

CONSEIL D'ETAT
SECTION DU CONTENTIEUX
REQUÊTE en ANNULATION

POUR :

- **Imaginons un réseau internet solidaire (IRIS)**, association régie par la loi du 1^{er} juillet 1901, dont le siège est établi à Paris 20^e, 40 rue de la Justice, représentée par sa présidente en exercice, Meryem MARZOUKI ;

- la **Ligue des droits de l'Homme (LDH)**, association régie par la loi du 1^{er} juillet 1901, dont le siège est établi à Paris (18^e), 138 rue Marcadet, représentée par son président en exercice, Jean-Pierre DUBOIS.

Les associations requérantes désignent comme mandataire unique Jean-Pierre Dubois, domicilié à la Ligue des droits de l'homme, 138 rue Marcadet, 75018 Paris.

CONTRE :

Le Premier ministre

OBJET :

Demande d'annulation du décret n° 2008-426 du 30 avril 2008 modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques (NOR:IOCD0807352D, JO du 4 mai 2008)

*

Les associations exposantes défèrent à la censure du Conseil d'État le décret n° 2008-426 du 30 avril 2008 du Premier ministre référencé ci-dessus.

À l'appui de leurs requêtes, elles entendent faire valoir les faits et moyens suivants.

FAITS

Le 4 mai 2008 est paru au Journal Officiel le décret du Premier ministre n° 2008-426 du 30 avril 2008 modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques.

L'avis de la CNIL avait été sollicité le 27 septembre 2007, conformément aux dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. La CNIL a rendu son avis dans sa délibération n° 2007-368 du 11 décembre 2007.

Cet avis n'a été publié au Journal Officiel que le 10 mai 2008, soit 6 jours après la publication du décret contesté.

À la nouvelle finalité d'élaboration de statistiques près, le décret contesté poursuit les mêmes finalités que le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques. Il impose toutefois la collecte et le traitement automatisé de nouvelles données à caractère personnel, dont la nature, la quantité et la durée de conservation leur confèrent un caractère disproportionné au regard de ces finalités.

Le décret déféré à la censure du Conseil d'État insère en effet un article 6-1, imposant la collecte des empreintes digitales de huit doigts du demandeur de passeport. Cette collecte concerne en particulier tout mineur âgé de plus de 6 ans. Le décret contesté introduit de surcroît une modification de l'article 18, ayant pour objet la création d'une base de données dénommée « *TES* » afin de conserver et traiter de manière centralisée les données collectées sur le demandeur du passeport, en particulier et par modification de l'article 19, l'image numérisée de son visage et celle de ses huit empreintes digitales.

Les associations requérantes entendent montrer que le décret attaqué a été pris selon une procédure irrégulière et qu'il ne respecte pas les obligations imposées par les différents textes de droit interne, de droit international et de droit communautaire relatifs à la protection des personnes à l'égard du traitement des données à caractère personnel.

Elles entendent également montrer que, le décret contesté ayant été pris sur le fondement de l'article 27 de la loi n° 78-17 du 6 janvier 1978 et non sur le fondement de son article 26, la méconnaissance de la procédure prévue à cet article 26 résulte d'un détournement de procédure, ou à tout le moins d'une erreur de droit.

DISCUSSION

Sur la recevabilité :

Les deux associations requérantes sont recevables à déférer le texte litigieux devant le Conseil d'État.

– L'association Imaginons un réseau Internet solidaire (IRIS) est une association de défense de l'ensemble des droits et libertés fondamentaux dans l'usage de l'informatique et des réseaux et a été amenée, depuis sa création en octobre 1997, à agir constamment en faveur de la protection de la vie privée et des données personnelles dans le contexte du traitement numérique de telles données comme de leur circulation sur les réseaux.

– La Ligue des droits de l'homme (LDH), qui s'est donné pour but de défendre l'ensemble des droits et libertés fondamentaux, a inscrit de façon spécifique dans ses statuts la lutte « en faveur du respect des libertés individuelles en matière de traitement des données informatisées ».

Sur le fond :

I. Légalité externe

Le décret attaqué a été pris selon une procédure irrégulière.

1/ Sur la méconnaissance de l'obligation de publier simultanément l'avis de la CNIL avec l'acte autorisant le traitement

Les requérantes soutiennent tout d'abord que le décret n° 2008-426 du 30 avril 2008 modifiant celui du 30 décembre 2005 relatif aux passeports électroniques n'a pas respecté l'article 26 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Ces dispositions prévoient en effet que « *sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en oeuvre pour le compte de l'État et :*

1° Qui intéressent la sûreté de l'État, la défense ou la sécurité publique ;

2° Ou 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.

L'avis de la commission est publié avec l'arrêté autorisant le traitement ».

Ce principe s'applique également lorsque les traitements visés à l'article 26 « *portent sur des données mentionnées au I de l'article 8* » et qui font apparaître, même indirectement comme en l'espèce, les origines raciales ou ethniques, à l'instar de l'image numérisée du visage qui sera conservée dans la base de données « *TES* » (Rapport « *Mesure de la diversité et protection des données personnelles* » du 25 mai 2007 présenté à la CNIL).

Or, le décret attaqué a justement pour finalité, par la création de cette base de données, de lutter contre la constitution de faux passeports, activité qui se rattache à des préoccupations de sécurité publique ou, à tout le moins, à la constatation et la poursuite d'infractions pénales.

Il en résulte que ces dispositions auraient dû être adoptées dans le respect de la procédure prévue à l'article 26 de loi du 6 janvier 1978. En ne s'y conformant pas, le Premier Ministre s'est donc affranchi d'une garantie essentielle de la loi *Informatique & libertés*, cet article imposant que l'avis de la CNIL soit publié avec l'acte qui autorise le traitement intéressant la sécurité publique ou, à tout le moins, la constatation et la poursuite d'infractions pénales.

En l'espèce, le Conseil pourra constater que cette obligation n'a pas été remplie, le décret ayant été publié au Journal Officiel du 4 mai 2008 alors que l'avis de la CNIL est paru à celui du 10 mai 2008. Le Conseil voudra bien en déduire que le décret contesté devra être annulé au motif du non-respect de la procédure prévue par les dispositions de l'article 26 de la loi du 6 janvier 1978.

II. Légalité interne

1/ Rappel des textes et des principes applicables

Le recueil et le traitement des données personnelles comportent une série de risques pour les libertés des personnes fichées : il faut donc apprécier la légalité des mesures prises au regard

des principes qui régissent la protection des personnes à l'égard du traitement des données à caractère personnel.

- Aux termes de l'article 8 § 2 de la Convention européenne des droits de l'homme, il ne peut y avoir ingérence d'une autorité publique dans l'exercice du droit au respect de la vie privée que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire – notamment – à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales. On sait que, pour la Cour européenne des droits de l'homme, le respect de ces conditions implique des exigences relatives à la qualité de la base juridique de l'ingérence, à la proportionnalité des mesures et à la nécessité de garanties adéquates contre les abus.
- La Convention n° 108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel énoncent de leur côté des principes fondamentaux que doit respecter la mise en œuvre de traitements informatisés. Ces principes sont repris dans la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée en dernier lieu par la loi du 6 août 2004. Il s'agit notamment des principes de pertinence et de proportionnalité, de finalité et de l'exigence, là encore, de garanties suffisantes.
- Concernant plus spécifiquement les enfants, la Convention des Nations Unies relatives aux droits de l'enfant du 20 novembre 1989 prévoit en particulier en son article 16 que « *nul enfant ne fera l'objet d'immixtions arbitraires ou illégales dans sa vie privée* ».

C'est à la lumière de ces principes généraux qu'il convient d'examiner les dispositions du décret du 30 avril 2008.

2/ Sur la violation de l'article 6, 3° de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Les requérantes soutiennent que le décret litigieux ne respecte pas le principe de proportionnalité de l'article 6, 3° de la loi n° 78-17 du 6 janvier 1978 selon lequel un traitement ne peut porter que sur des données à caractère personnel qui sont « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs* ».

Or, ces dispositions sont fondamentales. Elles sont d'ailleurs consacrées par l'article 5 de la Convention 108 du Conseil de l'Europe et l'article 6 de la directive 95/46/CE qui rappellent, en des termes similaires, que 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, et qu'elles doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées. Ces dispositions constituent donc des conditions de licéité applicables à tout traitement de données à caractère personnel, y compris à ceux mis en œuvre en l'espèce par le décret n° 2008-426 du 30 avril 2008.

Leur respect est en cela impératif, d'autant que l'article 6, 3° précité a été consacré par le Conseil Constitutionnel comme l'une des garanties essentielles du respect du droit à la vie privée découlant de l'article 2 de la Déclaration des Droits de l'Homme et du Citoyen de 1789

(Cons. const., Déc. n° 2007-557 DC du 15 novembre 2007, Loi relative à la maîtrise de l'immigration, à l'intégration et à l'asile ; Cons. const., Déc. n° 2008-562 DC du 21 février 2008, Loi relative à la rétention de sûreté et à la déclaration d'irresponsabilité pénale pour cause de trouble mental).

En l'espèce, le Conseil pourra constater que ces dispositions n'ont été respectées :

- ni par l'article 6-1 inséré par le décret contesté, en ce qu'il impose la collecte des empreintes digitales de huit doigts, et que de surcroît ces dispositions s'appliquent à tout mineur âgé de plus de 6 ans ;
- ni par la modification de ses articles 18 et 19, l'article 18 ayant pour objet la création d'une base de données dénommée « TES », alors qu'elle n'a pas été rendue obligatoire par le règlement communautaire n° 2252/2004 du 13 décembre 2004.

Sur le caractère disproportionné de la collecte des empreintes digitales de huit doigts

L'article 6-1 inséré par le décret n° 2008-426 du 30 avril 2008 pose comme principe que « lors du dépôt de la demande de passeport, il est procédé au recueil de l'image numérisée du visage et des empreintes digitales de huit doigts du demandeur ».

Or, comme le souligne la CNIL dans son avis, le règlement communautaire n° 2252/2004 du 13 décembre 2004 n'impose, en matière d'empreintes digitales, que la collecte de deux empreintes.

Il n'apparaît dans le décret contesté aucune finalité additionnelle qui pourrait justifier cette augmentation de la quantité de données biométriques recueillies, ce qui lui confère un caractère excessif et non pertinent.

Il convient toutefois de relever que le passeport est un titre d'identité tout autant qu'un titre de voyage. Il n'est alors pas inutile de s'interroger sur le fait que le décret contesté puisse s'inscrire dans un projet plus global d'élaboration et de délivrance de tels titres, y compris la carte nationale d'identité. La seule justification de la collecte des empreintes digitales de huit doigts résiderait alors non pas dans les finalités énoncées du décret contesté, mais dans des finalités extérieures à ce décret. Le caractère excessif et non pertinent des données collectées se doublerait alors de la poursuite de finalités autres que celles déclarées par le décret contesté.

Dans son avis, la CNIL considère à cet égard que « l'ampleur de la réforme qui se dessine et l'importance des questions qu'elle peut soulever justifieraient que [...] le Parlement en soit saisi sous forme d'un projet de loi ».

Les requérantes estiment en effet qu'un tel projet de loi, s'il n'était soumis qu'ultérieurement au Parlement, entraverait la liberté de choix des parlementaires en la contraignant par avance par des dispositions adoptées dans le décret contesté. Il en résulterait donc un grave déficit démocratique.

Sur le caractère disproportionné de la collecte des empreintes digitales des enfants de moins de 6 ans

De surcroît, l'article 6-1 inséré par le décret n° 2008-426 du 30 avril 2008 fixe un âge minimal en deçà duquel le principe de collecte des empreintes digitales ne s'applique pas. Il prévoit en effet que « les empreintes digitales des enfants de moins de six ans ne sont pas

recueillies ». Il en résulte *a contrario* que ces dispositions s'appliquent à tout mineur dès l'âge de 6 ans.

Force est de constater qu'en retenant comme âge minimum celui de six ans pour le recueil des empreintes digitales, le décret n° 2008-426 du 30 avril 2008 étend de manière excessive l'application de ce dispositif à un nombre important de très jeunes enfants, sans l'encadrer pour autant des garanties les plus élémentaires.

Or, de nombreuses dispositions rappellent que les enfants disposent d'un droit au respect de la vie privée et qu'on ne saurait traiter de la même manière tous les enfants âgés de six à dix-huit ans.

Au niveau international, tout d'abord, l'article 16 de la Convention des Nations Unies relatives aux droits de l'enfant du 20 novembre 1989 prévoit que « *nul enfant ne fera l'objet d'immixtions arbitraires ou illégales dans sa vie privée* ».

Plus récemment et dans le domaine qui nous intéresse, le Groupe de l'article 29, qui rassemble les autorités européennes de protection des données à caractère personnel, a rappelé que « *dans toutes sociétés, les enfants devaient être traités en fonction de leur degré de maturité* » (Document de travail 1/2008 sur la protection des données à caractère personnel de l'enfant).

L'existence d'un droit des enfants au respect de leur vie privée est également garanti au niveau national. L'article 227-25 du Code pénal précise, par exemple, qu'il n'est en principe pas pénalement sanctionné d'avoir des relations sexuelles, à condition qu'elles soient sans contrainte, avec des mineurs âgés de plus de quinze ans (article 227-25 du Code pénal). Il résulte de ces dispositions qu'un enfant âgé de moins de quinze ans ne saurait être traité comme un adulte.

De manière plus intéressante encore, le droit français reconnaît qu'un enfant ne peut être traité d'une manière similaire à un adulte que s'il est âgé d'au moins treize ans. C'est ainsi à partir de seize ans que l'on considère qu'un mineur peut être jugé assez responsable pour avoir une autonomie juridique par le biais de l'émancipation (article 447 du Code civil).

Le droit pénal met également en place une gradation de la gravité des infractions commises sur des mineurs si la victime est ou non âgée de plus de quinze ans, en prévoyant une majoration des peines punissant certaines infractions, par exemple, en cas d'agressions sexuelles (article 222-29 du Code pénal), de provocation au suicide (article 222-13 du Code pénal) ou de tortures et actes de barbaries (article 222-3 du Code pénal). En dernier lieu, l'âge minimum à partir duquel un enfant peut être déclaré pénalement responsable est fixé à treize ans (article 122-8 du Code pénal).

Il n'est enfin pas inutile d'ajouter à ces exemples celui de la collecte de données à caractère personnel auprès d'enfants lors de leur connexion à des sites Internet. Les responsables de sites Internet fixent au moins à treize ans l'âge à partir duquel ils procèdent à cette collecte sans obtenir l'autorisation des parents.

Rappelons d'ailleurs que les commentaires de la CNIL relatifs aux dispositions de l'article 6-1 inséré par le décret litigieux ont été sur ce point plus que sévères. Elle a en effet considéré que « *l'âge à partir duquel les empreintes sont relevées n'est pas seulement un élément technique mais une question de principe méritant un large débat voire un amendement à la convention sur les droits de l'enfant et que pour préserver la dignité de la personne et pour*

garantir la fiabilité de la procédure, la collecte et le traitement des empreintes digitales doivent être limités pour les enfants » (Délibération n° 2007-368 du 11 décembre 2007).

Au regard de l'ensemble de ces éléments, et compte tenu du très faible risque de fraude pour les enfants en bas âge, il apparaît plus que disproportionné d'imposer la constitution d'un passeport électronique pour les enfants dès l'âge de six ans.

Sur ces fondements, le Conseil voudra bien annuler l'article 6-1 inséré par le décret n° 2008-426 du 30 avril 2008.

Sur le caractère disproportionné de la création de la base de données dénommée TES

L'article 18 modifié du décret n° 2008-426 du 30 avril 2008 prévoit qu' « *afin de mettre en œuvre les procédures d'établissement, de délivrance, de renouvellement et de retrait des passeports mentionnés aux articles 1^{er} et 17-1, ainsi que pour prévenir et détecter leur falsification et leur contrefaçon, le ministre de l'Intérieur est autorisé à créer un système de traitement automatisé de données à caractère personnel dénommés TES* ».

Au regard de ces éléments, la constitution d'une telle base de données se justifierait :

- d'une part, par la possibilité de faciliter l'établissement, la délivrance, le renouvellement et le retrait des passeports, et
- d'autre part, par la nécessité de prévenir et détecter la falsification et la contrefaçon des passeports.

Le Conseil pourra néanmoins constater que la constitution d'une telle base de données n'est pas adéquate, n'est pas pertinente et est excessive au sens des dispositions de l'article 6, 3° de la loi *Informatique et libertés*.

D'après le Premier Ministre, la constitution de la base de données « *TES* » a tout d'abord pour objectif de faciliter l'établissement, la délivrance, le renouvellement et le retrait des passeports.

Une telle justification ne semble cependant pas tenir eu égard aux forts risques d'inefficacité de ce dispositif. Comme l'a en effet relevé la CNIL, la péremption des données fournies lors de la première délivrance du passeport impose en tout état de cause que celles-ci soient à nouveau recueillies lors de son renouvellement (Délibération n° 2007-368 du 11 décembre 2007).

L'article 4 du décret prévoit en effet que les passeports ont une durée de validité de dix ans en général et de cinq ans lorsqu'ils sont délivrés à un mineur. Le temps ainsi écoulé entre deux périodes d'établissement d'un passeport est suffisamment important pour que les informations initialement recueillies perdent toute leur fiabilité et leur pertinence.

Il en est ainsi encore plus pour un mineur dont l'évolution sur une période de cinq ans demeure considérable (taille, physionomie, changement de domicile, domicile partagé, etc.).

Il résulte de ces éléments que la constitution d'une base de données conservant les informations biométriques contenues dans un passeport ne peut pas être justifiée par le fait qu'elle faciliterait l'établissement, la délivrance, le renouvellement et le retrait de celui-ci.

À supposer qu'elle le soit, le Conseil ne manquera pas de constater qu'elle est excessive. Elle expose en effet les personnes concernées à un risque important d'atteintes à leur liberté

individuelle et à leur vie privée. On en veut pour preuve le fait que le décret contesté vise à recueillir un nombre important de données (pas moins de 25 catégories différentes) qui pourront être conservées pendant quinze ans lorsque le passeport est délivré à un majeur et pendant dix ans lorsqu'il est délivré à un mineur (article 24 du décret du 30 avril 2008) et ce alors que ces documents ont eux-mêmes une durée de validité de dix ans pour les majeurs et de cinq ans pour les mineurs.

Le Conseil voudra donc bien annuler l'article 18 du décret n° 2008-426 du 30 avril 2008 en ce que le traitement ainsi mis en œuvre est disproportionné au sens de l'article 6,3° de la loi n° 78-17 du 6 janvier 1978.

L'article 18 du décret prévoit, en second lieu, que la constitution de la base de données TES est justifiée par la nécessité de prévenir et détecter la falsification et la contrefaçon des passeports.

Or, à juste titre, la CNIL a relevé « *qu'aucune mesure particulière n'est prévue, parallèlement à la conservation de données biométriques, pour s'assurer de l'authenticité des pièces justificatives fournies à l'appui des demandes* ».

Une telle absence présente pourtant de très importants risques car, une fois les données enregistrées, ce sont elles qui feront foi. Si leur authenticité n'est pas vérifiée dans des conditions légalement prévues, il est permis de douter de l'efficacité de la constitution d'une telle base de données pour prévenir et détecter les cas de falsification, le recoupement des informations dans ce cadre étant également peu fiable.

À supposer qu'elle soit efficace, la constitution de cette base de données demeure elle aussi excessive au regard de la finalité poursuivie par le décret. Elle accroît en effet le risque d'atteintes à la liberté individuelle et à la vie privée des personnes concernées sans apporter de garanties supplémentaires.

Or, le contrôle de l'authenticité des passeports peut être effectué à partir d'autres moyens moins attentatoires à la liberté individuelle et à la vie privée comme, par exemple, le contrôle visuel ou le recours à des techniques de fabrication des passeports rendant ces derniers difficilement falsifiables voire infalsifiables.

Il en résulte que les dispositions de l'article 18 du décret n° 2008-426 du 30 avril 2008 méconnaissent le principe de proportionnalité visé à l'article 6, 3° de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, à l'article 5 c de la Convention n° 108 du Conseil de l'Europe, et à l'article 6.1 c de la directive n° 95/46/CE.

Sur ce fondement, votre Conseil voudra bien annuler l'article 18 du décret n° 2008-426 du 30 avril 2008.

3/ Sur la méconnaissance de la procédure prévue à l'article 26 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Les requérantes considèrent par ailleurs que le décret litigieux n'a pas respecté les dispositions de l'article 26 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés auxquelles il était pourtant soumis.

Sur le détournement de la procédure prévue à l'article 26

Si les dispositions du décret contesté relatives à la création d'un passeport biométrique devaient effectivement être prises sur le fondement de l'article 27 de la loi du 6 janvier 1978, les dispositions du même décret relatives à la création de la base de données « TES » devaient, en revanche, être adoptées sur le fondement de l'article 26.

Ces dispositions prévoient en effet que « *sont autorisés par arrêté du ou des ministres compétents, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en oeuvre pour le compte de l'État et :*

1° Qui intéressent la sûreté de l'État, la défense ou la sécurité publique ;

2° Ou 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.

L'avis de la commission est publié avec l'arrêté autorisant le traitement ».

Elles précisent également que « *ceux de ces traitements qui portent sur des données mentionnées au I de l'article 8 sont autorisés par décret en Conseil d'État pris après avis motivé et publié de la commission ; cet avis est publié avec le décret autorisant le traitement ».*

Le I de l'article 8 vise les données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, comme, par exemple, l'image numérisée du visage qui sera conservée dans la base de données « TES » (Rapport « *Mesure de la diversité et protection des données personnelles* » du 25 mai 2007 présenté à la CNIL).

Or, en l'espèce, le décret n° 2008-426 du 30 avril 2008 a notamment pour finalité la sécurité publique ou, à tout le moins, la constatation ou la poursuite d'infractions pénales. L'article 18 du décret précise en effet que la base de données « TES » permettra de lutter contre la constitution de faux passeports, activité qui se rattache à des préoccupations de sécurité publique ou, à tout le moins, à la constatation et la poursuite d'infractions pénales.

L'article 21-1 du décret prévoit en outre que « *peuvent accéder aux données enregistrées dans le traitement prévu à l'article 18, à l'exclusion de l'image numérisée des empreintes digitales, dans les conditions fixées aux articles 9 et 33 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles transfrontaliers :*

- « *les agents des services de la direction générale de la police nationale et de la direction générale de la gendarmerie nationale chargés des missions de prévention et de répression des actes de terrorisme individuellement désignés et spécialement habilités respectivement par le directeur général de la police nationale et le directeur général de la gendarmerie nationale ;*
- *les agents des services de renseignement du ministère de la défense chargés des missions de prévention des actes de terrorisme individuellement désignés et spécialement habilités respectivement par le directeur général de la sécurité extérieure, le directeur de la protection et de la sécurité de la défense ou le directeur du renseignement militaire ».*

Au regard de ces éléments, il ne fait aucun doute que les dispositions du décret n° 2008-426 du 30 avril 2008 relatives à la base de données « TES » poursuivent une finalité de sécurité publique, ou, à tout le moins, relative à la constatation ou à la poursuite d'infractions pénales,

l'une ou l'autre étant d'ailleurs seule de nature à pouvoir justifier la création d'une telle base de données.

Il en résulte que ces dispositions auraient dû être adoptées dans le respect de la procédure prévue à l'article 26 de la loi du 6 janvier 2008. En choisissant de ne pas appliquer ces dispositions à la finalité de prévention et de détection des passeports, le Premier Ministre a donc commis un détournement de procédure (CE, Ass., 24 juin 1960, Société Frampar et Société France Éditions et Publications).

Le Premier Ministre s'est en cela affranchi d'une garantie essentielle prévue par l'article 26 de la loi du 6 janvier 1978, cet article imposant que l'avis de la CNIL soit publié avec le décret qui autorise le traitement intéressant la sécurité publique.

Sur ce fondement, le Conseil ne pourra qu'annuler les dispositions de l'article 18 du décret n° 2008-426 du 30 avril 2008 relatives à la constitution de la base de données « *TES* ».

En outre, à supposer que le Premier Ministre n'ait pas procédé à un tel détournement de procédure, votre Conseil ne pourra que constater qu'une erreur de droit a été commise.

Sur l'erreur de droit résultant de la violation des dispositions de l'article 26 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Comme il a été précédemment précisé, les dispositions relatives à la constitution de la base de données « *TES* », compte tenu de leur finalité spécifique, auraient dû être adoptées dans le cadre de la procédure de l'article 26 de la loi du 6 janvier 1978. Il en résulte que le Premier Ministre, en adoptant de telles dispositions sur le fondement de l'article 27 de la loi du 6 janvier 1978 :

- a méconnu les dispositions de l'article 26 de la loi du 6 janvier 1978 ;
- et
- est allé au-delà du champ d'application de l'article 27 de la même loi.

Le Premier Ministre a donc commis une erreur de droit qui l'a notamment conduit à publier le décret n° 2008-426 du 30 avril 2008, sans y joindre l'avis pourtant exigé de la CNIL.

En outre, s'il était considéré que les données recueillies dans la base de données « *TES* » ne sont pas des données sensibles au sens du I de l'article 8 de la loi du 6 janvier 1978, l'erreur de droit commise par le Premier Ministre méconnaît l'attribution de compétence effectuée en faveur des ministres concernés. Or, ces derniers ont seulement contresigné le décret n° 2008-426 du 30 avril 2008 dont seul le Premier Ministre demeure l'auteur. Les ministres compétents ne sont donc pas les coauteurs de l'acte administratif autorisant la création de la base de données « *TES* », en violation totale de l'article 26 de la loi du 6 janvier 1978 qui impose que de tels traitements « sont autorisés par arrêté du ou des ministres compétents ».

Au regard de ces éléments, votre Conseil ne pourra donc qu'annuler les dispositions du décret n° 2008-426 du 30 avril 2008 relatives à la constitution de la base de données « *TES* ».

En conclusion,

Les dispositions du décret attaqué violent :

- l'article 16 de la Convention des Nations Unies relatives aux droits de l'enfant du 20 novembre 1989, dans la mesure où la collecte des empreintes digitales des enfants seront collectées *à partir de l'âge de six ans, sans aucune garantie spécifique eu égard à leur âge.*
- l'article 5c de la Convention n° 108 du Conseil de l'Europe, l'article 6.1.c de la directive n° 95/46/CE, l'article 6, 3° de la loi du 6 janvier 1978, dans la mesure où *la création de la base de données dénommée TES présente un caractère disproportionné ;*
- l'article 26 de la loi du 6 janvier 1978, en tant *qu'il prévoit que l'avis de la CNIL soit publié avec le décret qui autorise le traitement intéressant la sécurité publique.*

PAR CES MOTIFS, et tous autres à produire, déduire ou suppléer, les associations exposantes concluent à ce qu'il plaise au Conseil d'État :

ANNULER :

Le décret n° 2008-426 du 30 avril 2008.