

N° 317827

Association pour la promotion de l'image, Confédération française de la photographie, société Photomaton, société Photo Élisabeth et société Duka

N° 317952

M. Didier C... et autres

N° 318013

Associations Imaginons un réseau internet solidaire (IRIS) et Ligue des droits de l'homme (LDH)

N° 318051

M. Raymond A...

Assemblée

Séance du 30 septembre 2011

Lecture du 26 octobre 2011

Conclusions

Julien Boucher, rapporteur public

(Ce texte est celui qui a été prononcé par M. Boucher en séance publique ; il a toutefois dû subir quelques modifications uniquement destinées à permettre d'identifier sans ambiguïté les références de jurisprudence citées dont les noms étaient effacés pour la mise en ligne.)

1. La biométrie, si l'on se fie à l'étymologie de ce terme apparu vers le milieu du XIX^e siècle, est la « mesure du vivant ». On a d'abord entendu par-là, de fait, l'application des techniques quantitatives, et notamment statistiques, à l'étude des phénomènes biologiques : on parle aussi, en ce sens, de biostatistique.

C'est toutefois un autre sens, apparu beaucoup plus récemment, qui tend aujourd'hui à s'imposer dans le langage courant. Dans cette acception nouvelle, la biométrie est un ensemble de techniques permettant la reconnaissance d'un individu au moyen de caractéristiques morphologiques ou biologiques, voire comportementales, supposées uniques et permanentes.

Il est certes clair que, même ainsi définie, la biométrie n'est pas une nouveauté absolue, mais trouve son origine dans des techniques utilisées de longue date, en particulier, dans le domaine de l'identification judiciaire. On peut notamment citer, à cet égard, la méthode anthropométrique mise en œuvre à la préfecture de police de Paris, à partir des années 1880, par Alphonse Bertillon¹, ou encore les travaux, à la même époque, du britannique Francis Galton, cousin de Charles Darwin, qui, dans le cadre des recherches qui lui ont valu la renommée ambiguë de fondateur de l'eugénisme, a été l'un des premiers à mettre en évidence l'intérêt des empreintes digitales comme instrument d'identification².

Ce qui est nouveau, en revanche, c'est l'automatisation des dispositifs biométriques, dans laquelle beaucoup ont vu un véritable changement de nature³. Cette automatisation, permise notamment par les progrès de l'informatique et l'essor des technologies numériques, a en tout cas ouvert la voie, dans les années récentes, à un développement sans précédent, tant en ce qui concerne la variété des usages que l'importance de la population concernée, du recours à la biométrie.

Quelle que soit la sophistication des dispositifs mis en œuvre, qu'il s'agisse des capteurs utilisés ou des algorithmes mobilisés aux différentes étapes du processus, le principe de la reconnaissance biométrique est simple.

Dans un premier temps, on recueille, auprès d'un individu dont l'identité est établie par ailleurs, la caractéristique biométrique désirée, et on enregistre une représentation de cette caractéristique en l'associant à cette identité – on parle d'« enrôlement ». Au nombre des caractéristiques théoriquement utilisables à cette fin, on peut notamment citer les traits du visage, les empreintes digitales ou palmaires, la géométrie du contour de la main, l'image de l'iris de l'œil, la voix, le profil génétique ou encore, s'agissant de la biométrie comportementale, la démarche ou la façon de frapper sur un clavier d'ordinateur⁴. Puis, dans un second temps, en présence d'un individu dont l'identité doit être établie, on recueille auprès de lui la caractéristique biométrique requise et on la compare à l'enregistrement préalablement réalisé – étant précisé que, en pratique, la comparaison, pour pouvoir être automatisée, porte seulement sur des « gabarits », qui condensent les éléments les plus distinctifs de la caractéristique biométrique utilisée par le système. Si le résultat de la comparaison est positif, on est assuré, en principe, d'avoir affaire à la même personne.

¹ V., pour un exposé détaillé, Ilse About, « Les fondations d'un système national d'identification policière en France (1893-1914) », *Genèses*, 2004/1, n° 54, pp. 28-52.

² V. par ex., sur le sujet, Jonathan Finn, « Photographing Fingerprints: Data Collection and State Surveillance », *Surveillance & Society*, 3(1): 21-44.

³ V. sur cette problématique Gérard Dubey, « Les deux corps de la biométrie », *Communications*, 2007, vol. 81, n° 1, p. 153.

⁴ V. par ex., sur ce dernier point, la délibération de la Commission nationale de l'informatique et des libertés (CNIL) n° 2011-183 du 23 juin 2011 autorisant la mise en œuvre par la société JVL d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance de la frappe au clavier et ayant pour finalité la démonstration de son fonctionnement à de potentiels clients.

Il importe de souligner dès ce stade que, selon le terme de comparaison retenu, la reconnaissance biométrique peut avoir deux objets, que l'on désigne généralement par les termes d'*identification*, d'une part, et d'*authentification*, d'autre part.

L'identification consiste à déterminer quelle est l'identité d'une personne qui ne peut ou ne veut la révéler. Pour cela, il faut pouvoir comparer la caractéristique biométrique pertinente de cette personne avec celle de l'ensemble des personnes auprès desquelles on a préalablement recueilli la même caractéristique : on parle de comparaison « un contre n », n étant le nombre de personnes « enrôlées ». L'utilisation de la biométrie à des fins d'identification suppose donc l'existence d'un fichier rassemblant les données relatives à l'ensemble de la population concernée.

C'est sur ce principe que, de longue date, repose l'identification judiciaire : un bon exemple en est donné par le fichier automatisé des empreintes digitales (FAED) du ministère de l'intérieur⁵, qui permet notamment de rechercher l'identité d'un individu à partir de traces ou empreintes digitales ou palmaires. En dehors même du champ judiciaire, les dispositifs d'identification biométrique se sont multipliés ces dernières années, notamment dans une perspective de maîtrise des flux migratoires. On peut citer, en particulier, le système « Eurodac », créé, en l'an 2000, par un règlement européen⁶ : ce système, qui repose sur une base de données centralisée, gérée par la Commission européenne, rassemble les empreintes des dix doigts de l'ensemble des demandeurs d'asile âgés de quatorze ans au moins ainsi que des personnes ayant franchi irrégulièrement une frontière extérieure de l'Union, afin notamment de permettre, par confrontation avec ces données biométriques, de déterminer si une personne sollicitant l'asile n'a pas précédemment présenté une demande dans un autre État membre et ainsi de faciliter la détermination de l'État responsable de l'examen de sa demande dans le cadre de la convention de Dublin.

Mais la biométrie peut également, et plus modestement, se voir assigner une fonction d'authentification. Celle-ci consiste à s'assurer qu'une personne a bien l'identité qu'elle revendique. Pour cela, il suffit de comparer la caractéristique biométrique pertinente de cette personne avec la représentation de cette caractéristique associée à son identité dans l'enregistrement réalisé lors de l'enrôlement : on parle de comparaison « un contre un ». À la différence de l'identification, l'authentification ne rend donc pas absolument nécessaire la constitution d'un fichier : les données biométriques peuvent en effet être enregistrées sur un support décentralisé, par exemple un ordinateur doté d'un capteur d'empreintes digitales, dont on veut s'assurer que seul son légitime propriétaire y a accès.

2. Le développement de documents d'identité ou de voyage biométriques s'inscrit dans cette logique d'authentification.

⁵ Régi par le décret n° 87-249 du 8 avril 1987.

⁶ V. le règlement (CE) n° 2725/2000 du Conseil du 11 décembre 2000 concernant la création du système « Eurodac » pour la comparaison des empreintes digitales aux fins de l'application efficace de la convention de Dublin.

Jusqu'à récemment, en effet, seule la comparaison visuelle de la photographie figurant généralement sur le document et du visage de celui qui le présentait permettait de s'assurer qu'il en était bien le titulaire : or chacun sait que, indépendamment même de la possibilité de falsifier la photographie, cette vérification n'a rien d'infailible. L'utilisation des techniques biométriques contemporaines a, en revanche, permis d'envisager de créer un lien beaucoup plus fiable entre le document et son titulaire, en enregistrant, dans un support de stockage sécurisé – en pratique un circuit intégré – inclus dans l'épaisseur du document, une ou plusieurs caractéristiques biométriques du titulaire.

Des projets en ce sens, inspirés essentiellement par le souci de lutter contre la fraude dite « documentaire », existent de longue date, en France et ailleurs, mais ils ont reçu une impulsion décisive dans le contexte créé par les attentats terroristes du 11 septembre 2001. À tort ou à raison⁷, en effet, un consensus s'est alors installé, dans les pays occidentaux, pour considérer que la biométrie, en permettant notamment de mieux contrôler les déplacements internationaux des personnes, avait vocation à occuper une place de choix parmi les instruments de lutte contre le terrorisme et, plus largement, contre la criminalité sous toutes ses formes.

C'est ainsi que l'Organisation de l'aviation civile internationale (OACI) a, à partir de 2003, travaillé à l'élaboration de spécifications en vue de la mise en place, au niveau international, d'un passeport biométrique standardisé ayant vocation, à terme, à se substituer au traditionnel passeport lisible à la machine. Ces spécifications prévoient notamment l'enregistrement, sur un circuit intégré contenu dans le passeport, d'une image numérisée du visage du titulaire, l'État émetteur pouvant en outre, s'il l'estime utile, compléter cet élément biométrique « principal » par des empreintes digitales ou oculaires⁸.

Les États membres de l'Union européenne ont été d'autant plus incités à adopter rapidement ce nouveau standard que, à la même époque, les États-Unis ont, par étapes, décidé de subordonner le bénéfice de leur programme de dispense de visa (*Visa Waiver Program*), qui profite aux ressortissants d'un certain nombre de pays européens, dont la France, à la présentation d'un passeport biométrique répondant aux spécifications de l'OACI.

C'est dans ce contexte que le Conseil européen de Thessalonique des 19 et 20 juin 2003 a posé le principe de mesures communes ayant notamment pour objet l'intégration d'éléments biométriques dans les passeports des citoyens de l'Union européenne. Cette orientation a débouché sur l'adoption d'un règlement du Conseil, en

⁷ V., pour un point de vue critique, Laurent Laniel et Pierre Piazza, « L'encartement, réponse au terrorisme (France/Grande-Bretagne) ? », in Xavier Crettiez et Pierre Piazza (dir.), *Du papier à la biométrie – Identifier les individus*, Presses de la FNSP, 2006, p. 211.

⁸ Pour le détail de ces spécifications, voir la 6^e édition (2006) du Doc 9303 de l'OACI (« Documents de voyage lisibles à la machine »), Partie 1 (« Passeports lisibles à la machine »), Volume 2 (« Spécifications pour passeports à composant électronique contenant des éléments d'identification biométrique »).

date du 13 décembre 2004⁹, lequel a prévu, en son article 1^{er}, que les passeports et documents de voyage délivrés par les États membres devraient désormais comporter un « *support de stockage de haute sécurité* » contenant deux éléments biométriques, à savoir « *une photo faciale* » et « *deux empreintes digitales relevées à plat* ». L'article 6 de ce règlement précisait que les États membres devaient se conformer à leurs obligations en la matière au plus tard 18 mois après l'adoption des spécifications techniques complémentaires à établir en vertu de son article 2, en ce qui concerne la photo faciale, et au plus tard 36 mois après cette même date en ce qui concerne les empreintes digitales. Ces délais ont couru à compter du 28 juin 2006, date à laquelle est intervenue la décision de la Commission fixant les spécifications en cause.

C'est pour l'application de ce règlement qu'a été pris, dans un premier temps, le décret du 30 décembre 2005 relatif aux passeports électroniques¹⁰, lequel a prévu l'inclusion, dans les différentes catégories de passeports, d'un « *composant électronique* » contenant l'ensemble des mentions devant figurer sur le passeport – à l'exception de la signature du titulaire – ainsi que l'« *image numérisée* » du visage de ce dernier.

Le même décret a en outre, à son article 18, autorisé le ministre de l'intérieur à créer un fichier informatique national pour « *mettre en œuvre les procédures d'établissement, de délivrance, de renouvellement, de remplacement et de retrait des passeports [...], ainsi que pour prévenir, détecter et réprimer leur falsification et leur contrefaçon* ». En réalité, un tel fichier national existait depuis 1999, comme composante du système de fabrication et de gestion informatisée des passeports dénommé « DELPHINE »¹¹. Soulignons également que l'image numérisée du visage du titulaire n'était pas au nombre des données pouvant être traitées : elle ne figurait donc, à l'époque, que sur le composant électronique du passeport.

Par la suite, et afin notamment de respecter l'échéance du 28 juin 2009, un décret du 30 avril 2008¹² est venu modifier celui du 30 décembre 2005 pour prévoir l'inclusion, dans le composant électronique du passeport, en sus de la photographie numérisée du demandeur, de « *l'image numérisée des empreintes digitales de deux doigts* ». Mais les auteurs de ce décret sont allés au-delà des exigences du règlement européen du 13 décembre 2004, en prévoyant que, lors du dépôt de la demande de passeport, il serait procédé au recueil de l'image numérisée du visage et, sauf en ce qui concerne les enfants de moins de six ans, « *des empreintes digitales de huit doigts du demandeur* », et non seulement des deux prévues par le règlement, toutes ces données biométriques devant être enregistrées dans le traitement automatisé régi par le décret

⁹ 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.

¹⁰ N° 2005-1726.

¹¹ V. l'arrêté interministériel du 22 novembre 1999 portant création par le ministère de l'intérieur d'un traitement automatisé d'informations nominatives relatif à la délivrance des passeports.

¹² Décret n° 2008-426 modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques.

du 30 décembre 2005, qui reçoit la dénomination de « TES ». Le décret du 30 avril 2008 prévoit en outre que les pièces du dossier de demande de passeport seront dorénavant numérisées et que leur image sera versée dans ce traitement. Enfin, dernière innovation, il est précisé que, sauf si le demandeur fournit deux photographies d'identité répondant à certaines spécifications, *« l'image numérisée de son visage est recueillie par la mise en œuvre [par l'administration] de dispositifs techniques appropriés »*.

3. Quatre recours pour excès de pouvoir ont été formés devant vous à l'encontre du décret du 30 avril 2008.

Sous le n° 317952, vous avez été saisis par neuf particuliers, dont le premier dénommé est M. Didier C..., qui se prévalent de la qualité non contestée de titulaires de passeports français, laquelle suffit à leur conférer un intérêt à demander l'annulation du décret litigieux, auquel ils reprochent essentiellement de prévoir l'enregistrement des données biométriques dans le fichier TES. Ce sont des griefs du même ordre qui ont conduit M. Raymond A..., qui se prévaut lui aussi de la qualité de titulaire d'un passeport français, à vous saisir sous le n° 318051.

Sous le n° 318013, un recours a été présenté par les associations Imaginons un réseau internet solidaire (IRIS) et Ligue des droits de l'homme (LDH). Nous ne sommes pas convaincu que l'objet statutaire de l'association IRIS, qui est de *« favoriser la défense et l'élargissement des droits de chacun à la libre utilisation des réseaux électroniques »*, lui confère un intérêt lui donnant qualité pour demander l'annulation du décret litigieux. Mais ceci est de peu de conséquence, en l'absence de conclusions propres de cette association, dans la mesure où l'intérêt pour agir de la LDH, qui s'est notamment donné pour objet de *« lutte[r] en faveur du respect des libertés individuelles en matière de traitement de données informatiques »*, et qui est régulièrement représentée par son président en exercice, est, quant à lui, incontestable.

Enfin, sous le n° 317827, vous avez été saisis par l'Association pour la promotion de l'image (API), la Confédération française de la photographie (CFP), la société Photomaton, la société Studio Photo Élisabeth et la société Duka. L'API rassemble diverses organisations professionnelles du secteur de l'image, notamment photographique, et a pour objet, entre autres, de *« représenter l'ensemble de la profession quand ses intérêts sont en jeu »* ; tel est également l'un des objets statutaires de la CFP. La raison sociale de la société Photomaton dit assez son activité, et les deux derniers requérants sont apparemment de petites entreprises de photographie. Ces différentes personnes morales se plaignent essentiellement de l'atteinte que le décret du 30 avril 2008 porte au secteur économique de la photographie d'identité, en prévoyant la possibilité pour les demandeurs de passeport de faire recueillir l'image numérisée de leur visage par les services chargés de recevoir les demandes. Dans cette mesure, l'intérêt à agir de ces personnes morales, qui sont régulièrement représentées, nous paraît incontestable.

4. Les quatre requêtes nous paraissent donc recevables. Elles articulent des moyens de légalité externe qui sont très largement similaires.

4.1. Il est d'abord soutenu, à cet égard, que le décret attaqué est intervenu dans le champ de compétence du législateur.

La critique s'écarte aisément en ce qui concerne les dispositions relatives au fichier TES, dans la mesure où le 2° du I de l'article 27 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés¹³ prévoit expressément que sont autorisés par décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés (CNIL), les « *traitements de données à caractère personnel mis en œuvre pour le compte de l'État qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes* ». Cette disposition, issue d'une loi du 6 août 2004¹⁴, a été adoptée spécialement pour permettre la création, par voie réglementaire, de traitements tels que le fichier TES¹⁵.

On peut avoir davantage d'hésitation en ce qui concerne les dispositions du décret attaqué qui réglementent la délivrance des passeports, dans la mesure où, la détention de ce document étant généralement nécessaire pour franchir les frontières, tout refus ou retrait de passeport met en cause la liberté fondamentale d'aller et venir, laquelle, selon la formule jurisprudentielle, n'est pas limitée au territoire national, mais comporte également le droit de le quitter (v. TC 9 juin 1986, *Commissaire de la République de la région Alsace et autres c/ E...*, n° 2434, p. 301). Toutefois, l'exigence d'un passeport pour franchir les frontières ne résulte évidemment pas du décret attaqué ou du décret du 30 décembre 2005 qu'il modifie, et ce dernier texte, qui énonce seulement, à son article 4, que « *le passeport est délivré, sans condition d'âge, à tout Français qui en fait la demande* », ne définit nullement les cas dans lesquels il pourrait être refusé ou retiré – vous estimez en effet que ces cas continuent d'être définis par un décret législatif de la convention nationale du 7 décembre 1792 (v. sur ce point Assemblée, 8 avril 1987, *Ministre de l'intérieur et de la décentralisation c/ P...*, n° 55895, p. 128). Or la seule énumération des pièces et informations à fournir en vue de la délivrance d'un passeport, dès lors que ces exigences ne sont pas excessives ou impossibles à remplir pour certaines catégories de citoyens, ne nous paraît pas, quant à elle, mettre en cause les « *garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* » au sens de l'article 34 de la Constitution (v., en ce sens, 5 mai 2008, *K... et autre*, n°s 293934-294056).

¹³ N° 78-17.

¹⁴ Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

¹⁵ V. par ex. l'intervention de M. Francis Delattre, député, à l'Assemblée nationale, lors de la séance du 29 avril 2004, *J.O. Débats*, p. 3248, 2^e col., § 5.

Il est également soutenu, par l'API et autres, que l'intervention du législateur était nécessaire pour confier aux maires, en tant qu'agents de l'État, le soin de recevoir les demandes de passeport et de remettre aux demandeurs les documents une fois élaborés, compte tenu des dispositions de l'article L. 1611-1 du code général des collectivités territoriales (CGCT) selon lesquelles : « *Aucune dépense à la charge de l'État ou d'un établissement public à caractère national ne peut être imposée directement ou indirectement aux collectivités territoriales ou à leurs groupements qu'en vertu de la loi.* » C'est en application de ces dispositions, en effet, que vous avez annulé les articles 7 et 9 du décret du 26 février 2001¹⁶ qui confiaient aux maires, agissant en qualité d'agents de l'État, la tâche de recueillir les demandes de passeport, de les transmettre aux préfets ou aux sous-préfets et de remettre aux demandeurs les passeports qui leur sont adressés par ces derniers (5 janvier 2005, *Commune de Versailles*, n° 232888, p. 5). Mais force est de constater que ni le décret attaqué, ni le décret du 30 décembre 2005 qu'il modifie, qui ont prudemment laissé de côté cette question pratique d'une grande importance, ne font état d'une quelconque intervention des maires dans la délivrance des passeports : le moyen manque dont en fait.

4.2. Il est ensuite soutenu que le décret attaqué, en tant qu'il porte sur le fichier TES, a été pris selon une procédure irrégulière, dans la mesure où l'avis de la CNIL n'a été publié au *Journal officiel* que le 10 mai 2008, alors que le décret l'avait été dès le 4 mai. Or, selon les requérants, une publication simultanée était requise à peine d'irrégularité du décret.

Nous pensons effectivement qu'une publication simultanée était en principe requise. On peut certes douter que cette exigence résulte, comme le soutiennent certains des requérants, des dispositions de l'article 26 de la loi du 6 janvier 1978, qui prévoient que l'avis de la CNIL est publié « *avec* » l'acte réglementaire qui autorise les traitements visés par cet article, au nombre desquels figurent ceux qui « *ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté* ». Sans doute, dans la mesure où il a notamment pour objet de « *prévenir et détecter [la] falsification et [la] contrefaçon* » des passeports, peut-on soutenir que le fichier TES est au nombre de ces traitements. Mais l'autorisation de ces derniers ne justifie en principe que le recours à un arrêté ministériel, et si, en l'espèce, un décret en Conseil d'État était nécessaire, c'est en vertu des dispositions déjà citées du 2° du I de l'article 27 de la loi, qui vise, nous vous l'avons dit, les « *traitements de données à caractère personnel mis en œuvre pour le compte de l'État qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes* ».

Ceci étant dit, les dispositions du I de l'article 27 prévoient également que le décret autorisant le traitement doit être pris « *après avis motivé et publié* » de la CNIL et, si la loi n'exige pas elle-même une publication simultanée, c'est son décret

¹⁶ N° 2001-185.

d'application, en date du 20 octobre 2005¹⁷, qui s'en est chargé : son article 18 dispose en effet que « *les avis motivés de la commission émis en application des articles 26 et 27 de la loi du 6 janvier 1978 [...] et les actes sur lesquels ils portent sont publiés à la même date par le responsable du traitement* ».

Pour autant, nous ne croyons pas que la méconnaissance de cette exigence soit de nature à entacher d'illégalité le décret attaqué, dès lors que l'avis de la CNIL a bien été rendu avant sa signature. Dans la mesure où les textes n'exigent pas une publication de l'avis de la CNIL préalable à l'édition de l'acte autorisant le traitement, il nous semble en effet que les conditions de cette publication ne peuvent que demeurer sans influence sur la légalité de ce dernier. Peut-être pourrait-on, en revanche, soutenir que la mise en œuvre du traitement ne peut intervenir avant la publication de l'avis de la CNIL, ou encore que les délais de recours à l'encontre de l'acte autorisant le traitement ne courent qu'à compter de cette publication : mais ce sont des questions que la présente affaire ne vous conduira pas à trancher.

4.3. Enfin, il ne ressort pas des pièces du dossier que les informations transmises à la CNIL, en application de l'article 30 de la loi du 6 janvier 1978, à l'appui de la demande d'avis présentée par le ministre de l'intérieur, de l'outre-mer et des collectivités territoriales, aient été, comme le soutient M. A..., incomplètes ou insuffisantes pour lui permettre de se prononcer en toute connaissance de cause.

5. S'agissant maintenant de la légalité interne du décret attaqué, nous observerons d'emblée que, si l'on fait abstraction, à ce stade, du débat relatif aux modalités de recueil de l'image numérisée du visage du demandeur, aucun des requérants ne conteste, dans son principe ou dans ses modalités, le stockage, sur le composant électronique du passeport, de cette image ainsi que de celle de deux empreintes digitales. Cette exigence résulte d'ailleurs directement, nous vous l'avons dit, du règlement européen du 13 décembre 2004.

Les requérants critiquent en revanche vigoureusement le principe de l'enregistrement des données biométriques collectées auprès des demandeurs de passeport dans le fichier national TES, et, à supposer même que le principe puisse en être admis, ils estiment injustifiés la collecte et l'enregistrement de huit empreintes digitales dans ce fichier, alors que seules deux figurent dans le composant électronique du passeport. Selon eux, en effet, l'ampleur et la sensibilité des données collectées sont disproportionnées par rapport aux finalités assignées au fichier en cause. Le décret attaqué méconnaîtrait ainsi, sur ce point, les stipulations de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (convention EDH) et les dispositions de l'article 6 de la loi du 6 janvier 1978, en particulier son 3°.

¹⁷ Décret n° 2005-1309.

5.1. Ces dernières dispositions, qui fixent les conditions générales auxquelles doivent satisfaire les données à caractère personnel faisant l'objet d'un traitement, sont évidemment applicables à la collecte et à l'enregistrement, dans le fichier TES, des données biométriques des titulaires de passeports : en effet, ces données, qui sont associées dans le fichier à l'identité des intéressés, constituent, de ce fait, des informations relatives à des personnes physiques identifiées, et donc des données à caractère personnel au sens de l'article 2 de la loi.

Il importe également de relever, d'emblée, que le contrôle auquel les requérants vous invitent à vous livrer au regard des dispositions de l'article 6 de la loi du 6 janvier 1978 se confond, pour l'essentiel, avec la vérification du respect des exigences résultant de l'article 8 de la convention EDH, en tant qu'il protège le droit au respect de la vie privée.

Selon la Cour européenne des droits de l'homme (Cour EDH), en effet, la collecte et le traitement de données relatives à la vie privée d'un individu constituent une ingérence dans son droit au respect de celle-ci et entrent, par suite, dans le champ d'application des stipulations de l'article 8 (Cour EDH, 26 mars 1987, *Leander c/ Suède*, n° 9248/81). Peu important, pour apprécier l'existence d'une ingérence, l'utilisation faite des données recueillies ou encore leur caractère intrinsèquement sensible ou non (16 février 2000, *Amann c/ Suisse*, n° 27798/95). Des données de nature publique peuvent même relever de la vie privée lorsqu'elles sont, d'une manière systématique, recueillies et mémorisées dans des fichiers tenus par les pouvoirs publics, à plus forte raison lorsque ces données concernent le passé lointain d'une personne (Cour EDH [GC], 4 mai 2000, *Rotaru c/ Roumanie*, n° 28341/95). Dans son arrêt *S. et Marper c/ Royaume-Uni*, rendu en grande chambre le 4 décembre 2008 (n°s 30562/04 et 30566/04), la Cour a d'ailleurs expressément jugé que la conservation, dans des fichiers des autorités, des empreintes digitales d'un individu identifié ou identifiable constituait une ingérence dans son droit au respect de sa vie privée.

Il en résulte que le traitement de telles données ne peut être regardé comme compatible avec les stipulations de l'article 8 de la convention que si l'ingérence qui en résulte est prévue par la loi, poursuit un but légitime et apparaît nécessaire dans une société démocratique. Pour exercer le contrôle de proportionnalité qu'appelle l'appréciation de cette nécessité, la Cour EDH se réfère explicitement, à l'occasion, aux exigences de la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981 (v. not. l'arrêt *S. et Marper c/ Royaume-Uni* précité, §§ 101 et s.). Or l'article 5 de cette convention, qui en constitue le cœur, a été repris presque mot pour mot à l'article 6 de la directive du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la

libre circulation de ces données¹⁸, lequel a été fidèlement transposé, à l'article 6 de la loi du 6 janvier 1978, par la loi du 6 août 2004.

On comprend, dans ces conditions, que la Cour de justice de l'Union européenne (CJUE) ait pu juger qu'une réglementation nationale instituant un traitement de données à caractère personnel ne pouvait satisfaire aux exigences de l'article 6 de la directive du 24 octobre 1995 si elle était incompatible avec les stipulations de l'article 8 de la convention (v. not. CJCE 20 mai 2003, *Österreichischer Rundfunk e.a.*, C-465/00, C-138/01 et C-139/01, Rec. 2003 p. I-4989). Vous ne pouvez que faire de même en ce qui concerne l'article 6 de la loi du 6 janvier 1978, dont on peut considérer, dans ces conditions, qu'il constitue l'explicitation, en ce qui concerne le traitement des données à caractère personnel, des exigences du droit européen en matière de protection de la vie privée.

Deux principes essentiels, pour ce qui nous occupe aujourd'hui, se trouvent exprimés à cet article.

Selon son 2°, qui énonce ainsi ce qu'il est convenu d'appeler le principe de *finalité*, les données à caractère personnel doivent être « *collectées pour des finalités déterminées, explicites et légitimes* » et ne pas être « *traitées ultérieurement de manière incompatible avec ces finalités* ». L'exigence que les finalités soient déterminées tend à exclure ce qu'on pourrait appeler les collectes de précaution : il s'agit de couper court à la tentation qu'a spontanément toute organisation de recueillir autant de données que possible afin d'être assurée, le moment venu, de disposer de celles qui s'avéreront utiles. L'exigence d'explicitation des finalités se traduit notamment, s'agissant des traitements soumis à autorisation, par l'obligation d'indiquer celles-ci dans l'acte d'autorisation¹⁹. Il faut évidemment que les finalités poursuivies soient légitimes, exigence qui inclut, sans s'y résumer, la prohibition de la poursuite de buts illicites, par exemple discriminatoires. Enfin, les données ne doivent pas être détournées de leurs finalités.

Le 3° de l'article 6 de la loi du 6 janvier 1978 contient quant à lui l'expression du principe de *proportionnalité* appliqué à la matière du traitement des données à caractère personnel : il énonce en effet que ces dernières doivent être « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs* ». Selon votre jurisprudence, « *les données pertinentes au regard de la finalité d'un traitement [...] sont celles qui sont en adéquation avec la finalité du traitement et qui sont proportionnées à cette finalité* » (v. 19 juillet 2010, *F... et Mme C...*, n^{os} 317182-323441, p. 320, reprenant, à propos de l'article 6 de la loi du 6 janvier 1978, la formulation retenue, en ce qui concerne l'article 5 de la convention n° 108 du Conseil de l'Europe, par Section, 30 octobre 2001, *Association française des sociétés financières et autres*, n° 204909, p. 518).

¹⁸ Directive 95/46/CE du Parlement européen et du Conseil.

¹⁹ Art. 29, 1° de la loi du 6 janvier 1978.

Une donnée est adéquate si, compte tenu du traitement envisagé, elle est apte à atteindre les objectifs poursuivis par le responsable de ce traitement : il est donc interdit de collecter des données superflues. L'exigence de proportionnalité, quant à elle, doit se comprendre à la lumière du principe, énoncé à l'article 1^{er} de la loi du 6 janvier 1978, selon lequel l'informatique 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* ». Plus précisément, l'atteinte que le traitement de données à caractère personnel porte inéluctablement, en particulier, à la vie privée, doit être regardée comme nécessaire pour atteindre les finalités poursuivies. Ceci implique de mettre en rapport, d'une part, l'ampleur de cette atteinte, en tenant compte non seulement de la nature des données mais aussi, par exemple, des garanties offertes contre les risques de détournement des finalités du traitement, et, d'autre part, le gain escompté du traitement des données litigieuses, eu égard, notamment, à l'existence éventuelle de moyens moins intrusifs de parvenir au même résultat.

On voit donc que l'article 6 de la loi du 6 janvier 1978, contrairement à son article 8 qui prohibe en principe le traitement de certaines données regardées comme intrinsèquement sensibles, laisse aux responsables des traitements une importante marge de manœuvre quant à la nature et à la quantité des données qui peuvent être traitées ; mais il les oblige à une stricte cohérence par rapport aux finalités affichées, et c'est à l'aune de cette exigence qu'il vous faut passer au crible la collecte, dans le fichier TES, des données biométriques des demandeurs de passeports.

5.2. La première question qui vous est posée consiste à savoir si, compte tenu des finalités poursuivies par ce fichier et de l'ensemble de ses caractéristiques, il était légalement possible de prévoir l'enregistrement, dans celui-ci, des données biométriques figurant sur le composant électronique du passeport, à savoir l'image numérisée du visage du demandeur et de deux empreintes digitales. Les requérants soutiennent en substance, à cet égard, que la constitution d'une base de données biométriques susceptible de concerner une grande partie de la population française comporte nécessairement des risques importants, notamment d'utilisation de ces données à des fins autres que celles ayant justifié leur collecte, et que c'est inutilement que l'on court ces risques, dans la mesure où le bon fonctionnement du passeport biométrique ne nécessite pas l'existence d'un tel fichier, puisque sa fonction d'authentification est assurée par le rapprochement des données biométriques du porteur avec celles contenues dans le composant électronique du passeport.

5.2.1. Cette argumentation, comme le soulignent les requérants, peut se recommander de la position prise par diverses autorités, tant européennes que nationales.

Ainsi, à l'occasion de l'élaboration du règlement du 13 décembre 2004, le Parlement européen s'est prononcé²⁰ contre toute centralisation des données

²⁰ Par une résolution législative du 2 décembre 2004.

biométriques, le rapporteur s'étant déclaré « *particulièrement préoccupé* » par cette perspective, au motif qu'une « *base de données centralisée n'[était] pas nécessaire pour établir un lien plus fiable entre le passeport et son titulaire* » et que « *le risque de dérapage* », c'est-à-dire d'« *utilisation des données à d'autres fins que celles initialement prévues* », était « *trop grand* ».

Dans un avis plus récent²¹, émis dans la perspective de la modification du règlement du 13 décembre 2004, le contrôleur européen de la protection des données (CEPD) a émis un avis similaire, invitant la Commission à « *proposer de nouvelles mesures d'harmonisation afin que les données biométriques collectées pour être intégrées dans les passeports délivrés par les États membres de l'[Union européenne] ne puissent être stockées que sur un support décentralisé* ». Selon cette autorité, en effet, la création d'une base centralisée « *présente des risques supplémentaires à l'égard de la protection des données à caractère personnel, comme l'apparition d'autres finalités non prévues par le règlement, voire la pratique d'une "pêche aux informations" dans la base de données, qu'il sera difficile de modérer* ». Le groupe de travail sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel institué par la directive du 24 octobre 1995, dit « groupe de l'article 29 », a, quant à lui, fait savoir son opposition à toute constitution d'un fichier centralisant, au niveau européen, les données biométriques des titulaires de passeports²².

Enfin, la CNIL, dans son avis du 11 décembre 2007 sur le projet de décret en litige, s'est, pour des raisons similaires, déclarée défavorable à l'enregistrement des données biométriques dans le fichier TES, qu'elle a estimé disproportionné par rapport aux objectifs poursuivis : selon elle, « *si légitimes soient-elles, les finalités invoquées ne justifient pas la conservation, au plan national, de données biométriques telles que les empreintes digitales* », car « *les traitements ainsi mis en œuvre seraient de nature à porter une atteinte excessive à la liberté individuelle* ».

5.2.2. Face aux risques ainsi évoqués, le débat entre les parties, et l'audience d'instruction à laquelle a procédé votre 10^e sous-section, ont donc porté, en large part, sur le point de savoir ce qu'apporte, par rapport à un stockage des données biométriques sur le seul support décentralisé que constitue le composant électronique du passeport, une centralisation de celles-ci dans un fichier national.

Ce débat, de façon quelque peu nouvelle dans votre prétoire, met en cause l'architecture même du système globalement formé par le passeport biométrique et le fichier TES. Mais ceci ne doit pas occulter que, fondamentalement, la question posée revient à se demander, de façon très classique, si les auteurs du décret attaqué ont pu, sans enfreindre le principe de proportionnalité, prévoir que certaines données seraient enregistrées dans ce fichier. Dans une affaire où elle était notamment invitée à prendre

²¹ Avis 2008/C 200/01 du 26 mars 2008, publié au J.O.U.E. C 200 du 6 août 2008, p. 1.

²² Avis n° 3/2005 du 30 septembre 2005.

parti sur la nécessité de faire figurer des données à caractère personnel dans un registre centralisé plutôt que de les maintenir dans les seuls registres décentralisés où elles figuraient précédemment, la CJUE a d'ailleurs traité cette question exactement dans les mêmes termes que celle consistant à savoir si telle ou telle catégorie de données pouvait figurer dans ce registre centralisé (v. CJCE [GC], 16 décembre 2008, *Heinz Huber c/ Allemagne*, C-524/06, spéc. point 62).

Au cas d'espèce, il résulte de l'article 18 du décret du 30 décembre 2005, dans sa rédaction issue du décret attaqué, que le fichier TES doit permettre de « *mettre en œuvre les procédures d'établissement, de délivrance, de renouvellement et de retrait des passeports* », ainsi que de « *prévenir et détecter leur falsification et leur contrefaçon* ». Telles sont les finalités explicites, dont la légitimité n'est discutée par aucun des requérants, au regard desquelles vous devrez apprécier la proportionnalité des données recueillies.

Précisons ensuite que, outre les données biométriques, le fichier rassemble quatre catégories d'informations : en premier lieu, des données relatives au titulaire du passeport, qui sont pour l'essentiel celles qui figurent sur le document lui-même ; en second lieu, des informations relatives au titre, telles que le numéro de celui-ci, la date et le lieu de sa délivrance, ou encore, le cas échéant, l'indication qu'il a été perdu, volé, détruit, annulé ou retiré ; en troisième lieu, des données relatives au fabricant du passeport et aux agents chargés de la délivrance de celui-ci ; enfin, et en quatrième lieu, l'image numérisée des pièces du dossier de demande.

Trois catégories de personnes ont accès à ce fichier, ce qui donne une idée du contexte dans lequel ses données ont vocation à être exploitées. Il s'agit d'abord, selon l'article 20 du décret du 30 décembre 2005, des fonctionnaires du ministère de l'intérieur affectés dans le service mettant en œuvre le fichier et des agents et personnels affectés à l'instruction des demandes de passeport, individuellement habilités à cet effet, selon le cas, par le ministre, le préfet, le sous-préfet, l'ambassadeur ou le consul. Il s'agit ensuite, d'après l'article 21 du même décret, des « *personnels chargés des missions de recherche et de contrôle de l'identité des personnes [et] 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* ». Enfin, d'après l'article 21-1, les agents individuellement désignés et spécialement habilités à cet effet des services chargés de la lutte contre le terrorisme peuvent également avoir accès aux données du fichier, étant toutefois précisé que ces agents n'ont pas accès à l'image numérisée des empreintes digitales.

Ajoutons que, selon l'article 23 du décret du 30 décembre 2005, le fichier TES est interconnecté avec les systèmes d'information Schengen et INTERPOL, cette interconnexion ne portant toutefois que « *sur les informations relatives aux numéros des passeports perdus ou volés ainsi que sur l'indication relative au pays émetteur, au type et au caractère vierge ou personnalisé du document* ».

Enfin, l'article 24 dispose que la durée de conservation des données à caractère personnel enregistrées dans le fichier est de quinze ans lorsque le titre est délivré à un majeur et de dix ans lorsqu'il est délivré à un mineur, soit la durée de validité du titre augmentée de cinq ans.

De l'ensemble de ces dispositions, éclairées notamment par les résultats de l'audience d'instruction, il se déduit que les données biométriques contenues dans le fichier, et notamment l'image numérisée des empreintes digitales, sont susceptibles d'être consultées dans deux types de circonstances : lors du dépôt d'une demande de délivrance ou de renouvellement d'un passeport, d'une part ; et lorsqu'il existe, notamment à la suite de contrôles ou d'investigations réalisés par les forces de police ou de gendarmerie, des raisons de penser qu'un passeport a été falsifié, d'autre part.

Pour prendre la mesure de l'intérêt de cette consultation dans ces deux hypothèses, il nous paraît essentiel de souligner à ce stade que, tel qu'il a été conçu, le fichier TES ne pourra servir à des fins d'identification. Comme nous vous l'avons dit tout à l'heure, l'identification biométrique consiste à déterminer l'identité d'une personne qui ne peut ou ne veut la révéler, par une comparaison « un contre n » de ses caractéristiques biométriques. Or une telle comparaison est expressément prohibée par le dernier alinéa ajouté à l'article 19 du décret du 30 décembre 2005 par le décret attaqué, selon lequel : « *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.* » Le ministre de l'intérieur vous a d'ailleurs fait savoir que les données biométriques et les données relatives à l'identité de la personne étaient stockées dans des bases distinctes, et qu'un mécanisme dit de « double hachage » interdisait en pratique de remonter des données biométriques jusqu'aux données d'identité. En d'autres termes, on ne peut « entrer » dans le fichier que par l'identité de la personne, et non directement par ses données biométriques.

5.2.3. Cette limitation des fonctionnalités du fichier, conçue comme une garantie contre les usages abusifs, ne nous semble pas priver d'intérêt sa consultation dans les deux hypothèses que nous avons mentionnées tout à l'heure.

En effet, en ce qui concerne, d'une part, l'instruction des demandes de passeport, la présence dans le fichier des données biométriques n'est certes d'aucune utilité pour prévenir la fraude consistant à présenter des demandes multiples sous des identités différentes, puisqu'il n'est pas possible de comparer la photographie et les empreintes du demandeur à celles des personnes enrôlées dans la base. En revanche, si une personne, prétextant par exemple la perte ou le vol de son passeport, en demande le remplacement en usurpant l'identité d'une autre personne déjà présente dans la base, la comparaison « un contre un » des données biométriques, et notamment des empreintes digitales, permet normalement de déjouer cette fraude.

Il est clair, d'autre part, que des données biométriques enregistrées sur le composant électronique du passeport sont, en dépit de toutes les précautions prises pour en assurer l'intégrité, nécessairement plus vulnérables que celles enregistrées dans un fichier national. On comprend, dans ces conditions, que l'administration ait entendu conserver une copie de ces données dans un tel fichier, afin d'être en mesure de pallier à un éventuel dysfonctionnement du composant (le titulaire pouvant alors établir son identité par rapprochement avec les données figurant dans la base), mais aussi, et surtout, de déjouer la fraude consistant à altérer le composant électronique du passeport, par exemple pour y substituer les empreintes du fraudeur à celles du titulaire légitime. En effet, en présence d'un passeport contenant les empreintes digitales du porteur, mais dont les autorités auraient d'autres raisons de soupçonner qu'il a été falsifié, le rapprochement avec les données biométriques du fichier TES permettrait seul d'établir une éventuelle falsification.

Il existe donc, selon nous, un réel intérêt à l'enregistrement dans le fichier TES des données biométriques qui doivent figurer dans le composant électronique du passeport. Cet intérêt est-il suffisant pour contrebalancer les risques mis en avant par les différents avis que nous vous avons cités tout à l'heure ? L'hésitation est assurément permise, et les États européens ont, sur la question de la centralisation, fait des choix différents, certains, comme l'Allemagne ou l'Espagne, s'étant refusés à toute constitution d'un fichier central, tandis que d'autres, comme les Pays-Bas ou la Finlande, l'ont au contraire estimée utile. À la réflexion, nous croyons toutefois que vous pourrez admettre, dans son principe, la centralisation à laquelle procède le décret litigieux.

Il faut, en effet, prendre la juste mesure de la sensibilité des données biométriques concernées. Celles-ci ne sont pas porteuses, par elles-mêmes, d'informations sensibles que les demandeurs de passeport pourraient souhaiter ne pas voir divulguer. Ainsi, si l'image du visage véhicule incontestablement un certain nombre d'informations, notamment sur l'origine ethnique réelle ou supposée, voire le cas échéant sur l'état de santé, il s'agit d'informations que, par construction, on ne peut raisonnablement prétendre tenir secrètes dès lors que l'on a un minimum de vie sociale. Quant aux empreintes digitales, et ainsi que la Cour EDH l'a relevé dans l'arrêt *S. et Marper* précité, si elles « *contiennent objectivement des informations uniques sur l'individu concerné* » et si leur conservation peut dès lors « *donner lieu, en dépit du caractère objectif et irréfutable de ces données, à des préoccupations importantes concernant le respect de la vie privée* » (§§ 84-85), elles constituent des données moins sensibles, par elles-mêmes, que, par exemple, les profils génétiques qui étaient également en cause dans la même affaire.

En réalité, si la collecte de telles empreintes appelle une vigilance particulière, c'est surtout, ainsi que la CNIL a eu l'occasion de le relever à de nombreuses

reprises²³, parce qu'il s'agit de traces que chacun est susceptible de déposer à son insu, ce qui, comme en témoigne le succès de la dactyloscopie dans le domaine judiciaire, rend théoriquement possible leur utilisation à des fins de surveillance des déplacements, voire de l'activité des personnes concernées.

Or, au cas d'espèce, il nous semble précisément que ce dernier risque est limité, dès lors au moins que le nombre d'empreintes relevées est limité au strict nécessaire et que, comme il est expressément prévu par le décret attaqué, on relève ces empreintes à plat, et non roulées comme il est d'usage dans le domaine de l'identification judiciaire, ce qui les rend moins aptes à servir à l'identification de traces digitales. En outre, la prohibition de toute recherche, dans le fichier TES, à partir des éléments biométriques, qui se traduit, nous vous l'avons dit, par un stockage dans des bases différentes de celle où figurent les renseignements nominatifs, rend assez improbable une utilisation ponctuelle et discrète à des fins d'identification. Compte tenu, enfin, de la limitation du nombre des destinataires des données et de la durée raisonnable de conservation de celles-ci, il nous paraît difficile d'affirmer, dans ces conditions, que, au total, les bénéfices de la centralisation des données seraient, dans le cas d'un fichier ayant les finalités limitées qui sont celles du fichier TES, sans rapport avec les risques inhérents à celle-ci.

Certains requérants soutiennent certes que, en tout état de cause, une conclusion différente s'imposerait en ce qui concerne les mineurs, qui sont concernés, s'agissant de la collecte des empreintes digitales, dès l'âge de six ans. Ils se prévalent, à cet égard, des stipulations de l'article 16 de la convention relatives aux droits de l'enfant, selon lesquelles : « *Nul enfant ne fera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.* »

La parenté de ces stipulations avec celles de l'article 8 de la convention EDH justifie, à l'évidence, l'application d'une même grille d'analyse. Et nous n'entendons pas nier, à cet égard, qu'une vigilance particulière s'impose en ce qui concerne la collecte de données à caractère personnel concernant les enfants, notamment lorsque sont en cause des caractéristiques biométriques que, à la différence d'un code secret éventé, on ne peut pas remplacer lorsqu'elles ont été accaparées de façon illégitime. Mais, au cas d'espèce, nous ne voyons pas que l'objectif de lutte contre la fraude poursuivi par la centralisation des données biométriques soit moins impérieux en ce qui concerne les mineurs, compte tenu notamment des trafics dont, ainsi que le souligne le ministre de l'intérieur, ils peuvent être l'objet²⁴.

²³ V. par ex. sa communication de 2007 relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, consultable en ligne à l'adresse <http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/Communication-biometrie.pdf>.

²⁴ Ajoutons, à titre d'élément de contexte, que, si le règlement européen du 28 mai 2009, qui modifie celui du 13 décembre 2004 pour introduire le principe « une personne, un passeport », a prévu que les enfants de moins de 12 ans devraient être exemptés de l'obligation de donner leurs empreintes digitales en vue de leur enregistrement

5.3. L'enregistrement dans le fichier TES des données biométriques figurant dans le composant électronique du passeport nous paraît donc pouvoir être admis. En revanche, nous n'apercevons pas de justification convaincante à la collecte, dans ce même fichier, de huit empreintes digitales, alors que seules deux ont vocation à figurer dans le composant électronique du passeport.

En effet, une telle collecte n'a aucun intérêt pour détecter l'éventuelle falsification d'un passeport, cette finalité justifiant seulement de conserver un double des données figurant sur celui-ci. Elle ne pourrait avoir un sens, en théorie, que dans les hypothèses où l'on chercherait, par exemple à l'occasion d'une demande de renouvellement ou de remplacement d'un passeport, à vérifier, au moyen des données du fichier, que le demandeur a bien l'identité qu'il revendique. Mais est-elle véritablement nécessaire à cet effet ?

Le ministre de l'intérieur vous indique, en défense, que le risque d'erreur diminue significativement avec le nombre d'empreintes collectées. Ainsi, selon lui, *« si l'identification avec deux doigts est correcte pour 99 % des cas sur une population de un million de personnes, elle tombe à 98 % si le référentiel est de 10 millions et à 97 % s'il est de 100 millions »*. Ces statistiques ne sont pas contestées par les requérants, et nous ne songeons pas à les mettre en doute. Cependant, il nous semble qu'elles ne seraient pertinentes que si, précisément, le fichier TES s'était légalement vu attribuer une fonction d'identification, c'est-à-dire permettait une comparaison « un contre n » des empreintes digitales : en effet, à mesure que la population enrôlée augmenterait, le risque d'erreur d'identification, avec seulement deux empreintes, pourrait devenir significatif. C'est la raison pour laquelle on collecte généralement dix empreintes dans les bases de données importantes ayant des finalités d'identification. Nous vous avons déjà mentionné le cas de la base Eurodac, et il est intéressant de relever, par exemple, que, dans le cadre du programme « US-VISIT » (pour *United States Visitor and Immigrant Status Indicator Technology*), mis en œuvre à partir de 2004 par le ministère de la sécurité intérieure américain (*Department of Homeland Security*), et qui repose notamment sur la collecte d'empreintes digitales auprès des demandeurs de visa et de la plupart des voyageurs lors du franchissement des frontières des États-Unis, afin d'assurer le respect de la législation sur l'entrée et le séjour des étrangers mais aussi d'identifier plus aisément, grâce notamment au rapprochement avec les bases de données des services de police ou de renseignement, les personnes regardées comme une menace pour la sécurité du pays, les autorités américaines ont éprouvé le besoin, après quelques années de fonctionnement, de passer de deux à dix empreintes pour tenir compte de l'accroissement de la population enrôlée.

En revanche, une telle nécessité n'existe pas, en tout cas pas avec la même force, en ce qui concerne un dispositif d'authentification permettant uniquement une

sur le composant électronique du passeport, il a organisé une période transitoire de quatre ans en faveur des États ayant antérieurement prévu une limite d'âge inférieure.

comparaison « un contre un », dans le cadre duquel il n'est pas besoin d'être un expert en statistiques pour apercevoir que le risque d'erreur lié à la similitude des empreintes comparées est beaucoup plus faible – d'autant qu'il est possible, s'agissant du fichier TES, de corroborer le résultat de la comparaison des empreintes digitales par celui de la comparaison des visages. C'est la raison pour laquelle les mécanismes d'authentification n'utilisent souvent qu'un nombre limité d'empreintes : le choix fait par le législateur européen en ce qui concerne le passeport biométrique est révélateur à cet égard, et on peut relever qu'il a été reconduit, en ce qui concerne le modèle uniforme de titre de séjour pour les ressortissants des pays tiers, lorsque ce modèle, établi par un règlement de 2002²⁵, a été modifié, en 2008²⁶, pour prévoir l'intégration, dans un support de stockage intégré dans le titre, d'une image numérisée du visage et de deux empreintes digitales du titulaire.

Dans le dernier état de ses écritures, le ministre de l'intérieur fait certes valoir que le recueil de huit empreintes lors du dépôt de la demande de passeport permet de sélectionner les deux « meilleures », qui seront celles enregistrées dans le composant électronique du passeport. Mais, à supposer qu'une telle façon de procéder soit conforme aux spécifications du passeport biométrique établies au niveau européen, cette justification, si elle pourrait peut-être valoir pour le recueil transitoire et local de huit empreintes, ne peut certainement pas être admise, en tout état de cause, en ce qui concerne leur enregistrement durable dans le fichier TES.

Dans ces conditions, l'intérêt de l'enregistrement, dans ce fichier, d'empreintes digitales supplémentaires par rapport à celles figurant dans le composant électronique du passeport ne nous paraît pas démontré, alors que cette collecte surnuméraire accroît, au moins en théorie, les risques de détournement des finalités du fichier à des fins d'identification. En tout état de cause, dès lors que la collecte d'une donnée apparaît inadéquate, c'est-à-dire inutile, il n'est pas même besoin, aux fins de l'application de l'article 6 de la loi du 6 janvier 1978, de s'interroger sur l'intensité de l'atteinte portée par cette collecte au droit des intéressés au respect de leur vie privée : son inutilité suffit à la condamner.

Nous vous invitons donc à annuler l'article 19 du décret du 30 décembre 2005, dans sa rédaction issue du décret attaqué, en tant qu'il prévoit l'enregistrement dans le fichier TES d'empreintes digitales autres que celles devant figurer dans le composant électronique du passeport en vertu de l'article 2 du même décret.

Si vous nous suivez, votre décision, qui n'aura aucune conséquence sur les passeports eux-mêmes, obligera en revanche l'administration à cesser de collecter plus de deux empreintes digitales lors des demandes de passeport et, dans un délai raisonnable, à supprimer du fichier TES les empreintes surnuméraires. Il ressort des

²⁵ Règlement (CE) n° 1030/2002 du Conseil du 13 juin 2002 établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers.

²⁶ Par le règlement (CE) n° 380/2008 du Conseil du 18 avril 2008.

écritures du ministre de l'intérieur que la modification du système pour prévoir l'enregistrement dans le fichier des seules empreintes destinées à être stockées dans le composant électronique du passeport ne devrait pas poser de difficulté technique majeure, aucune modification de la base, qui a été conçue pour accueillir entre zéro et huit empreintes, n'étant nécessaire. En revanche, le ministre souligne que l'effacement des données déjà enregistrées nécessitera des manipulations longues et coûteuses, compte tenu du nombre de personnes enrôlées dans la base, soit 6,3 millions : dans un mémoire produit hier soir, il évalue le délai de ces opérations à six mois et leur coût à 500 000 €. Et, sans présenter de conclusions expresses en ce sens, il suggère à demi-mot qu'il pourrait être justifié que vous fassiez usage des pouvoirs de modulation dans le temps des effets des annulations contentieuses que vous vous êtes reconnus par votre décision d'Assemblée du 11 mai 2004, *Association AC ! et autres* (n^{os} 255886 et autres, p. 197).

Sans méconnaître les difficultés soulignées par l'administration, nous croyons toutefois exclu que vous alliez en ce sens. En effet, il ne servirait à rien, concrètement, de priver d'effet rétroactif l'annulation que nous vous invitons à prononcer : si cela permettrait d'éviter de regarder rétrospectivement la collecte des empreintes surnuméraires comme irrégulière, il n'en demeurerait pas moins que, pour l'avenir, leur conservation dans le fichier TES demeurerait illégale, et il n'en faudrait pas moins procéder à leur effacement. Pour donner satisfaction au ministre, il faudrait donc, en réalité, reporter dans l'avenir la prise d'effet de votre décision, et ce à une date qui, pour les 6,3 millions de personnes déjà enrôlées, se situerait au moment du renouvellement de leur passeport, soit, pour les derniers passeports délivrés, à l'issue d'une période de dix ans à compter de ce jour. Il ne nous paraît pas envisageable que vous fassiez, de la jurisprudence issue de votre décision *Association AC ! et autres*, une application qui conduise de la sorte à priver votre décision de l'essentiel de sa portée. Les difficultés alléguées nous paraissent donc seulement pouvoir être prises en compte pour apprécier la durée du délai raisonnable dont disposera l'administration pour se conformer à votre décision.

Nous voudrions également souligner, pour conclure sur ce point, que cette décision, prise au vu de l'ensemble des caractéristiques du traitement TES tel qu'il se présente actuellement, ne préjugera pas de ce que vous pourriez décider à propos d'autres traitements de données biométriques. Nous pensons en particulier à celui dont la création est prévue par la proposition de loi relative à la protection de l'identité, adoptée en première lecture par l'Assemblée nationale le 7 juillet dernier, qui prévoit que la carte nationale d'identité et le passeport comporteront désormais, sans autre précision, les « *empreintes digitales* » du titulaire, ces données étant en outre versées dans un fichier national. Votre décision, qui ne devra pas non plus être interprétée comme une position de principe pour ou contre l'usage de la biométrie en matière de sécurisation des documents d'identité et de voyage, aura simplement pour vertu de rappeler à tous, y compris au législateur, astreint aux disciplines du droit européen des droits de l'homme, l'exigence fondamentale de proportionnalité qui doit présider à

toute collecte de données à caractère personnel, et l'impossibilité, à cet égard, de se contenter de justifications trop générales ou imprécises.

6. Vous pourrez écarter les autres moyens soulevés par les requérants, et notamment M. A..., à l'encontre du décret attaqué.

6.1. Nous pensons, d'abord, que l'enregistrement dans le fichier TES de l'image numérisée des pièces du dossier de demande de passeport ne méconnaît pas les exigences de l'article 6 de la loi du 6 janvier 1978. Cet enregistrement présente en effet des avantages réels en matière, notamment, de gestion du processus de délivrance et de renouvellement des passeports, en permettant notamment le dépôt d'une demande en tout point du territoire. Or, si les pièces concernées, notamment les actes d'état civil et les justificatifs de domicile, comportent des informations nombreuses sur la vie privée des personnes concernées, ces informations, qui pour beaucoup revêtent un caractère public, ne sont pas d'une sensibilité particulière.

6.2. Il nous semble, par ailleurs, que la circonstance que le décret attaqué ne prévoit pas de mesures de sécurité particulières en ce qui concerne les données contenues dans le fichier TES ne le rend pas illégal : l'article 29 de la loi du 6 janvier 1978 n'exige pas que l'acte autorisant la mise en œuvre d'un traitement comporte ce type d'informations, et la circonstance que le ministère de l'intérieur n'aurait pas pris, en violation de l'article 34 de la même loi, « *toutes précautions utiles [...] pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* », est sans influence sur la légalité du décret lui-même.

6.3. Nous ne croyons pas davantage que des droits d'accès excessifs aient été ménagés : comme nous vous l'avons dit, en effet, n'ont un accès complet au fichier, outre les agents chargés de sa mise en œuvre, que les agents des services de l'État chargés de la délivrance des passeports et de l'application de la réglementation relative au passeport, d'une part, et les agents des services chargés des missions de recherche et de contrôle de l'identité des personnes, ainsi que de vérification de la validité et de l'authenticité des passeports. On voit mal comment, sans priver d'intérêt la création du fichier, il aurait été possible de restreindre davantage le champ des personnes ainsi concernées. Quant aux agents des services chargés de la lutte antiterroriste, ils n'ont pas accès à l'image numérisée des empreintes digitales, en vertu des dispositions expresses de l'article 21-1 du décret du 30 décembre 2005, et ils doivent être individuellement et spécialement habilités à l'effet d'accéder au fichier TES.

6.4. La durée de conservation des données peut davantage prêter à discussion : nous vous avons dit qu'elle était de cinq ans après la date d'expiration du passeport. Mais, ainsi que l'observe le ministre de l'intérieur, le renouvellement d'un passeport n'est pas toujours demandé immédiatement après son expiration, de sorte que la conservation des données pendant une durée raisonnable après celle-ci se justifie par l'objectif de faciliter la procédure de délivrance. Par ailleurs, il est clair qu'une

destruction immédiate, en privant l'administration de tout point de comparaison en cas de nouvelle demande sous la même identité, affaiblirait beaucoup la fonction de lutte contre la fraude documentaire assignée au fichier. Nous pensons donc que la durée de conservation retenue n'est pas contraire aux dispositions du 5° de l'article 6 de la loi du 6 janvier 1978 selon lesquelles les données *« sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées »*.

6.5. Le moyen tiré de l'existence d'interconnexions irrégulières nous paraît, quant à lui, manquer en fait en ce qui concerne le décret attaqué, qui n'a pas modifié l'article 23 du décret du 30 décembre 2005, lequel prévoit, nous vous l'avons dit, des interconnexions limitées avec les systèmes d'information Schengen et INTERPOL. Ceci rend également vaine toute discussion sur le point de savoir si une autorisation de la CNIL aurait pu être requise au titre du 5° du I de l'article 25 de la loi du 6 janvier 1978, qui vise les *« traitements automatisés ayant pour objet : / – l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents ; / – l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes »*. En tout état de cause, la procédure de création par décret en Conseil d'État qui a été suivie en l'espèce nous semble clairement exclusive de toute autorisation par la Commission.

6.6. Enfin, l'invocation d'un avis du conseil consultatif national d'éthique est évidemment inopérante à l'appui d'un recours pour excès de pouvoir, et le détournement de pouvoir allégué ne nous paraît pas établi.

7. Il nous faut maintenant en venir aux moyens plus spécifiquement développés, par les professionnels de la photographie, à l'appui de la requête n° 317827. Les requérants, nous vous l'avons dit, critiquent plus particulièrement les dispositions du second alinéa de l'article 6-1 inséré dans le décret du 30 décembre 2005 par le décret attaquée, et selon lesquelles : *« 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 dispositions ont clairement eu pour portée, à compter de leur entrée en vigueur, d'ouvrir au demandeur d'un passeport une alternative : soit il fournit, à l'appui de sa demande, une photographie d'identité répondant aux spécifications indiquées, qu'il aura fait réaliser, en pratique, par un photographe professionnel ou dans une cabine automatique installée dans un espace public, cette photographie étant ensuite numérisée par les soins de l'administration afin de l'inclure dans le passeport ; soit l'image numérisée de son visage est directement recueillie à l'occasion du dépôt de sa demande, en mairie ou en préfecture, au moyen d'un *« dispositif technique approprié »*. En pratique, une circulaire du 7 mai 2008, également critiquée par les requérants, est venue préciser que seraient implantées, dans 2 000 communes, des

« stations d'enregistrement des données » permettant tout à la fois de numériser les documents d'état civil produits à l'appui de la demande et de recueillir l'image numérisée des empreintes digitales ainsi que du visage du demandeur.

La faculté ainsi offerte aux administrés de faire l'économie d'un passage chez le photographe ou dans une cabine automatique, ajoutée à l'assurance d'éviter le désagrément d'avoir à refaire les photographies au motif qu'elles ne répondent pas aux spécifications réglementaires, a conduit, dès 2009, d'après les chiffres communiqués par le ministre de l'intérieur, à ce que, pour plus de 45 % des passeports délivrés, la photographie soit réalisée sur place. Il en est résulté une contraction d'autant de la demande adressée au secteur de la photographie d'identité, dont on comprend, dans ces conditions, que ses représentants cherchent à obtenir l'annulation de la disposition à l'origine de ce préjudice.

7.1. Nous nous empressons toutefois de préciser que la position que vous prendrez sur ce point, qui revêtera une incontestable portée théorique, n'aura, en principe, que des retombées pratiques limitées. En effet, sensible aux préoccupations exprimées par les professionnels de la photographie, le législateur a progressivement restreint la possibilité pour l'administration de recueillir elle-même l'image numérisée du visage du demandeur.

Dans un premier temps, la loi de finances rectificative pour 2008²⁷ est venue prévoir une diminution d'un euro – sur 89 en ce qui concerne les adultes – du droit de timbre prévu par l'article 953 du code général des impôts en faveur des personnes qui fourniraient elles-mêmes les photographies d'identité à l'appui de leur demande, tout en précisant que, « dans le cadre de sa mission de réception et de saisie des demandes de passeport », le maire pourrait « décider de ne pas procéder au recueil de l'image numérisée du visage du demandeur », le demandeur n'ayant, alors, pas d'autre choix que de procéder ainsi. L'avantage pécuniaire ainsi accordé aux personnes fournissant elles-mêmes les photographies d'identité a ensuite été porté à trois euros par la loi de finances pour 2010²⁸.

Puis, dans un second temps, la loi d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011²⁹ est venue poser en principe que, à compter de la promulgation de cette loi, « les photographies destinées à la réalisation des passeports, cartes nationales d'identité et autres titres sécurisés [seraient obligatoirement] réalisées par un professionnel de la photographie dans des conditions fixées par voie réglementaire ». À titre dérogatoire, le législateur a toutefois prévu que le recueil sur place de l'image numérisée du demandeur pourrait continuer d'avoir lieu dans les communes « équipées à cette fin à la date du 1^{er} janvier 2011 et pour une période définie par décret ». Un décret du 22 juillet 2011 est alors intervenu

²⁷ N° 2008-1443 du 30 décembre 2008, art. 104.

²⁸ N° 2009-1673 du 30 décembre 2009, art. 55.

²⁹ N° 2011-267, art. 16.

pour modifier l'article 6-1 du décret du 30 décembre 2005 relatif aux passeports, qui dispose désormais que peuvent seuls recueillir l'image numérisée du visage du demandeur les ambassades et les postes consulaires et, jusqu'au 31 décembre 2011, les communes équipées à cet effet au 1^{er} janvier de la même année.

Cette dernière modification ne prive toutefois pas d'objet les conclusions tendant à l'annulation de l'article 6-1 dans sa rédaction d'origine, qui a reçu application. Il vous faut donc examiner les moyens articulés par les requérants à son encontre.

7.2. Ceux-ci voient, dans les dispositions critiquées, une atteinte illégale tant au principe de liberté du commerce et de l'industrie qu'au principe de libre concurrence. Ils font valoir, en effet, que la prise en charge par l'État d'une activité de prise de photographies numériques ne répond à aucun intérêt public et que cette activité, en contrepartie de laquelle il n'est pas prévu, dans le décret, qu'une rémunération sera exigée, concurrence illégalement les services privés de photographie d'identité.

Les requérants se prévalent, à cet égard, de votre décision d'Assemblée du 31 mai 2006, *Ordre des avocats du barreau de Paris* (n° 275531, p. 272). Comme vous le savez, cette décision a précisé les principes applicables, d'une part, à la décision, par une personne publique, de prendre en charge une activité économique, d'autre part, aux conditions d'exercice de cette activité, lorsque sa prise en charge par une personne publique apparaît légitime. Le *principe* de l'intervention publique est encadré par la liberté du commerce et de l'industrie, qui impose que cette intervention réponde à un intérêt public, lequel peut résulter notamment de la carence de l'initiative privée. Une fois admise dans son principe, une telle intervention ne doit pas se réaliser suivant des *modalités* telles que le libre jeu de la concurrence sur le marché considéré en serait faussé. Or il est soutenu, au cas d'espèce, qu'il n'existe nulle carence de l'initiative privée justifiant une intervention de l'État sur le marché de la photographie d'identité, et que, à supposer que tel soit le cas, cette intervention est de nature à fausser le libre jeu de la concurrence, faute que des garanties appropriées aient été prévues.

7.2.1. Nous doutons toutefois que ces principes puissent être utilement invoqués en l'espèce. En effet, comme le souligne votre décision du 31 mai 2006, qui rappelle que « *les personnes publiques sont chargées d'assurer les activités nécessaires à la réalisation des missions de service public dont elles sont investies* », les principes qu'elle énonce ne s'appliquent que lorsqu'une collectivité publique entend « *prendre en charge une activité économique* », c'est-à-dire offrir des biens ou des services sur un marché. Or tel n'est pas le cas dans deux hypothèses essentielles.

Il peut d'abord ne pas exister de marché pour la prestation effectuée par la collectivité publique, cette prestation étant, par sa nature, hors du commerce. C'est cette première hypothèse qu'illustre, précisément, votre décision du 31 mai 2006, qui juge qu'en chargeant la mission d'appui à la réalisation des contrats de partenariat, qui est un service de l'État, d'apporter aux personnes publiques qui le lui demandent un

appui dans la préparation, la négociation et le suivi des contrats de partenariat, le décret contesté s'était borné à « *mettre en œuvre la mission d'intérêt général, qui relève de l'État, de veiller au respect, par les personnes publiques et les personnes privées chargées d'une mission de service public, du principe de légalité* ». Il s'agissait donc d'une mission propre à la puissance publique, qui n'était susceptible d'entrer en concurrence avec aucune activité privée. Vous avez donné une autre illustration de ce cas de figure par une décision du 28 mai 2010, *Société Enfanceconfiance* (n° 328731, à mentionner aux tables du recueil), selon laquelle ne constitue pas une activité économique emportant intervention sur un marché la diffusion gratuite sur un site internet, par la Caisse nationale des allocations familiales, d'informations relatives aux structures d'accueil recueillies auprès des collectivités territoriales et des acteurs de la petite enfance.

Le cas d'espèce ne relève toutefois pas de cette hypothèse : la prise de photographie numérique ne saurait en effet être regardée comme une activité non économique par nature, propre à la puissance publique. Mais – et c'est la seconde hypothèse annoncée – une prestation peut également être dépourvue de caractère économique, non par nature, mais parce qu'elle revêt un caractère interne à une collectivité publique et, de ce fait, n'est pas offerte sur un marché.

En effet, par construction, les échanges qui peuvent avoir lieu au sein d'une organisation complexe, qu'il s'agisse d'une collectivité publique ou d'une entreprise, se déroulent en dehors du marché. Les autorités chargées d'assurer le respect des règles de concurrence en tirent les conséquences en excluant, de la délimitation du marché pertinent, ce qu'on appelle parfois l'« autoprestation ». Ainsi l'Autorité de la concurrence estime-t-elle, de manière constante, que « *l'autoconsommation [ne doit] pas [être] prise en compte pour mesurer le périmètre du marché dans la mesure où, n'étant pas offerte sur le marché, elle ne vient pas concurrencer les biens ou services fournis sur celui-ci* » (v. par ex. avis n° 05-A-03 du 31 janvier 2005 relatif à une demande d'avis présentée par l'Autorité de régulation des télécommunications en application de l'article L. 37-1 du code des postes et communications électroniques, § 84 ; ou encore décision n° 09-D-31 du 30 septembre 2009 relative à des pratiques mises en œuvre dans le secteur de la gestion et de la commercialisation des droits sportifs de la Fédération française de football, § 242). La pratique de la Commission européenne va dans le même sens (v. par ex. décision du 3 mai 2000 déclarant une concentration compatible avec le marché commun et l'accord EEE, dans l'affaire n° COMP/M.1693 – Alcoa/Reynolds, J.O.C.E. L 58 du 28 février 2002, p. 25, § 13).

C'est, implicitement mais nécessairement, au bénéfice d'une analyse similaire que vous avez jugé, par votre fameuse décision du 29 avril 1970, *Société Unipain* (n° 77935, p. 280), que « *le principe de la liberté du commerce et de l'industrie ne fai[sait] pas obstacle à ce que l'État satisfasse, par ses propres moyens, aux besoins de ses services* ». Était en cause dans cette affaire, vous vous en souvenez, la décision, par l'État, d'étendre les fournitures d'une boulangerie militaire à divers établissements

pénitentiaires, laquelle avait conduit ces établissements à ne plus s'approvisionner auprès des boulangeries privées. Dans ses conclusions, Guy Braibant avait relevé que les règles régissant l'intervention économique des collectivités publiques, et notamment le principe de liberté du commerce et de l'industrie, « *ne jouent que si la collectivité vend des biens ou des services au public, et intervient ainsi sur le marché* » : elles cessent en revanche de recevoir application « *dès lors que la collectivité publique fabrique des produits pour elle-même, pour la satisfaction de ses propres besoins* ». C'est à partir de ce constat que votre décision affirme que le choix, par une collectivité publique, d'internaliser ou d'externaliser une prestation, est en principe libre – de même, soulignons-le, qu'est libre le choix du mode de gestion du service public, et vous n'exercez aucun contrôle, même restreint, sur la décision de déléguer ou au contraire d'exploiter en régie un tel service (v. 18 mars 1988, *L...c/ C^{ne} de Montreuil-Bellay*, n° 57893, T. p. 975).

Loin d'avoir été remise en cause par les développements jurisprudentiels récents, cette approche a été étendue, au-delà du cas où l'autoprestation est le fait des services mêmes de la collectivité concernée, à l'hypothèse où elle se réalise par le biais d'opérateurs sur lesquels cette collectivité exerce un contrôle analogue à celui qu'elle exerce sur ses propres services et qui, de ce fait, apparaissent comme de simples démembrements de celle-ci. Vous aurez reconnu l'analyse faite par la CJUE lorsqu'elle a été confrontée à la nécessité de délimiter le champ d'application du droit européen des marchés publics, dont l'objet essentiel est d'éviter que l'achat public perturbe le fonctionnement du marché. Par son fameux arrêt *Teckal* du 18 novembre 1999 (C-107/98, Rec. p. I-8121), la Cour, vous le savez, a posé en principe que les directives relatives aux marchés publics sont en principe applicables dès lors qu'un contrat est conclu entre une collectivité publique et une personne juridiquement distincte de celui-ci, sauf lorsque la collectivité publique « *exerce sur la personne en cause un contrôle analogue à celui qu'elle exerce sur ses propres services et où cette personne réalise l'essentiel de son activité avec la ou les collectivités qui la détiennent* » (point 50). C'est que, dans ce cas, on demeure, en réalité, « dans la maison », *in house*, c'est-à-dire dans le champ de l'autoprestation, que les disciplines de marché n'ont pas vocation à régir.

C'est dans ce contexte que la Cour a, elle aussi, été conduite à affirmer la liberté de principe des collectivités publiques d'externaliser ou d'internaliser une prestation répondant à leurs besoins. Elle l'a fait notamment par un arrêt *Stadt Halle* du 11 janvier 2005 (C-26/03), dont la parenté d'inspiration avec votre décision *Unipain* est frappante : la Cour y affirme en effet qu'« *une autorité publique, qui est un pouvoir adjudicateur, a la possibilité d'accomplir les tâches d'intérêt public qui lui incombent par ses propres moyens, administratifs, techniques et autres, sans être obligée de faire appel à des entités externes n'appartenant pas à ses services* » (point 48). C'est que, comme le souligne un autre arrêt, « *le rapport entre une autorité publique [...] et ses propres services est régi par des considérations et des exigences propres à la*

poursuite d'objectifs d'intérêt public », et par conséquent étrangères aux logiques de marché (CJCE, 10 novembre 2005, *Commission c/ Autriche*, C-29/04, point 47).

Il n'y a donc rien d'étonnant que ce soit dans le contexte de l'application de la jurisprudence de la Cour relative aux contrats *in house* que vous ayez, par une décision du 4 mars 2009, *Syndicat national des industries d'information de santé* (n° 300481, p. 76), quelque peu reformulé le considérant de principe de votre décision *Unipain*, en jugeant que « *les collectivités publiques peuvent recourir à leurs propres moyens, pour assurer, dans le cadre de leurs compétences, les prestations répondant à leurs besoins* » et ainsi « *ne sont pas tenues de faire appel à des tiers, en particulier à des entreprises, en passant avec eux des marchés publics* ».

7.2.2. Or il nous semble qu'au cas d'espèce, l'État, par la disposition contestée du décret attaqué, s'est borné à faire usage de la liberté qui lui est ainsi reconnue par le dernier état de votre jurisprudence.

Il est vrai que, de prime abord, on peut avoir l'impression que, en décidant de prendre en charge, à la discrétion du demandeur du passeport, le recueil de l'image numérisée de son visage, l'État répond, non pas à un besoin qui lui est propre, mais à un besoin de l'administré. Cette impression provient du fait que, dans la situation antérieure au décret attaqué, l'État, pour la réalisation de cette prestation, ne faisait pas directement appel au marché, mais reportait sur le demandeur le soin de s'adresser à celui-ci. En d'autres termes, la réglementation relative au passeport avait pour effet de créer, chez le demandeur, le besoin de disposer de photographies d'identité, et il est tentant de considérer que c'est ce besoin que, au moyen des dispositifs installés dans les mairies, l'État entend, au moins en partie, satisfaire.

À notre avis, c'est une tentation à laquelle il faut résister, car elle repose sur une illusion d'optique. En effet, dès lors qu'il fait usage de la possibilité qui lui est offerte de voir l'image de son visage recueillie directement par l'administration, le besoin que l'état antérieur de la réglementation avait fait naître chez l'administré disparaît. Demeure uniquement, de sa part, la demande de délivrance d'un passeport, dont nul ne peut sérieusement songer à contester qu'il appartient à l'État seul, dans le cadre de ses fonctions régaliennes, de la satisfaire. Et c'est exclusivement dans le chef de l'État que l'exercice de cette mission consistant à délivrer des passeports à ses ressortissants fait alors naître le besoin de plusieurs consommations intermédiaires, en particulier la réalisation du livret du passeport et le recueil de l'image numérisée des empreintes digitales et du visage du demandeur.

Dans le cas du livret, l'État ne peut s'adresser au marché, dans la mesure où sa confection ressortit dans sa totalité, ainsi que vous l'avez jugé par une décision du 3 mars 2006, *S^{té} François-Charles Oberthur Fiduciaire* (n^{os} 287960-287964-288809, T. pp. 867-1001-1016-1090), au monopole légal de l'Imprimerie nationale, qui est une société au capital entièrement détenu par l'État. S'agissant du recueil des empreintes digitales et de la photographie, l'administration a sans doute la possibilité de recourir

au marché – il est d’ailleurs envisagé d’externaliser la prestation de recueil des empreintes digitales des demandeurs de visa dans certains postes diplomatiques et consulaires : mais il résulte des principes issus de votre décision *Unipain* qu’elle n’est pas tenue de le faire.

Toute autre analyse reviendrait à considérer que l’État, en procédant au recueil de l’image numérisée du visage du demandeur, fournit à celui-ci une prestation annexe à la délivrance du passeport et séparable de celle-ci. Mais cette présentation ne nous semble pas correspondre à la réalité : le résultat de la prestation de photographie numérique est entièrement intégré au processus de réalisation et de délivrance du passeport, lequel, soulignons-le au passage, demeure la propriété de l’État. Contrairement à celui qui choisit de s’adresser au marché, le demandeur qui profite de la possibilité qui lui est offerte par le décret attaqué de se faire photographier à l’occasion du dépôt de sa demande ne reçoit, même un instant de raison, aucune photographie, sous quelque forme que ce soit : il se verra seulement, au bout du compte, remettre un passeport incluant son image numérisée, de laquelle il ne pourra évidemment faire aucun autre usage. Ce n’est donc qu’indirectement, par le biais de l’accomplissement, par l’État, de sa mission de délivrance des passeports, qu’il bénéficie de la prestation photographique ; sans que doive faire illusion la circonstance que c’est l’image de l’administré qui est recueillie, cette prestation répond d’abord à un besoin de l’administration.

Nous pensons, dans ces conditions, que ce que réalise la disposition critiquée est bien une simple internalisation, qui modifie la frontière entre l’intérieur et l’extérieur de l’administration, entre l’État et le marché, mais ne comporte aucune intervention sur celui-ci. Cette décision a incontestablement un impact sur le périmètre du marché, et donc sur l’activité des professionnels de la photographie. Mais nombreuses sont les décisions de l’administration et des entreprises qui ont un tel effet, sans pour autant qu’elles soient justiciables du respect des règles du droit de la concurrence. Une décision de l’Autorité de la concurrence du 26 octobre 2009 relative à des pratiques mises en œuvre par la société Photomaton (n° 09-D-32) donne des exemples de ces décisions qui, selon le cas, conduisent à une extension ou, au contraire, à une contraction du marché global de la photographie d’identité : dans le sens de l’extension, elle mentionne ainsi « *l’introduction de nouveaux documents nécessitant l’apposition d’une photo d’identité ou la décision prise d’apposer une photo sur des documents existants, comme cela a été le cas récemment pour la Carte Vitale* » ; mais elle relève que, « *à l’inverse, des projets comme la réalisation gratuite en boutique RATP des photos nécessaires au Pass Navigo ou la mise en place dans 2 000 mairies de stations biométriques réalisant directement les photographies destinées aux passeports biométriques entraîneront une baisse du nombre de photos d’identité acquises en cabine ou auprès des photographes* ».

Cette conséquence, dont nous n’entendons pas minimiser la gravité, est inhérente à toute décision d’internalisation prise par une collectivité de la taille de

l'État ou par une grande entreprise. C'est seulement sur le terrain de la responsabilité que, le cas échéant, le préjudice subi par la profession pourrait être pris en compte, à supposer que les requérants s'estiment en mesure de démontrer que sont remplies les conditions restrictives d'engagement de la responsabilité de l'État pour rupture de l'égalité devant les charges publiques, voire, puisqu'ils estiment avoir été victimes d'incitations fautives de la part du ministère de l'intérieur, sur le terrain de la responsabilité pour faute.

8. Il ne reste plus, avant d'en terminer, qu'à examiner les conclusions que les mêmes requérants ont formulé, dans leur requête, à l'encontre d'une circulaire du ministre de l'intérieur du 7 mai 2008, « *relative aux choix des 2 000 communes appelées à recevoir des stations d'enregistrement des données personnelles pour le nouveau passeport* ». Cette circulaire expose que, compte tenu de l'exigence d'un équipement spécifique pour le recueil et la numérisation des données biométriques, les demandes de passeport n'auront plus vocation à être présentées, à compter, au plus tard, du 28 juin 2009, que dans 2 000 communes, regroupant actuellement 70 % des demandes de titres. Elle a pour objet essentiel d'inviter les préfets à organiser une concertation pour soumettre à l'administration centrale une liste de communes susceptibles de participer au dispositif, compte tenu d'un certain nombre de critères qu'elle énumère.

La circulaire précise que, dans ces communes, seront implantées des « *stations d'enregistrement des données* » qui permettront à la fois de numériser les pièces justificatives du dossier de demande, de recueillir les empreintes digitales et de prendre des photographies numériques. Sur ce dernier point, la circulaire indique que : « *Les citoyens auront toute faculté de se présenter avec une photographie d'identité [...]. La photographie pourra aussi être prise par la station d'enregistrement qui ne délivrera aucun cliché au demandeur.* » Elle ajoute que les stations d'enregistrement seront fournies par l'agence nationale des titres sécurisés (ANTS), laquelle « *prendra en charge les frais d'acquisition, d'installation des stations, leur maintenance et leur remplacement, ainsi que l'abonnement de raccordement au réseau informatique.* »

Signalons d'abord qu'il est vraisemblable que cette circulaire, qui n'a apparemment pas été publiée sur le site internet « circulaires.gouv.fr », a été abrogée par l'effet de l'article 2 du décret du 8 décembre 2008 relatif aux conditions de publication des instructions et circulaires³⁰. Mais cette circonstance, à notre avis, ne vous dispensera pas de statuer sur les conclusions présentées à son encontre, dès lors qu'il n'est guère douteux que les décisions dont elle fait état avaient connu, à tout le moins, un début d'exécution avant cette abrogation.

On pourrait, ensuite, douter du caractère impératif de cette circulaire en tant qu'elle se livre à la description du dispositif de recueil de l'image numérisée du visage des demandeurs de passeports dont la mise en place a été décidée : son objet n'est pas

³⁰ N° 2008-1281.

tant de prescrire cette mise en place que d'exposer un contexte pour expliquer la commande adressée aux préfets. Il nous semble toutefois que, compte tenu du luxe de détails qu'elle comporte sur ce point, la circulaire a en réalité entendu faire d'une pierre deux coups, car les préfets étaient concernés à un double titre par la mise en place du dispositif de collecte des données biométriques : d'une part, ainsi que le précise la circulaire elle-même, des stations d'enregistrement devaient être implantées dans les préfetures ; d'autre part, c'est en tant qu'agents de l'État que les maires interviennent dans le dispositif, si bien qu'ils sont, à cet égard, placés sous l'autorité des préfets (comp., pour de prétendues instructions adressées à des préfets et chefs de service qui ne disposaient d'aucun pouvoir dans la matière concernée, 26 mai 2009, *Syndicat national des personnels techniques et de travaux de l'équipement de la confédération générale du travail*, n° 306757, T. pp. 599-880).

Les requérants reprochent d'abord à la circulaire attaquée d'être entachée d'incompétence pour revêtir un caractère réglementaire. Elle ajouterait en effet à l'état du droit en prévoyant que des stations d'enregistrement seraient implantées dans 2 000 mairies et dans les préfetures, qu'elles le seraient par l'ANTS et qu'elles pourraient recueillir la photographie des demandeurs. Sur ce dernier point, la circulaire ne nous semble rien ajouter au décret, qui, nous vous l'avons dit, ne peut être lu que comme prévoyant le recueil de l'image numérisé du demandeur par le service chargé de la réception des demandes de passeport. Là où la circulaire innove, c'est en indiquant que ces services seront les communes et dans certains cas les préfetures, que les communes concernées seront au nombre de 2 000, et enfin que l'ANTS sera en charge de l'installation de stations d'enregistrement. Toutefois, à supposer que la circulaire puisse être regardée comme contenant la décision même de mise en place d'un tel dispositif, ce qui pourrait prêter à discussion, il nous semble que le ministre de l'intérieur était bien compétent pour prendre ce qui s'apparente selon nous à de simples mesures d'organisation du service.

Les requérants soutiennent également que les mesures litigieuses relevaient du domaine de la loi en ce qu'elles imposent une charge financière supplémentaire aux communes : on retrouve le moyen tiré de la violation de l'article L. 1611-1 du CGCT, que nous avons précédemment examiné en tant qu'il était dirigé contre le décret du 30 avril 2008. La critique a ici davantage de pertinence, puisqu'il est bien question de l'intervention des communes dans le dispositif. Mais il pourra être répondu aux requérants que la circulaire s'est bornée à prévoir le principe de l'installation de stations d'enregistrements dans les mairies, d'ailleurs aux frais de l'ANTS, sa mise en œuvre étant subordonnée au recueil des propositions des préfets. Notons au surplus que, depuis lors, le législateur est intervenu pour prévoir expressément l'intervention des maires dans la délivrance des titres d'identité : tel est en effet l'objet de l'article L. 1611-2-1 du CGCT, issu de la loi du 30 décembre 2008 de finances rectificative pour 2008³¹, et selon lequel : « *Dans le cadre des missions confiées aux maires en tant*

³¹ N° 2008-1443, art. 103.

qu'agents de l'État, les communes assurent la réception et la saisie des demandes de cartes nationales d'identité et de passeports ainsi que la remise aux intéressés de ces titres. »

Il est également soutenu, à titre subsidiaire, que M^{me} Bernadette Malgorn, secrétaire générale du ministère de l'intérieur, qui a signé la circulaire, ne disposait pas d'une délégation régulière du ministre. Mais la simple consultation du *Journal officiel* montre que l'intéressée a été nommée secrétaire générale du ministère de l'intérieur et de l'aménagement du territoire, à compter du 28 août 2006, par un décret du 20 juillet 2006, publié le 22. Par conséquent, elle pouvait, dès le 28 août, signer, en vertu du 1^o du décret du 27 juillet 2005 relatif aux délégations de signature des membres du Gouvernement³², les actes relatifs aux affaires des services placés sous son autorité, au nombre desquels figure évidemment la circulaire litigieuse.

Sur le fond, enfin, vous ne pourrez qu'écarter comme inopérants, si vous nous avez suivi dans notre analyse de la légalité, sur ce point, du décret du 30 avril 2008, les moyens tiré de la violation du principe de liberté du commerce et de l'industrie et du principe de libre concurrence, ainsi que de l'erreur manifeste qu'aurait commise le ministre de l'intérieur en procédant à l'internalisation partielle de la réalisation des photographies d'identité destinées aux passeports, dès lors que, comme nous vous l'avons dit, vous vous refusez à contrôler une telle décision.

Et par l'ensemble de ces motifs, nous concluons :

– à l'annulation de l'article 19 du décret du 30 décembre 2005, dans sa rédaction issue du décret du 30 avril 2008, en tant qu'il prévoit l'enregistrement dans le fichier TES d'empreintes digitales autres que celles devant figurer dans le composant électronique du passeport en vertu de l'article 2 du même décret ;

– et au rejet du surplus des conclusions des requêtes.

* * *

³² N° 2005-850.