*A Messieurs les président et Conseillers*
*du CONSEIL D'ETAT*

# RECOURS ET
# MEMOIRE INTRODUCTIF

**POUR** :

1. **Monsieur Didier C**
2. **Madame Agnès C**
3. **Monsieur Clément M**
.
4. **Madame Hélène M**
5. **Monsieur Richard C**
6. **Monsieur Thierry B**


***Ayant pour Avocat :*** **Maître Christophe LEGUEVAQUES**
*SELARL Christophe LEGUEVAQUES Avocat*
Avocat au Barreau de Paris
1, rue Le Goff - 75005 PARIS
Tél. : 01 46 34 03 07 – Fax. : 01 43 25 34 47
Palais K 055


**CONTRE** : Le **décret n° 2008-426 du 30 avril 2008** modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques (JORF n° 0105 du 4 mai 2008, p. 7446 et s.)

*Pièce n° 1*

Les Requérants défèrent le **décret n° 2008-426 du 30 avril 2008** à la censure du Conseil d'Etat pour les motifs ci-après exposés dans la présente Requête.

# PLAN DU MEMOIRE

Dans son article consacré à la biométrie[1], Monsieur Christian BYK[2] synthétise la forme moderne du conflit ancien entre la protection des libertés individuelles et la recherche de la sécurité pour tous les citoyens.

> *« L'informatique doit être au service de chaque citoyen (…) Elle doit porter atteinte ni à l'identité humaine ni aux droits de l'homme ni à la vie privée, ni aux libertés individuelles publiques.*

> *« Procédé d'identification utilisant les données individuelles physiologiques ou comportementales, la biométrie bénéficie d'un essor rapide (…) Au regard du droit des libertés publiques, la biométrie oppose, à l'évidence, le droit individuel de la protection des données et au respect de la vie privée à l'exigence collective de sûreté. Elle invite donc à trouver un équilibre entre ces droits et intérêts légitimes.*

> *En l'absence de régime spécifique, l'essor de cette technique, notamment avec la mise en place du passeport biométrique, semble montrer que son « encadrement juridique » aboutit à un* ***déséquilibre préjudiciable aux libertés ».***

L'auteur conclut son exposé par le souhait d'une intégration future des principes devant gouverner l'usage de la biométrie dans la Constitution.

Le Conseil d'Etat n'est pas le lieu pour proposer une nouvelle modification de la Constitution. Dès lors, les Requérants limiteront leur recours.

Tout d'abord, les Requérants tiennent à préciser qu'ils n'entendent pas contester la légitimité de l'objectif de contrôle et de lutte contre la *fraude aux documents administratifs,* cause principale et unique à l'intégration dans les passeports de données biométriques.

En revanche, les Requérants n'acceptent pas que le décret du 30 avril 2008 instaurant un passeport biométrique :

- outrepasse les exigences européennes et
- constitue, ainsi, une atteinte disproportionnée aux libertés publiques.

---

[1] Christian BYK, *Biométrie et constitution : est-il déjà trop tard pour les libertés publiques,* JCP (G) 2008, n° 25, p. 19

[2] Christian BYK est magistrat, secrétaire général de l'*Association internationale, droit, éthique et science* (www.iales.org).

Ainsi, la **création d'une base de données comprenant des informations biométriques** sur un grand nombre de citoyens Français (à termes tous ceux qui demanderaient un passeport seraient concernés) est une source d'inquiétude pour les libertés publiques.

En effet, la technologie permettra, le moment venu, de faire évoluer la finalité initiale de la création de cette base de données pour contrôler, dans un premier temps, les allers et venues des citoyens ; puis, par le mécanisme d'interconnexion des fichiers, de contrôler le comportement de tout un chacun, sans le moindre intérêt légitime. L'histoire française permet d'affirmer que, dans un passé pas si lointain, des fichiers de données personnelles ont pu être une source d'arbitraire et de mesures aussi coercitives qu'indignes des Lois de la République.

C'est pourquoi, les Requérants souhaitent limiter l'usage des informations biométriques dans le cadre qui a été tracé pour l'Union européenne afin d'éviter une dérive nationale attentatoire aux libertés fondamentales et sources de discriminations à l'intérieur de l'Union européenne.

En conséquence, il est demandé au Conseil d'Etat, garant de l'Etat de droit, d'annuler ce texte pour excès de pouvoir.

# I. RAPPEL DES FAITS ET DE LA PROCEDURE

Avant d'étudier le contenu du décret du 30 avril 2008 (**C**), il convient de rappeler les sources européennes de ce texte (**B**). Au préalable, un certain nombre de précisions doit être porté à la connaissance de la Haute-Assemblée afin de lui permettre d'appréhender cette question sensible (**A**).

## A. Précisions terminologiques et principales atteintes aux libertés fondamentales signalées par les défenseurs des droits de l'homme.

Afin d'éclairer le débat, il n'est pas inutile de donner quelques définitions (**1°**). De même, les associations de défense des droits de l'homme n'ont pas manqué de signaler les risques de la biométrie pour les libertés fondamentales (**2°**).

## 1°) Quelques définitions

D'après le doyen Gérard Cornu[3], le passeport est :

> *« un titre délivré par l'autorité administrative qui certifiant l'identité, la nationalité et le domicile de son titulaire, permet à celui-ci de voyager librement, notamment de franchir les frontières ».*

La Commission nationale informatique et libertés (CNIL) définit la biométrie[4] en ces termes :

> *« La biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être* ***uniques et permanentes*** *(ADN, empreintes digitales…). Elles se rapprochent ainsi de ce qui pourrait être défini comme un* ***«identificateur unique universel »****, permettant de ce fait le* ***traçage des individus ».***

Il convient de relever qu'il existe des réserves scientifiques sur la pertinence et l'efficacité de la biométrie :

- Comme le souligne, Monsieur Alex Türk[5], président de la CNIL, il n'existe pas encore d'évaluation suffisante des risques d'erreurs des systèmes biométriques, dont on sait pourtant qu'ils sont intrinsèquement faillibles (les reconnaissances qu'ils opèrent ne sont toujours que des « probabilités » plus ou moins fortes) ; une telle évaluation scientifique et objective doit être engagée.

- Dans le même sens, le G29[6] insiste[7] sur le fait que *« l'intérêt croissant porté au recours à des techniques d'identification biométriques impose que soit menée une analyse extrêmement prudente quant à la légalité du traitement de telles données pour des besoins d'identification. En effet, les données biométriques comportent, en tant que telles,* ***de réels risques pour les personnes concernées si ces données sont perdues ou utilisées de manière détournée quant à leur finalité »****.*

---

3 Gérard CORNU, *Vocabulaire juridique, Puf Quadrige, 7ème éd°, p. 653.*

4 CNIL, *27ème rapport d'activité 2006,* p. 13

5 Conférence d'ouverture de M. le sénateur Alex TÜRK, au « Forum Public sur les enjeux éthiques de la biométrie, Commission d'éthique de la science et de la technologie », Montréal, 13 oct. 2005.

6 Les autorités administratives équivalentes à la CNIL dans les différents Etats-Membres de l'Union européenne sont regroupées dans un groupe dit de l'article 29 (G29).

7 Avis 7/2004 sur l'insertion d'éléments biométriques dans les visas et titres de séjour en tenant compte de la création du système Européen d'information sur les visas (VIS) *11.8.2004 Markt/11487/04/EN*

– Dans une lettre adressée au Président du Conseil de l'Union européenne en date du 30 novembre 2004, le G29 relève que *« Des résultats d'essais ont toutefois montré que* ***les procédés reposant sur des éléments biométriques ne garantissaient ni la sécurité requise ni la commodité escomptée pour les voyageurs, vu que le pourcentage d'acceptation erronée ou de rejet erroné du détenteur du passeport par le système de sécurité de reconnaissance semble élevé.*** *Le groupe de travail "Article 29" émet dès lors des réserves quant à l'utilisation* ***de procédés biométriques qui n'ont pas fait la preuve de leur efficacité*** *et, en particulier, l'utilisation obligatoire d'éléments biométriques qui,* ***telles les empreintes digitales****, permettent une identification de type "un à plusieurs" et un traçage des individus ».*

– Dans son «Document de travail sur la biométrie[8]», le G29 a souligné que *« les progrès rapides des technologies biométriques et la généralisation de leur application ces dernières années nécessitent un examen minutieux sous l'angle de la protection des données.* ***Leur utilisation incontrôlée suscite des inquiétudes en ce qui concerne la protection des libertés et des droits fondamentaux des individus****. Les données de ce type sont d'une nature particulière parce qu'elles ont trait aux caractéristiques comportementales et physiologiques d'une personne et qu'elles peuvent permettre de l'identifier sans ambiguïté ».*

Dans ces conditions, on comprend mieux l'inquiétude exprimée par la CNIL de la constitution d'une *« société de surveillance »* qui serait attentatoire aux libertés fondamentales.

Cette *« société de surveillance »* s'intègre dans la mise en place insidieuse d'un biopouvoir et dans un nivellement du principe de proportionnalité.

Dans la continuation de l'œuvre de Michel Foucault, des auteurs ont analysé l'émergence d'un biopouvoir dont la biométrie serait tout à la fois un attribut et un moyen de contrôle social. Ainsi, le biopouvoir constitue un *« ensemble de mécanismes de micro-pouvoirs hétérogènes, régionaux, multiples, qui s'exercent en des points innombrables et n'émane pas d'une instance souveraine qui serait extérieure »*[9]. Il s'agit d'une privatisation de l'espace public. Dès lors, *« la biométrie révèle le passage d'un pouvoir qui s'exerce sur le corps par le corps. Muni de puces, notre corps devient transparent pour les acteurs du biopouvoir. Il est le témoin, voire le mouchard qui authentifie ce que nous sommes et ce que nous faisons »*[10].

On comprend mieux dans ces conditions, les risques signalés par les associations de défense des droits de l'homme.

---

8 JO L 281 du 23.11.1995, p. 31, http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_fr.htm

9 Pierre JOLICOEUR, *Introduction à la biométrie,* éd° Decarie-Masson, 1991.

10 Christian BYK, *op. cit.,* p. 20

## 2°) Principales atteintes au droit de l'homme liées à la biométrie

### a) Le risque de « réductionnisme » et l'atteinte à la dignité humaine

Dans son avis relatif à l'inclusion d'éléments biométriques dans la carte nationale d'identité[11], la Commission nationale consultative des droits de l'homme (CNCDH) relève que :

> *« la collecte de ces éléments représentatifs de l'être touche la dignité humaine en ce qu'elle réduit chacun à l'extraction de son patrimoine biologique ».*

Ce risque de réductionnisme est repris également dans l'avis du Comité national d'éthique[12] qui qualifie *« de question éthique centrale »* le fait de savoir si ces nouvelles méthodes d'identification respectent l'**identité personnelle, élément essentiel de la dignité et espace de liberté.**

### b) Le droit à la vie et les autres droits fondamentaux constitutionnellement protégés

Dans son rapport au Sénat, Monsieur le sénateur LECERF citent les réserves de la Ligue des droits de l'homme et du Conseil national des barreaux qui ont insisté sur un fait historique avéré : sous l'Occupation, de nombreuses personnes avaient eu la vie sauve en utilisant de fausses identités. La biométrie ne permettrait plus une telle possibilité[13].

Au-delà de la question de la vie privée et de la protection des données personnelles, *« c'est le socle même du contrat social qui devient entamé par la biométrie »*[14]. Si certains auteurs (Christian BYK) en appelle à la Constitution, il paraît d'ores et déjà évident que la matière est au moins du ressort de la loi et non d'un simple règlement.

Cette analyse se confirme lorsqu'on étudie les sources du décret du 30 avril 2008.

---

11 Avis de la CNCDH du 1er juin 2006.

12 CCNE, avis n° 98 ; 20 juin 2007, *Biométrie, données identifiantes et droits de l'homme*.

13 J.-R. LECERF, *Identité intelligente et respect des libertés*, Rapport Sénat n° 439 (2004-2005), mission d'information de la commission des lois, 29 juin 2005 – Auditions.

14 M. MARZOUKI, *La loi « Informatique et Libertés » de 1978 à 2004 : du scandale pour les libertés à une culture de la sécurité,* Intervention lors du colloque de la CNIL « Informatique : servitudes ou libertés ? », Paris, 7-8 novembre 2005.

# B. Transposition d'une norme européenne

Le décret du 30 avril 2008 se présente comme un simple instrument de transposition d'une norme européenne.

Il n'en est rien.

Après avoir rappelé les recommandations du G29 (**1°**), il conviendra d'étudier en détail le Règlement du Conseil européen[15] n°2252/2004 en date du 13 décembre 2004 (ci-après le *« Règlement 2252/2004 »*) (**2°**).

## 1°) Les recommandations du G29

Dans son avis[16] relatif aux visas mais pouvant servir de source d'inspiration pour les passeports des citoyens européens, le G29 commence par rappeler cette évidence : *« Toutes les initiatives dans ce domaine sont susceptibles d'avoir de fortes répercussions sur les droits fondamentaux des personnes concernées (…). À ce titre, les décisions futures portant sur la création et la mise en œuvre de ces nouveaux systèmes d'informations européens devront être prises en tenant dûment compte des principes de protection des données consacrés par l'article 8 de la charte européenne des droits fondamentaux, énoncés par la directive 95/46/CE et les lois nationales en la matière »*.

A la suite de ce rappel, le G29 précise que *« l'introduction d'éléments d'identification biométriques (…) et les traitements de données à caractère personnel correspondants doivent respecter un certain nombre de principes ayant vocation à protéger les droits et libertés fondamentaux des personnes, et particulièrement leurs droits au regard du traitement de leurs données à caractère personnel. Le respect de ces principes est d'autant plus essentiel quant au traitement de données biométriques qui fournissent, par leur nature même, des informations sur une personne précise, et ce d'autant plus que certaines d'entre elles peuvent laisser des traces dans la vie quotidienne des personnes, à l'insu desquelles elles peuvent dès lors être collectées (empreintes digitales, notamment) »*.

Par ailleurs, le G29 rappelle le principe de spécialité qui s'impose au législateur européen, et, par voie de conséquence, au législateur national. En effet, selon l'article 6 de la directive 95/46/CE, *« les données à caractère personnel doivent n'être collectées que pour des **finalités déterminées, explicites et légitimes**, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. (…) »*

---

15 Règlement du Conseil européen n°2252/2004 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 Etats membres, *JOUE, L 385/1, 29 décembre 2004*.

16 Avis 7/2004 sur l'insertion d'éléments biométriques dans les visas et titres de séjour en tenant compte de la création du système Européen d'information sur les visas (VIS) *11.8.2004 Markt/11487/04/EN*

Pour le G29, *« le respect de ces principes rend tout d'abord indispensable une définition claire de la finalité pour laquelle les données biométriques sont collectées et traitées.* ***La définition de cette finalité claire et explicite permettrait alors d'apprécier la légitimité*** *de l'introduction de données biométriques, en rendant possible l'appréciation de la proportionnalité de la collecte et du traitement ultérieur de ces données par rapport à cette finalité d'origine ».*

Au final, le président du G29 synthétise la position du groupe sous la forme de propositions concrètes insérées dans une lettre en date du 18 août 2004 adressée à différentes autorités de l'Union européenne.

> *«1.* ***Le groupe de travail s'oppose fermement au stockage des données biométriques*** *et autres, de tous les titulaires d'un passeport au sein de l'UE* ***dans une base de données centralisée*** *des passeports et documents de voyages européens.*
>
> *2.* ***L'objectif*** *de l'insertion d'éléments biométriques dans les passeports et documents de voyage, conformément au règlement,* ***doit être explicite, approprié, proportionné et clair.***
>
> *3. Les États membres doivent garantir d'une manière techniquement appropriée que les passeports contiennent un support de stockage doté d'une capacité suffisante et qui est à même de préserver l'intégrité, l'authenticité et la confidentialité des données stockées.*
>
> *4. Le règlement doit définir qui peut avoir accès au support de stockage et dans quel but (lire, stocker, modifier ou effacer des données) (…) »*

C'est en tenant compte de ces recommandations que le Règlement 2252/2004 a été adopté.

## 2°) Le Règlement 2252/2004

L'exposé des motifs du Règlement 2252/2004 reprend la plupart des recommandations du G29 :

- Le principe de la liberté d'aller et de venir reste la règle (§1),

- Le but du Règlement 2252/2004 est *« la protection du passeport contre une utilisation frauduleuse »* (§3), **c'est au regard de ce but que devra s'apprécier le principe de proportionnalité** ;

- Dès lors le Règlement 2252/2004 *« se limite à l'harmonisation des éléments de sécurité »* (§ 4). Autrement dit, il n'impose la création d'aucune base de données centralisant les informations biométriques,

- Le Règlement 2252/2004 exige des précautions pour éviter la divulgation de données biométriques (§ 7), question difficile en présence d'une *« puce électronique »* dite RFID permettant une lecture à distance du contenu du passeport[17],

- Le Règlement 2252/2004 insiste –encore une fois- au § 9 sur le respect du principe de proportionnalité.

L'article 1er § 2 du Règlement 2252/2004 précise que les *« passeports (…)* ***comportent*** *un support de stockage qui contient une photo faciale ».* C'est la seule donnée biométrique commune à tous les Etats-membres. Par ailleurs, le Règlement prévoit que chaque Etat membre ajoute des empreintes digitales enregistrées *« dans les formats interopérables »*.

Le Règlement 2252/2004, en tant que tel, ne prévoit ni nombre minimal ni nombre maximal d'empreintes digitales.

Toutefois, la Commission européenne a proposé de limiter *« à* ***deux images d'empreintes digitales*** *du titulaire prises à plat »* (Avis du G29 n° 7/2004).

L'élément le plus important du texte réside dans l'usage du verbe « comporter ». En effet, cela signifie sans équivoque que les données biométriques ne peuvent qu'être **incorporées** au passeport lui-même afin d'éviter toute altération de ce dernier.

En l'état de la technique et compte tenu de la faible fiabilité des éléments biométriques, **le Règlement 2252/2004 ne prévoit aucune base de données visant à centraliser ces informations**.

---

17 CNIL, *Rapport 2007*, p. 27. *« L'INVASION DES PUCES - Les puces RF ID (Radio Frequency Identification) permettent d'identifier et de localiser des objets ou des personnes. Elles sont composées d'une micropuce (également dénommée étiquette ou tag) et d'une antenne qui dialoguent par ondes radio avec un lecteur, sur des distances pouvant aller de quelques centimètres à plusieurs dizaines de mètres. (…)Cette technologie soulève de nouvelles problématiques en matière de protection des données personnelles au premier rang desquelles figure leur (quasi) invisibilité. Comment garantir le respect de la loi en présence de technologies invisibles ? En outre, n'importe qui, dès lors qu'il est muni du lecteur adéquat, peut lire le contenu d'une puce RFID. Et une puce peut comporter des données personnelles (ou qui peuvent devenir personnelles par interconnexion à une base) permettant ainsi d'identifier à distance son porteur. Si tous ces objets journaliers (carte de transport, vêtement, téléphone, voiture, bracelet…) sont ainsi « tagués », il sera possible de* ***pister les individus*** *dans tous les actes de la vie quotidienne ».*

Cette analyse est encore corroborée par l'article 4 § 3 qui dispose que :

> *« aux fins du présent règlement, les éléments biométriques des passeports et des documents de voyage ne sont utilisés que pour vérifier :*
>
> *a) l'authenticité du document ;*
>
> *b) l'identité du titulaire grâce à des éléments comparables directement disponibles lorsque la loi exige la production du passeport ou d'autres documents de voyage ».*

Enfin, il y a lieu de prendre connaissance du rapport de la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen en date du 25 octobre 2004 qui concluait que :

> *« **la création d'une base de données centralisée violerait les principes de finalité et de proportionnalité.** Elle accroîtrait le risque d'abus et de dérapages. Enfin, elle augmenterait également le risque d'utilisation des éléments d'identification biométrique comme «clés d'accès» à diverses bases de données, mettant ainsi en connexion différents fichiers».*

## C. Le décret du 30 avril 2008

Le décret du 30 avril 2008 vise à modifier le décret n°2005-1726 du 30 décembre 2005 qui avait permis la réalisation de la première étape prévue aux termes du règlement européen, en permettant la délivrance de passeports dotés d'un composant électronique intégrant l'image numérisée du visage du titulaire.

Le décret du 30 avril 2008 se présente comme la poursuite du processus d'adaptation du droit interne du Règlement 2252/2004 en intégrant dans le même composant l'image numérisée de **HUIT de ses empreintes digitales** (article 6.1)**.**

Par ailleurs, les articles 8 et 9 du décret prévoient également l'enregistrement de données biométriques se rapportant aux demandeurs (images numérisées de la photographie et des empreintes digitales) dans le système de traitement automatisé de données à caractère personnel relatif au passeport, dénommé « DELPHINE ».

En outre, le décret du 30 avril 2008 apporte un certain nombre de modifications affectant les conditions d'accès aux données à caractère personnel contenues dans le système de traitement « DELPHINE » en même temps qu'il lui confère une finalité nouvelle, à savoir l'élaboration de statistiques.

Force est de constater que le décret du 30 avril 2008 déroge sur deux points essentiels au Règlement 2252/2004, à savoir :

- Numérisation de HUIT doigts au lieu de DEUX (article 5) ;
- Finalité nouvelle ajoutée par simple décision de l'autorité administrative sans le moindre contrôle (article 8 et 9) ;
- Création d'une base centralisée des données biométriques (article 7).

**Ces trois « innovations » constituent autant de violations de la lettre et de l'esprit du Règlement 2252/2004 ainsi que de la loi « Informatique et Libertés », sans parler de l'ensemble des recommandations des autorités protectrices des libertés fondamentales de l'Union européenne.**

# II. DISCUSSION

## A. Sur la recevabilité du présent recours

### 1°) Compétence exclusive du Conseil d'Etat

Le Conseil d'État est resté, en vertu du décret du 30 septembre 1953 portant réforme du contentieux administratif, juge de premier ressort dans les domaines où, selon les termes de l'article R. 311-1 du Code de justice administrative, *« l'objet du litige ou l'intérêt d'une bonne administration de la justice »* justifie que cette compétence lui soit attribuée, ce qui est souvent présenté comme visant, d'une part, l'importance du litige et, d'autre part, la nécessité de trouver un juge et un seul pour chaque litige.

Les matières ainsi visées sont énumérées à l'article R. 311-1 du Code de justice administrative, à savoir, notamment :

> *« 1° Des recours dirigés contre les ordonnances du Président de la République et les **décrets** » ;*
>
> *Dès lors, compte tenu de la nature de la présente requête visant à l'annulation d'un décret, seul le Conseil d'Etat est compétent.*

## 2°) Intérêt à agir des requérants.

Les requérants sont des citoyens français, titulaires d'un passeport.

Ils voyagent fréquemment.

Ils ne souhaitent pas que des données biométriques les concernant soient centralisées dans une base unique à la disposition du Ministère de l'Intérieur.

Ils ont un intérêt direct et légitime à protéger leurs libertés fondamentales d'aller et de venir et de ne pas accumuler des informations personnelles les concernant. D'autant plus que cette accumulation d'informations biométriques peut faire l'objet d'un usage différent de celui annoncé pour le moment.

## 3°) Sur la dispense de représentation des Requérants par un avocat au Conseil d'Etat

L'Article R. 432-1 du Code de Justice administrative dispose que :

> *« La requête et les mémoires des parties doivent, à peine d'irrecevabilité, être présentés par un avocat au Conseil d'Etat. Leur signature par l'avocat vaut constitution et élection de domicile chez lui. »*

L'article R. 432-2 du Code de justice administrative dispose quant à lui :

> « *Toutefois, les dispositions de l'article R. 432-1 ne sont pas applicables :*
>
> - *1° **Aux recours pour excès de pouvoir contre les actes des diverses autorités administratives ;***
> - ***2° Aux recours en appréciation de légalité ;***
> - *3° Aux litiges en matière électorale ;*
> - *4° Aux litiges concernant la concession ou le refus de pension.*
>
> *Dans ces cas, la requête doit être signée par la partie intéressée ou son mandataire* ».

Or, en l'espèce, la présente requête tend à :

> *CONSTATER QUE le **décret n° 2008-426 du 30 avril 2008** modifiant le décret n° 2005-1726 du 30 décembre 2005, relatif aux passeports électroniques, est entaché d'illégalités.*

*En conséquence,* ***ANNULER le décret n° 2008-426 du 30 avril 2008****.*

Dès lors, l'article R 432-2 du Code de justice administrative a vocation à s'appliquer.

En conséquence, le choix du mandataire était totalement ouvert.

Il pouvait s'agir d'un parent, d'un ami *(CE, ass., 14 mars 1952, Chillou de Saint-Albert : Rec. CE 1952, p. 162)*, d'un mandataire professionnel autre qu'un avocat au Conseil d'État *(CE, 24 oct. 1951, Thimeur : Rec. CE 1951, p. 496)*.

En l'espèce, la dernière occurrence a été choisie.

Bien évidemment, il était indispensable, que la personne présentant la requête, Maître Christophe LEGUEVAQUES, Avocat au Barreau de Paris, justifie expressément, par un mandat, de sa qualité pour agir *(CE, 15 mars 1995, n° 160632, Lefghayar)*.

Cette production a bien été effectuée.

*Pièce n° 2*

**Dès lors, le Conseil d'Etat ne pourra que déclarer ladite requête parfaitement recevable.**

## B – Sur les chefs d'illégalité

### 1°) Illégalité externe

Le décret devra être annulé en raison d'un vice de procédure (**a**).

Par ailleurs, la Haute-Juridiction rappellera que la théorie de l'état de la législation antérieure est inapplicable (**b**).

Enfin, les dispositions contenues dans le décret du 30 avril 2008 en ce qu'elles tendent à limiter plusieurs libertés fondamentales ne sont pas du domaine réglementaire mais du domaine législatif (**c**).

L'autorité administrative était donc incompétente pour prendre par décret de telles dispositions. En conséquence, le Conseil d'Etat devra annuler le décret du 30 avril 2008.

### a) Vice de procédure : publication de l'avis de la CNIL *postérieurement* à la publication du décret

L'article 26 II de la Loi « Informatique et Libertés » prévoit que **l'avis de la CNIL** ***« est publié avec le décret autorisant le traitement ».***

Or, il est patent que l'avis de la CNIL en date du 11 décembre 2007 n'a été publié qu'au Journal Officiel de la République française en date du **10 mai 2008**.

Le décret du 30 avril 2008, quant à lui, a été publié le **4 mai 2008**.

La violation de la loi est d'autant plus flagrante qu'elle a été ressentie comme un « pied de nez » du gouvernement à la CNIL[18].

Un tel mépris pour une autorité administrative et surtout pour la Loi devra être sanctionné par la nullité du décret du 30 avril 2008.

### b) L'impossible application de l'état de la législation antérieure

Dans sa réponse, le Ministère de l'Intérieur pourrait être tenté de développer l'argument suivant : le décret du 30 avril 2008 ne fait que modifier un texte de même nature, le décret n°2005-1726 du 30 décembre 2005 relatif aux passeports électroniques.

Il est vrai qu'il fut une époque où, pour identifier le domaine respectif de la loi et du règlement, le Conseil constitutionnel avait recours au critère de *« l'état de la législation antérieure »* selon lequel la nature d'un principe doit être appréciée au regard des législations successives[19].

Toutefois, MM. Favoreu et Philip[20] considèrent que ce principe est tombé en désuétude depuis 1973 et ce critère ne présente aujourd'hui guère d'intérêt pour identifier le domaine de la loi et du règlement.

Au demeurant, compte tenu des remises en cause des libertés fondamentales, il est évident que certaines dispositions du décret du 30 avril 2008 n'appartiennent pas au domaine réglementaire mais exclusivement au domaine de la loi.

---

18 *Le Monde*, 18 mai 2008.

19 Cons. Const., déc. N° 59-1 FNR 27 nov. 1959, Rec. Cons. Const. 1959, p. 71)

20 L. Favoreu et L. Philip, *Les grands arrêts du Conseil constitutionnel,* Dalloz, 2001, p. 84

## c) Atteintes aux libertés fondamentales

- *L'Article 8 de la Charte des droits fondamentaux relatif à la protection des données à caractère personnel*

Cet article dispose que :

> *« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.*
>
> *2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre* ***fondement légitime prévu par la loi.***
>
> *Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.*
>
> *3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».*

Dans l'attente de l'entrée en vigueur du Traité de Lisbonne, cette charte n'a pas de valeur juridique mais permet de préciser l'inspiration de l'Union européenne.

- *Le caractère supra-législatif des dispositions de la loi « Informatique et Libertés »,*

Dans la décision n° 97-389 DC du 22 avril 1997, le Conseil constitutionnel intègre des règles dépourvues de valeurs constitutionnelles comme normes de référence, en tant qu'elles représentent une garantie légale du respect d'un principe constitutionnel.

Dépourvus de valeur constitutionnelle, les principes posés par la législation, relatifs à l'informatique et aux libertés, occupent une place à part dans la hiérarchie des normes, ils se situent, de fait, à un rang supra-législatif, car **toute disposition législative créant un fichier informatique doit les respecter sauf à violer le principe constitutionnel de la liberté individuelle.**

Cette affirmation est d'autant plus vrai en présence d'un texte réglementaire qui tente de déroger ni plus ni moins à l'article 1er de la loi « Informatique et Libertés » lequel dispose que :

> *« L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. »*
>
> *« Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. »*

C'est la raison pour laquelle, la CNIL précise dans son avis[21] sur le décret attaqué que :

> *« La Commission considère enfin que l'ampleur de la réforme qui se dessine et l'importance des questions qu'elle peut soulever justifieraient que, comme elle l'a rappelé à plusieurs reprises, le Parlement en soit saisi sous forme d'un **projet de loi**, qui lui serait préalablement soumis pour avis ».*

Ce faisant, la CNIL fait écho à l'avis n° 3/2005 du G29 lequel concluait en ces termes :

> *« Avant d'intégrer des éléments biométriques dans les passeports, autres documents de voyage ou cartes d'identité, un débat approfondi au sein de la société est nécessaire ».*

**Quel lieu, autre que le Parlement, est-il mieux approprié pour approfondir le débat ?**

- *Liberté d'aller et de venir*

L'article 2 du Protocole n° 4 additionnel à la CONVENTION DE SAUVEGARDE DES DROITS DE L'HOMME ET DES LIBERTES FONDAMENTALES vise à assurer la liberté pour toute personne de circuler à l'intérieur du territoire dans lequel elle se trouve ainsi que de le quitter.

Aux termes de l'article 2-3, son exercice *« ne peut faire l'objet d'autres restrictions que celles qui, prévues par la **loi** »*, constituent des mesures nécessaires, dans une société démocratique, à la sécurité nationale, à la sûreté publique, au maintien de l'ordre public, à la prévention des infractions pénales, à la protection de la santé, de la morale, des droits et libertés d'autrui.

Ainsi, **le décret des 1er février-28 mars 1792 relatif aux passeports a le caractère d'une loi au sens de cette disposition protectrice d'une liberté fondamentale**[22].

---

[21] Délibération n°2007-368 du 11 décembre 2007 portant avis sur un projet de décret en Conseil d'Etat modifiant le décret n°2005-1726 du 30 décembre 2005 relatif aux passeports électroniques, *JO, 10 mai 2008*

[22] CE, 8 déc. 2000, *Rahal*; Dr. adm. 2001, comm. 47

### d) les dispositions du décret du 30 avril 2008 sont du ressort de la loi.

L'Assemblée du contentieux du Conseil d'État dans son arrêt *Union maritime CFDT et Fédération nationale des syndicats maritimes CGT*[23] est venue apporter une précision utile pour délimiter les compétences respectives de la loi et du règlement.

La délimitation entre la loi et le règlement repose, en effet, **non pas sur le contenu des dispositions en cause, mais sur son but et son effet.** Le Conseil d'État était saisi d'un décret du 20 mars 1987 relatif à l'immatriculation et à l'armement des navires dans le territoire des Terres australes et antarctiques françaises. Comme le Commissaire du Gouvernement l'a reconnu, le régime de l'immatriculation des navires français relève sans conteste du pouvoir réglementaire. À considérer le contenu même du décret attaqué, on ne pouvait donc conclure qu'à la compétence de son auteur. Or, le Conseil d'État est parvenu à la conclusion inverse, parce que ledit décret avait pour but et pour effet de modifier les champs d'application respectifs de deux lois, à savoir le Code du travail maritime et le Code du travail de l'outre-mer. Les dispositions du décret ainsi annulées par le Conseil d'État pour incompétence ont logiquement été reprises par la loi n° 96-151 du 26 février 1996 relative aux transports.

Une analyse similaire doit s'appliquer au décret soumis à la censure du Conseil d'Etat.

En effet, le contenu d'un passeport excède le simple domaine réglementaire.

En revanche, le traitement électronique de données hautement sensibles (informations biométriques) est du ressort exclusif de la loi car il peut entraîner des atteintes aux libertés individuelles, au droit de la personne humaine et constitue une limitation à la liberté d'aller et de venir, principe qui *« ne peut faire l'objet d'autres restrictions que celles, prévues par la **loi** »*

## 2°) Illégalité interne

Le décret du 30 avril est vicié en raison de deux illégalités internes :

- d'une part, la violation manifeste du Règlement 2252/2004 (**a**), et
- d'autre part, la violation du principe de proportionnalité (**b**).

---

[23] CE Ass. 27 oct. 1995 : Rec. CE, p. 369 ; JCP 1996, éd. G, IV, 124, obs. M.-Ch. Rouault ; AJDA 1995, p. 940 et p. 875, chron. J.-H. Stahl et D. Chauvaux ; RFD adm. 1996, p. 415, concl. M. Denis-Linton

### a) Violation du Règlement 2252/2004

Tout comme la CNIL dans son avis du 11 décembre 2007, force est de constater que *« le recueil de huit empreintes digitales, d'une part, et la conservation en base centrale de l'image numérisée de ces dernières ainsi que celle du visage du titulaire, d'autre part, ne résultent pas des prescriptions »* du Règlement 2252/2004.

En conséquence, le décret du 30 avril 2008 ne peut pas prétendre être l'instrument de transposition du Règlement 2252/2004.

Bien au contraire, comme cela a été relevé lors de la présentation du texte (Cf. I.B), le décret du 30 avril 2008 :

- ajoute au texte,
- ne respecte pas le nombre d'empreintes digitales fixé par le G29 et retenu par la Commission européenne, et
- ne tient pas compte des prises de position tranchées tant du G29 que du Parlement européen.

En raison de cette violation manifeste du Règlement 2252/2004, le décret du 30 avril 2008 devra être déclaré nul.

### b) Violation du principe de proportionnalité

L'article 8 précité du Décret méconnait également le principe de proportionnalité inscrit respectivement dans le Règlement 2252/2004 et dans les articles 6 et 7 de la loi « Informatique et Libertés ».

Dans son avis n° 3/2005, le G29 considère que :

> ***La création d'une base de données centralisée*** *contenant les données personnelles et en particulier les données biométriques de tous les citoyens (européens)* ***risquerait de violer le principe de base de proportionnalité.***
>
> *Toute base de données centralisée accroîtrait les risques* ***d'utilisation abusive*** *et d'****appropriation frauduleuse****.*
>
> *Elle accroîtrait également le risque d'abus et de* ***dérapages****.*
>
> *Enfin, elle augmenterait également le risque d'utilisation des éléments d'identification biométrique comme «clés d'accès» à diverses bases de données, et partant d'interconnexion de différents fichiers.*

Dans son avis du 11 décembre 2007, la CNIL considère que le principe de proportionnalité n'est pas respecté pour les raisons suivantes :

- *le recueil de l'image numérisée du visage du demandeur et des empreintes digitales de huit doigts ainsi que leur conservation dans le système de traitement « DELPHINE », pourraient ainsi constituer la première base centralisée de données biométriques à finalité administrative portant sur des ressortissants français.*
- *(…) la Commission tient à rappeler 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 Commission 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.*

  *En outre, au regard des éléments dont elle dispose et dans la mesure où le dispositif envisagé se limite à rendre possible l'accès ponctuel des autorités judiciaires aux données biométriques, en exécution de réquisitions ou de commissions-rogatoires, la Commission estime que ledit dispositif ne paraît pas constituer, en l'état, un outil décisif de lutte contre la fraude documentaire de nature à lever les préventions exprimées jusqu'alors par la Commission à l'endroit de la constitution de bases centralisées de données biométriques. En effet, la Commission observe qu'aucune mesure particulière n'est prévue, parallèlement à la conservation de données biométriques, pour s'assurer de l'authenticité des pièces justificatives fournies à l'appui des demandes (…)*

  *Par conséquent, même si le Ministère de l'Intérieur, de l'Outre-mer et des Collectivités territoriales s'engage à préciser aux termes du projet de décret qu'il ne sera pas possible de procéder à une recherche en identification à partir de l'image numérisée des empreintes digitales et que le système envisagé ne comportera pas de dispositif de reconnaissance faciale à partir de l'image numérisée de la photographie,* ***la conservation dans une base centrale des images numérisées du visage et des empreintes digitales semble disproportionnée ».***

Comme le rappelle M. Alain Bensoussan dans son ouvrage de référence[24], le principe de proportionnalité est un principe général du droit, régulièrement utilisé comme tel par le Conseil constitutionnel[25].

Ce principe a été introduit dans la loi « Informatique et Libertés » par la loi du 6 août 2004 afin d'assurer l'équilibre entre les prérogatives des responsables des traitements et les droits des personnes concernées.

Le principe de proportionnalité résulte :

- D'une part, de l'article 6 qui énonce que *« Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes : (…) les données (…) sont adéquates, pertinentes et* ***non excessives*** *au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs »* ;

- D'autre part, de l'article 7 qui précise *« Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes (5°). La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire,* ***sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée ».***

Si l'autorité administrative indépendante[26] en charge de la régulation du secteur d'activité considère qu'une disposition est disproportionnée, il faut donc en conclure que ce décret viole à l'évidence une loi qui s'impose pourtant à lui.

**En conséquence, le décret du 30 avril 2008 devra être annulé pour violation ensemble :**
**- de l'article 27 de la loi « Informatique et Libertés »,**
**- des principes édictés à l'article 4 du Règlement CEE 2252/2004 du 13 décembre 2004, et**
**- du principe de proportionnalité inscrit dans le Règlement 2252/2004 précité et dans les articles 6 et 7 de la loi « Informatique et Libertés »,.**

---

24 Alain Bensoussan, *Informatique et libertés,* Ed° Francis Lefebvre, 2008, n° 220 et s.

25 Cons. const. Décision du 16 août 2007, décision n° 2007-555 DC

26 Patrice Gélard et al., *Les autorités administratives indépendantes : évaluation d'un objet juridique non identifié*, Rapport n° 404 (2005/2006) au nom de l'Office parlementaire d'évaluation de la législation.

### d) Illégalité en raison du but de l'acte (détournement de pouvoir)

A toutes fins utiles, il convient de rappeler les dispositions de l'article 8 de la Convention européenne des droits de l'homme :

> ***Article 8 . Droit au respect de la vie privée et familiale***
>
> *1- Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.*
>
> *2- Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la **loi** et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.*

Le recours à un simple acte réglementaire pour créer une base de données contenant des informations biométriques représente un détournement de pouvoir. En effet, en violation de l'article 8 de la CEDH, il sera possible à un gouvernement de porter atteinte au respect de la vie privée et familiale par une simple modification réglementaire des finalités de la base de données ainsi créée.

La violation du principe de finalité constitue un détournement de pouvoir souhaitée sciemment afin d'empêcher tout contrôle démocratique de la base de données ainsi créée.

C'est une marche forcée en direction d'une *« société de surveillance »*, inacceptable pour les Requérants.

Là encore, la Haute-Juridiction sanctionnera le détournement de pouvoir en annulant le décret du 30 avril 2008.

# PAR CES MOTIFS

**Et tous autres à produire, déduire ou suppléer au besoin même d'office, plaise au Conseil d'Etat :**

CONSTATER QUE le décret n° 2008-426 du 30 avril 2008 modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques est entaché d'illégalités.

En conséquence, ANNULER le décret n° 2008-426 du 30 avril 2008.

*SOUS TOUTES RESERVES*

## BORDEREAU DE PIECES COMMUNIQUEES

Pièce n° 1- Décret n° 2008-426 du 30 avril 2008

Pièce n° 2 - Mandat d'ester en justice des Requérants

Pièce n° 3 - Avis n° 7/2004 du G29

Pièce n° 4 - Lettre du président du G29 au président du Conseil de l'Union européenne en date du 30 novembre 2004

Pièce n° 5 - Règlement 2252/2004 du 13 décembre 2004

Pièce n° 6 Avis n° 3/2005 du G29

Pièce n° 7 Extraits du 27ème rapport de la CNIL

Pièce n° 8 Avis de la CNIL sur le projet de décret attaqué.

**Pièce n° 1**

4 mai 2008 JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE Texte 4 sur 52

# Décrets, arrêtés, circulaires

## TEXTES GÉNÉRAUX

### MINISTÈRE DE L'INTÉRIEUR, DE L'OUTRE-MER ET DES COLLECTIVITÉS TERRITORIALES

### Décret n° 2008-426 du 30 avril 2008 modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques

NOR : *IOCD0807352D*

Le Premier ministre,

Sur le rapport de la ministre de l'intérieur, de l'outre-mer et des collectivités territoriales et du ministre des affaires étrangères et européennes,

Vu le règlement (CE) n° 2252/2004 du 13 décembre 2004 du Conseil ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 27 ;

Vu le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques, modifié par les décrets n° 2007-86 du 23 janvier 2007 et n° 2007-893 du 15 mai 2007 ;

Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 11 décembre 2007 ;

Vu l'avis du conseil général de Mayotte en date du 9 novembre 2007 ;

Vu l'avis du gouvernement de la Polynésie française en date du 31 octobre 2007 ;

Vu l'avis du gouvernement de la Nouvelle-Calédonie en date du 15 octobre 2007 ;

Vu la saisine du conseil territorial de Saint-Pierre-et-Miquelon en date du 28 septembre 2007 ;

Le Conseil d'Etat (section de l'intérieur) entendu,

Décrète :

**Art. 1er.** – Le décret du 30 décembre 2005 susvisé est modifié conformément aux articles 2 à 11 du présent décret.

**Art. 2.** – I. – Dans l'intitulé, le mot : « électroniques » est supprimé.

II. – Dans l'ensemble du décret, les mots : « passeport électronique » sont remplacés par le mot : « passeport ».

**Art. 3.** – Au premier alinéa de l'article 2, il est ajouté à la fin de la première phrase : « , ainsi que, hors le cas prévu au premier alinéa de l'article 6-1, l'image numérisée des empreintes digitales de deux doigts ».

**Art. 4.** – L'article 5 est ainsi modifié :

1° Au premier alinéa, les mots : « de la copie intégrale » sont supprimés ;

2° Au deuxième alinéa, les mots : « à l'article 28 du code civil » sont remplacés par les mots : « aux articles 28 et 28-1 du code civil » ;

3° Le quatrième alinéa est supprimé.

**Art. 5.** – Après l'article 6 du même décret, il est inséré un article 6-1 ainsi rédigé :

« *Art. 6-1.* – Lors du dépôt de la demande de passeport, il est procédé au recueil de l'image numérisée du visage et des empreintes digitales de huit doigts du demandeur. Les empreintes digitales des enfants de moins de six ans ne sont pas recueillies.

« A moins que le demandeur ne fournisse deux photographies d'identité de format 35 × 45 mm identiques, récentes et parfaitement ressemblantes, le représentant de face et tête nue, l'image numérisée de son visage est recueillie par la mise en œuvre de dispositifs techniques appropriés. Ces photographies et cette image sont conformes aux spécifications arrêtées sur le fondement de l'article 2 *(c)* du règlement (CE) n° 2252/2004 du 13 décembre 2004 du Conseil. »

**Art. 6.** – Après l'article 17, est inséré un chapitre V ainsi rédigé :

« CHAPITRE V

**« Conditions de délivrance du passeport temporaire**

« *Art. 17-1.* – A titre exceptionnel et pour des motifs de nécessité impérieuse ou d'urgence dûment justifiée, il peut être délivré un passeport d'une durée de validité d'un an ne comportant pas de composant électronique lorsque les conditions ci-dessus ne permettent pas de délivrer le titre dans les conditions prévues aux chapitres Ier à IV.

« Ces passeports temporaires sont délivrés par l'autorité administrative compétente pour la délivrance des passeports mentionnés à l'article 1er.

« Les dispositions des articles 1er, 3 et 6-1 sont applicables au passeport temporaire. »

**Art. 7.** – L'article 18 est rédigé comme suit :

« *Art. 18.* – Afin de mettre en œuvre les procédures d'établissement, de délivrance, de renouvellement et de retrait des passeports mentionnés aux articles 1er et 17-1, ainsi que pour prévenir et détecter leur falsification et leur contrefaçon, le ministre de l'intérieur est autorisé à créer un système de traitement automatisé de données à caractère personnel dénommé TES. »

**Art. 8.** – L'article 19 est ainsi modifié :

1° Le *a* est complété par un alinéa ainsi rédigé :

« – l'image numérisée du visage et celle des empreintes digitales ; ».

2° Après le *c*, il est inséré un *d* ainsi rédigé :

« *d)* L'image numérisée des pièces du dossier de demande de passeport. »

3° Après le *d*, il est ajouté un alinéa ainsi rédigé :

« Le traitement ne comporte ni dispositif de reconnaissance faciale à partir de l'image numérisée du visage ni dispositif de recherche permettant l'identification à partir de l'image numérisée des empreintes digitales enregistrées dans ce traitement. »

**Art. 9.** – L'article 21-1 est ainsi modifié :

1° Au premier alinéa, après les mots : « à l'article 18 », sont insérés les mots : « , à l'exclusion de l'image numérisée des empreintes digitales, ».

2° Le deuxième alinéa est ainsi complété :

« individuellement désignés et spécialement habilités respectivement par le directeur général de la police nationale et le directeur général de la gendarmerie nationale ; ».

3° Le troisième alinéa est ainsi complété :

« individuellement désignés et spécialement habilités respectivement par le directeur général de la sécurité extérieure, le directeur de la protection et de la sécurité de la défense ou le directeur du renseignement militaire. »

**Art. 10.** – L'article 25 est ainsi modifié :

1° La première phrase est ainsi complétée :

« ainsi que d'une notice d'information sur la nature des données à caractère personnel enregistrées dans le traitement automatisé établie dans les conditions prévues à l'article 32 de la loi du 6 janvier 1978 susvisée. »

2° Il est ajouté un alinéa ainsi rédigé :

« La copie prévue au premier alinéa ne comporte, s'agissant des empreintes digitales recueillies, que l'indication du nombre et de la nature des empreintes enregistrées dans le composant électronique. »

**Art. 11.** – Les articles 28 et 30 sont abrogés.

**Art. 12.** – Le décret n° 2001-847 du 11 septembre 2001 relatif à la durée des passeports délivrés en Nouvelle-Calédonie, en Polynésie française, dans les îles Wallis et Futuna, à Mayotte et à Saint-Pierre-et-Miquelon est abrogé.

**Art. 13.** – Un arrêté du ministre de l'intérieur fixe les dates à partir desquelles les règles fixées par le présent décret seront applicables aux demandes présentées dans les départements en métropole.

Un arrêté conjoint du ministre de l'intérieur et du ministre chargé de l'outre-mer fixe les dates à partir desquelles les règles fixées par le présent décret seront applicables aux demandes présentées dans les départements d'outre-mer, dans les collectivités d'outre-mer et en Nouvelle-Calédonie.

Un arrêté conjoint du ministre de l'intérieur et du ministre des affaires étrangères fixe les dates à partir desquelles les règles fixées par le présent décret seront applicables aux demandes présentées par les Français établis hors de France.

**Art. 14.** – Le présent décret est applicable sur tout le territoire de la République.

**Art. 15.** – La ministre de l'intérieur, de l'outre-mer et des collectivités territoriales, le ministre des affaires étrangères et européennes, la garde des sceaux, ministre de la justice, le ministre de la défense, le ministre du budget, des comptes publics et de la fonction publique et le secrétaire d'Etat chargé de l'outre-mer sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel* de la République française.

Fait à Paris, le 30 avril 2008.

FRANÇOIS FILLON

Par le Premier ministre :

*La ministre de l'intérieur,*
*de l'outre-mer et des collectivités territoriales,*
MICHÈLE ALLIOT-MARIE

*Le ministre des affaires étrangères*
*et européennes,*
BERNARD KOUCHNER

*La garde des sceaux, ministre de la justice,*
RACHIDA DATI

*Le ministre de la défense,*
HERVÉ MORIN

*Le ministre du budget, des comptes publics*
*et de la fonction publique,*
ERIC WOERTH

*Le secrétaire d'Etat*
*chargé de l'outre-mer,*
YVES JÉGO