CONSEIL CONSTITUTIONNEL

Commentaire

Décision n° 2012-652 DC du 22 mars 2012

Loi relative à la protection de l'identité

La loi relative à la protection de l'identité est issue d'une proposition de loi déposée par MM. Lecerf et Houel, sénateurs (Sénat, 27 juillet 2010, n° 682). Ce texte a été adopté par le Sénat et l'Assemblée nationale en première lecture les 31 mai 2011 et 7 juillet 2011, puis en deuxième lecture les 3 novembre 2011 et 13 décembre 2011. Après la commission mixte paritaire (CMP) le 10 janvier 2012, le texte résultant des conclusions de la CMP a d'abord été soumis au vote de l'Assemblée nationale le 12 janvier 2012, qui l'a amendé, puis a été rejeté par le Sénat le 26 janvier 2012. À l'issue d'une nouvelle lecture à l'Assemblée nationale le 1er février 2012, puis au Sénat, qui a rejeté le texte le 21 février 2012, le Gouvernement a demandé à l'Assemblée nationale de statuer définitivement sur la proposition de loi, ce qu'elle a fait le 6 mars 2012.

Le Conseil constitutionnel a été saisi le 7 mars 2012 par plus de soixante députés et plus de soixante sénateurs qui contestaient en particulier les articles 5 et 10 de la loi.

Dans sa décision n° 2012-652 DC, le Conseil constitutionnel a déclaré ces articles de la loi (ainsi que d'autres dispositions qui n'en étaient pas séparables) contraires à la Constitution. Il a également examiné d'office et déclaré contraire à la Constitution son article 3.

I – La loi déférée

A. – Les articles de la loi déférée :

Cette loi est issue d'une proposition de loi. Elle n'a pas été soumise pour avis au Conseil d'État et est dépourvue d'étude d'impact. On apprend seulement dans les documents parlementaires qu'environ 15 000 infractions d'usurpation d'identité sont constatées chaque année, pour 100 000 infractions potentielles.

L'article 1er de la loi prévoit que l'identité d'une personne se prouve par tout moyen. La présentation d'une carte nationale d'identité ou d'un passeport français en cours de validité suffit à en justifier.

L’article 2 prévoit que la carte d’identité et le passeport comportent un composant électronique sécurisé contenant les données suivantes :

1° Le nom de famille, le ou les prénoms, le sexe, la date et le lieu de naissance du demandeur ;

2° Le nom dont l’usage est autorisé par la loi, si l’intéressé en a fait la demande ;

3° Son domicile ;

4° Sa taille et la couleur de ses yeux ;

5° Deux de ses empreintes digitales ;

6° Sa photographie.

L’article 3 prévoyait la possibilité que soit adjoint au titre d’identité un composant électronique permettant l’identification dans les relations commerciales.

L’article 4 prévoit que les agents recueillant une demande de titre d’identité ou du passeport vérifient directement les données de l’état civil fournies par l’usager.

L’article 5 autorisait la création d’un traitement de données intégrant les données de toutes les cartes d’identité et de passeport (« fichier central commun »).

L’article 6 est relatif à l’accès aux données électroniques sécurisées par les agents chargés des missions de recherche et de contrôle de l’identité des personnes ainsi qu’à la consultation du fichier aux fins de vérification d’identité en cas de doute sérieux sur l’identité de la personne ou lorsque le titre présenté est défectueux ou paraît endommagé ou altéré.

L’article 7 renvoie à un décret en Conseil d’État, pris après avis motivé et publié de la Commission nationale de l’informatique et des libertés (CNIL), les conditions dans lesquelles le fichier peut être consulté par les administrations publiques, les opérateurs assurant une mission de service public et les opérateurs économiques pour s’assurer de la validité de la carte nationale d’identité ou du passeport français présenté par son titulaire pour justifier de son identité.

L’article 8 renvoie à un décret en Conseil d’État, pris après avis motivé et publié de la CNIL, les modalités d’application de la loi, et notamment la durée de

conservation des données dans le fichier et les modalités et la date de mise en œuvre des fonctions électroniques facultatives prévues par l'article 3.

L'article 9 aggrave les peines en cas d'atteinte à un traitement de données à caractère personnel mis en œuvre par l'État.

L'article 10 permettait, à des fins de sécurité, aux agents des services de police et de gendarmerie d'accéder au fichier central commun aux passeports et aux cartes nationales d'identité.

L'article 11 prévoit que toute décision juridictionnelle rendue en raison de l'usurpation d'identité dont une personne a fait l'objet et dont la mention sur les registres de l'état civil est ordonnée doit énoncer ce motif dans son dispositif.

L'article 12 précise que la loi est applicable à l'ensemble du territoire de la République.

B. – L'objet de la saisine du Conseil constitutionnel

M. Lecerf avait présenté en juin 2005 un rapport d'information au Sénat[1] sur « *Identité intelligente et respect des identités* » qui distingue bien les deux fonctions de la biométrie.

D'une part, la biométrie peut avoir une fonction d'authentification. Il s'agit alors de s'assurer qu'une personne a bien l'identité qu'elle revendique. À cet effet trois techniques sont possibles : une carte à puce biométrique sans fichier central, une carte à puce biométrique avec un fichier central unidirectionnel dans le sens « identité vers biométrie », ou, enfin, une carte à puce biométrique avec un fichier central dit à « lien faible ». Ce dernier système permet d'assurer l'unicité de l'identité tout en garantissant l'anonymat.

Selon la formule de Philippe Goujon : « *Dans une base de données à "lien faible", les données biographiques et biométriques d'une personne ne peuvent être croisées, sauf au moment de la délivrance du titre. En effet, à une empreinte correspond techniquement dans de telles bases de données non pas une identité mais un ensemble d'identités. Il n'est donc pas possible de déterminer l'identité qui correspond à une empreinte donnée.* »[2]

D'autre part, la biométrie peut avoir une fonction d'identification. Ici il s'agit de comparer les données biométriques avec celles contenues dans la base afin de

[1] Sénat, session ordinaire, n° 439.

[2] Rapport sur la proposition de loi, adoptée avec modifications par le Sénat en deuxième lecture, relative à la protection de l'identité, Assemblée nationale, XIII^{e} législature, n° 4016, 30 novembre 2011, p. 8.

retrouver l'identité de la personne. Une base de données à « lien fort » permet de faire correspondre données biométriques et donnés biographiques. L'objectif est de déterminer l'identité d'une personne qui ne peut ou ne veut la révéler. Dès lors, les caractéristiques biométriques de cette personne sont comparées avec celles de l'ensemble des personnes du fichier. C'est d'après ce principe que fonctionne l'identification judiciaire, par exemple le fichier automatisé des empreintes digitales.

Avec la fonction d'identification, il s'agit de retrouver l'identité à partir de la biométrie et inversement. Un fichier central est absolument nécessaire. Il n'en va pas de même avec la fonction d'authentification. L'apparition de documents d'identité ou de voyages biométriques s'inscrit dans cette logique d'authentification. Il s'agit de vérifier que celui qui dispose d'un tel document en est bien le titulaire en examinant non seulement sa photo mais les autres caractéristiques qui ont été recueillies et qui figurent dans le document d'identité.

Le règlement n° 2252/2004 du Conseil européen du 13 décembre 2004[3] a prévu que les passeports délivrés par les États membres devaient désormais comporter sur une puce deux éléments biométriques : « *une photo faciale* » et « *deux empreintes digitales relevées à plat* ». Pour l'application de ce règlement, la France a pris un décret le 30 décembre 2005 relatif aux passeports électroniques, qui a été modifié par un décret du 30 avril 2008[4]. Ce dernier décret était allé au-delà des exigences du règlement européen en prévoyant le recueil de l'image numérisée du visage et, sauf pour les enfants de moins de six ans, « *des empreintes digitales de huit doigts du demandeur* ».

Le décret de 2008 a fait l'objet de recours pour excès de pouvoir devant le Conseil d'État. Celui-ci a jugé deux points principaux[5].

– En premier lieu, il était soutenu que les mesures de collecte et de traitement des données personnelles constituaient une atteinte disproportionnée à la vie privée notamment protégée par la CEDH. Le Conseil d'État a rappelé que l'ingérence dans l'exercice du droit de toute personne au respect de sa vie privée que constituent la collecte, la conservation et le traitement, par une autorité publique, d'informations personnelles nominatives ne peut être légalement autorisée que si elle répond à des finalités légitimes et si le choix, la collecte et

[3] Règlement (CE) n° 2252/2004 du Conseil, du 13 décembre 2004, établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres.

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

[5] Conseil d'État, Ass, 26 octobre 2011, *Association pour la promotion de l'image et autres,* n° 317827, conclusions Julien Boucher.

le traitement des données sont effectués de manière adéquate et proportionnée au regard de ces objectifs.

Examinant les dispositions contestées à la lumière de ces principes, le Conseil d'État a tout d'abord précisé la finalité du fichier TES (Titres électroniques sécurisés) en relevant qu'il servait seulement « *à confirmer que la personne présentant une demande de renouvellement d'un passeport [était] bien celle à laquelle le passeport a été initialement délivré ou à s'assurer de l'absence de falsification des données contenues dans le composant électronique du passeport* ».

Au regard de cet objectif, il a jugé que la collecte et la conservation d'un plus grand nombre d'empreintes digitales que celles figurant dans le composant électronique n'étaient ni adéquates, ni pertinentes et apparaissaient excessives au regard des finalités du traitement informatisé. Il a donc annulé partiellement l'article 5 du décret, en tant qu'il prévoyait la conservation des empreintes digitales qui ne figurent pas dans le composant électronique du passeport. De telles mesures ne sont pas adaptées, nécessaires et proportionnées. Le Conseil d'État a ainsi ordonné la destruction de 40 millions d'empreintes.

– En deuxième lieu, le Conseil d'État a jugé que, compte tenu de ses effets (facilitation des démarches pour les usagers, renforcement de l'efficacité de la lutte contre la fraude documentaire, meilleure protection des données recueillies), et des restrictions et précautions prévues par le décret (utilisation des données strictement limitée et précisément encadrée, durée de conservation restreinte), le système centralisé TES était en adéquation avec les finalités légitimes du traitement institué et ne portait pas au droit des individus au respect de leur vie privée une atteinte disproportionnée aux buts de protection de l'ordre public en vue desquels il avait été créé.

Le Conseil d'État n'a ainsi pas suivi la CNIL qui, dans un avis du 11 décembre 2007, s'était déclarée défavorable à l'enregistrement des données biométriques dans le fichier TES, qu'elle estimait disproportionné aux objectifs poursuivis. Le Conseil d'État a relevé que le fichier n'était consulté qu'en cas de demande ou de renouvellement d'un passeport ou en cas de falsification probable de celui-ci. En outre, et surtout, toute recherche dans le fichier TES à partir d'éléments biométriques est impossible, notamment du fait du stockage dans des bases différentes des données biométriques et des données d'identité. Le Conseil d'État a ainsi d'abord pris en compte cette absence de fonction d'identification du fichier TES pour ne pas censurer l'enregistrement des données biométriques alors même que cet enregistrement n'est pas nécessaire à la fonction d'authentification.

La loi déférée au Conseil constitutionnel posait précisément cette question de l'utilisation d'un fichier biométrique national à des fins d'identification. C'est sur ce point que le Sénat et l'Assemblée nationale se sont opposés.

La CNIL a produit, le 25 octobre 2011, après l'examen en première lecture de la proposition de loi, une note d'observations exprimant un avis défavorable à un tel choix. Elle a notamment indiqué :

« *La spécificité des données biométriques a pour conséquence d'accroître le niveau d'exigence quant à leur utilisation. En particulier, deux principes fondateurs du droit à la protection des données à caractère personnel doivent être impérativement respectés :*

« *– le principe de finalité : les traitements de données doivent poursuivre des finalités "*déterminées, explicites et légitimes*" (article 6-2° de la loi "informatique et libertés") et les données concernées ne doivent pas être utilisées à d'autres fins que celles qui ont été définies ;*

« *– le principe de proportionnalité : les dispositifs envisagés doivent être strictement proportionnés au regard des objectifs du traitement. Plus précisément, les données traitées doivent être "*adéquates, pertinentes et non excessives*" au regard des finalités attribuées au traitement (article 6-3°), leur durée de conservation dans le traitement ne doit pas excéder la durée nécessaire à ces finalités (article 6-5°) et elles ne doivent être rendues accessibles qu'aux destinataires ayant un intérêt légitime à en connaître.*

« *Le respect de ces principes est d'autant plus impérieux lorsque les données biométriques sont collectées dans le cadre des procédures de délivrance de titres d'identité ou de voyage qui sont détenus par la quasi-totalité de la population française.* (…)

« *Comme elle l'a rappelé dans son avis sur les passeports biométriques, tout comme dans son avis sur le précédent projet du ministère de l'intérieur relatif aux cartes d'identité biométriques, la Commission estime que l'introduction d'un composant électronique contenant des données biométriques est proportionnée par rapport à l'objectif de renforcement de la sécurité de l'établissement et de la vérification des titres (…).*

« *En ce qui concerne la proportionnalité d'une base centrale d'éléments biométriques, la Commission relève qu'il existe des modalités de lutte contre la fraude qui apparaissent tout à la fois aussi efficaces et plus respectueuses de la protection de la vie privée des personnes, en particulier celles qui s'attachent à*

sécuriser les "documents sources" à produire pour la délivrance de titres d'identité.

« *Ainsi en est-il de la procédure de vérification des données d'état civil, prévue par la proposition de loi. La Commission rappelle à cet égard que cette procédure a été appelée de ses vœux à de nombreuses reprises depuis 1986, et notamment dans sa délibération sur le passeport biométrique, dans la mesure où elle permet de renforcer la sécurité du processus de délivrance des titres d'identité, en se prémunissant de certaines modalités de fraude documentaire, comme l'invention d'identité, la présentation de faux actes d'état civil ainsi que la présentation d'actes d'état civil de tiers. Cette procédure a finalement été prévue par un décret du 10 février 2011, pris après avis de la CNIL.*

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

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

Le Sénat avait adopté un article 5 permettant la création d'un fichier central mais n'autorisant son interrogation qu'avec la technique dite du « lien faible ». Ainsi, était rendue possible la fonction d'authentification mais était écartée la recherche d'une identité par les seules données biométriques. Trois sous-fichiers étanches étaient envisagés (respectivement pour l'image numérisée, les empreintes digitales et le reste des données). Pour chacun de ces sous-fichiers, des sous-ensembles de quelques milliers de personnes auraient été créés. Les liens entre les données des sous-fichiers n'auraient pu être vérifiés que par le biais de ces sous-ensembles. La détection d'une tentative d'usurpation d'identité aurait reposé sur le fait que chaque sous-ensemble correspondant à un nombre de personnes réduit (quelques milliers), la probabilité que le fraudeur figurât dans les mêmes sous-ensembles que la personne dont il tente d'usurper l'identité était infinitésimale. La valeur de la technique du « lien faible » repose donc sur une hypothèse probabiliste.

La version retenue par l'Assemblée nationale, et déférée au Conseil constitutionnel, était très différente. L'article 5 disposait :

« *I. – Afin de préserver l'intégrité des données requises pour la délivrance du passeport français et de la carte nationale d'identité, l'État crée, dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, un traitement de données à caractère personnel facilitant leur recueil et leur conservation.*

« *Ce traitement de données, mis en œuvre par le ministère de l'intérieur, permet l'établissement et la vérification des titres d'identité ou de voyage dans des conditions garantissant l'intégrité et la confidentialité des données à caractère personnel ainsi que la traçabilité des consultations et des modifications effectuées par les personnes y ayant accès.*
« *L'identification du demandeur d'un titre d'identité ou de voyage ne peut s'y effectuer qu'au moyen des données énumérées aux 1° à 5° de l'article 2.*

« *Il ne peut y être procédé au moyen des deux empreintes digitales recueillies dans le traitement de données que dans les cas suivants :*

« *1° Lors de l'établissement des titres d'identité ou de voyage ;*

« *2° Dans les conditions prévues aux articles 55-1, 76-2 et 154-1 du code de procédure pénale ;*

« *3° Sur réquisition du procureur de la République, aux fins d'établir, lorsqu'elle est inconnue, l'identité d'une personne décédée, victime d'une catastrophe naturelle ou d'un accident collectif.*

« *Aucune interconnexion au sens de l'article 30 de la loi n° 78-17 du 6 janvier 1978 précitée ne peut être effectuée entre les données mentionnées aux 5° et 6° de l'article 2 de la présente loi contenues dans le traitement prévu par le présent article et tout autre fichier ou recueil de données nominatives.*

« *II. – L'article 55-1 du code de procédure pénale est complété par un alinéa ainsi rédigé :*

"Si les nécessités de l'enquête relative aux infractions prévues aux articles 226-4-1, 313-1, 313-2, 413-13, 433-19, 434-23, 441-1 à 441-4, 441-6 et 441-7 du code pénal, aux articles L. 225-7, L. 225-8 et L. 330-7 du code de la route, à l'article L. 2242-5 du code des transports et à l'article 781 du présent code l'exigent, le traitement de données créé par l'article 5 de la loi n° du relative à la protection de l'identité peut être utilisé pour identifier, sur

autorisation du procureur de la République, à partir de ses empreintes digitales, la personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis ou tenté de commettre une de ces infractions. La personne en est informée. Cette utilisation des données incluses au traitement susvisé doit être, à peine de nullité, mentionnée et spécialement motivée au procès-verbal. Les traces issues de personnes inconnues, y compris celles relatives à l'une des infractions susvisées, ne peuvent être rapprochées avec lesdites données."

« *III. – Le second alinéa de l'article 76-2 du même code est ainsi rédigé :*

"Les trois derniers alinéas de l'article 55-1 sont applicables."

« *IV. – Le second alinéa de l'article 154-1 du même code est ainsi rédigé :*
"Les trois derniers alinéas de l'article 55-1 sont applicables."

« *V. – La sous-section 1 de la section 3 du chapitre I*^{er} *du titre III du livre I*^{er} *du même code est complétée par un article 99-5 ainsi rédigé :*

"Art. 99-5. – Si les nécessités de l'information relative à l'une des infractions mentionnées au dernier alinéa de l'article 55-1 l'exigent, l'officier de police judiciaire peut, avec l'autorisation expresse du juge d'instruction, utiliser le traitement de données créé par l'article 5 de la loi n° du relative à la protection de l'identité pour identifier une personne à partir de ses empreintes digitales sans l'assentiment de la personne dont les empreintes sont recueillies." »

Cet article 5 devait se lire également en combinaison avec l'article 10 qui ajoutait à l'article 9 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 frontaliers un sixième alinéa ainsi rédigé :

« *– le système de gestion commun aux passeports et aux cartes nationales d'identité* ».

Cet article 9 liste tous les traitements automatisés auxquels les agents individuellement désignés et dûment habilités de certains services de police et de gendarmerie peuvent avoir accès : « *pour les besoins de la prévention et de la répression des atteintes à l'indépendance de la Nation, à l'intégrité de son territoire, à sa sécurité, à la forme républicaine de ses institutions, aux moyens de sa défense et de sa diplomatie, à la sauvegarde de sa population en France et à l'étranger et aux éléments essentiels de son potentiel scientifique et économique et des actes de terrorisme.* »

Au total, avec ces articles 5 et 10, le fichier pouvait, indépendamment de l'établissement des titres d'identité ou de voyage, être consulté dans trois cas :

– Sur réquisition du procureur de la République, aux fins d'établir, lorsqu'elle est inconnue, l'identité d'une personne décédée, victime de catastrophe naturelle ou d'accident collectif.

– Directement par les forces de police et de gendarmerie « *pour les besoins de la prévention des atteintes à (la) sécurité (du territoire), (…) à la sauvegarde de la population…* »

– Dans les conditions prévues aux articles 55-1, 76-2 et 154-1 du code de procédure pénale, c'est-à-dire dans le cadre d'une enquête de flagrance, d'une enquête préliminaire ou d'une commission rogatoire – les conditions étant précisées aux II, III, IV et V de l'article 5.

À l'article 5, le paragraphe II pour la flagrance, le paragraphe III pour l'enquête préliminaire et le paragraphe IV pour la commission rogatoire prévoyaient que la comparaison d'une empreinte relevée avec celles contenues dans le fichier central était possible sur autorisation du procureur de la République, pour les nécessités de l'enquête, à l'encontre d'une personne pour laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis ou tenté de commettre une des infractions suivantes :

– l'usurpation d'identité (article 226-4-1 du code pénal), qui a été créée par la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure ;

– l'escroquerie (articles 313-1 et 313-2 du même code) ;

– l'atteinte aux services spécialisés de renseignement (article 413-13 du même code) ;

– l'atteinte à l'état civil des personnes (article 433-19 du même code) ;

– l'entrave à l'exercice de la justice (article 434-23 du même code) ;

– le faux et l'usage de faux (article 441-1 du même code), le faux commis dans un document délivré par une administration publique (article 441-2 du même code), la détention frauduleuse d'un tel document (article 441-3 du même code), le faux en écriture publique (article 441-4 du même code), le fait de se faire délivrer frauduleusement un document par une administration publique

(article 441-6 du même code), l'établissement d'un faux certificat (article 441-7 du même code) ;

– la fraude au permis de conduire (articles L. 225-7 et L. 225-8 du code de la route) ;

– la fraude aux plaques d'immatriculation (article L. 330-7 du même code) ;

– la mention d'une fausse adresse ou identité aux agents assermentés des transports (article L. 2245-5 du code des transports) ;

– la demande indue de délivrance d'un extrait du casier judiciaire d'un tiers (article L. 781 du code de procédure pénale).

Il était prévu que la personne concernée devait être informée de cette consultation. Par ailleurs, cette utilisation des données du fichier central devait, à peine de nullité, être mentionnée et spécialement motivée dans le procès-verbal. Enfin, les traces issues de personnes inconnues – c'est-à-dire les empreintes relevées sur une scène d'infraction sans que l'on puisse les attribuer à une personne mise en cause – y compris celles relatives à l'une des infractions concernées, ne pouvaient être rapprochées avec lesdites données.

Le paragraphe V de l'article 5 de la loi déférée prévoyait que, si les nécessités de l'information relative à l'une des infractions mentionnées précédemment l'exigeaient, l'officier de police judiciaire pouvait, avec l'autorisation expresse du juge d'instruction, utiliser le fichier central pour identifier une personne à partir de ses empreintes digitales. Dans ce cas, compte tenu de l'autorisation expresse du juge d'instruction, il devenait possible de procéder à cette consultation sans l'assentiment de la personne dont les empreintes sont recueillies.

C. – Les griefs des requérants

Les requérants contestaient les articles 5 et 10 de la loi en invoquant principalement le caractère excessif du traitement de données à caractère personnel institué. Ils soutenaient en premier lieu que l'instauration d'un fichier de la population contenant des données de biométrie et consultable à des fins de police constituait, en elle-même, une menace pour les libertés publiques et les libertés de l'individu et, en particulier, le respect de la vie privée. Ils dénonçaient le choix du « lien fort » permettant l'identification d'une personne à partir de se empreintes digitales. Ils soutenaient à titre subsidiaire que le législateur avait insuffisamment encadré les conditions dans lesquelles les services de police judiciaire ou les autorités judicaires pourraient utiliser ce fichier et dénonçaient à

ce titre l'incompétence négative du législateur et l'absence de garanties légales de nature à éviter l'arbitraire dans la mise en œuvre de ce traitement.

La décision du Conseil constitutionnel de censurer les articles 5 et 10 de la loi est fondée sur le premier grief.

II – Examen de la constitutionnalité des articles 5 et 10

A. – Le cadre constitutionnel

Le cadre constitutionnel du droit des traitements de données à caractère personnel est désormais bien fixé par le Conseil constitutionnel :

* Avant tout le Conseil s'assure du respect de la vie privée. L'article 2 de la Déclaration des droits de l'homme et du citoyen dispose : « *Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression* ». La liberté proclamée par cet article implique le respect de la vie privée[6].

* Il est à tout moment loisible au législateur, statuant dans le domaine de sa compétence, de modifier des textes antérieurs ou d'abroger ceux-ci en leur substituant, le cas échéant, d'autres dispositions, dès lors que, ce faisant, il ne prive pas de garanties légales des exigences constitutionnelles[7]. C'est notamment à ce contrôle que s'est livré le Conseil constitutionnel lors de la refonte de la loi du 6 janvier 1978[8].

* Il appartient au législateur, en vertu de l'article 34 de la Constitution, de fixer les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques. Il lui incombe notamment d'assurer la conciliation entre, d'une part, la sauvegarde de l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la protection de principes et de droits de valeur constitutionnelle et, d'autre part, les autres droits et libertés

---

[6] Décisions n[os] 99-416 DC du 23 juillet 1999, *Loi portant création d'une couverture maladie universelle*, cons. 45 ; 99-419 DC du 9 novembre 1999, *Loi relative au pacte civil de solidarité*, cons. 72 à 75.

[7] Décisions n[os] 86-210 DC du 29 juillet 1986, *Loi portant réforme du régime juridique de la presse*, cons. 2 ; 98-396 DC du 19 février 1998, *Loi organique portant recrutement exceptionnel de magistrats de l'ordre judiciaire et modifiant les conditions de recrutement des conseillers de cour d'appel en service extraordinaire*, cons. 16 ; n° 2001-446 DC du 27 juin 2001, *Loi relative à l'interruption volontaire de grossesse et à la contraception*, cons. 4.

[8] Décision n° 2004-499 DC du 29 juillet 2004, *Loi 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*, cons. 17 à 29.

constitutionnellement protégés[9]. Ce contrôle de proportionnalité est constamment exercé par le Conseil constitutionnel.

* En matière pénale, le Conseil constitutionnel doit en outre s'assurer du respect du principe de « rigueur nécessaire » qui résulte des articles 7 et 9 de la Déclaration de 1789[10].

Parmi les traitements de données à caractère personnel, les principaux sont des fichiers de police et de justice. Ils ont donné lieu à plusieurs décisions du Conseil constitutionnel. Ces fichiers de police judiciaire font l'objet d'un contrôle qui prend en compte la finalité de recherche des auteurs d'infraction. Le Conseil constitutionnel contrôle la conciliation, qui ne doit pas être manifestement déséquilibrée, entre, d'une part, la sauvegarde de l'ordre public et la recherche des auteurs d'infraction et, d'autre part, le respect de la vie privée. En outre le Conseil vérifie qu'est respecté le principe de « rigueur nécessaire » en matière de procédure pénale. Il en va ainsi pour les fichiers d'antécédents judiciaires (« STIC » et « JUDEX ») pour les fichiers d'analyse sérielle (« SALVAC », « ANACRIM ») et pour les logiciels de rapprochement judiciaire[11]. Ce contrôle a par exemple conduit le Conseil à exclure que les logiciels de rapprochement judiciaire permettent à tous les services de police judiciaire de mettre en commun leurs informations exploitées par ces logiciels. Ceci aurait conduit à des traitements de données à caractère personnel au champ manifestement excessif. En outre le Conseil a alors limité à trois ans la conservation des données[12].

De même, dans sa décision n° 2010-25 QPC du 16 septembre 2010, le Conseil constitutionnel a eu à connaître du fichier national automatisé des empreintes génétiques (FNAEG). En l'espèce, le Conseil a jugé que le législateur a assuré « *une conciliation qui n'est pas manifestement déséquilibrée* » entre le respect de la vie privée et la sauvegarde de l'ordre public[13]. Il a, à cette fin, énuméré les garanties résultant du code de procédure pénale lui-même (fichier placé sous le contrôle d'un magistrat, simple but d'identification et de recherche de certaines infractions, procédure d'effacement pour les personnes simplement soupçonnées), mais aussi de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

---

[9] Décision n° 2003-467 DC du 13 mars 2003, *Loi pour la sécurité intérieure*, cons. 17 à 46.
[10] *Ibid*, cons. 39.
[11] Décisions n[os] 2003-467 DC du 13 mars 2003 précitée, cons. 33 à 43 ; 2004-492 DC du 2 mars 2004, *Loi portant adaptation de la justice aux évolutions de la criminalité*, cons. 74 à 95 ; n° 2008-562 DC du 21 janvier 2008, *Loi relative à la rétention de sûreté et à la déclaration d'irresponsabilité pénale pour cause de trouble mental*, cons. 17 à 21 ; n° 2011-625 DC du 10 mars 2011 *Loi d'orientation et de programmation pour la performance de la sécurité intérieure*, cons. 9 à 13.
[12] Décision n° 2011-625 DC du 10 mars 2011, précitée, cons. 67 à 73.
[13] Décision n° 2010-25 QPC du 16 septembre 2010, *M. Jean-Victor C. (Fichier empreintes génétiques)*, cons. 16.

L'utilisation à des fins administratives de ces fichiers de police judiciaire n'est pas exclue mais est strictement encadrée. La décision n° 2010-25 QPC traduit une exigence de proportionnalité forte. En matière pénale, on doit en effet déduire de la décision, *a contrario*, que l'enregistrement des empreintes génétiques est constitutionnellement prohibé dans l'hypothèse où l'infraction considérée ne serait pas de celles dont une empreinte génétique pourrait permettre de rapporter la preuve.

De même, le Conseil constitutionnel avait contrôlé l'encadrement de l'utilisation à des fins administratives du fichier judiciaire automatisé des auteurs d'infractions sexuelles (FIJAIS)[14] et jugé :

« *32. Considérant qu'aucune norme constitutionnelle ne s'oppose par principe à l'utilisation à des fins administratives de données nominatives recueillies dans le cadre d'activités de police judiciaire ; que, toutefois, cette utilisation méconnaîtrait les exigences résultant des articles 2, 4, 9 et 16 de la Déclaration de 1789 si, par son caractère excessif, elle portait atteinte aux droits ou aux intérêts légitimes des personnes concernées* ».

En l'espèce, la consultation du FIJAIS avait pour unique objet de vérifier que le comportement des candidats à des emplois publics participant de la souveraineté de l'État n'est pas incompatible avec l'exercice des fonctions envisagées. Le Conseil avait jugé :

« *33. Considérant qu'eu égard aux motifs qu'elle fixe pour ces consultations, comme aux restrictions et précautions dont elle les assortit, la loi déférée ne méconnaît par elle-même aucune des exigences constitutionnelles ci-dessus mentionnées* ».

Dès que n'est plus en cause un fichier de police et de justice, le contrôle du Conseil se renforce. L'objectif de recherche des auteurs d'infraction n'est en effet plus invocable. Il en va ainsi lorsqu'est mis en place un fichier privé d'infractions pour lutter contre les atteintes à la propriété littéraire et artistique. Faute de garanties suffisantes, le Conseil a opéré une censure[15] :

« *11. Considérant que le 3° de l'article 9 de la loi du 6 janvier 1978, dans la rédaction que lui donne l'article 2 de la loi déférée, permettrait à une personne morale de droit privé, mandatée par plusieurs autres personnes morales estimant avoir été victimes ou être susceptibles d'être victimes d'agissements passibles de sanctions pénales, de rassembler un grand nombre d'informations nominatives portant sur des infractions, condamnations et mesures de sûreté ;*

[14] Décision n° 2003-467 DC du 13 mars 2003 précitée.
[15] Décision n° 2004-499 DC du 29 juillet 2004 précitée.

qu'en raison de l'ampleur que pourraient revêtir les traitements de données personnelles ainsi mis en œuvre et de la nature des informations traitées, le 3° du nouvel article 9 de la loi du 6 janvier 1978 pourrait affecter, par ses conséquences, le droit au respect de la vie privée et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; que la disposition critiquée doit dès lors comporter les garanties appropriées et spécifiques répondant aux exigences de l'article 34 de la Constitution ;

« *12. Considérant que, s'agissant de l'objet et des conditions du mandat en cause, la disposition critiquée n'apporte pas ces précisions ; qu'elle est ambiguë quant aux infractions auxquelles s'applique le terme de « fraude » ; qu'elle laisse indéterminée la question de savoir dans quelle mesure les données traitées pourraient être partagées ou cédées, ou encore si pourraient y figurer des personnes sur lesquelles pèse la simple crainte qu'elles soient capables de commettre une infraction ; qu'elle ne dit rien sur les limites susceptibles d'être assignées à la conservation des mentions relatives aux condamnations ; qu'au regard de l'article 34 de la Constitution, toutes ces précisions ne sauraient être apportées par les seules autorisations délivrées par la Commission nationale de l'informatique et des libertés ; qu'en l'espèce et eu égard à la matière concernée, le législateur ne pouvait pas non plus se contenter, ainsi que le prévoit la disposition critiquée éclairée par les débats parlementaires, de poser une règle de principe et d'en renvoyer intégralement les modalités d'application à des lois futures ; que, par suite, le 3° du nouvel article 9 de la loi du 6 janvier 1978 est entaché d'incompétence négative* ».

On retrouve cette exigence du Conseil constitutionnel pour le contrôle des fichiers relatifs aux étrangers. Le Conseil a ainsi censuré l'accès au fichier de l'OFPRA par les services de police et de gendarmerie[16] :

« *22. Considérant qu'il résulte du premier alinéa de l'article 8-3 que les empreintes digitales des étrangers, non ressortissants d'un État membre de l'Union européenne, qui sollicitent la délivrance d'un titre de séjour dans les conditions prévues à l'article 6 de l'ordonnance précitée, sont en situation irrégulière en France ou font l'objet d'une mesure d'éloignement du territoire français, peuvent être relevées, mémorisées et faire l'objet d'un traitement automatisé dans les conditions fixées par la loi du 6 janvier 1978 susvisée ; qu'en application du second alinéa de l'article 8-3, les données du fichier automatisé des empreintes digitales géré par le ministère de l'intérieur et celles du fichier informatisé des empreintes digitales des demandeurs du statut de réfugié peuvent être consultées par les agents expressément habilités des services du ministère de l'intérieur et de la gendarmerie nationale en vue de*

[16] Décision n° 97-389 DC du 22 avril 1997, *Loi portant diverses dispositions relatives à l'immigration*.

l'identification d'un étranger qui n'a pas justifié des pièces sous le couvert desquelles il est autorisé à circuler ou séjourner en France, n'a pas présenté les documents de voyage permettant l'exécution d'une mesure de refus d'entrée en France, d'un arrêté d'expulsion ou d'une mesure d'éloignement du territoire français, ou qui, à défaut desdits documents, n'a pas communiqué les renseignements permettant cette même exécution, ou qui, expulsé ou ayant fait l'objet d'une interdiction du territoire, aura pénétré de nouveau sans autorisation sur le territoire national (…)

« *25. Considérant en second lieu qu'aux termes du quatrième alinéa du Préambule de la Constitution du 27 octobre 1946 : " Tout homme persécuté en raison de son action en faveur de la liberté a droit d'asile sur les territoires de la République " ; qu'il incombe au législateur d'assurer en toutes circonstances l'ensemble des garanties légales que comporte cette exigence constitutionnelle ;*

« *26. Considérant que la confidentialité des éléments d'information détenus par l'office français de protection des réfugiés et des apatrides relatifs à la personne sollicitant en France la qualité de réfugié est une garantie essentielle du droit d'asile, principe de valeur constitutionnelle qui implique notamment que les demandeurs du statut de réfugié bénéficient d'une protection particulière ; qu'il en résulte que seuls les agents habilités à mettre en œuvre le droit d'asile, notamment par l'octroi du statut de réfugié, peuvent avoir accès à ces informations, en particulier aux empreintes digitales des demandeurs du statut de réfugié ; que dès lors la possibilité donnée à des agents des services du ministère de l'intérieur et de la gendarmerie nationale d'accéder aux données du fichier informatisé des empreintes digitales des demandeurs du statut de réfugié créé à l'office français de protection des réfugiés et apatrides prive d'une garantie légale l'exigence de valeur constitutionnelle posée par le Préambule de la Constitution de 1946 ;*

« *27. Considérant qu'il résulte de ce qui précède qu'au second alinéa de l'article 8-3 les mots " et du fichier informatisé des empreintes digitales des demandeurs du statut de réfugié " doivent être jugés contraires à la Constitution* ».

Deux autres décisions du Conseil soulignent la vigilance de celui-ci dans son contrôle :

* Dans sa décision n° 2003-484 DC du 20 novembre 2003[17], le Conseil constitutionnel s'est assuré de l'existence de garanties suffisantes pour valider une disposition permettant un traitement automatisé des demandes de validation des attestations d'accueil de personnes étrangères :

« *23. Considérant que la finalité des traitements automatisés de données nominatives que les maires peuvent instituer en leur qualité d'agents de l'État, en vertu de la disposition critiquée, est la lutte contre l'immigration irrégulière ; que cette finalité participe de la sauvegarde de l'ordre public qui est une exigence de valeur constitutionnelle ; que la loi renvoie à un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, le soin de fixer les garanties des personnes qui pourront faire l'objet du traitement automatisé, dans le respect de la loi du 6 janvier 1978 susvisée ; qu'eu égard aux motifs qu'elle fixe pour la consultation des données nominatives, comme aux restrictions et précautions dont elle assortit leur traitement, notamment en prévoyant la limitation de la durée de leur conservation, la loi déférée opère, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée* ».

* Dans sa décision n° 2007-556 DC du 16 août 2007[18], il s'est assuré que la collecte des données relatives aux déclarations individuelles de participation à un mouvement de grève ne saurait faire l'objet d'un usage détourné :

« *31. Considérant, en quatrième lieu, que, selon les termes de l'article 5, les informations issues des déclarations individuelles ne pourront être utilisées que pour "l'organisation du service durant la grève" ; qu'elles sont couvertes par le secret professionnel ; que leur utilisation à d'autres fins ou leur communication à toute personne autre que celles désignées par l'employeur comme étant chargées de l'organisation du service sera passible des peines prévues à l'article 226-13 du code pénal ; que, dans le silence de la loi déférée, les dispositions de la loi du 6 janvier 1978 susvisée s'appliquent de plein droit aux traitements de données à caractère personnel qui pourraient éventuellement être mis en œuvre ; qu'ainsi, l'obligation de déclaration individuelle s'accompagne de garanties propres à assurer, pour les salariés, le respect de leur droit à la vie privée* ».

Dans sa décision du 22 mars 2012, le Conseil constitutionnel a rappelé la jurisprudence précitée sur la compétence du législateur et la conciliation qu'il lui

[17] Décision n° 2003-484 DC du 20 novembre 2003, *Loi relative à la maîtrise de l'immigration, au séjour des étrangers en France et à la nationalité.*
[18] Décision n° 2007-556 DC du 16 août 2007, *Loi sur le dialogue social et la continuité du service public dans les transports terrestres réguliers de voyageurs.*

appartient d'opérer entre « *d'une part, la sauvegarde de l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la protection de principes et de droits de valeur constitutionnelle et, d'autre part, le respect des autres droits et libertés constitutionnellement protégés* » (cons. 7).

Le Conseil a toutefois précisé, dans un considérant de principe, la nature du contrôle exercé en matière de traitement de données à caractère personnel. Il a jugé que le droit au respect de la vie privée, qui résulte de l'article 2 de la Déclaration de 1789, impliquait que « *la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel (soient) justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif* » (cons. 8).

B – La contrariété à la Constitution des dispositions des articles 5 et 10

Avec les articles 5 et 10, la loi déférée n'avait plus seulement pour objet la lutte (aussi bien préventive que répressive) contre l'usurpation d'identité. Elle mettait un fichier à la disposition des forces de l'ordre pour leur mission générale et pour certaines missions de flagrance, d'enquête et de commission rogatoire. La question était, pour le Conseil constitutionnel, de savoir si de telles orientations étaient proportionnées ou si elles portaient une atteinte excessive au respect de la vie privée.

Le Conseil constitutionnel a répondu à cette question en prenant en compte quatre arguments :

– En premier lieu, la taille du fichier envisagé était sans précédent. Il devait réunir des données concernant 45 à 60 millions de personnes (pour 6,5 millions de personnes dans le fichier TES utilisé pour les passeports). La création d'une base centralisée de données biométriques d'une telle ampleur comportait des risques importants et impliquait des sécurités techniques complexes et supplémentaires. En effet, un fichier est d'autant plus vulnérable, convoité et susceptible d'utilisations multiples qu'il est de grande dimension, qu'il est relié à des milliers de points d'accès et de consultation, et qu'il contient des informations très sensibles comme des données biométriques.

– En deuxième lieu, les données biométriques enregistrées dans le fichier présentent un caractère particulièrement sensible. C'est ce que soulignait la note d'observations du 25 octobre 2011 de la CNIL : « *La Commission rappelle que les données biométriques ne sont pas des données à caractère personnel "comme les autres". Elles présentent en effet la particularité de permettre à tout moment l'identification de la personne concernée sur la base d'une réalité biologique qui lui est propre, permanente dans le temps et dont elle ne peut*

s'affranchir. À la différence de toute autre donnée à caractère personnel, la donnée biométrique n'est donc pas attribuée par un tiers ou choisie par la personne : elle est produite par le corps lui-même et le désigne ou le représente, lui et nul autre, de façon immuable. Elle appartient donc à la personne qui l'a générée et tout détournement ou mauvais usage de cette donnée fait alors peser un risque majeur sur l'identité de celle-ci. »

Le Conseil a quant à lui reconnu la particulière sensibilité de ces données « *susceptibles d'être rapprochées de traces physiques laissées involontairement par la personne ou collectées à son insu* » (cons. 10).

– En troisième lieu, les caractéristiques techniques du fichier rendaient possible l'identification d'une personne à partir des empreintes digitales. C'est la conséquence du choix du « lien fort ».

La constitution d'un tel fichier pour atteindre l'objectif fixé par la loi de lutte contre l'usurpation d'identité ne s'imposait pas :

Des techniques sans fichier permettent d'atteindre cet objectif, avec des cartes à puce biométrique. S'il est fait le choix de constituer un fichier, des techniques, notamment celle du « lien faible », permettent d'écarter les risques d'autres utilisations. C'est ce qui avait conduit la CNIL à indiquer que « *la comparaison entre la donnée biométrique enregistrée dans le composant et l'empreinte lue en direct sur un lecteur pourrait se faire dans la carte elle-même. La mise en œuvre de cette technique, dite "*match on card*", serait susceptible d'apporter une garantie supplémentaire à la protection des données à caractère personnel, en évitant toute possibilité de copie externe (…).*

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

La CNIL en avait conclu : « *Dans ces conditions, la Commission estime, tout comme dans le cadre de son avis sur le projet de loi présenté en 2008 par le ministère de l'intérieur, que la proportionnalité de la conservation sous forme centralisée de données biométriques, au regard de l'objectif légitime de lutte contre la fraude documentaire, n'est pas à ce jour démontrée (…).*

« *D'autres mesures permettraient également de limiter les possibilités d'utilisation de la base de données biométriques à la seule fin de lutte contre la*

fraude à l'identité. Ainsi de l'absence de lien univoque entre les données biométriques enregistrées dans le traitement central et les données d'état civil des personnes auxquelles ces données correspondent, ou de l'interdiction expresse de procéder à des recherches en identification sur la base des éléments biométriques enregistrées dans la base. »

Le Conseil d'État n'a jugé le fichier TES des passeports biométriques conforme à la CEDH que parce qu'il présentait certaines de ces garanties techniques, notamment des bases de données différentes pour les données biométriques et les données d'identité, ce qui rendait possible l'interrogation du fichier pour les seuls demande et renouvellement de titre.

– En quatrième lieu, le fichier tendait à une pluralité de « finalités » : ce fichier aurait pu être utilisé à des fins d'identification et non uniquement d'authentification.

Initialement, le rapporteur à l'Assemblée nationale, M. Philippe Goujon, soulignait *« tout particulièrement que le fichier central dont traite cette proposition de loi ne constitue pas un fichier de police mais un fichier administratif* »[19]. Dès lors des garanties moindres étaient suffisantes. Or, avec les amendements successifs, le fichier est aussi devenu aussi un fichier de police.

L'article 5 permettait l'utilisation du fichier pour des infractions autres que celles relatives aux délits d'usurpation d'identité. Comme le relevait M. François Pillet, rapporteur au Sénat :

« *Plusieurs des infractions visées ne présentent pas de lien direct avec ce délit, ou sont bien plus générales que ce seul délit, ce qui autoriserait les forces de police à faire usage du fichier alors qu'aucune usurpation d'identité n'est en cause.*

« *Il en est ainsi du délit de révélation de l'identité d'agent des services spécialisés de renseignement : l'identité de l'auteur de l'infraction n'est pas en cause. De la même manière, on peut légitimement se demander ce que le faux en écriture publique qui ne porte pas sur l'identité d'une personne a à voir avec l'usurpation d'identité ou ce que l'escroquerie a à voir avec l'usurpation d'identité, lorsque le délinquant ne se présente pas sous une fausse identité, mais qu'il agit, sous sa véritable identité, par des manœuvres frauduleuses.* »[20]

[19] Rapport sur la proposition de loi adoptée par le Sénat, relative à la protection de l'identité , Assemblée nationale, XIII[e] législature, 29 juin 2011, n° 3599, p. 10.
[20] Rapport sur la proposition de loi adoptée par l'Assemblée nationale en nouvelle lecture, relative à la protection de l'identité, session ordinaire 2011-2012, Sénat, 8 février 2012, n° 339, p. 11-12.

L'utilisation du fichier dans le cadre de l'article 10 était également problématique. Actuellement les services en charge de la lutte contre le terrorisme ne peuvent pas utiliser les empreintes digitales ou les images numérisées des détenteurs de titre contenues dans les fichiers pour identifier un individu à partir de ces seuls éléments. L'article 19 du décret du 30 décembre 2005 l'exclut pour les passeports biométriques avec le fichier TES. Pour le fichier de gestion des cartes nationales d'identité, les empreintes digitales n'y figurent pas[21].

Ces fins d'identification ne pouvaient d'ailleurs qu'être vouées à se développer. Comme l'indiquait M. François Pillet, rapporteur au Sénat, « *une fois créé, le fichier central est susceptible de constituer, s'il n'est pas entouré des garanties requises, une bombe à retardement pour les libertés publiques* »[22].

Dans sa décision du 22 mars 2012, le Conseil a reconnu que « *la création d'un traitement de données à caractère personnel destiné à préserver l'intégrité des données nécessaires à la délivrance des titres d'identité et de voyage permet de sécuriser la délivrance de ces titres et d'améliorer l'efficacité de la lutte contre la fraude* » est « *justifiée par un motif d'intérêt général* » (cons. 9). Il a toutefois estimé que, compte tenu des quatre caractéristiques du dispositif décrites ci-dessus (ampleur du fichier, sensibilité des données, caractéristiques techniques permettant l'identification à partir des données biométriques et finalités de police administrative ou judiciaire autres que celles nécessaires à la délivrance ou au renouvellement des titres d'identité et de voyage et à la vérification de l'identité du possesseur d'un tel titre) l'instauration d'un tel traitement de données à caractère personnel portait une atteinte au respect de la vie privée qui ne pouvait être regardée comme proportionnée au but poursuivi.

Le Conseil a donc déclaré contraires à la Constitution les articles 5 et 10 de la loi ainsi que les dispositions qui n'en étaient pas séparables (en particulier, parce qu'elles faisaient référence à l'article 5, le troisième alinéa de l'article 6, l'article 7 et la seconde phrase de l'article 8).

Par cette décision, le Conseil constitutionnel ne s'est pas prononcé pour ou contre la biométrie. Il ne s'est pas davantage prononcé pour ou contre un fichier réunissant des données biométriques. Il a estimé que les garanties entourant la mise en œuvre d'un tel fichier, compte tenu de l'ensemble de ses caractéristiques, n'étaient pas suffisantes. Ce faisant, il n'a pas entendu substituer son appréciation à celle du législateur sur les choix susceptibles de

[21] Décret n° 55-1397 du 22 octobre 1955 instituant la carte nationale d'identité.
[22] Rapport sur la proposition de loi, modifiée par l'Assemblée nationale, relative à la protection de l'identité, Sénat, session ordinaire 2011-2012, 19 octobre 2011, n° 39, p. 11.

permettre la création d'un fichier des identités contenant des données biométriques (choix de données biométriques non traçantes ; techniques interdisant l'indentification à partir des données biométriques ; garanties légales assurant que le traitement ne peut être utilisé à d'autres fins que celles nécessaires à la délivrance, au renouvellement ou à la vérification des titres d'identité…).

III. – Les fonctionnalités d'identification sur internet et de la signature électronique

Adopté conforme dès la première lecture, l'article 3 disposait : « *Si son titulaire le souhaite, la carte nationale d'identité contient en outre des données, conservées séparément, lui permettant de s'identifier sur les réseaux de communications électroniques et de mettre en œuvre sa signature électronique. L'intéressé décide, à chaque utilisation, des données d'identification transmises par voie électronique.*

« *Le fait de ne pas disposer de la fonctionnalité décrite au premier alinéa ne constitue pas un motif légitime de refus de vente ou de prestation de services au sens de l'article L. 122-1 du code de la consommation ni de refus d'accès aux opérations de banque mentionnées à l'article L. 311-1 du code monétaire et financier.*

« *L'accès aux services d'administration électronique mis en place par l'État, les collectivités territoriales ou leurs groupements ne peut être limité aux seuls titulaires d'une carte nationale d'identité présentant la fonctionnalité décrite au premier alinéa*. »

Cet article permettait que la CNI soit dotée d'un second composant électronique destiné à des usages en ligne (puce « eService »). Cet article introduisait dans notre droit, pour la première fois, la possibilité qu'un titre d'identité serve à la fois d'outil d'identification et d'instrument de transaction commerciale.

Cet article créait une identification sur les réseaux de communication au public en ligne tant dans les relations privées qu'à l'égard de l'administration. Cette identification « officielle » sur internet avait été critiquée par la CNIL dans la mesure où elle présentait le risque de conduire à ce que les bases de données commerciales, enrichies à mesure de l'utilisation d'internet dans la vie civile, puissent se référer à un « identifiant unique » et authentifié permettant de cerner avec certitude les modes de vie, les habitudes de consommation, les pratiques de loisirs… La crainte était, à terme, la perte par les utilisateurs d'internet de la capacité à préserver leur anonymat par l'usage d'alias.

C’est en réponse aux interrogations de la CNIL que l’article 3 prévoyait que la puce électronique « eService » était facultative, affirmait que le fait de ne pas en disposer ne peut constituer un motif de refus de vente et disposait que « *l’intéressé décide, à chaque utilisation, des données d’identification transmises par voie électronique* ».

La création d’une identification à distance au moyen de la carte d’identité soulevait toutefois des interrogations juridiques.

En premier lieu, l’article était étonnamment silencieux sur les « données » au moyen desquelles l’authentification aurait pu s’effectuer et au régime de ces données enregistrées sur la CNI à la demande du titulaire (en particulier la garantie d’intégrité et de confidentialité).

En deuxième lieu, l’article 3 entendait procéder à une transposition sur les réseaux en ligne, des utilisations courantes de la CNI pour s’authentifier. Présenter sa carte d’identité à la caisse d’un grand magasin au moment de payer par chèque (article L. 131-15 du code monétaire et financier) ou aux contrôles de la sûreté aéroportuaire a pour effet de permettre de s’authentifier au moyen de l’image du visage reproduite sur le titre. La transposition d’une telle logique d’authentification sur les réseaux pose inévitablement la question des modalités selon lesquelles s’opère cette authentification.

Comment pouvait être garanti le fait que celui qui, devant son ordinateur, déclare s’identifier au moyen de la carte d’identité est effectivement le porteur de la carte ? Des dispositifs techniques peuvent apporter cette garantie. Ils supposent un lecteur de puce sur chaque ordinateur relié à un référent biométrique garantissant que la personne qui met en œuvre le dispositif est le porteur de la carte d’identité correspondant. Les travaux parlementaires de la loi déférée paraissaient exclure une telle orientation et laisser place à un dispositif de certificat installé sur la puce et accompagné d’un mot de passe.

Une telle faculté présentait le risque, en pratique, du prêt d’identité consistant à remettre à un tiers la carte et le code sans que l’interlocuteur sur les réseaux ou le contractant n’en soit aucunement informé. Indépendamment de toute question de fraude, de tels prêts pourraient être réalisés pour des raisons de commodité entre des personnes qui se font confiance (personnes âgées ou malades à l’égard des personnes qui les aident, conjoints) à l’instar de ce qui se pratique pour la carte bancaire. Toutefois, un prêt de carte bancaire s’analyse comme un mandat donné (certes en violation des liens contractuels qui lient le titulaire du compte à la banque). Il n’en va pas de même avec la remise de la carte d’identité.

La question se posait de façon plus cruciale à l'égard des personnes qui ne jouissent pas de l'exercice de leurs droits (mineurs et majeurs protégés), pour lesquels la loi ne prévoyait aucun encadrement.

Sur ces questions, la loi était totalement silencieuse. Le législateur s'était abstenu d'en dire plus pour deux raisons. D'une part, il présupposait que la question ne pose pas plus de difficultés que les autres modes de signature électronique utilisés avec les moyens de paiement. D'autre part, il laissait la plus grande marge de liberté pour la définition des modalités techniques du dispositif.

Le Conseil constitutionnel a jugé qu'un tel laconisme relevait de l'incompétence négative : la création d'une identification officielle sur internet et de la signature électronique au moyen de l'identité garantie par l'État qui délivre la carte d'identité appelle un minimum d'encadrement législatif au regard tant des règles concernant le droits civiques, l'exercice des libertés publiques et l'état et la capacité des personnes que des principes fondamentaux des obligations civiles et commerciales.

Le Conseil a d'abord jugé « *qu'en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services dans la vie économique et sociale, les conditions générales dans lesquelles la carte national d'identité délivrée par l'État peut permettre à une personne de s'identifier sur les réseaux de communication électronique et de mettre en œuvre sa signature électronique, notamment à des fins civiles et commerciales, affectent directement les règles et les principes précités et, par suite, relèvent du domaine de la loi* » (cons. 13). Cette motivation s'inspire des termes de sa décision n° 2010-45 QPC du 6 octobre 2010 relative aux noms de domaine sur internet : « *en l'état actuel des moyens de communication et eu égard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services dans la vie économique et sociale, notamment pour ceux qui exercent leur activité en ligne, l'encadrement, tant pour les particuliers que pour les entreprises, du choix et de l'usage des noms de domaine sur internet affecte les droits de la propriété intellectuelle, la liberté de communication et la liberté d'entreprendre* »[23].

Ce faisant, le Conseil constitutionnel a confirmé refuser que le législateur abandonne sa compétence à la norme réglementaire ou technique en raison des difficultés liées à l'innovation et à la complexité technique du développement d'internet. Il appartient au législateur d'exercer pleinement sa compétence, y compris quant aux usages d'internet.

[23] Décision n° 2010-45 QPC du 6 octobre 2010, *M. Mathieu P. (Noms de domaine Internet)*, cons. 5.

Dans sa décision du 22 mars 2012, le Conseil constitutionnel a jugé que « *l'article 3 se borne, d'une part, à permettre que la carte nationale d'identité comprenne des "fonctions électroniques" permettant à son titulaire de s'identifier sur les réseaux de communication électroniques et de mettre en œuvre sa signature électronique et, d'autre part, à garantir le caractère facultatif de ces fonctions ; que les dispositions de l'article 3 ne précisent ni la nature des "données" au moyen desquelles ces fonctions peuvent être mises en œuvre ni les garanties assurant l'intégrité et la confidentialité de ces données ; qu'elles ne définissent pas davantage les conditions dans lesquelles s'opère l'authentification des personnes mettant en œuvre des fonctions, notamment lorsqu'elles sont mineures ou bénéficiant d'une mesure de protection juridique ; que, par suite, le législateur a méconnu l'étendue de sa compétence* » (cons. 14).

Par suite, le Conseil constitutionnel a également déclaré contraire à la Constitution l'article 3 de la loi relative à la protection de l'identité.