tel exercice sous la dénomination d'"inversion de dictionnaire" dans les cours d'informatique de première année [13]

79 Ainsi, la simple mise en place d'un lien unidirectionnel entre les différentes bases de données n'est pas suffisant pour garantir contre les manipulations visant a détourner le système de son usage prévu. En effet, il est impossible dans l'absolu d'apporter de telles garanties face a des manipulations de type "recherche exhaustive". Tout au mieux des techniques palliatives peuvent être prises pour diminuer l'efficacité de ce type de manipulation. Cependant, la réponse du ministère ne fait état d'aucune mesure préventive de cette sorte.

80 **En conclusion**, les aspects techniques décrits par le gouvernement ne peuvent être qualifiés de garanties propres à assurer la sécurité de données de citoyens et le non-détournement de celles-ci de leur objectif initial. À cet

13. A titre illustratif, voir par exemple http://cs.colgate.edu/ mesmith/COSC101_F16/c/materials/n26_dictionaries2_solutions.pdf, exercice réalisé dans le cadre du cours "Computer Litteracy 101" de l'Indiana University of Pennsylvania. Voir également, de façon schématique, l'annexe 1.

égard, le fichier autorisé ne saurait être considéré comme autorisant une atteinte à la vie proportionnée à l'objectif qu'il poursuit.

81 À ce titre, également, l'annulation est inévitable.

3.3. Sur l'étendue des utilisations permises du fichier

82 Le gouvernement ne fait qu'énumérer les agents qui auraient accès au fichier, et dans quelle mesure cet accès serait encadré. Ces détails factuels ne modifient en rien l'argumentation développée par la requérante à la partie 1.1 de son mémoire complémentaire.

83 En complément, sur ce point, la requérante rappelle également qu'**en droit**, dans une logique analogue, dans sa décision du 13 mars 2014 portant sur les dispositions de la loi n° 2014-344 du 17 mars 2014 relative à la consommation (dite *loi Hamon*), plus particulièrement sur celles relatives à la création d'un registre national des crédits aux particuliers, le Conseil Constitutionnel avait estimé que, «*eu égard à la nature des données enregistrées, à l'ampleur du traitement, à la fréquence de son utilisation, au grand nombre de personnes susceptibles d'y avoir accès et à l'insuffisance des garanties relatives à l'accès au registre, les dispositions contestées portent au droit au respect de la vie privée une atteinte qui ne peut être regardée comme proportionnée au but poursuivi* » (Décision n° 2014-690, DC du 13 mars 2014).

84 En outre, selon la CNIL dans sa délibération n° 2017-058 du 16 mars 2017 portant avis sur un projet de décret modifiant le décret n° 55-1397 du 22 octobre 1955 instituant la carte nationale d'identité et relatif aux conditions de recueil et de conservation des empreintes digitales du demandeur de carte nationale d'identité, le recours au fichier TES à des fins d'« identification certaine d'une personne dans le cadre d'une procédure judiciaire », et compte tenu de la rédaction adoptée, peut « *renvoyer à des hypothèses diverses et nombreuses, sans rapport avec les finalités administratives à l'origine du traitement* ». Toujours selon la Commission, cette formulation serait de nature à créer une confusion sur la nature du fichier papier dont il est question et dont la création était justifiée par des motifs administratifs.

85 **En l'espèce**, quelles que soient ses modalités d'accès, et tel que le prévoit l'article 4 du décret attaqué, les données enregistrées dans le fichier pourront être consultées par : « les agents des services de la police nationale », « les militaires des unités de la gendarmerie nationale » et « les agents des services spécialisés du renseignement », pour la « prévention et de répression des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme».

86 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.

87 **En conclusion**, les mesures prévues par le décret litigieux ne sauraient être regardées comme proportionnées au regard du but poursuivi et constituent une atteinte à la vie privée, c'est pourquoi son annulation est requise.

3.4. Sur le stockage des données sous leur forme « brute »

88 Les données biométriques contenues dans le fichier TES étant des données sensibles, celui-ci doit donc prévoir un haut degré de sécurité. (cf mémoire complémentaire *3.3 Sur la sécurité*, p. 26)

89 À ce titre, le mémoire en réplique du ministre insiste à plusieurs reprises (p. 10, 23 et 26) sur la nécessité du stockage des données biométriques elles-même sous leur forme "brute" d'images, afin de les comparer à des données ultérieures.

90 Or, cette assertion est factuellement incorrecte.

91 Pour rappel, la comparaison de données biométriques se fait en extrayant de la donnée capturée une représentation mathématique de ses traits caractéristiques. La comparaison de ces traits fournit une mesure de la similarité entre les données à comparer.

92 Dans l'hypothèse d'une empreinte digitale, cette représentation est générée à partir d'un ensemble dit de "points de minutie" (les creux, bosses, cicatrices etc. caractéristiques de l'empreinte).

93 Il est donc possible, et généralement recommandé, de stocker la représentation mathématique *issue* de la donnée biométrique plutôt que l'image capturée elle-même. Cette méthode constitue une première étape et une première alternative possible afin de restreindre la portée des données collectées et limiter partiellement les conséquences d'une éventuelle faille de sécurité.

94 Par ailleurs, il est intéressant de noter qu'une problématique analogue existe dans une autre branche de l'informatique : le stockage des mots de passe. En effet, pour authentifier un utilisateur, un serveur de données compare le mot de passe fourni à un mot de passe précédemment défini. Cependant, le fait de stocker directement ce mot de passe dans une base de données à ces fins d'authentification implique un risque majeur en cas de faille de sécurité, d'autant qu'un utilisateur est susceptible d'avoir utilisé un même mot de passe pour différents services.

95 La solution généralement adoptée est d'utiliser un outil cryptographique appelé "fonction de hachage". Une fonction de hachage permet, à partir d'une donnée numérique, de produire une donnée dérivée appelé *condensat* (ou *empreinte*). Ce condensat a pour propriété de pouvoir identifier la donnée initiale, mais sans pour autant permettre de la reconstruire. Ainsi, un schéma simple pour un système d'authentification à base de mot de passe consiste à stocker le condensat du mot de passe de l'utilisateur.

96 De cette manière, lorsque l'utilisateur saisit à nouveau le mot de passe pour s'authentifier, le condensat est recalculé, puis comparé au condensat de référence précédemment stocké. Si les deux condensats sont identiques, le système peut estimer avec confiance que l'utilisateur a saisi le bon mot

de passe [14]. Notons qu'il s'agit là d'une explication simplifiée du principe de fonctionnement. En pratique, des étapes supplémentaires sont ajoutées au processus pour prévenir contre certains types d'attaques, comme les attaques par recherche exhaustive notamment [15].

97 Il est important de souligner que, dans un tel schéma de fonctionnement, le mot de passe en lui même n'est jamais stocké sur le serveur. C'est uniquement sa représentation dérivée sous forme de condensat qui est enregistrée.

98 Bien que les méthodes classiques de génération de condensat ne puissent pas être directement utilisées concernant des données biométriques en raison des variations mineures entre les différentes captures, des méthodes spécifiques ont été développées pour ce type de données. Ces méthodes génèrent un condensat à partir de la représentation mathématique de la donnée biométrique, qui permettra là comparaison aux condensats obtenus ultérieurement.

99 À titre d'exemple, Apple décrit le fonctionnement de son système *Touch ID*, utilisé pour le déverrouillage de l'iPhone, de la façon suivante :

> "*Touch ID* ne stocke aucune image de vos empreintes digitales, et se base à la place sur une représentation mathématique. Il n'est pas possible pour quelqu'un de recréer l'image de votre empreinte digitale à partir des données stockées". [16]

100 Des mécanismes similaires sont mis en place pour *Face ID*, la technologie d'Apple pour le déverrouillage des appareils par reconnaissance faciale :

> "Les images du visage capturées durant le fonctionnement normal ne sont pas sauvegardées, mais sont à la place immédiatement détruites une fois le calcul de la représentation mathématique effectué [...]" [17].

101 Depuis les années 1970, les recherches en cryptographie mettent à notre disposition un ensemble de techniques permettant d'éviter la nécessité de stocker les données sensibles utilisées a des fins de comparaison (tels que les mots de passe, ou les données biométriques). Ces techniques, appliquées aux données biométriques, offrent une sécurité bien supérieure aux stockages

14. Voir par exemple à ce sujet la page de Wikipédia en français sur les fonctions de hachage, en particulier le passage sur l'utilisation pour le stockage des éléments d'authentification https://fr.wikipedia.org/wiki/Fonction_de_hachage section « Contrôle d'accès ».

15. Voir par exemple, toujours dans la page de Wikipédia en français sur les fonctions de hachage, la notion de *salage* des données.

16. Traduction libre de "Touch ID doesn't store any images of your fingerprint, and instead relies only on a mathematical representation. It isn't possible for someone to reverse engineer your actual fingerprint image from this stored data." Disponible à l'adresse : https://support.apple.com/en-us/HT204587

17. Traduction libre de "Face images captured during normal operation aren't saved, but are instead immediately discarded once the mathematical representation is calculated". Disponible à l'adresse : https://images.apple.com/business/docs/FaceID_Security_Guide.pdf

des données biométriques “brutes” tout en répondant à l'objectif poursuivi par le décret attaqué dans la mise en place du fichier.

102 En l'absence de précisions supplémentaires, l'affirmation du ministère selon laquelle le stockage des images des données biométriques en elles-mêmes serait une nécessité technique au bon fonctionnement du système apparaît dès lors largement infondée. Or, stocker de telles données sous forme brute créé un risque qu'elles puissent être facilement réutilisées via des copies identiques, afin d'usurper l'identité d'une personne, typiquement, ce que le stockage de simples condensats rendrait bien plus difficile.

103 À ce titre, encore, l'annulation ne saurait être écartée.

104 Néanmoins, si ces développements s'avéraient insuffisants pour emporter l'annulation du décret attaqué, ils devraient faire naître dans l'esprit du juge des doutes suffisants quand à la sécurité alléguée du fichier, justifiant qu'il soit demandé, à titre subsidiaire, une expertise approfondie.

4. Sur les conclusions aux fins de demande d'expertise et de documentation

105 **En droit** et à titre principal, l'association exposante rappelle que le Conseil d'État « se donne les moyens de trancher avec (...) la plus grande profondeur de champ et le maximum de pédagogie [18] » l'espèce, qui relève d'un domaine éminemment technique et complexe.

106 Dès lors, il est rappelé au Conseil d'État qu'il peut être fait application de l'article R. 625-2 du code de justice administrative qui dispose que :

> « Lorsqu'une question technique ne requiert pas d'investigations complexes, la formation de jugement peut charger la personne qu'elle commet de lui fournir un avis sur les points qu'elle détermine. Le consultant, à qui le dossier de l'instance n'est pas remis, n'a pas à opérer en respectant une procédure contradictoire à l'égard des parties. »

107 Cette disposition a déjà été mise en application par le Conseil d'État qui a sollicité un commissaire aux comptes afin d'apprécier et déterminer les modalités de certains coûts en matière de tarifs d'utilisation des réseaux publics d'électricité (CE, 28 mars 2012, *Société Direct Energie*, n°330548).

108 Des points plus techniques ont également pu être soulevés et résolus devant les juridictions administratives. La méthode retenue par le Conseil supérieur de l'audiovisuel (CSA) pour déterminer les populations desservies par un service de radio autorisé en mode analogique par voie hertzienne terrestre a par exemple pu être examiné par le Conseil d'État. Il a alors vérifier

18. Monsieur J.-M. Sauvé, vice-président du Conseil d'État, lors d'un discours sur les *enjeux et défis du Conseil d'Etat de France, Université catholique de Louvain (KU Leuven) – mardi 15 octobre 2013.*

que le respect du plafond de couverture de la population par un même opérateur ne conduirait pas à une sous-évaluation des populations desservies (CE, 22 juillet 2015, *Syndicat interprofessionnel des radios et télévisions indépendantes*, n° 374114).

109 **En l'espèce**, la garantie que le choix du lien unidirectionnel entre deux bases de données distincte est supposée assurer en matière de sécurité ne peut être affirmée avec assurance : elle mériterait des investigations supplémentaires.

110 En effet, au regard du rapport remis par l'INRIA, ce modèle d'architecture comporte des failles et des risques qui peuvent être évités par le choix de structures alternatives. Par ailleurs, il peut être démontré qu'un lien unidirectionnel puisse être facilement détourné afin de permettre une fonction d'identification.

111 A titre subsidiaire, s'il s'avère que des investigations supplémentaires sont nécessaires à la résolution du litige, la requérante rappelle également que le Conseil d'État peut procéder à la mise en œuvre d'une procédure d'expertise, en application de l'article R. 621-1 du code de justice administrative.

112 De plus, l'article R. 621-7-1 du code de justice administrative permet notamment à l'expert d'exiger la production sans délai des documents qu'il estime utiles à l'accomplissement de sa mission.

113 À défaut, l'expert devra informer de ces difficultés le président de la juridiction ou le magistrat qui l'a chargé des questions d'expertise et du suivi des opérations d'expertise, en vertu de l'article R. 621-1-1 du code de justice administrative, afin qu'il provoque ou ordonne sous astreinte la production de ces pièces.

114 Si certaines informations pouvant servir de base à l'opinion du juge sont couvertes par le secret, le Conseil d'État a admis que celles-ci doivent néanmoins lui être communicables, mais à lui seul, en motivant sa décision ainsi : « si un tel défaut de publication interdit la communication de l'acte litigieux aux parties autres que celle qui le détient, dès lors qu'une telle communication priverait d'effet la dispense de publication de l'acte attaqué, il ne peut, en revanche, empêcher sa communication au juge lorsque celle-ci est la seule voie lui permettant d'apprécier le bien-fondé d'un moyen » (CE, 31 juillet 2009, *Association AIDES et autres.*, req. n° 320196, Rec. p. 341, à propos d'un décret autorisant la création d'un fichier de traitement automatisé de données à caractère personnel).

PAR CES MOTIFS, et tous autres à produire, déduire, suppléer, au besoin même d'office, l'association requérante persiste dans les conclusions de ses précédentes écritures, et y ajoutant :

A TITRE SUBSIDIAIRE, si par extraordinaire le Conseil d'État estimerait que les précisions techniques versées au dossier sont insuffisantes pour l'éclairer sur les nombreuses illégalités manifestes qui entachent le décret attaqué, il ne manquera pas de diligenter la mesure d'expertise qu'il jugera la plus adéquate.

Le 30 mai 2018, à Paris,

Pour La Quadrature du Net

Benjamin Bayart