COMMISSION NATIONALE
DE L'INFORMATIQUE ET DES LIBERTÉS

PLAINTE AU TITRE DE L'ARTICLE 38 DE LA LOI N° 78-17 DU 6 JANVIER 1978

POUR :

1°) **L'association « La Quadrature du Net » (LQDN), association régie par la loi du 1er juillet 1901 dont le siège social est situé au 115, rue de Ménilmontant à Paris (75020), enregistrée en préfecture de police de Paris sous le numéro W751218406, représentée par [redacted], membre du collège solidaire en exercice**

2°) **Les 15 248 plaignants ayant mandaté La Quadrature du Net**

CONTRE : **Le ministre de l'intérieur**

Table des matières

Procédure **3**

Discussion **5**

I Sur la disproportion de la mise en œuvre du TES **6**

II Sur l'absence de respect de l'obligation de sécurité par la mise en œuvre du TES **17**

A. En ce qui concerne la prévention de détournement 19

B. En ce qui concerne les restrictions d'accès 23

Bordereau des productions **26**

PROCÉDURE

1. Aux termes de l'article 38 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (ci-après « loi Informatique et Libertés ») :

> « *Toute personne peut mandater* […] *une association ou une organisation dont l'objet statutaire est en relation avec la protection des droits et libertés lorsque ceux-ci sont méconnus dans le cadre d'un traitement de données à caractère personnel* […] *aux fins d'exercer en son nom les droits prévus aux articles 77 à 79 et 82 du règlement (UE) 2016/679 du 27 avril 2016. Elle peut également les mandater pour agir devant la Commission nationale de l'informatique et des libertés, contre celle-ci devant un juge ou contre le responsable de traitement ou son sous-traitant devant une juridiction lorsqu'est en cause un traitement relevant du titre III de la présente loi.* »

2. De même, aux termes du 1 de l'article 77 du règlement UE n° 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après « RGPD ») :

> « *Sans préjudice de tout autre recours administratif ou juridictionnel, toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle, en particulier dans l'État membre dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise, si elle considère que le traitement de données à caractère personnel la concernant constitue une violation du présent règlement.* »

3. La Quadrature du Net est une association de loi 1901 déclarée en préfecture le 5 février 2013. Elle prévoit dans ses statuts que « *l'Association a pour objet désintéressé et non lucratif la promotion et la défense des droits et des libertés fondamentales dans l'environnement numérique* », notamment, « *la promotion et la défense du droit à l'intimité, à la vie privée, à la protection de la confidentialité des*

communications et du secret des correspondances et à la protection des données à caractère personnel » et « *la lutte contre la surveillance généralisée ou politique, d'origine privée ou publique* ».

4. Du 24 mai au 24 septembre 2022, en application de l'article article 38 de la loi Informatique et Libertés, La Quadrature du Net a invité tout individu résidant en France à la mandater via son site `https://technopolice.fr/plainte` pour qu'il exerce, en son nom, les droits que lui confère l'article 38 de la loi Informatique et Libertés afin d'introduire la présente réclamation devant la Commission nationale de l'informatique et des libertés (ci-après « la CNIL »).

5. 15 248 plaignants ont ainsi mandaté La Quadrature du Net pour ce faire (la liste de leurs noms est jointe en annexe, *cf.* pièce n° 1).

DISCUSSION

6. Le décret du 22 octobre 1955 instituant la carte d'identité fixe les conditions de délivrance et de renouvellement de la carte nationale d'identité. L'article 1er de ce décret prévoit la durée de validité de la carte ainsi que les informations mentionnées sur la carte d'identité.

7. Le décret du 30 décembre 2005 fixe les conditions de délivrance et de renouvellement du passeport. L'article 1er prévoit les informations mentionnées sur le passeport et l'article 17-1 prévoit les conditions de délivrance du passeport d'urgence.

8. Conformément à l'article 1er du décret no 2016-1460 du 28 octobre 2016, le ministre de l'intérieur est responsable du traitement de données personnelles dénommé « titres électroniques sécurisés » (ci-après « TES »).

9. Ce même article prévoit que le fichier TES peut être mis en œuvre pour les finalités suivantes :

— procéder à l'établissement, à la délivrance, au renouvellement et à l'invalidation des cartes nationales d'identité mentionnées à l'article 1er du décret du 22 octobre 1955 et des passeports mentionnés aux articles 1er et 17-1 du décret du 30 décembre 2005 ;
— prévenir et détecter leur falsification et contrefaçon ;
— et, depuis sa modification par le décret du 13 mars 2021, lutter contre l'usurpation d'identité.

10. Le fichier TES centralise les données relatives au demandeur d'une carte d'identité ou d'un passeport et notamment :

> « *a) Le nom de famille, le nom d'usage, les prénoms* » ; […]
>
> *i) L'image numérisée du visage et celle des empreintes digitales qui peuvent être légalement recueillies* »

11. En 2021, le décret n° 2021-279 a ajouté un article 1-1 au décret du 30 décembre 2005 qui prévoit que la carte nationale d'identité comporte désormais un composant électronique contenant les données mentionnées à l'article 1er, dont l'image numérisée de la photographie et l'image numérisée des empreintes digitales de deux doigts, sauf certaines exceptions.

12. Par la présente plainte, La Quadrature du Net et les 15 248 personnes concernées par ce traitement et l'ayant mandatée entendent contester les atteintes aux droits générés par la mise en œuvre de ce traitement, en ce que celle-ci centralise les données biométriques de la quasi-totalité de la population.

13. Il sera démontré que le ministre de l'intérieur met en œuvre le traitement TES de façon illégale et inconventionnelle dès lors que son utilisation ne répond pas aux exigences de proportionnalité prévue par la loi Informatique et Libertés (I) et qu'il échoue à satisfaire à son obligation de sécurité prévu par la même loi (II).

I. Sur la disproportion de la mise en œuvre du TES

14. **En premier lieu**, la mise en œuvre du traitement TES est contraire à la loi Informatique et Libertés et au RGPD en ce qu'elle est disproportionnée.

15. **En droit**, le 3° de l'article 4 de la loi Informatique et Libertés prévoit qu'un traitement de données ne peut être licite que si les données personnelles traitées sont « *adéquates, pertinentes et, au regard des finalités pour lesquelles elles sont traitées, limitées à ce qui est nécessaire* ».

16. L'article 6 de la même loi prévoit une interdiction de « *traiter des [. . .] données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.* »

17. En application de l'article 9 du RGPD, un traitement de données biométriques peut être mis en œuvre par exception uniquement si « *le traitement 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, res-*

pecter 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 ».

18. Ce principe de proportionnalité doit être apprécié et appliqué au regard de la jurisprudence de la Cour européenne des droits de l'homme (ci-après « CEDH ») et de la Cour de Justice de l'Union européenne (CJUE).

19. Dans son arrêt du 18 avril 2013, *M. K c. France*, la CEDH a jugé, au sujet du fichier automatisé des empreintes digitales (FAED) et au regard de l'article 8 de la Convention européenne des droits de l'homme et des libertés fondamentales (ci-après « CESDH »), 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* ». (*cf.* CEDH, 18 avril 2013, *M. K. c. France*, n° 19522/09, § 40)

20. Ainsi, la Cour s'opposait à ce que la lutte contre l'usurpation d'identité puisse justifier le fichage de l'intégralité de la population française.

21. Quant à la CJUE, elle a été amenée dans l'arrêt *Schwarz* du 17 octobre 2013 (*cf.* CJUE, 17 octobre 2013, *Schwarz*, aff. C-291/12), 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.

22. 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* ». En réponse à quoi la Cour de justice a considéré que :

« *[…] il importe de rappeler que l'article 1er, paragraphe 2, du règlement nº 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 nº 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 nº 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. » (*cf.* CJUE, 17 octobre 2013, *Schwarz*, préc., pts. 59 à 63)

23. 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 :

« *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 consi-*

dérations 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 » (*cf.* pts. 56 et 58 des conclusions)

24. Ainsi, le principe de proportionnalité doit être interprété en ce qu'il exclue la constitution de bases de données centralisée dès lors que les mêmes données peuvent être stockées sur un support individuel sécurisé pour atteindre la même finalité de gestion des titres d'identité, cette exigence étant d'autant plus importante lorsque l'ensemble de la population d'un État est concernée.

25. Cette analyse est également partagée par le Conseil constitutionnel. Celui-ci s'est en effet penché sur la conformité d'une base centralisée de données biométriques à la Constitution, en prenant en compte les dispositions de la loi Informatique et Libertés.

26. 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 (*cf.* Cons. const., 22 mars 2012, *Loi relative à la protection de l'identité*, n° 2012-652 DC, cons. 9-10).

27. Afin de conclure à l'inconstitutionnalité de la mesure, le Conseil a pris en compte des critères identiques à ceux de la CJUE et de la CEDH, qui sont analysées de la manière suivante dans le commentaire des Cahiers :

— En premier lieu, « *la taille du fichier envisagé était sans précédent. Il devait réunir des données concernant 45 à 60 millions de personnes (pour 6,5 millions de personnes dans le fichier TES utilisé pour les passeports). La création d'une base centralisée de données biométriques d'une telle ampleur compor-*

tait des risques importants et impliquait des sécurités techniques complexes et supplémentaires. En effet, un fichier est d'autant plus vulnérable, convoité et susceptible d'utilisations multiples qu'il est de grande dimension, qu'il est relié à des milliers de points d'accès et de consultation, et qu'il contient des informations très sensibles comme des données biométriques. »

— En deuxième lieu, « *les données biométriques enregistrées dans le fichier présentent un caractère particulièrement sensible* », ce que le Conseil a reconnu en les décrivant comme « *susceptibles d'être rapprochées de traces physiques laissées involontairement par la personne ou collectées à son insu* ».

— En troisième lieu, « *les caractéristiques techniques du fichier rendaient possible l'identification d'une personne à partir des empreintes digitales. C'est la conséquence du choix du "lien fort". La constitution d'un tel fichier pour atteindre l'objectif fixé par la loi de lutte contre l'usurpation d'identité ne s'imposait pas : des techniques sans fichier permettent d'atteindre cet objectif, avec des cartes à puce biométrique. S'il est fait le choix de constituer un fichier, des techniques, notamment celle du "lien faible", permettent d'écarter les risques d'autres utilisations.* »

28. Enfin, la CNIL a toujours partagé cette interprétation exigeante du principe de proportionnalité et a affirmé à plusieurs reprises son opposition à la centralisation de données biométriques, au regard, d'une part, des risques inhérents à l'architecture d'une telle base quand d'autres moyens techniques étaient possibles pour atteindre une finalité choisie et, d'autre part, de l'aggravation de ces risques lorsqu'elle concerne la totalité de la population.

29. Ainsi, dans sa délibération n° 2007-368 du 11 décembre 2007, s'agissant d'une réforme du fichier TES concernant alors seulement les passeports, la CNIL exigeait déjà dans un avis 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.* »

30. À nouveau, en 2011, au moment de la création du traitement TES uniquement pour les données relatives aux passeports, elle estimait que :

« *l'introduction d'un composant électronique contenant des données biométriques est proportionnée par rapport à l'objectif de renforcement de la sécurité de l'établissement et de la vérification des titres* [. . .].

En ce qui concerne la proportionnalité d'une base centrale d'éléments biométriques, la Commission relève qu'il existe des modalités de lutte contre la fraude qui apparaissent tout à la fois aussi efficaces et plus respectueuses de la protection de la vie privée des personnes, en particulier celles qui s'attachent à sécuriser les "documents sources" à produire pour la délivrance de titres d'identité.

[. . .]

D'autres mesures de lutte contre la fraude sont actuellement mises en œuvre ou à l'étude, comme l'insertion de composants électroniques dans les titres, la sécurisation des justificatifs de domicile présentés lors des demandes de carte d'identité ou de passeport, ou encore la gestion d'un traitement spécifique de lutte contre la fraude documentaire au sein du ministère de l'intérieur. La Commission considère que l'efficacité de l'ensemble de ces mesures devrait être précisément évaluée avant d'envisager la généralisation du traitement en base centralisée des identifiants biométriques des individus. Dans ces conditions,

la Commission estime, tout comme dans le cadre de son avis sur le projet de loi présenté en 2008 par le ministère de l'intérieur, que la proportionnalité de la conservation sous forme centralisée de données biométriques, au regard de l'objectif légitime de lutte contre la fraude documentaire, n'est pas à ce jour démontrée. »

31. Ensuite, dans sa délibération n° 2016-292 du 29 septembre 2016 rendu au moment de l'extension du traitement TES aux données relatives aux cartes d'identité, la CNIL réitérait sa position, à laquelle elle ajoutait des alertes importantes compte tenu du changement d'échelle que le traitement ainsi étendu allait prendre :

« *Si la base actuelle des passeports TES contient 15 millions de jeux de données comparables à celles qui sont appelées à figurer dans la base commune envisagée par le présent projet, le passage à une base réunissant des données biométriques relatives à 60 millions de personnes, représentant ainsi la quasi-totalité de la population française, constitue un changement d'ampleur et, par suite, de nature, considérable. La Commission considère en outre que, compte tenu de la nature des données traitées, les conséquences qu'aurait un détournement des finalités du fichier imposent des garanties substantielles et une vigilance particulière.*

[…]

S'agissant des garanties, la Commission regrette que les dispositifs présentant moins de risques pour la protection des données personnelles, tels que la conservation de données biométriques sur un support individuel exclusivement détenu par la personne, n'aient pas été expertisés. »

Elle poursuivait, concernant la possibilité d'introduire un composant électronique sécurisé dans la carte nationale d'identité :

« *L'application de cette mesure législative serait de nature à faciliter la lutte contre la fraude documentaire, tout en présentant moins de risques de détournement et d'atteintes au droit au respect de la vie privée. Elle*

permettrait de conserver les données biométriques sur un support individuel exclusivement détenu par la personne concernée, qui conserverait donc la maîtrise de ses données, réduisant les risques d'une utilisation à son insu. La Commission regrette dès lors que les actes réglementaires permettant l'entrée en vigueur d'une telle mesure n'aient pas été adoptés, alors qu'est envisagée la création d'une base de données centralisée, présentant davantage de risques au regard de la protection des droits et libertés. »

Enfin, lors de la modification du décret n° 2016-1460, la CNIL rappelait dans sa délibération n° 2021-022 du 11 février 2021 la disproportion inhérente à une telle base centralisée :

« *A ce jour, le TES demeure un fichier singulier, compte tenu tant de son périmètre d'une ampleur inégalée, que de la nature particulièrement sensible des données biométriques qu'il contient.*

[…]

S'agissant plus particulièrement des usages régaliens, le recours à des dispositifs de reconnaissance biométrique est considéré comme légitime pour s'assurer de l'identité d'une personne, dès lors que les données biométriques sont conservées sur un support dont la personne a l'usage exclusif, comme c'est le cas pour le passeport biométrique. La Commission estime à ce titre, ainsi qu'elle l'a rappelé dans de nombreuses délibérations, que la mise en place et le maintien d'une base centrale de données biométriques ne peut être admise que dans la mesure où des exigences impérieuses en matière de sécurité ou d'ordre public le justifient. Le traitement de données biométriques (image du visage et empreintes digitales), sous une forme centralisée, engendre en effet davantage de risques du point de vue de la protection des données à caractère personnel, 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. »

32. **En l'espèce**, depuis 2016, le TES est mis en œuvre de façon à centrali-

ser les données de l'ensemble des personnes disposant d'une carte d'identité, c'est à dire la quasi-totalité de la population française, afin de remplir les finalités précitées de facilitation d'authentification et renouvellement des titres d'identités. En pratique, les agents habilités ont pour but de vérifier que la personne qui renouvelle son passeport ou sa carte d'identité est bien celle à qui ce titre a été initialement délivré.

33. Pourtant, afin de parvenir à cette finalité, d'autres choix techniques auraient pu être opérés. Pour le démontrer, l'INRIA a fait une étude comparative des différentes architectures qui auraient pu être adoptées pour atteindre les objectifs du TES [1].

34. Ainsi, pour les auteurs de cette note, l'architecture du TES est celle qui, parmi toutes les solutions pouvant être envisagées, permet le moins d'assurer l'objectif énoncé à l'article 1er du décret, à savoir la lutte contre la fraude documentaire [2]. Les auteurs font bien apparaître ce point en classant les différentes architectures possibles de A0 (la solution sur laquelle le TES repose), jusqu'à A4 (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* »).

35. Alors que l'architecture A0 retenue pour le TES 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. Cette architecture dite A4 est aussi une des deux architectures présentant moins de risques que l'architecture retenue par le décret. En effet, une centralisation implique systématiquement, par nature, le risque que ces données soient utilisées pour d'autres finalités que celles ayant justifié leur collecte initiale.

36. Or, depuis 2021, les nouvelles cartes d'identité devront comporter un composant électronique contenant la photographie des visages, qui peut être lu par les agents au moment du renouvellement du titre afin que ceux-ci procèdent à la comparaison biométrique de la personne qui est présentée devant eux, avec l'image

1. Claude Castelluccia et Daniel Le Métayer, *Titres électroniques sécurisés : la centralisation des données biométriques est-elle vraiment inévitable ? – Analyse comparative de quelques architectures*, 15 février 2017, URL : `https://hal.inria.fr/hal-01467902/file/TES-White_Paper_Inria_2017_VF%201_0802.pdf`

2. *Idem*., p. 9, tableau 2.

du visage contenue dans le titre d'identité.

37. En effet, l'article 3 du décret n° 2016-1460 prévoit depuis 2011 que les agents cités à cette disposition « *peuvent accéder, à raison de leurs attributions et dans la limite du besoin d'en connaître, à tout ou partie des données enregistrées dans le traitement mentionné à l'article 1er et dans le composant électronique prévu à l'article 1-1 du décret du 22 octobre 1955 susvisé et à l'article 2 du décret du 30 décembre 2005 susvisé* ».

38. De la même manière, l'article 5 du même décret prévoit que «*Pour les besoins exclusifs de l'accomplissement de leurs missions, les personnels chargés des missions de recherche et de contrôle de l'identité des personnes, de vérification de la validité et de l'authenticité des passeports au sein des services de la police nationale, de la gendarmerie nationale et des douanes peuvent accéder aux données enregistrées dans le composant électronique prévu à l'article 2 du décret du 30 décembre 2005 susvisé.* »

39. Le cadre réglementaire a donc permis l'utilisation d'une solution moins attentatoire aux libertés pour remplir l'objectif poursuivi par le TES, à savoir un composant électronique sur les titres d'identité. Dès lors, une base de données centralisant les données biométriques, et qui créé des ingérences bien plus graves aux droits et libertés des personnes concernées, ne peut plus être considérée comme nécessaire, et donc proportionnée, au regard des finalités prévues par le décret.

40. Si le cadre réglementaire offre une panoplie de possibilités (centralisation des données ; décentralisation sur les titres électroniques), la mise en œuvre de ce cadre doit alors opérer une conciliation équilibrée entre, d'une part, les possibilités offertes par le cadre réglementaire et, d'autre part, les droits et libertés protégés.

41. Si le Conseil d'État a pu valider par le passé le principe de la constitution d'une base centralisée pour les passeports, et ce alors même que les données biométriques figurent déjà dans le composant électronique (CE, Ass., 26 oct. 2011, *APIM*, n° 317827, Rec.), l'interprétation qu'il avait retenu, valable pour le cadre réglementaire du TES, ne peut être appliquée à la mise en œuvre de ce même traitement.

42. En effet, **premièrement**, cette décision du Conseil d'État ne concerne pas

la mise en œuvre du TES, mais seulement la validité de son cadre réglementaire. Si le cadre réglementaire a été validé, il ne dispense pas le ministre de l'intérieur, en tant que responsable de traitement, de mettre en place, parmi les solutions autorisées, le traitement de façon à limiter au maximum les atteintes au droits et libertés, conformément au principe général de proportionnalité. Ainsi, si la centralisation des données peut être combinée avec l'existence de titres électroniques, c'est en raison de la circonstance particulière que l'ensemble des titres d'identité ne comportaient pas de puce électronique. Or, aujourd'hui, l'ensemble des titres d'identité comportant une puce électronique depuis le décret n° 2021-279 du 13 mars 2021, l'utilisation d'un fichier centralisé n'est plus nécessaire pour les nouveaux titres d'identité, mais seulement pour les précédents.

43. **Deuxièmement**, la situation soumise au Conseil d'État ne concernait que les bases de données relatives aux passeports, soit 6,5 millions de personnes [3]. Or, avec l'ajout des cartes d'identités, non seulement le nombre de personnes concernées est bien supérieur, mais il concerne la quasi-totalité de la population, ce qui, symboliquement, politiquement et juridiquement pose des problématiques différentes au regard du pouvoir accordé à l'État. Comme cela a été souligné ci-avant, le fait qu'un fichier puisse concerner la totalité de la population a été retenu pour juger un traitement comme excessif. Il convient donc d'examiner la proportionnalité de l'atteinte de façon différente, en prenant en compte ce critère.

44. **Troisièmement**, dans sa décision, le Conseil d'État analyse la proportionnalité de l'accès au traitement pour atteindre la finalité d'authentification uniquement en considérant les empreintes digitales, sans porter une attention particulière à la consultation par reconnaissance biométrique de la photographie. Or, ce procédé a également changé de nature et de contexte depuis 2011. S'il existe bien une réserve interdisant la reconnaissance faciale, elle ne saurait suffire à limiter tous les dangers qui sont aujourd'hui liées à cette technologie. L'état de la technique en termes de reconnaissance faciale s'est drastiquement transformé en onze ans, celle-ci devenant une technologie mature, utilisée par la police quotidiennement et qui est à la portée de toute personnes par des outils, certes illégaux, mais facilement accessibles (tels que PimEyes ou Clearview AI). Puisque l'exclusion textuelle ne concerne que le traitement lui même, elle ne prend pas en compte les autres outils permettant le détournement du fichier centralisé.

3. Voir le commentaire des Cahiers du Conseil constitutionnel précité.

45. Ainsi, le principe de proportionnalité doit être interprété en ce qu'une base de données centralisant des données biométriques, lorsque ces mêmes données peuvent être stockées sur un support individuel pour remplir l'objectif poursuivi par le traitement, n'est pas adéquate ni nécessaire à la finalité du traitement. L'atteinte aux libertés est d'autant plus importante quand ce traitement concerne la totalité de la population.

46. **Il en résulte que**, la mise en œuvre du TES faite par le ministre de l'intérieur, en ce qu'elle consiste à la fois à mobiliser une base de données centralisée et les puces de données biométriques contenues dans les titres, doit être considérée comme disproportionnée et donc illégale. Afin de s'y conformer, le ministre de l'intérieur ne peut que cesser d'utiliser la base de données centralisée pour les titres émis depuis l'entrée en application du décret n° 2021-279 du 13 mars 2021.

47. **Au surplus**, il convient de tirer les conclusions de cette illégalité et de considérer, en conséquence, comme dénué de fondement tout accès par des tiers à ce fichier pour des finalités différentes que celles du TES. En effet, dès lors que ce traitement n'a plus lieu d'exister et n'est plus légal, un accès à cette base ne reposerait sur aucun fondement légitime. Ainsi, l'accès par les services de renseignement « *pour les seuls besoins de la prévention des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme* » prévu à l'article 4 du décret n° 2016-1460 constituerait dans les faits une possibilité, sans aucun cadre juridique, d'accéder à une liste de l'ensemble des français ainsi que leurs adresses, dates de naissance et toutes autres données contenues au sein du fichier centralisé TES. L'article L. 222-1 en application duquel est prévu ce droit ne saurait constituer une base légale suffisante, dès lors qu'elle ne prévoit aucune finalité spécifique ou garanties techniques encadrant cet accès, comme il sera démontré *infra*.

II. Sur l'absence de respect de l'obligation de sécurité par la mise en œuvre du TES

En deuxième lieu, la mise en œuvre du TES est contraire à la loi Informatique et Libertés et au RGPD en ce qu'elle ne permet pas de remplir l'obligation de sécurité des données traitées.

En droit, le 6° de l'article 4 de la loi Informatique et Libertés prévoit que pour être licite, les données à caractère personnel 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, ou l'accès par des personnes non autorisées, à l'aide de mesures techniques ou organisationnelles appropriées.* »

Cette obligation de sécurité est prévue par l'article 32 du RGPD qui prévoit notamment que :

> « *Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* […] »

48. **En l'espèce**, lorsque le Conseil d'État a apprécié la légalité du décret n° 2016-1460 en 2018, celui-ci a estimé que les dispositions « *relatives aux obligations du responsable du traitement dans le fonctionnement de ce dernier, ne peuvent être utilement invoquées à l'appui de conclusions dirigées contre l'acte réglementaire portant création du traitement automatisé dont la légalité n'est pas susceptible d'être affectée par les conditions dans lesquelles ce traitement sera mis en œuvre* », le conduisant à écarter « *le moyen tiré de l'erreur de fait qu'aurait commise le ministre de l'intérieur en omettant de prendre en compte "la réalité de l'insécurité permanente" induite par le traitement* » (*cf.* CE, 18 octobre 2018, *La Quadrature du Net et autres*, n°s 404996, 405036, 405710, 405895, 406299, 406347, 406421, 408359, pt. 22).

49. Ainsi, le Conseil d'État en appelait à examiner la mise en œuvre effective du traitement afin de vérifier si l'obligation de sécurité du ministre de l'intérieur est exécutée conformément à la loi. C'est la fonction et le but de la présente plainte.

50. Sur ce point, la CNIL a émis des observations et directives sur la manière d'apprécier cette obligation de sécurité dans sa délibération de 2021 précitée :

> « *Elle souligne par ailleurs que dans son avis du 23 février 2016, le Conseil d'Etat a rappelé qu'eu égard à l'ampleur et au caractère particulièrement sensible du TES, qui pourrait rassembler les données relatives à l'identité ainsi que les photographies et les empreintes digitales numérisées de plusieurs dizaines de millions de personnes, la mise en œuvre de ce traitement informatique de données devait obéir à des règles de sécurité strictes. La Commission rappelle quant à elle que la mise en œuvre de mesures de sécurité adéquates nécessite notamment d'assurer l'effectivité des restrictions d'accès prévues par le cadre normatif en vigueur, la traçabilité des consultations ainsi que la prévention de tout détournement des données.* »

51. Doivent donc être examinées notamment la prévention de tout détournement (A) des données et l'effectivité des restrictions d'accès (B).

A. En ce qui concerne la prévention de détournement

52. Dans les faits, le ministre de l'intérieur n'a effectué aucune diligence pour satisfaire à l'exigence de prévention de détournement du traitement. Au contraire, en maintenant une architecture centralisée, il n'a pas mis en œuvre de mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque pourtant dénoncé depuis la création du traitement.

53. Comme cela a été démontré, le ministre de l'intérieur 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. Comme le rappellent les auteurs de la note de l'INRIA précitée, les risques causés par une éventuelle intrusion dans le fichier auraient des conséquences irréversibles et extrêmement dommageables pour l'ensemble des personnes concernées, c'est-à-dire pour la quasi-totalité de la population française.

54. En outre, les modalités techniques du traitement 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. En effet, les analyses techniques démontrent qu'il est possible de détourner l'utilisation du fichier pour identifier les

personnes à partir des photographies pour remonter à leur état civil. Ainsi que le précise les chercheurs de l'INRIA dans leur analyse du fichier TES précitée (p. 3) :

> « *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.* »

55. Autrement dit, le traitement est mis en œuvre de façon à ce que l'enregistrement et la conservation des données biométriques et des données d'identité soient dans une (ou plusieurs) base(s) de données de l'administration. 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 du traitement.

56. En effet, les auteurs de cette note insistent sur le fait que l'architecture retenue par le gouvernement ne pallie aucunement les insuffisances du traitement (p. 11) :

> « *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.)* »

57. La conclusion des chercheurs de l'INRIA mérite quelques explications supplémentaires.

58. Déjà, le lien à sens unique n'est pas efficace pour se prémunir contre l'utilisation du TES à des fins d'identification. En effet, quand une base de données est structurée à sens unique, comme c'est le cas en l'espèce (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 ne consititue absolument pas une garantie que l'usage de ces données ne pourra pas être détourné.

59. C'est d'ailleurs le constat fait par l'Agence nationale de la sécurité des systèmes d'information (ci-après « ANSSI ») dans son audit du TES [4] :

> « *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 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*. »

60. Il apparaît clairement que, par les choix techniques opérés, le ministre de l'intérieur ne prend délibérément pas en compte le niveau de risques et le degré de gravité des atteintes possibles aux données personnelles des personnes concernées. En ne garantissant pas l'absence d'utilisation du fichier à des fins d'identification, et donc de détournement de ses finalités, le ministre de l'intérieur manque à son obligation de sécurité.

61. **Au surplus**, ce manquement à l'obligation de sécurité est d'autant plus renforcé, comme il a été rappelé, qu'aujourd'hui les possibilités de recourir à des outils de reconnaissance faciale est bien plus aisée et performante.

62. Il est d'ailleurs à noter que dans l'audit, l'ANSSI relevait que [5] :

> « *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 réquisitions 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 titres ne se justifie que pour faciliter les contrôles lors des renouvellements de titre.* »

4. Audit réalisé par l'ANSSI et remis au ministre de l'intérieur le 13 janvier 2017, p. 4, URL : `https://www.interieur.gouv.fr/content/download/100011/786238/file/rapport-commun-public-tes-13-01-20172.pdf`

5. *Idem*., p. 6.

B. En ce qui concerne les restrictions d'accès

63. L'accès au TES n'est pas limité aux seuls agents chargés du renouvellement des titres d'identités. En effet, l'article 4 du décret n° 2016-1460 prévoit que peuvent accéder aux données du traitement « *pour les besoins exclusifs de leurs missions* » et « *à l'exclusion de l'image numérisée des empreintes digitales* », dans les conditions fixées par l'article L. 222-1 du code de la sécurité intérieure» :

> « *1° Les agents des services de la police nationale et les militaires des unités de la gendarmerie nationale chargés des missions de prévention et de répression des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme, individuellement désignés et dûment habilités par le directeur dont ils relèvent ;*
>
> *2° Les agents des services spécialisés du renseignement mentionnés à l'article R. 222-1 du code de la sécurité intérieure, individuellement désignés et dûment habilités par le directeur dont ils relèvent, pour les seuls besoins de la prévention des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme.* »

64. Or, l'article L. 222-1 du code de la sécurité intérieure prévoit uniquement le fait que ces services peuvent avoir accès au « *système de gestion des cartes nationales d'identité* » et au « *système de gestion des passeports* » pour les finalités énoncées ci-dessus. Cette disposition ne détaille à aucun moment les garanties techniques ou opérationnelles précises devant être mises en œuvre pour limiter au strict nécessaire cet accès, surtout pour des finalités aussi larges que la « *prévention des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme* ».

65. Ainsi, il n'existe nulle part une obligation pour ces services tiers de mettre en place des limitations effectives pour que l'accès au traitement ne permette de consulter ni l'image numérisée ni les empreintes digitales. Il est donc tout à fait possible que le logiciel aujourd'hui utilisé par ces agents ne soit pas assez sécurisé pour empêcher un accès total au TES ou empêcher de croiser les données du TES avec d'autres données. Ainsi, le ministre de l'intérieur n'a pas prévu de contraintes réglementaires ou techniques pour circonscrire cet accès à des situations précises et limitées au strict nécessaire.

66. Dans sa délibération précitée de 2016, la CNIL s'en inquiétait et estimait que l'exclusion de la reconnaissance faciale devait être effective. Elle écrivait ainsi que :

> « [Cette effectivité de l'exclusion d'usages de traitements de reconnaissance faciale] *suppose la mise en œuvre de mesures de sécurité strictes et un contrôle permanent des accès aux données ainsi que de leur utilisation, doit impérativement être assurée.*
>
> *Au vu des risques graves d'atteinte à la vie privée soulevés par la mise en œuvre de ce traitement, la commission se montrera particulièrement attentive à ses conditions réelles de mise en œuvre, notamment dans le cadre de ses pouvoirs de contrôle prévus à l'article 44 de la loi du 6 janvier 1978 modifiée*. »

67. **En conclusion**, dès lors qu'aucune mesure technique ou opérationnelle n'a été mise en place par le ministre de l'intérieur pour restreindre ces accès et garantir que lesdits accès au TES soient strictement limités à ce qui est prévu par la loi, mais également pour empêcher tout croisement avec d'autres fichiers auxquels les services de renseignement et de police ont accès, celui-ci faillit, à nouveau, à remplir son obligation de sécurité.

68. En outre, le contrôle de ce fichier n'entre pas dans le champ de prérogatives de la Commission nationale de contrôle des techniques de renseignement (CNCTR), ce qui signifie qu'il n'y a à ce jour aucun contrôle sur ce le périmètre effectif de l'accès de ces agents de police et de renseignement au TES. Nous invitons donc la CNIL à exercer ses pouvoirs de contrôle pour vérifier que l'exclusion prévue par l'article 4 du décret n° 2016-1460 est bien mise en œuvre.

69. À tous égards, la sanction de la mise en œuvre du traitement TES par le ministre de l'intérieur s'impose.

PAR CES MOTIFS, l'association La Quadrature du Net et les 15 248 plaignants l'ayant mandatée concluent qu'il plaise à la CNIL de :

— Sur l'utilisation disproportionnée du traitement de données :

CONTRÔLER l'utilisation du traitement TES par le ministre de l'intérieur ;

ENJOINDRE au le ministre de l'intérieur de cesser d'utiliser la base de données centralisée du traitement TES en ce qu'elle est ni nécessaire, ni proportionnée ;

SANCTIONNER le ministre de l'intérieur pour les violations constatées.

— Sur l'exécution de l'obligation de sécurité :

CONTRÔLER l'exécution de l'obligation de sécurité du ministre de l'intérieur relative au traitement TES ;

ENJOINDRE au ministre de l'intérieur de cesser d'utiliser une base de données centralisée au regard du manque de garanties techniques et opérationnelles permettant d'assurer un niveau de sécurité adéquat ;

ENJOINDRE au ministre de l'intérieur de restreindre de manière effective les accès au traitement TES ;

SANCTIONNER le ministre de l'intérieur pour les violations constatées.

Fait à Marseille, le 24 septembre 2022

[redacted]

Membre du collège solidaire de La Quadrature du Net

[redacted]

BORDEREAU DES PRODUCTIONS

Pièce n° 1 : Liste des 15 248 plaignants ayant donné mandat à La Quadrature du Net pour déposer en leur nom la présente plainte ;