N° 432

SÉNAT

SESSION ORDINAIRE DE 2010-2011

Enregistré à la Présidence du Sénat le 13 avril 2011

RAPPORT

FAIT

au nom de la commission des lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) sur la proposition de loi de MM. Jean-René LECERF et Michel HOUEL **relative** *à la* **protection** *de l'***identité***,*

Par M. François PILLET,

Sénateur

(1) Cette commission est composée de : M. Jean-Jacques Hyest*, président ;* M. Nicolas Alfonsi, Mme Nicole Borvo Cohen-Seat, MM. Patrice Gélard, Jean-René Lecerf, Jean-Claude Peyronnet, Jean-Pierre Sueur, Mme Catherine Troendle, M. Yves Détraigne*, vice-présidents ;* MM. Laurent Béteille, Christian Cointat, Charles Gautier, Jacques Mahéas*, secrétaires ;* MM. Jean-Paul Amoudry, Alain Anziani, Mmes Éliane Assassi, Nicole Bonnefoy, Alima Boumediene-Thiery, MM. François-Noël Buffet, Gérard Collomb, Pierre-Yves Collombat, Jean-Patrick Courtois, Mme Anne-Marie Escoffier, MM. Louis-Constant Fleming, Gaston Flosse, Christophe-André Frassa, Bernard Frimat, René Garrec, Jean-Claude Gaudin, Mme Jacqueline Gourault, Mlle Sophie Joissains, Mme Virginie Klès, MM. Antoine Lefèvre, Dominique de Legge, Mme Josiane Mathon-Poinat, MM. Jacques Mézard, Jean-Pierre Michel, François Pillet, Hugues Portelli, André Reichardt, Bernard Saugey, Simon Sutour, Richard Tuheiava, Alex Türk, Jean-Pierre Vial, Jean-Paul Virapoullé, Richard Yung, François Zocchetto.

Voir le(s) numéro(s) :

Sénat : **682** (2009-2010) et **433** (2010-2011)

SOMMAIRE

Pages

LES CONCLUSIONS DE LA COMMISSION DES LOIS

La commission des lois, réunie le mercredi 13 avril 2011, sous la présidence de **M. Jean-Jacques Hyest**, président, a examiné le rapport de M. François Pillet et établi son texte sur la proposition de loi n° 682 (2009-2010) relative à la protection de l'identité, présentée par MM. Jean-René Lecerf et Michel Houel.

Le rapporteur a observé que, même si le phénomène de la fraude à l'identité et en particulier celui de l'usurpation d'identité a pu être surévalué, la réalité et la gravité de cette délinquance ne peuvent être niées, ce qui impose de renforcer les moyens de lutte existants.

Appuyant son analyse sur les travaux précédents de la commission des lois et, en particulier, ceux de la mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire, il a constaté que toutes les solutions aux défaillances de la chaîne de l'identité présentées en 2005 n'avaient pas été exploitées et que la proposition de loi offrait l'occasion de les mettre en œuvre.

La création de titres d'identité biométriques et d'un fichier central biométrique de gestion de ces titres apparaissant comme le moyen de lutte le plus efficace contre la fraude à l'identité, le rapporteur a proposé à la commission d'adopter le dispositif prévu par la proposition de loi en y apportant toutefois les garanties nécessaires à la protection de la liberté individuelle et le respect de la vie privée.

À son initiative, la commission des lois a adopté plusieurs amendements tendant à :

- limiter l'usage du fichier biométrique à la seule lutte contre la fraude à l'identité, en doublant les garanties juridiques de garanties matérielles, afin d'en interdire l'utilisation dans le cadre de recherches criminelles (article 5) ;

- prévoir que les vérifications d'identité par les empreintes digitales ne puissent être effectuées que par des agents habilités et à partir des données enregistrées sur la puce électronique du titre d'identité (article 5 *bis*) ;

- renforcer les autres instruments de lutte contre la fraude documentaire en créant un fichier portant sur la validité des titres, sur le modèle de celui existant pour les chèques irréguliers (article 5 *ter*) ;

- donner au titulaire de la carte d'identité la pleine maîtrise de la fonctionnalité d'identification électronique, en lui permettant de décider quelles informations il communique, et interdire que ceux qui refusent cette fonctionnalité soient évincés de certains services ou transactions en ligne (article 3).

La commission des lois a adopté la proposition de loi **ainsi rédigée**.

Mesdames, Messieurs,

Votre commission est saisie de la proposition de loi relative à la protection de l'identité, présentée par nos collègues MM. Jean-René Lecerf et Michel Houel[1]. Le but assigné à cette proposition de loi est de mettre en place les instruments susceptibles de renforcer la lutte contre la fraude à l'identité.

La commission des lois a déjà eu à connaître des questions qu'abordent la proposition de loi à travers les travaux conduits par la mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire[2]. Cette mission, présidé par notre collègue Charles Guéné, et dont l'auteur de la proposition de loi, M. Jean-René Lecerf, était le rapporteur, a à la fois dressé le constat de défaillances dans la chaîne de l'identité, proposé des solutions pour y remédier et, explorant les nouvelles perspectives de sécurisation de l'identité qu'offraient les technologies de reconnaissance biométriques, examiné à quelles conditions de tels dispositifs pourraient être utilisés afin de mieux protéger l'identité de tous, dans le respect de la liberté individuelle et de la vie privée de chacun.

Si le gouvernement a conduit, parallèlement, sa propre réflexion sur le sujet, et si plusieurs avant-projets ont esquissé le dispositif qui pourrait être retenu, aucun projet de loi n'a finalement été déposé devant le Parlement.

Pour autant, des choix importants ont été effectués, sur une base réglementaire, notamment lorsque le passeport biométrique a été mis en place, conformément aux engagements européens de la France. Cette question a été soumise à la vigilance du Sénat par les travaux budgétaires que nos collègues Mme Michèle André[3] et de M. Alain Anziani[4] ont consacré à la mise en œuvre concrète, à travers l'action de l'agence nationale des titres sécurisés (ANTS) et des communes, du système de passeport biométrique.

---

[1] *Proposition de loi n° 682 (2009-2010) relative à la protection de l'identité, présentée par MM. Jean-René Lecerf et Michel Houel,*

[2] *Rapport d'information de la mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire (n° 439, 2004-2005), fait au nom de la commission des lois du Sénat, p. 17 (http://www.senat.fr/rap/r04-439/r04-439.html).*

[3] *«* La nouvelle génération de titres d'identité : bilan et perspectives *», rapport d'information n° 486 (2008-2009) de Mme Michèle André, fait au nom de la commission des finances (http://www.senat.fr/notice-rapport/2008/r08-486-notice.html) et «* Le véritable prix du passeport biométrique *», rapport d'information n° 596 (2009-2010) de Mme Michèle André, fait au nom de la commission des finances (http://www.senat.fr/notice-rapport/2009/r09-596-notice.html)*

[4] *«* Projet de loi de finances pour 2011 : Administration générale et territoriale de l'État *», avis n° 116 (2010-2011) de M. Alain ANZIANI, fait au nom de la commission des lois (http://www.senat.fr/rap/a10-116-1/a10-116-1.html).*

Votre rapporteur a souhaité inscrire ces travaux dans le prolongement des conclusions formulées par la mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire. Les auditions qu'il a conduites lui ont permis de recueillir à la fois le point de vue de l'administration, de représentants de la société civile, d'historiens, de représentants des industries œuvrant dans le domaine de la sécurisation de l'identité, des juristes ainsi que celui de la commission nationale de l'informatique et des libertés.

La proposition de loi constitue la première occasion pour le Parlement de se prononcer sur les moyens d'assurer la sécurité de l'identité, dans une juste conciliation entre les impératifs de préservation de l'ordre public et les exigences de protection des libertés individuelles.

I. LA FRAUDE À L'IDENTITÉ

A. UNE DÉLINQUANCE AVÉRÉE QUOIQUE D'UNE AMPLEUR LIMITÉE, QUI PEUT TOUTEFOIS PRÉSENTER DE GRAVES CONSÉQUENCES POUR SES VICTIMES

1. Un phénomène polymorphe

La mission d'information de votre commission, sur la nouvelle génération de documents d'identité et la fraude documentaire avait déjà souligné le caractère protéiforme de la fraude à l'identité[1]. Celle-ci recouvre à la fois l'identité fictive, l'usurpation d'identité, l'échange d'identité entre deux complices, l'utilisation de l'identité d'une personne décédée.

Généralement[2], la fraude est appuyée sur la production d'un document destiné à attester de l'identité alléguée. Ce document peut résulter :

- du vol d'un document authentique vierge, personnalisé par la suite ;

- d'une falsification qui consiste en la modification d'un ou plusieurs éléments d'un document authentique ;

- d'une contrefaçon, qui consiste en la reproduction totale d'un document authentique ;

- de l'obtention frauduleuse d'un document authentique. Le fraudeur parvient à faire établir par l'administration un document authentique à partir de l'identité qu'il allègue, en lui fournissant de fausses pièces d'état civil. Le fraudeur possède alors un « *vrai faux document d'identité* » ;

---

[1] Rapport d'information de la mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire (n° 439, 2004-2005), fait au nom de la commission des lois du Sénat, p. 17

[2] La fraude peut aussi résulter d'une simple fausse déclaration, comme lorsque le délinquant interpellé se présente aux forces de police sous une fausse identité ou une identité fictive.

- de l'usage frauduleux du document d'un tiers, emprunté ou volé à ce dernier.

La fraude à l'identité ne se réduit pas à celle sur le passeport ou la carte nationale d'identité : l'identité se prouvant par tout moyen, elle peut aussi résulter d'autres documents officiels (permis de conduire, permis de chasser, carte d'invalidité, carte du combattant…)

La fraude à l'identité présente une particularité. Elle sert souvent de support à une autre infraction : escroquerie bancaire, fraude aux prestations sociales, délinquance routière, entrée ou séjour illégal sur le sol français, crime organisé ou terrorisme… L'identité usurpée permet alors au fraudeur de tromper ses victimes ou d'échapper aux poursuites de la police.

Enfin, il convient de souligner la dimension internationale de la fraude à l'identité commise en France : elle concerne aussi bien les titres français que les titres ou les actes d'état civil étrangers.

2. Une répression pénale partielle, récemment étendue

Jusqu'à l'adoption de loi n° 2011-267 d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011, il n'existait pas d'infraction propre à l'usurpation d'identité. La fraude à l'identité était réprimée à travers plusieurs types d'infractions différentes, soit à titre autonome, soit comme un élément constitutif de ces infractions[1].

Ainsi l'article 434-23 du code pénal punit de cinq ans d'emprisonnement et de 75 000 euros d'amende le fait de prendre le nom d'un tiers dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales. La fausse déclaration relative à l'état civil d'une personne, lorsque celle-ci a eu ou aurait pu avoir le même effet contre un tiers, est également punie des mêmes peines. Ces peines se cumulent, le cas échéant, avec celles encourues au titre de l'infraction à l'occasion de laquelle l'usurpation d'identité a été commise.

L'article L. 225-7 du code de la route punit des mêmes peines le fait de prendre le nom d'une personne dans des circonstances qui ont déterminé ou auraient pu déterminer l'enregistrement à son encontre d'une condamnation judiciaire ou d'une décision administrative.

L'article 781 du code de procédure pénale punit de 7 500 euros d'amende le fait de fournir des renseignements d'identité imaginaires qui ont provoqué ou auraient pu provoquer des mentions erronées au casier judiciaire.

La fraude documentaire est elle-même plus particulièrement visée par l'article 433-19 du code pénal qui punit d'une peine de six mois d'emprisonnement et de 7 500 euros d'amende le fait, dans un acte public ou

---

[1] *Tel est le cas pour l'escroquerie, l'usage d'un faux nom étant un élément constitutif de cette infraction (article 31-1 du code pénal).*

dans un document administratif destiné à l'autorité publique, de prendre un nom ou un accessoire du nom autre que celui assigné par l'état civil et de changer, altérer ou modifier ceux-ci.

Tel est aussi le cas des articles 441-2, 441-3, 441-5 et 441-6 du même code qui punissent de peines d'emprisonnement allant de deux à sept ans et des amendes correspondantes, respectivement, la fabrication et l'usage, la détention, la fourniture et l'obtention indue d'un faux document administratif constatant un droit, une identité ou une qualité ou accordant une autorisation.

Enfin, l'article L. 2242-5 du code des transports, qui reprend les dispositions de la loi du 15 juillet 1845 relative à la police des chemins de fer punit d'une amende de 3 750 euros la fourniture d'une fausse identité ou d'une fausse adresse à un agent assermenté pour constater les infractions à la police et à l'exploitation des chemins de fer.

Cette répression pénale est aujourd'hui complétée par l'article 226-4-1 du code pénal qui punit d'un an d'emprisonnement et de 15 000 euros d'amende le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, que ces faits soient commis ou non sur un réseau de communication au public en ligne.

3. Une délinquance d'ampleur limitée mais avérée

a) Un chiffre de 210 000 usurpations d'identités par an qui appelle les plus grandes réserves

Le centre de recherche pour l'étude et l'observation des conditions de vie (CREDOC) a publié, au mois de juin 2009 une étude sur l'usurpation d'identité. Cette étude, commandée par la société *Fellowes*, qui produit des équipements bureautiques et notamment des « *destructeurs de documents* », a conclu qu'il y avait chaque année plus de 210 000 cas d'usurpation d'identité en France, soit un chiffre supérieur à celui des cambriolages du domicile principal (164 000), des vols automobiles (127 000) ou des falsifications et usages frauduleux de chèques ou de carte de paiement (120 000).

Ce chiffre, particulièrement inquiétant, a été largement repris par les médias ainsi que dans les débats sur le sujet. L'exposé des motifs de la présente proposition de loi s'ouvre d'ailleurs sur la mention de ce nombre très élevé d'usurpation d'identités.

Cette évaluation appelle toutefois d'importantes réserves. Plusieurs des personnes entendues par votre rapporteur ont en effet contesté la méthodologie suivie par le CREDOC en la matière.

Cette évaluation repose sur une enquête, réalisée auprès de 1 000 puis 2 000 personnes de plus de quinze ans, sélectionnées selon la méthode des quotas et auxquelles a été posée la question suivante : « *depuis 1999 avez-vous été victime d'une usurpation d'identité, c'est-à-dire l'usage à des fins*

malhonnêtes de données personnelles afin de contracter un emprunt, de prendre une carte de crédit ou de réaliser toute action interdite par la loi avec votre identité ».

Le nombre de réponses positives a ensuite été rapporté à la population française, puis divisé par le nombre d'années écoulées depuis 1999, pour obtenir le chiffre de 210 000 usurpations d'identité par an.

M. Cyril Rizk, responsable des statistiques à l'observatoire national de la délinquance et des réponses pénales (ONDRP), ainsi que M. Pierre Piazza, maître de conférences en science politique à l'université de Cergy-Pontoise, ont émis plusieurs réserves sur cette enquête et le résultat auquel elle conclut :

- la question posée repose sur une définition très large de l'usurpation d'identité, puisqu'elle porte sur « *usage de données personnelles* » et non pas exclusivement sur son identité civile. Elle est ainsi susceptible d'inclure l'usage frauduleux de titres de paiement, qu'il s'agisse de cartes bancaires (61 000 faits de ce type constatés par les services de police et de gendarmerie en 2009[1]) ou de chèques volés (50 000 en 2009[2]), qui ne correspondent pas directement à une usurpation d'identité. De la même manière, l'utilisation frauduleuse de codes d'accès personnels à des services électroniques n'est pas assimilable à une usurpation d'identité civile ;

- interroger les enquêtés sur une période de dix ans crée un biais, puisque, si les intéressés conservent en mémoire l'évènement décrit, ils ne savent pas nécessairement s'il remonte à moins de dix ans ou un peu plus. Les enquêtes de victimation de l'ONDRP portent ainsi sur une période de trois années seulement ;

- l'enquête repose non pas sur des faits constatés, objectifs, mais seulement sur des déclarations qui laissent nécessairement place à la subjectivité. Ce premier biais est aggravé lorsque le chiffre de 210 000 usurpations d'identité est rapporté aux chiffres des cambriolages ou des vols automobiles constatés par les services de police et de gendarmerie, qui correspondent, eux, à des infractions ayant donné lieu au dépôt d'une plaine ou fait l'objet d'un signalement.

Interrogés par votre rapporteur sur la fiabilité du chiffre résultant de l'étude du CREDOC, les services du ministère de l'intérieur et de la Chancellerie ont indiqué qu'il semblait manifestement surévalué par rapport aux chiffres dont eux-mêmes disposaient.

En dépit de la fortune médiatique qu'il a connue, et compte tenu des doutes sérieux que peut inspirer le chiffre de 210 000 cas d'usurpation d'identité par an en France, votre rapporteur considère qu'il ne devrait pas être repris, sans réserves, dans le débat sur la nécessité de lutter contre les fraudes à l'identité.

---

[1] *La criminalité en France, Rapport de l'observatoire national de la délinquance et des réponses pénales 2010, ONDRP-INHESJ, novembre 2010, p. 435.*

[2] Loc. cit.

b) L'évaluation de la fraude à l'identité par l'Observatoire national de la délinquance et de la réponse pénale

La mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire, avait considéré qu'il serait utile de confier à l'observatoire national de la délinquance la mission d'élaborer un outil performant de mesure de la fraude à l'identité.

Sans disposer encore des outils statistiques nécessaires pour mener à bien cette mission, l'ONDRP s'est attaché, depuis son rapport annuel pour 2007, à présenter les principales mesures disponibles en la matière, en se basant à la fois sur l'état 4001 recensant les infractions constatées par les services de police et de gendarmerie, ainsi que sur les données fournies par la direction centrale de la police aux frontières et par le bureau de la nationalité des titres d'identité et de voyage de la direction des libertés publiques et des affaires juridiques du ministère de l'intérieur.

Les principaux éléments de connaissance de la fraude aux documents et à l'identité en 2009, fournis par l'ONDRP

« *En 2009, près de 13 900 faits constatés de fraudes documentaires et à l'identité ont été enregistrés par les services de police et les unités de gendarmerie.*

Tandis que les faits constatés sont en baisse sur la période récente, le nombre de personnes mises en cause a crû de 3 % entre 2008 et 2009 : 8 508 personnes ont été mises en cause en 2009 contre 8 260 en 2008.

La baisse du nombre des faits constatés de l'index « faux documents d'identité *» explique en grande partie la diminution du nombre total des faits constatés de fraudes documentaires et/ou identitaires.*

En 2009, les services de la police aux frontières ont réalisé sur les points de passage autorisés près de 6 300 interceptions de documents frauduleux (toutes nationalités confondues). Ces documents recouvrent plusieurs natures de fraude : les plus fréquentes sont la contrefaçon et la falsification (deux tiers de la fraude).

Sur l'ensemble du territoire français, 4 011 documents frauduleux français ont été saisis par la police aux frontières (PAF) en 2009. Parmi ces faux documents, on dénombre 1 640 certificats d'acte de naissance, 1 070 cartes d'identité, 1 035 passeports et 266 permis de conduire.

De 2004 à 2009, le nombre de signalements de personnes utilisant au moins deux identités a crû de 129,9 %[1]. »

Source : rapport 2010 de l'observatoire national de la délinquance et des réponses pénales, novembre 2010, p. 285.

[1] *Ce chiffre est obtenu notamment à partir du rapprochement entre l'identité alléguée par la personne interpellée et celle qui est, le cas échéant, associée à ces empreintes dans le fichier automatique des empreintes digitales. Ainsi en 2009, 98 350 personnes ont été signalées avec deux états civils différents. Toutefois ce chiffre ne permet pas de tirer de conclusions assurées. En effet, l'identité multiple peut résulter d'une erreur orthographique ou de transcription phonétique du nom au moment de l'enregistrement dans la base, ou, le plus souvent, de la présentation à chaque fois, d'une identité totalement fictive, pour dissimuler son identité véritable.*

L'ONDRP relève ainsi que les services de police et de gendarmerie ont constaté 13 900 cas de fraude documentaire à l'identité. Ce chiffre, qui rend compte de l'activité des services de police et de gendarmerie ne correspond pas à celui des fraudes effectivement commises, puisqu'échappe à cette recension, celles qui sont restées suffisamment discrètes pour ne pas avoir donné lieu à une alerte, ou celles qui n'ont pas fait l'objet d'un dépôt de plainte. Toutefois, rapporté à d'autres faits constatés de délinquance, ce chiffre montre que l'ampleur de la fraude à l'identité, lorsqu'elle lèse directement une victime conduite à porter plainte, reste limitée : on compte ainsi environ 127 000 vols d'automobiles, 164 000 cambriolages de résidence principale, 88 400 vols à la tire, 112 000 vols avec violence ou 120 000 falsifications et usages frauduleux de chèques et de cartes de crédit.

Les condamnations pour fraude documentaire à l'identité

La direction des affaires criminelles et des grâces recense 11 621 condamnations en 2009 pour l'une des neuf infractions précitées[1] qui correspondent à la « fraude documentaire à l'identité » et le délit de recel qui peut y être associé (article 312-1 du code pénal).

Le nombre de condamnations a peu évolué au cours des cinq dernières années. Toutefois, les condamnations prononcées sur le fondement de l'article 434-23 du code pénal (le fait d'usurper le nom d'un tiers dans des circonstances qui ont déterminé ou auraient pu déterminer contre celui-ci des poursuites pénales) ont progressé de 15 % entre 2005 et 2008. Cette augmentation reflète l'importante croissance des infractions à la circulation routière associées aux condamnations pour usurpation d'identité (+ 50 % en quatre ans, de 1153 infractions en 2005 à 2026 en 2008).

L'observatoire constate par ailleurs, sur les titres frauduleux saisis par la police aux frontières[2], que près des deux tiers des titres d'identités et des passeports saisis, toutes nationalités confondues, sont des vrais faux documents, obtenus frauduleusement de l'autorité administrative en produisant des pièces d'état civil falsifiées ou contrefaites. C'est là le signe que les sécurités mises en place sur le titre d'identité conduisent les fraudeurs à privilégier l'obtention frauduleuse d'un titre authentique à partir d'un acte d'état civil plus facilement contrefait.

Jusqu'au printemps 2010, la direction des libertés publiques et des affaires juridiques centralisait les dossiers de fraude documentaire à l'identité détectés par les préfectures. En 2009, cette direction a été saisie de 2 042 dossiers, dont un tiers correspondait à une fraude matérielle (falsification du titre d'identité) et deux tiers à une fraude intellectuelle (tentative d'obtenir un document authentique en alléguant d'une identité fictive ou usurpée). Ces signalements ont donné lieu à 1 750 inscriptions au fichier des personnes recherchées.

---

[1] *Cf. partie I)A)1)b).*

[2] *Il s'agit principalement de passeports, carte d'identité, permis de conduire et de certificats d'acte de naissance.*

Les chiffres fournis à l'ONDRP par le bureau de la nationalité et des titres d'identité et de voyage du ministère de l'intérieur montrent enfin que le passeport et la carte nationale d'identité restent des titres recherchés par les fraudeurs, puisqu'en 2009, 351 000 cartes nationales d'identité ont été déclarées perdues ou volées, ainsi que 79 916 passeports[1]. La fraude associée à ces vols ou ces pertes peut consister à falsifier le document, ou bien à déclarer mensongèrement la perte pour obtenir un nouveau titre et faire bénéficier un tiers du titre déclaré perdu ou volé.

M. Cyril Rizk, responsable des statistiques de l'ONDRP a observé que si les chiffres de la fraude documentaire à l'identité paraissaient stables, et si l'usurpation totale d'identité restait un phénomène rare, en revanche, l'escroquerie économique et financière était en forte progression, de nouvelles techniques permettant de recueillir les données bancaires personnelles des individus étant apparues depuis quelques années.

Il a conclu que l'usurpation d'identité et la fraude documentaire, ne constituaient pas, par rapport à d'autres formes de délinquance, une préoccupation majeure de sécurité publique et qu'il convenait, s'agissant de la fraude aux données personnelles, d'apporter une attention accrue aux défauts de sécurisation des moyens de paiement.

Votre rapporteur note toutefois que, même si l'ampleur de la fraude à l'identité est limitée, la sécurisation de l'identité reste une nécessité, au regard des conséquences importantes que cette délinquance est susceptibles d'entraîner pour les victimes ou pour la collectivité publique, soit directement, soit en servant de support à la commission d'autres infractions plus graves encore.

4. Des conséquences graves pour l'État, les opérateurs économiques et les victimes de la fraude à l'identité

La mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire avait observé que le coût de la fraude à l'identité était largement ignoré. En l'absence d'études incontestables sur la question, la même conclusion s'impose aujourd'hui.

Le coût pour la collectivité publique est principalement celui des fraudes aux prestations sociales et aux services fiscaux, et des escroqueries financières ou aux moyens de paiement (captation de données de connexion sur les services bancaires en ligne, utilisation frauduleuse de moyens de paiement, ouverture frauduleuse d'un compte bancaire ou souscription d'un emprunt sous une autre identité).

---

[1] *Ces chiffres sont à rapporter aux 5 millions de CNI et 3 millions de passeports délivrés chaque année et aux 45 millions de CNI et 15 millions de passeports en circulation.*

Les conséquences pour les particuliers victimes, qui peuvent être limitées lorsqu'une fois la fraude constatée, l'établissement de crédit, rembourse la victime du débit frauduleux, peuvent aussi être beaucoup plus graves, notamment lorsque l'usurpation d'identité est totale.

Ainsi, l'intéressé peut se voir opposer un refus de délivrance d'un titre d'identité ou de voyage, l'administration considérant, de bonne foi, qu'il n'en est pas le titulaire légitime, puisqu'elle a déjà délivré un tel titre au fraudeur. Tant que la fraude n'aura pas été établie – ce qui, compte tenu parfois de la complexité de l'affaire, peut prendre du temps –, la victime se trouvera privée du titre nécessaire, et interdite de voyager hors de l'espace Schengen s'il s'agit d'un passeport, ou empêchée de prouver aisément, à chaque fois que nécessaire, son identité s'il s'agit d'une CNI.

La victime peut aussi subir un important préjudice financier, à raison des emprunts contractés en son nom par l'usurpateur ou des paiements effectués à partir des chèques, cartes, ou comptes bancaires de l'intéressé.

Dans les cas les plus graves, l'usurpateur ayant choisi de vivre sous l'identité usurpée, l'état civil de la victime se trouvera modifiée à raison des démarches que le fraudeur aura effectuées, ce qui peut inclure des reconnaissances d'enfants ou des mariages.

Les règles de modification et de conservation du registre d'état civil étant rigoureuses, l'intéressé qui souhaitera obtenir la rectification des mentions résultant de la fraude devra obtenir une décision en ce sens du président du tribunal de grande instance, sur le fondement de l'article 99 du code civil, ou un jugement annulant l'acte litigieux. Votre rapporteur observe, qu'à plusieurs reprises, la commission des lois a été saisie de la difficulté que rencontrent les personnes victimes d'usurpation d'identité, la mention des actes résultant de l'usurpation n'étant pas supprimée, mais seulement rayée sans autre indication, ce qui ne permet pas de distinguer symboliquement les mentions qui leur sont propres et celles qui trouvent leur origine dans la fraude.

Enfin, lorsque l'identité usurpée est utilisée par le délinquant pour échapper aux recherches des services de police, le risque, pour la victime, est d'être poursuivie voire condamnée pour les infractions commises par le premier. Si, une fois l'usurpation établie, les poursuites cessent et les inscriptions indues au casier judiciaire sont effacées, tant que dure la méprise, la vie de l'intéressé peut être particulièrement affectée par les accusations qui sont portées contre elles et leurs conséquences.

Confronté aux conséquences de l'usurpation d'identité la victime doit, pour se protéger, informer ses partenaires privés et déposer plainte auprès des services de police ou de gendarmerie.

L'administration peut aussi prendre l'initiative, lorsqu'un dossier lui est signalé, de diligenter une enquête administrative avec l'appui des services de police. En cas de suspicion d'usurpation avérée, les titres indûment délivrés

sous l'état civil de la victime doivent en principe être invalidés sur les fichiers de gestion correspondants et inscrits au fichier des personnes recherchées. Enfin des poursuites pénales peuvent être engagées par le procureur de la République.

Nombre de dossiers n'aboutissent pas, en raison de l'impossibilité d'élucider les cas d'usurpation d'identité et à cause des nombreux classements sans suite effectués par le parquet sur ce type d'affaires.

B. LES RÉPONSES APPORTÉES JUSQU'À AUJOURD'HUI AUX DÉFAILLANCES DE LA CHAÎNE DE L'IDENTITÉ

Notre excellent collègue Jean-René Lecerf observait déjà, dans le rapport qu'il avait rédigé pour la mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire[1], que « *la fraude documentaire profite de la faiblesse de certains maillons de la chaîne de l'identité. Il est ainsi possible d'obtenir de vrais titres d'identités au moyen de fausses pièces justificatives. Les conditions de délivrance des cartes nationales d'identité et des passeports n'offrent pas toutes les garanties de sécurité. Enfin, les moyens de détection des faux documents doivent être renforcés* ».

Il préconisait pour remédier à ces lacunes des solutions simples. Force est de constater qu'elles n'ont pas toutes été mises en œuvre, ou très récemment.

1. Des contrôles déficients au moment de la délivrance des titres d'identité

Les conditions actuelles de sécurisation des cartes nationales d'identité (CNI) et des passeports biométriques

Ces conditions sont respectivement fixées pour les CNI par le décret n° 55-1397 du 22 octobre 1955 et pour les passeports biométriques par le décret n° 2005-1726 du 30 décembre 2005.

Les sécurités applicables à la demande du titre, à l'instruction du dossier et à la délivrance du titre d'identité :

- le principe de la double comparution : il permet de s'assurer que c'est la même personne qui sollicite et retire le titre, en vérifiant au surplus pour le passeport la correspondance entre les empreintes inscrites dans la puce du passeport avec celles de la personne qui le retire ;

- le formulaire de demande « *CERFA* » est signé par le demandeur qui engage ainsi sa responsabilité sur les informations déclarées ainsi que sur le principe même de sa demande ;

[1] *Rapport de la mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire,* op. cit., *p. 28.*

- le recueil de certaines données biométriques du demandeur : la photo et une empreinte digitale pour la CNI (toutefois, cette empreinte ne fait l'objet que d'une conservation « *papier* » et n'est pas enregistrée sous forme numérique dans la base de gestion informatique) ; une image numérisée du visage et huit empreintes digitales pour le passeport biométrique (toutes font l'objet d'un enregistrement dans le fichier central de gestion) ;

- l'exigence de pièces justificatives personnelles : un justificatif d'état civil (soit un titre d'identité en cours de validité, soit un acte d'état civil de moins de 3 mois) et un justificatif de domicile ;

- les vérifications opérées par examen croisés des fichiers entre l'application gestionnaire du titre d'identité et le fichier des personnes recherchées. L'application TES pour les passeports biométriques est aussi interconnectée au système d'information Schengen (SIS) et à Interpol.

- la restitution de l'ancien titre d'identité détenu (sauf cas de perte ou de vol déclaré) au moment de la remise du nouveau titre.

Par ailleurs, les titres d'identité font l'objet de sécurités technologiques renforcées rendant leur contrefaçon ou falsification peu aisées. La fabrication des titres est elle-même réalisée dans des lieux protégés, dans les locaux de l'imprimerie nationale à Douai pour les passeports biométriques et dans ceux du ministère de l'intérieur à Lognes et à Limoges pour les CNI.

Enfin, les bases informatiques de gestion des titres d'identité sont conçues de manière à garantir un niveau de protection très élevé des données qui y sont conservées. Les conditions d'accès aux informations conservées dans ces bases sont strictement encadrées : en droit, seul les agents habilités peuvent y avoir accès. La traçabilité des consultations de la base TES est par ailleurs assurée par la nécessité pour les intéressés de s'identifier au moyen d'une carte sécurisée qui leur est personnelle.

- Les défaillances dans la délivrance des actes d'état civil

Pour obtenir une carte nationale d'identité, un extrait d'acte de naissance comportant sa filiation suffit et, à défaut, une copie intégrale de l'acte de mariage. C'est aussi le cas pour un passeport, à défaut de CNI en cours de validité ou d'un précédent passeport à la condition qu'il ne soit pas périmé depuis plus de deux ans.

En principe, un extrait d'acte de naissance avec filiation ou une copie intégrale ne devraient pas pouvoir être délivrés à un tiers, à moins qu'il y soit autorisé par le procureur de la République. Cependant, ces actes pouvant être transmis par correspondance, il suffit pour qu'un tiers se les fasse remettre, qu'il soit en mesure d'indiquer les noms et prénoms usuels des parents de la personne que l'acte concerne.

Une fois l'extrait obtenu, il peut être falsifié ou contrefait, avant d'être produit à l'appui d'une demande de délivrance d'un titre d'identité authentique.

Le souci légitime de simplification administrative diminue ainsi la sécurité que l'on pourrait attendre dans la délivrance d'un document important pour les intéressés.

Une première réponse à cette difficulté a toutefois été apportée, d'abord par le décret n° 2004-1159 du 29 octobre 2004[1], puis, plus récemment, par le décret n° 2011-167 du 10 février 2011[2], qui autorisent les administrations à faire procéder à la vérification des données de l'état civil fournies par l'usager, auprès des officiers de l'état civil dépositaires de ces actes, dans le cadre des dossiers qu'elles instruisent. Les moyens de la lutte contre la fraude s'en trouvent renforcés, sans que pèsent sur les usagers une contrainte supplémentaire, puisque cette transmission entre administration les dispense de produire eux-mêmes les pièces nécessaires.

- Les difficultés de vérification propres aux actes d'état civil étranger

La fraude peut aussi s'appuyer sur des actes d'état civil dressés à l'étranger, qui concernent des français d'origine ou des personnes devenues françaises par la suite. Ces actes doivent en principe être transcrits à l'état civil français, mais les moyens de contrôle et de vérification des postes consulaires et de l'administration ne sont pas toujours adaptés.

Il revient, en dernier ressort au tribunal de grande instance de Nantes de statuer sur la validité de l'acte s'il a été saisi en ce sens par le procureur de la République, lui-même saisi par l'administration instruisant la demande.

2. Des contrôles inadaptés des titres d'identité en circulation

Les procédés techniques de fabrication des titres d'identité garantissent aujourd'hui leur résistance à la falsification ou à la contrefaçon.

Toutefois, pour être efficaces, ces sécurités doivent être utilisées. Dans la vie courante, le contrôle du titre se limite généralement à d'une part à un contrôle visuel entre la photographie imprimée et le visage de son titulaire et d'autre part à la vérification de la validité du titre. Les autres contrôles, sur l'absence de falsification, la lecture de la piste optique ou, pour le passeport biométrique, la lecture des empreintes digitales du titulaire du titre, n'ont lieu que dans des circonstances exceptionnelles (contrôle d'identité par les forces de police, passage en douane, demande de renouvellement de titre).

---

[1] *Décret n° 2004-1159 du 29 octobre 2004 portant application de la loi n° 2002-304 du 4 mars 2002 modifiée relative au nom de famille et modifiant diverses dispositions relatives à l'état-civil.*

[2] *Décret n° 2011-167 du 10 février 2011 instituant une procédure de vérification sécurisée des données à caractère personnel contenues dans les actes de l'état civil.*

Le nombre élevé de titres déclarés perdus ou volés chaque année – dont on peut observer qu'il a considérablement crû lorsque la carte d'identité est devenue gratuite[1] – montre qu'une part importante de la fraude exploite ces défaillances du contrôle.

La mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire avait à cet égard observé que « *les pertes de titres d'identité sont mal recensées. Les particuliers effectuent parfois des démarches tardives (déclarations) pour signaler la perte de leur titre auprès des mairies ou des préfectures. En théorie, la transmission de ces déclarations ainsi que de messages de vigilance signalant des pertes répétées aux services de police devrait être immédiate. Les pertes ne font pas l'objet d'un suivi précis (les fichiers de gestion semblent ne pas le permettre)* »[2].

Les auditions conduites par votre rapporteur et les informations transmises par les services du ministère de l'intérieur confirment ce constat et l'absence d'améliorations, sur ce point, depuis 2005. Or, comme MM. Guillaume Desgens-Pasanau et Éric Freyssinet, auteurs de l'ouvrage « *L'identité à l'ère du numérique* »[3], l'ont observé, un fichier central, instantanément mis à jour, susceptible d'informer toute personne sur la validité ou non du titre d'identité qui lui est présenté à l'appui d'une demande particulière, et notamment, par exemple, d'un paiement par chèque ou de l'ouverture d'un compte bancaire, constituerait un moyen de lutte très efficace contre la fraude documentaire, à l'instar de ce que le fichier national des chèques irréguliers (FNCI) a permis pour la lutte contre les chèques volés.

*

La fraude à l'identité est une délinquance dont l'ampleur reste, à ce jour, limitée. Toutefois, le phénomène est loin d'être négligeable et peut, dans certains cas rares, présenter des conséquences traumatisantes pour les personnes qui en sont victimes. Améliorer les moyens de lutte contre la fraude documentaire à l'identité est donc tout à fait justifié et certaines solutions simples, qui n'ont pas encore été mises en œuvre ou ne sont pas encore totalement entrées en application, devraient pouvoir rendre la fraude plus difficile.

La question se pose cependant de passer à un degré supérieur de sécurisation de l'identité, par l'utilisation des technologies biométriques et la constitution d'un fichier central des titres d'identités biométriques. Tel est le débat qu'ouvre la proposition de loi soumise à votre examen.

---

[1] *En 1997, on dénombrait 37 000 cartes d'identité déclarées perdues ou volées. On en compte aujourd'hui dix fois plus (351 000 en 2009), la gratuité étant intervenue le 1er septembre 1998. Il est vrai toutefois que le nombre de passeports déclarés volés ou perdus était de 80 000 en 2009, alors que ce titre de voyage est payant et qu'on compte en moyenne 1 passeport pour 3 cartes d'identité.*

[2]

[3] *G. Desgens-Pasanau et E. Freyssinet,* L'identité à l'ère numérique*, Dalloz, Collection PrésaJe, 2009.*

II. LES TERMES DU DÉBAT

A. LA SÉCURISATION DE L'IDENTITÉ PAR LE RECOURS À LA BIOMÉTRIE ET À LA CONSTITUTION D'UN FICHIER CENTRAL DE L'IDENTITÉ

1. La biométrie, technologie d'identification

La biométrie désigne l'ensemble des technologies de reconnaissance physique ou biologique des individus. Celles-ci prennent en compte les différences morphologiques et biologiques qui distinguent un individu d'un autre et permettent de l'identifier parmi plusieurs millions.

La vérification de l'identité d'un individu s'opère par la comparaison entre l'empreinte biométrique enregistrée, sous un format quelconque, papier, photographie ou fichier numérique, et la même empreinte présentée à l'instant du contrôle par l'individu.

Les principales données biométriques actuellement exploitées sont le visage, les empreintes digitales ou palmaires, le contour de la main, l'iris et les empreintes génétiques. D'autres éléments biométriques sont parfois utilisés, mais de manière plus confidentielle, comme la rétine ou le réseau vasculaire de la main.

Cette capacité d'identification de la biométrie autorise en effet trois usages :

- l'identification à des fins de recherche criminelle, dans le cadre notamment de procédures judiciaires. Tel a été historiquement le cas des empreintes digitales, regroupées dans le fichier automatisé des empreintes digitales (FAED) ou celui des empreintes génétiques dans le fichier national automatisé des empreintes génétiques (FNAEG) ;

- la sécurisation des accès à certains sites (site sensible, cantine scolaire…) ou à certaines opérations. L'accès n'est autorisé qu'aux individus dont les empreintes biométriques se retrouvent dans la base ;

- la vérification de l'identité de l'intéressé. C'est le rôle que joue, sur les titres d'identité la photographie du visage de l'intéressé.

Chacun de ces usages sollicite un degré plus ou moins poussé d'identification. On distingue à cet égard l'authentification de l'identification, *stricto sensu*.

L'**authentification** consiste à vérifier que l'identité alléguée par une personne est exacte. On compare alors les données biométriques de l'intéressé avec celles que l'on associe à l'identité alléguée. Il s'agit du contrôle effectué notamment à partir du titre d'identité présenté par la personne et qui permet de s'assurer qu'elle en est bien le titulaire légitime. Ainsi, dans le cas du passeport biométrique, les empreintes digitales du détenteur sont comparées avec celles contenues dans la puce électronique du passeport.

L'**identification** consiste à déterminer l'identité d'une personne uniquement à partir de son empreinte. Elle requiert la constitution d'un fichier central regroupant toutes les empreintes connues et les associant à une identité donnée. Les fichiers de police précités (FAED et FNAEG) sont utilisés à cette fin dans le cadre de recherches criminelles.

2. Une réflexion gouvernementale élaborée à travers plusieurs projets dont aucun n'a été déposé devant le Parlement

Depuis 2001, chacun des gouvernements successifs a réfléchi à la possibilité de mettre en place une carte d'identité biométrique. Si le projet de « *titre fondateur d'identité* » annoncé en juillet 2001 n'a pas dépassé le stade des travaux préparatoires, le projet INES (pour identité nationale électronique sécurisée) esquissé dès 2003 s'est concrétisé dans un avant projet de loi soumis à la CNIL en mai 2005.

Conçu afin de tirer parti des possibilités de plus haute sécurisation de l'identité que permettaient la biométrie et la constitution d'un fichier central d'identité, le projet INES fusionnait les procédures de délivrance du passeport et de la carte nationale d'identité. L'un et l'autre de ces titres devait être doté d'une puce électronique sur laquelle auraient été enregistrées les données relatives à l'état civil de son titulaire ainsi que sa photographie et ses empreintes digitales numérisées.

Le système proposé articulait quatre fichiers centraux : un fichier d'état civil, un fichier d'empreintes digitales, un fichier d'images faciales numérisées, un fichier des titres avec l'identité et un fichier archivant les justificatifs scannés présentés lors du dépôt de la demande du titre. Il prévoyait que la lecture de la puce électronique puisse s'effectuer « *sans contact* » physique direct (technologie RFID). Le projet de loi qui devait traduire ces fonctionnalités n'a jamais été déposé.

Le projet INES a donné lieu à une consultation publique, organisée par le Forum des Droits sur l'Internet, qui a remis son rapport au ministre de l'intérieur en juin 2005. L'avant-projet de loi a finalement été retiré.

Deux autres projets lui ont succédé, l'un comme l'autre soumis à la CNIL, respectivement en octobre 2006 pour le projet dit « *Protection de l'identité* » et en juillet 2008 pour le nouvel avant-projet de loi relatif à la protection de l'identité. Ces travaux n'ont pas abouti au dépôt d'un projet de loi devant le Parlement.

Si la mise en place d'une carte nationale d'identité électronique est maintenue au rang de priorité, le gouvernement a porté son effort en la matière sur la création du passeport biométrique, conformément aux engagements européens de la France. Il a privilégié à cette fin la voie réglementaire.

3. Une première étape : le passeport biométrique

La création en France d'un titre de voyage biométrique répond à des exigences européennes et internationales.

L'organisation de l'aviation civile internationale et les États-Unis exigent, avant 2015 pour les premiers et depuis le 26 octobre 2006 pour les seconds, l'intégration d'au moins une donnée biométrique dans les documents de voyage, qui peut être la photo numérisée du visage de son titulaire.

Le règlement communautaire du 13 décembre 2004[1], du 13 décembre 2004, modifié par le règlement du 28 mai 2009[2], impose aux États membres la création d'un passeport avec puce électronique, pour les citoyens européens âgés de plus de 12 ans et l'inscription, sur cette puce, de diverses informations (identité, taille, yeux *etc.*) et des deux données biométriques suivantes : une photographie numérisée du visage et deux empreintes digitales.

Le décret n° 2008-426 du 30 avril 2008 instaurant le passeport biométrique[3] est allé au-delà des prescriptions communautaires. Il a notamment prévu :

- la création d'un fichier central, le fichier « *TES* », regroupant l'ensemble des données recueillies pour la confection du titre, notamment les empreintes digitales, qui constitue le premier fichier de ce type et de cette ampleur en France. L'article 19 du décret précité interdit toutefois l'utilisation des empreintes digitales enregistrées dans ce fichier à des fins de police judiciaire. Le fichier ne comporte par ailleurs pas de dispositif de reconnaissance faciale ;

- le recueil de huit empreintes digitales, enregistrées dans la base. Toutefois seules deux empreintes sont inscrites dans la puce électronique du passeport ;

- l'application de l'obligation de disposer d'un passeport biométrique aux enfants âgés de 6 à 12 ans. La France a ainsi utilisé la possibilité de régime transitoire prévue par le règlement européen. Cet âge devra être relevé à 12 ans, en application du règlement, à compter du 29 juin 2013, le régime transitoire n'étant appelé à durer que quatre ans.

---

[1] *Règlement (CE) n° 2252/2004 du Conseil 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.*

[2] *Règlement (CE) n° 444/2009 du Parlement européen et du Conseil du 28 mai 2009 modifiant le règlement (CE) n° 2252/2004 du Conseil 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.*

[3] *Décret n° 2008-426 du 30 avril 2008 modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électronique.*

Le projet de décret a fait l'objet d'un avis critique de la commission nationale de l'informatique et des libertés, cette dernière considérant notamment que « *si légitimes soient-elles, les finalités invoquées ne justifient pas la conservation, au plan national, de données biométriques telles que les empreintes digitales et que les traitements ainsi mis en œuvre seraient de nature à porter une atteinte excessive à la liberté individuelle* ». Elle a par ailleurs estimé que « *l'ampleur de la réforme qui se dessine et l'importance des questions qu'elle peut soulever justifieraient que, comme l'a rappelé à plusieurs reprises, le Parlement soit saisi sous la forme d'un projet de loi, qui lui serait préalablement soumis pour avis* »[1].

Quatre requêtes ont été introduites devant le Conseil d'État contre le décret du 30 avril 2008. Elles ont été formées par les associations « *Imaginons un réseau solidaire* » (IRIS), la Ligue des droits de l'Homme et cinq associations représentant le secteur des photographes professionnels.

Déposées le 30 juin et le 4 juillet 2008, ces requêtes ont donné lieu à une séance publique le 30 juin 2010 qui a conduit à la réouverture de l'instruction et à la tenue d'une audience d'instruction le 8 septembre 2010. De nombreux échanges de mémoires sont intervenus jusqu'à ces dernières semaines. La décision sera rendue prochainement.

4. Des solutions différentes en Europe

La lutte contre la fraude à l'identité constitue, pour l'ensemble des pays européens, une priorité, dernièrement réaffirmée lors du conseil Justice Affaires intérieures des 2 et 3 décembre 2010. À cette occasion, les ministres de l'Intérieur ont examiné et adopté les conclusions sur la prévention de la fraude à l'identité et la lutte contre ce phénomène[2], appelant les États membres à se coordonner, échanger les informations nécessaires et veiller à ce que les documents « sources » d'état civil remplissent certaines conditions minimales de sécurité et de contenu pour être délivrés.

Pour autant les solutions de sécurisation de l'identité diffèrent sensiblement d'un État à l'autre.

Si plus de douze pays ont adopté une carte nationale d'identité électronique, en revanche, peu prévoient l'inclusion de données biométriques et presqu'aucun la mise en place d'un fichier central.

---

[1] *CNIL, délibération n° 2007-368 du 11 décembre 2007 portant avis sur un projet de décret en Conseil d'État modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques.*

[2] *Conclusions du 3051e Conseil Justice et Affaires intérieures, des 2 et 3 décembre 2010 sur la prévention de la criminalité liée à l'identité et la lutte contre ce phénomène et sur la gestion de l'identité, y compris la mise en place et le développement d'une coopération structurée permanente entre les États membres de l'Union européenne.*

Le tableau ci-dessous présente la situation chez les voisins immédiats de la France :

Carte d'identité	Allemagne	Royaume-Uni	Espagne	Belgique	Italie
Obligatoire ou facultatif	Facultatif	Pas de carte	Obligatoire	Obligatoire	Facultatif
Collecte d'empreintes digitales	Facultatif	Non	Obligatoire	Non	Obligatoire
Base centrale d'empreintes	Non	Non	Oui	Non	Non
Utilisation d'un numéro unique	Non	Pas de carte	Oui	Oui	Non
Maîtrise par l'intéressé des données divulguées lors d'une utilisation « internet »	Oui	Pas de carte	Non	Non	Non
Date de lancement	2010	Pas de carte	2006	2005	Non renseigné
Remarques	Puce sans contact Authentification mutuelle de la puce et du lecteur (norme allemande PACE dérivée de la norme EAC du passeport)	Abandon de la carte et du fichier central après les élections de 2010	Les empreintes digitales sont collectées pour la carte d'identité espagnole depuis les années 50.	Une carte pour les résidents étrangers et une carte pour les enfants existent également.	Historiquement, deux types de cartes existaient en Italie. Le succès est limité à ce jour (quelques millions de carte)

Source : CNIL

S'agissant du passeport biométrique, selon les informations fournies à votre rapporteur par le groupement professionnel des industries de composants et de systèmes électroniques (Gixel) ainsi que par M. Sébastien Huyghe, commissaire de la CNIL au cours de leur audition, l'Allemagne, l'Espagne et le Portugal, à la différence des Pays-Bas et de la Finlande, ont écarté la solution consistant à créer une base centrale : les informations biométriques sont uniquement enregistrées sur le titre.

5. Des enjeux économiques, financiers et industriels à prendre en considération

Le débat sur la création d'un nouveau titre d'identité biométrique ne se limite pas aux questions de sécurisation et de préservation des libertés publiques. D'autres enjeux entrent en ligne de compte.

- La sécurisation des échanges électroniques

Les projets initiaux du gouvernement tendaient à doter la carte nationale d'identité électronique d'une fonctionnalité d'identification et de « *signature électronique* » en vue de faciliter les démarches et les transactions, administratives ou privées.

Une telle fonctionnalité renforce l'attrait que peut présenter ce titre, puisqu'elle complète l'usage régalien qui en est fait par un usage quotidien. Le succès rencontré par la carte d'identité numérique belge, déployée à plus de 9 millions d'exemplaires depuis 2004, montre l'intérêt d'un tel dispositif pour les citoyens. Il convient toutefois d'observer que cette fonctionnalité est indépendante des choix effectués sur la mise en place ou non d'un contrôle biométrique de l'identité à partir des empreintes digitales ou de la constitution d'un fichier central biométrique : le dispositif belge ne prévoit ainsi ni l'un, ni l'autre.

La mission d'information de votre commission, sur la nouvelle génération de documents d'identité et la fraude documentaire avait proposé de développer les fonctions d'authentification à distance et de signature électronique qu'autorisent les titres d'identité électronique. Toutefois, elle avait formulé plusieurs recommandations concernant l'accès égal des citoyens à ces services et le champ qu'ils devaient couvrir : « *ces nouvelles fonctions devraient être limitées dans un premier temps à la sphère publique et ne devraient servir de prétexte ni à des vérifications abusives de l'identité des personnes ni à une remise en cause de la possibilité d'échanges électroniques anonymes. L'utilisation de ces fonctions devrait être ouverte à tous sur l'ensemble du territoire. L'utilisation d'un titre électronique pour des transactions privées requiert à ce stade une grande prudence en raison du respect de la concurrence, de la protection de la vie privée et des risques de mise en jeu de la responsabilité de l'État au regard de la prestation de services de certification* »[1].

Ces recommandations imposent de faire certains choix : sur la maîtrise par l'intéressé des informations transmises, sur le caractère optionnel ou non du dispositif, sur le périmètre des services couverts et sur la garantie que ceux qui n'auraient pas souscrit à cette fonctionnalité ne se verront pas refuser l'accès, pour ce seul motif, à un service commercial ou administratif.

---

[1] *Rapport d'information de la mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire,* op. cit.*, p. 9 et 75-88.*

- Le coût pour les administrés et les collectivités locales

Dans les travaux qu'elle a consacré à la question du passeport biométrique, notre excellente collègue, Mme Michèle André a souligné l'inflation fiscale subie par les administrés en raison de l'augmentation du droit de timbre, ainsi que la question de la juste indemnisation des communes auxquelles incombe une nouvelle charge de travail[1]. Notre excellent collègue Alain Anziani a dressé le même constat[2]. La création d'une carte d'identité électronique, pourrait autoriser des économies d'échelle en raison de la grande similarité des deux documents, tels qu'ils sont aujourd'hui conçus.

- Un enjeu industriel ?

Les représentants des industries œuvrant dans le domaine de la sécurité numérique et biométrique, regroupées au sein du Gixel (groupement professionnel des industries de composants et de systèmes électroniques) ont insisté sur le fait que la carte nationale d'identité électronique pourrait contribuer au développement économique de la France, notamment par les effets positifs de la sécurisation de l'identité dans les échanges commerciaux. Ils ont aussi fait valoir que « *l'absence de projets en France, pays qui a inventé la carte à puce et possède les champions du domaine, ne permet pas la promotion internationale d'un modèle français de gestion de l'identité. Leurs succès à l'international, face à une concurrence allemande ou américaine seront plus nombreux, s'ils peuvent s'appuyer sur un projet concret national* ».

B. LA NÉCESSITÉ DE CONCILIER LA PROTECTION DE LA LIBERTÉ INDIVIDUELLE ET LES EXIGENCES DE LA SÉCURITÉ PUBLIQUE

1. Les données biométriques : des données personnelles sensibles

La CNIL considère que « *les données biométriques ne sont pas des données à caractère personnel comme les autres* ». Elles présentent en effet, comme le rappelait notre collègue Jean-René Lecerf dans le rapport de la mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire « *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* »[3].

---

[1] *« La nouvelle génération de titres d'identité : bilan et perspectives », rapport d'information n° 486 (2008-2009) de Mme Michèle André, fait au nom de la commission des finances, déposé le 24 juin 2009 et « le véritable prix du passeport biométrique », rapport d'information n° 596 (2009-2010) de Mme Michèle André, fait au nom de la commission des finances, déposé le 30 juin 2010.*

[2] *« Projet de loi de finances pour 2011 : Administration générale et territoriale de l'État* », *avis n° 116 (2010-2011) de M. Alain Anziani, fait au nom de la commission des lois, déposé le 18 novembre 2010.*

[3] *Rapport de la mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire,* op. cit.*, p. 98.*

Pour la CNIL, « *à la différence de toute autre donnée d'identité, et à plus forte raison de toute autre donnée à caractère personnel, la donnée biométrique n'est 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. On comprend dès lors que toute possibilité de détournement ou de mauvais usage de cette donnée fait peser un risque majeur sur son identité. Confier ses données biométriques à un tiers, lui permettre de les enregistrer et de les conserver n'est donc jamais un acte anodin : cela doit répondre à une nécessité a priori exceptionnelle, justifiée, et être entouré de garanties sérieuses* »[1].

Il est possible à cet égard de distinguer les **données biométriques traçantes** comme les empreintes digitales, qui permettent de suivre un individu à la trace et **celles qui ne laissent pas de traces**, en l'état actuel des technologies, comme l'iris ou le réseau vasculaire de la main. Les premières peuvent être utilisées soit pour réunir des informations sur l'intéressé en reconstituant l'itinéraire qu'il a suivi et les actions qu'il accomplit à cette occasion, soit pour identifier les personnes qui ont été présentes à un moment, en un lieu, ce qui correspond à l'usage le plus courant dans le cadre de recherches judiciaires.

La sensibilité particulière des données biométriques se manifeste notamment dans le pouvoir de contrôle renforcé que le législateur a reconnu à la CNIL, puisque les traitements biométriques, autres que ceux mis en œuvre par l'État, sont désormais soumis, lorsqu'ils sont susceptibles de présenter des risques particuliers au regard de la vie privée et des libertés individuelles, à un régime d'autorisation par la CNIL en application de l'article 25 de la loi « *information et libertés* ».

2. La position de la CNIL sur l'usage des technologies biométriques : le nécessaire respect d'une exigence de proportionnalité

D'une manière générale, la CNIL considère comme **légitime le recours, pour s'assurer de l'identité d'une personne, à des dispositifs de reconnaissance biométrique dès lors que les données biométriques sont conservées sur un support dont la personne à l'usage exclusif**[2].

---

[1] *Communication de la CNIL relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données (http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/Communication-biometrie.pdf).*

[2] *CNIL, délibération n° 2007-368 du 11 décembre 2007 portant avis sur un projet de décret en Conseil d'État modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques.*

En revanche, **elle est plus réservée sur la constitution de bases de données centralisées de données biométriques**, dont elle estime qu'elle doit être justifiée par des forts impératifs de sécurité.

Dans la mesure où les traitements concernés utilisent une biométrie dite « *à trace* », en l'occurrence les empreintes digitales, qui ont la particularité de pouvoir être capturées et utilisées à l'insu des personnes concernées, ils appellent une vigilance toute particulière, tant de la part des personnes concernées que de celle des autorités de protection des données. En effet, ces traces peuvent être exploitées pour l'identification des personnes et tout traitement de données est donc susceptible d'être utilisé à des fins étrangères à sa finalité première, notamment à des fins d'usurpation d'identité dans un but frauduleux.

À cet égard, ces traitements qui repose sur l'enregistrement de ces données biométriques dans une base centrale posent question du point de vue de la protection des données. En effet, étant susceptibles d'être utilisés à d'autres fins que celles prévues initialement, il est possible que la personne perde la maîtrise de sa donnée biométrique, qui est ainsi détenue par un tiers. Dès lors, en cas d'intrusion dans le fichier, on peut accéder à l'ensemble des empreintes ou gabarits qui y sont stockés et qui sont généralement associés aux identités des personnes. Enfin, la création de telles bases de données implique des sécurités techniques complexes et supplémentaires, dans la mesure où 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.

Un principe guide l'analyse de la CNIL : celui du respect de la proportionnalité entre les objectifs poursuivis et les moyens déployés et les atteintes éventuellement portées aux libertés individuelles.

Lors de son audition, M. Sébastien Huyghe, commissaire de la CNIL a à cet égard considéré que la lutte contre la fraude et la constitution d'un nouvel outil de police judiciaire constituaient des finalités distinctes, qui n'appelaient pas les mêmes garanties de mise en œuvre. Il revient au législateur de préciser la ou les finalités poursuivies, afin d'interdire toute utilisation détournée du fichier ainsi créé.

C'est en fonction des finalités déterminées que la proportionnalité du dispositif projeté doit alors être appréciée : existe-t-il des procédés de lutte contre la fraude plus respectueux de la vie privée ? Quelles garanties mettre en œuvre s'il s'agit d'un outil de police ?

La CNIL, dans son avis rendu sur le décret mettant en place le passeport biométrique, a considéré que, si légitimes soient-elles, les finalités gestionnaires définies dans le décret (faciliter les procédures d'établissement, de délivrance, de renouvellement, de remplacement et de retrait des passeports ainsi que prévenir, détecter et réprimer leur falsification et leur contrefaçon),

« *ne justifiaient pas la conservation, au plan national, de données biométriques telles que les empreintes digitales et que les traitements ainsi mis en œuvre seraient de nature à porter une atteinte excessive à la liberté individuelle* »[1].

M. Sébastien Huyghe a estimé que, quelle que soit l'option retenue, la proposition de loi devra comporter les garanties indispensables pour assurer la protection des données à caractère personnel, par exemple la limitation des destinataires des données et la traçabilité de leurs actions, la fixation d'une durée de conservation et de mécanismes rigoureux de mise à jour des informations, ou la possibilité pour la CNIL de contrôler la mise en œuvre du système.

S'agissant des fonctionnalités supplémentaires ajoutées à la carte nationale d'identité, et notamment celles permettant de s'authentifier sur des réseaux de communication en ligne, il a indiqué que la CNIL s'était toujours montrée favorable au développement des e-services, publics ou privés. La mise en œuvre de ces outils doit cependant être accompagnée de garanties afin que seules les données personnelles nécessaires aux transactions soient communiquées (principe de la divulgation partielle), et qu'aucune exploitation par l'État d'informations sur ces transactions privées ne soit autorisée.

C. LES OPTIONS DISPONIBLES

La proposition de loi de nos collègues MM. Jean-René Lecerf et Michel Houel, constitue pour le législateur la première occasion véritable, depuis le début de la réflexion engagée par les gouvernements successifs sur la question du titre d'identité électronique, de se prononcer sur les choix à effectuer afin de garantir la sécurité de l'identité de nos concitoyens et de lutter contre les fraudes documentaires, dans le respect de la liberté individuelle.

Trois questions se posent.

1. Faut-il utiliser la biométrie pour sécuriser l'identité ?

La première question qui se pose, s'agissant de la généralisation des titres d'identité biométrique est celle de l'utilisation des données biométriques à des fins de vérification de l'identité des individus.

Votre rapporteur constate que cette utilisation n'a pas été contestée par les personnes qu'il a entendues, mais à la condition toutefois que l'intéressé conserve la maîtrise des données servant à son identification. Tel est le cas notamment lorsque les empreintes ne sont enregistrées que sur le document d'identité qu'il détient.

---

[1] Loc. cit.

Dans une telle configuration, les sécurisations techniques du titre d'identité, qui le rendent infalsifiable, permettent à l'empreinte biométrique d'être utilisée pour sécuriser l'identité de l'intéressé, puisqu'il est techniquement très difficile de modifier cette empreinte.

2. Faut-il mettre en place un fichier central d'identité biométrique ?

- Une base centrale de données biométriques pour lutter contre l'usurpation d'identité

Le recours à un fichier central des titres d'identité biométrique doit permettre de garantir qu'une même personne ne pourra disposer de deux identités différentes, puisque ces empreintes biométriques ne pourront correspondre qu'à une seule identité.

Ce dispositif ne prémunit pas contre l'usurpation initiale d'identité – c'est là le rôle des vérifications opérées en amont dans la chaîne de l'identité, notamment sur les extraits d'actes d'état civil fournis à l'appui de la demande – mais il interdit la multiplication de fausses identités ou d'identités usurpées.

Il ne constitue certes pas le seul instrument de lutte contre les usurpations d'identité[1]. Toutefois, il est l'un des plus efficaces.

- La crainte de la constitution d'un fichier national de la population française

M. Jean-Claude Vitran, représentant de la Ligue des droits de l'homme a considéré que la base biométrique, équivalait à la création d'un unique grand fichier général de la population française, croisant à la fois une identité civile et légale et une identité physique, ce que ne permet pas, en l'état actuel du droit, le répertoire national d'identification des personnes physiques (RNIPP) tenu par l'INSEE.

Évoquant les heures sombres de notre histoire, il a jugé la recherche d'une sécurité absolue de l'identité dangereuse, et s'est inquiété de l'usage qu'un régime différent de celui de la République pourrait faire de tels moyens.

3. Quelle(s) finalité(s) assigner au fichier central d'identité biométrique et de quelles garanties l'entourer ?

a) Le choix de la finalité de la base

La base centrale des données biométriques autorise deux usages :

- la vérification qu'une même personne n'est pas enregistrée sous deux identités différentes dans le système. La finalité est ici gestionnaire, il s'agit de garantir qu'un titre est attribué à la bonne personne ;

---

[1] *Ainsi actuellement, les services compétents interrogent le fichier des personnes recherchées pour savoir, au moment de la prise d'empreintes en vue de l'établissement d'un passeport biométrique, si l'individu fait l'objet d'une alerte pour demande frauduleuse d'un titre d'identité.*

- l'identification en matière de police, par comparaison des traces relevées sur une scène de crime par exemple avec les données enregistrées dans la base. La finalité poursuivie est ici de recherche judiciaire. Il peut aussi s'agir de retrouver l'identité d'une personne désorientée ou d'identifier un corps.

Votre rapporteur observe que la proposition de loi se donne pour finalité exclusive la gestion et la sécurisation des titres d'identité et qu'elle ne mentionne pas l'éventualité d'une utilisation à des fins policières.

On peut s'interroger sur la légitimité du glissement de cette première finalité vers la finalité accessoire que constituerait l'utilisation du fichier à des fins de recherches criminelles.

Actuellement, l'usage des fichiers portant sur des données personnelles dans le cadre d'investigations policières ou judiciaires emprunte deux formes :

- les fichiers de police proprement dits, comme le fichier automatisé des empreintes digitales (FAED) ou le fichier national automatisé des empreintes génétiques (FNAEG), dont l'objet principal est de faciliter la recherche et l'identification des auteurs d'infractions ainsi que la poursuite, l'instruction et le jugement des affaires dont l'autorité judiciaire est saisie. **La constitution de la base de données obéit à des conditions qui ont un lien direct avec la finalité assignée au fichier** : seules peuvent être relevées les empreintes dans le cadre d'une enquête de flagrance, d'une enquête préliminaire, d'une commission rogatoire, de l'exécution d'un ordre de recherche délivré par une autorité judiciaire, concernant des personnes à l'encontre desquelles il existe des indices graves et concordants rendant vraisemblable qu'elles aient pu participer à la commission d'un crime ou d'un délit, ou des personnes mises en cause dans une procédure pénale dont l'identification certaine s'avère nécessaire.

- la consultation ponctuelle de fichiers constitués dans un autre objectif. Cette consultation peut résulter d'une autorisation générale prévue dans le texte créant le fichier. Tel est par exemple le cas du fichier TES de gestion des passeports biométriques, que les services de lutte contre le terrorisme peuvent consulter, à l'exclusion des données relatives aux empreintes digitales des titulaires de passeports[1]. La consultation peut aussi être autorisée ponctuellement, par décision de l'autorité judiciaire.

La base centrale proposée par le présent projet de loi ne relève manifestement pas de la première solution : il ne s'agit pas d'un fichier de police, lequel, portant sur la totalité de la population française, ne serait sans

[1] *Art. 21-1 du décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports.*

doute conforme ni à la Constitution[1] ni à la convention européenne des droits de l'homme[2].

En revanche, en l'absence de précisions supplémentaires, la base centrale biométrique serait susceptible de faire l'objet de consultations ponctuelles à des fins de recherche ou d'identification criminelles.

Il n'y a à cet égard entre la première solution et la seconde pas de différence de nature, puisque la finalité d'utilisation serait la même, mais seulement une différence de degré, dans la mesure où le second type d'utilisation est entouré de garanties supplémentaires du fait de l'intervention nécessaire de l'autorité judiciaire.

Or, si l'utilisation ponctuelle à des fins de recherche criminelle de fichiers limités dans leur étendue ne fait pas débat, la question peut se poser s'agissant d'un fichier d'une ampleur aussi vaste que celle d'une base centrale de l'identité biométrique de la population française : il appartient au législateur de prendre en considération les conséquences d'un tel changement d'échelle dans l'utilisation des fichiers d'identité, sur la conciliation entre les impératifs de l'ordre public et la protection de la liberté individuelle et le respect de la vie privée.

Aucun fichier de ce type et de cette dimension n'existe actuellement. Il ne s'agit donc pas de limiter l'usage d'un dispositif existant, mais de décider, au moment de la conception de ce dispositif s'il pourra servir à d'autres fins que celles pour lesquelles il a initialement été constitué.

Or, si la lutte contre la fraude à l'identité peut justifier la mise en place d'une telle base de données, en dépit des réserves que suscitent un tel projet, il n'est pas acquis qu'elle rende légitime des utilisations d'opportunité qui ne présentent pas de lien direct avec elle.

b) Le choix de construction de cette base pour éviter tout détournement de la finalité de la base biométrique

Une fois fixées les finalités de la base biométrique, et compte tenu des craintes que suscitent un tel dispositif et des risques qu'il présente, toutes

---

[1] *Dans une décision récente rendue en matière de logiciel de rapprochement de fichiers de police, le Conseil constitutionnel a imposé au législateur de concilier 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 de la vie privée et des autres droits et libertés constitutionnellement protégés », en prenant en compte « la généralité de l'application de ces logiciels » (CC, Décision n° 2011-625 DC du 10 mars 2011), cons. 69 et 70)..*

[2] *Dans un arrêt Marper c. Royaume-Uni, la CEDH ainsi en effet jugé, à propos du le maintien dans un fichier de police des empreintes digitales de personnes mises hors de cause, que « le caractère général et indifférencié du pouvoir de conservation des empreintes digitales, échantillons biologiques et profils ADN des personnes soupçonnées d'avoir commis des infractions mais non condamnées, tel qu'il a été appliqué aux requérants en l'espèce, ne traduit pas un juste équilibre entre les intérêts publics et privés concurrents en jeu, et que l'Etat défendeur a outrepassé toute marge d'appréciation acceptable en la matière » (CEDH, n° 30562/04 et 30566/04,* S. *et Marper c. Royaume-Uni, 4 décembre 2008).*

les garanties doivent être apportées qu'elle ne pourra être utilisée pour d'autres objets. Ces garanties peuvent être de deux ordres : juridiques ou matérielles.

(1) Les garanties juridiques sont-elles suffisantes ?

La loi « informatique et libertés » soumet les traitements automatisés de données personnelles à un certain nombre d'obligations, protectrices de la liberté individuelle : droit d'accès ou de rectification, contrôle de la CNIL etc.

Le texte qui crée le système de traitement peut prévoir d'autres garanties, qui interdisent certaines utilisations. Ainsi le décret précité organisant le fichier TES sur les passeports biométriques interdit l'accès des forces de police œuvrant dans le domaine de l'antiterrorisme aux données relatives aux empreintes digitales pour identifier une personne.

De telles garanties sont solides. Cependant elles ne sont ni définitives, ni absolues : ainsi l'accès aux fichiers est toujours possible dans le cadre d'une procédure judiciaire, sous le contrôle d'un magistrat. De plus, la prohibition peut être levée, ce qui autorise pour l'avenir l'utilisation du fichier pour une autre finalité que sa finalité originelle : c'est ce qui a été proposé par la commission européenne s'agissant de la base EURODAC[1] qui enregistre les données biométriques des demandeurs d'asile et des personnes appréhendées à l'occasion du franchissement irrégulier d'une frontière extérieure à l'Union européenne.

(2) Des garanties matérielles sont-elles possibles ?

Si l'objectif poursuivi est d'interdire tout glissement dans les finalités d'utilisation d'un fichier donné, afin d'éviter toute contestation relative aux risques que ces utilisations accessoires pourraient présenter, il peut être utile de doubler les garanties juridiques, qui ne sont pas absolues, de garanties matérielles, qui rendront techniquement impossible un usage du fichier différent de celui originellement prévu.

Notre excellent collègue Jean-René Lecerf soulignait dans le rapport de la mission d'information de votre commission, sur la nouvelle génération de documents d'identité et la fraude documentaire que « *la technologie permet*

---

[1] *Opérationnelle depuis 2003, la base de données EURODAC qui enregistre et compare les empreintes digitales, a pour finalité d'établir l'identité des demandeurs d'asile et des personnes appréhendées à l'occasion du franchissement irrégulier d'une frontière extérieure à l'Union européenne. La Commission a adopté en septembre 2009 un train de mesures visant à autoriser les services répressifs, dont Europol à consulter la base de données aux fins de la lutte contre le terrorisme et autres infractions pénales graves. Actuellement, un troisième projet de règlement a été proposé par la Commission en octobre 2010. Dans la nouvelle proposition, la Commission européenne souhaite une approche globale de la problématique relative à l'accès aux données Eurodac par les services répressifs. Ce dispositif fait l'objet de nombreuses discussions entre les Etats membres pour savoir s'il convient de l'introduire ou non dans la proposition de la Commission. La France a soutenu la réintroduction de la disposition dans le texte.*

de constituer un fichier central des données biométriques garantissant l'unicité de l'identité lors de la délivrance d'un titre sans rendre possible l'utilisation de ce fichier à d'autres fins telles que l'identification »[1].

Deux dispositifs sont envisageables.

Le premier correspond à l'établissement d'un lien unidirectionnel entre l'identité et la biométrie. Le fichier serait ainsi construit qu'il ne serait possible d'interroger la base qu'à partir de l'identité, afin de vérifier ensuite si les données biométriques associées correspondent bien à celles de l'individu qui s'est présenté sous cette identité. En revanche, il ne devrait pas être possible d'interroger la base à partir des empreintes pour retrouver l'identité. L'unicité de l'identité est assurée à l'occasion de la délivrance du titre, sans qu'aucune identification ne soit possible à partir des seules empreintes : le dispositif est utilisable dans la lutte contre la fraude, mais il ne peut faire l'objet d'une utilisation à des fins de recherche criminelle.

Toutefois, selon les indications fournies par la CNIL à votre rapporteur, ce dispositif présente un défaut : le lien unidirectionnel peut être techniquement rendu bidirectionnel et la base peut être reconstruite, à partir de l'ensemble des données qu'elle contient, pour permettre une interrogation dans les deux sens. La seule limite à cela est le temps de calcul nécessaire et la capacité informatique mise à disposition.

Le second dispositif envisageable ne présente pas le même défaut. Il s'agit, de la technologie des bases dites à « *liens faibles* », breveté notamment par la SAGEM.

Dans le système précédent, une identité est reliée à une biométrie. Dans le système à « *lien faible* », un nombre très élevé d'identités sont reliés aux biométries correspondantes, sans qu'aucun lien univoque ne soit établi entre une de ces identités et une de ces biométries.

L'opération consiste à imputer à un nombre très élevé d'identités, par exemple 100 000, un numéro compris entre 1 et 1 000, ce qui revient à les ranger informatiquement dans un « *tiroir* » numéroté. Les biométries correspondant aux 100 000 identités précitées sont rangées, de leur côté, dans un tiroir portant le même numéro.

Ce système rend impossible l'identification d'une personne à partir d'une donnée biométrique. En effet, la consultation de la base ne produit comme résultat que le numéro du tiroir dans lequel cette empreinte est rangée, qui correspond alors à 100 000 identités possibles.

En revanche, le système permet la détection de la fraude à l'identité, par la mise en relation de l'identité alléguée et celle des empreintes du demandeur de titre. L'identité alléguée correspond à un numéro donné. Les empreintes du demandeur correspondent à un autre numéro. Il y a très peu de

---

[1] *Rapport d'information de la mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire,* op. cit.*, p. 9 et 64-65.*

chance pour que ces deux numéros soient les mêmes, c'est-à-dire que l'identité sous laquelle l'usurpateur est inscrit dans la base soit placée dans le même tiroir que l'identité qui fait l'objet de la tentative d'usurpation : pour un ensemble de 1 000 tiroirs, la probabilité de détection de la fraude est de 99,9 %.

Comme le notait notre collègue M. Jean-René Lecerf dans le rapport de la mission d'information de votre commission, sur la nouvelle génération de documents d'identité et la fraude documentaire, « *la probabilité est suffisamment grande pour offrir une assurance quasi-complète sur l'unicité de l'identité et pour dissuader les fraudeurs* »[1].

À la différence du premier système, celui des « liens faibles » ne peut faire l'objet d'une reconfiguration qui permette de rétablir des liens univoques entre l'identité et la biométrie : la sécurité proposée repose sur la façon dont les données sont enregistrées dans la base initialement et ne peut être remise en cause.

*

Les réponses apportées aux trois questions posées dessinent trois options possibles :

- garantir l'authentification du porteur du titre sécurisé sans prévoir la constitution d'un fichier central. Ce dispositif tirerait parti des sécurités propres aux titres d'identités biométriques, pour s'assurer que le possesseur du titre en est bien le détenteur légitime, sans toutefois apporter de réponse définitive au problème de l'usurpation d'identité ;

- la mise en place de titres d'identité biométriques, avec la constitution d'une base centrale susceptible de faire l'objet d'utilisations pour d'autres finalités que celles proposées ;

- la mise en place de titres d'identité biométriques, avec création d'une base centrale à « liens faibles », qui interdise tout possibilité d'identification à partir des celles empreintes contenues dans la base, mais qui satisfasse, en revanche, l'objectif de lutte contre l'usurpation d'identité en rendant la fraude quasi impossible.

---

[1] *Rapport d'information de la mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire,* op. cit.*, p. 65-66.*

III. LE DISPOSITIF DE LA PROPOSITION DE LOI ET LA POSITION DE VOTRE COMMISSION

A. LA PROPOSITION DE LOI : LA CONSÉCRATION DU MODÈLE RETENU POUR LE PASSEPORT BIOMÉTRIQUE

Le but de la proposition de loi est de renforcer les moyens de lutte contre les fraudes à l'identité, tout en simplifiant la vie quotidienne des citoyens en leur permettant de prouver facilement leur identité dans leurs démarches de la vie courante.

1. La création de titres d'identité biométrique et d'un fichier central national correspondant

Le système retenu par la proposition de loi est proche de celui que l'autorité réglementaire a mis en place pour le passeport biométrique. Il reprend, dans leurs grandes lignes, les avant-projets de loi élaborés par le gouvernement sur la question.

La sécurisation de l'identité envisagée par la proposition de loi consisterait à enregistrer, dans un fichier central, certaines données biométriques de la personne considérée afin de les associer définitivement à son identité. Ces données seraient ensuite enregistrées dans un titre d'identité sécurisé.

Un tel système garantirait d'une part, grâce au fichier central des français, qu'à une personne donnée ne puisse correspondre qu'une seule identité donnée, et, d'autre part, que l'on puisse s'assurer que la personne qui présente son titre d'identité en est bien le titulaire légitime, parce que ses empreintes digitales sont les mêmes que celles enregistrées sur la carte à puce de sa carte d'identité ou de son passeport.

Les données inscrites sur ces documents d'identité sont définis à **l'article 2** : il s'agirait de l'état civil de son titulaire (nom de famille et d'usage, prénoms, sexe, date et lieu de naissance), de son domicile, et de certaines de ses caractéristiques physiques ou biométriques (taille, couleur des yeux, empreintes digitales, photographie).

L'article 5 prévoit la création d'un fichier central permettant le recueil et la conservation des données personnelles inscrites sur la CNI et le passeport électronique, associant ainsi l'identité d'une personne à certaines de ses caractéristiques physiques. Ce fichier serait créé dans les conditions prévues par la loi informatiques et libertés (décret en Conseil d'État pris après avis de la CNIL, contrôle de la CNIL sur le fonctionnement du fichier et droit d'accès et de vérification pour l'intéressé des données le concernant).

L'article pose le principe selon lequel l'intégrité et la confidentialité des données à caractère personnel doivent être assurées, ce qui interdirait toute utilisation différente de celle de son objet principal. L'identification d'une personne enregistrée dans la base, par des procédés informatiques de reconnaissance faciale serait interdite.

L'article 4 vise à remédier à une des défaillances constatées de la chaîne de l'identité : celle du contrôle sur les actes d'état civil présentés à l'appui d'une demande de titre d'identité. L'administration à laquelle sera adressée la demande de titre d'identité devra procéder, en tant que de besoin, auprès de l'officier d'état civil dépositaire des registres concernés, à la vérification des données de l'état civil fournies par l'usager. Il s'agit d'une procédure de vérification directe des informations transmises.

L'article 7 porte à cinq ans d'emprisonnement et 300 000 euros d'amende les peines encourus pour les délits de piratage de fichiers informatiques, lorsqu'il s'agit de fichiers sous la responsabilité de l'État. Ceux-ci sont actuellement punis de deux ans d'emprisonnement ou 30 000 euros d'amende ou, si l'attaque a créé des dommages irrémédiables, de trois ans et 45 000 euros d'amende, voire cinq ans et 75 000 euros d'amende.

2. La facilitation des démarches des citoyens lorsqu'il leur est nécessaire de prouver leur identité

L'**article premier** a valeur seulement indicative, puisqu'il rappelle la règle selon laquelle l'identité se prouve par tout moyen (article 78-3 du code de procédure pénale). La présentation d'une carte nationale d'identité ou d'un passeport en cours de validité suffirait à en justifier.

L'**article 3** prévoit que, si l'intéressé le souhaite, sa carte nationale d'identité peut contenir des données lui permettant de s'identifier sur les réseaux de communications électroniques et de mettre en œuvre sa signature électronique. Ce dispositif répond au souci d'apporter une plus grande sécurité dans les démarches quotidiennes des citoyens et de leur donner accès aux nouveaux services électroniques qui y seront associés.

Les **articles 6 et 8** fixent les conditions d'application de la présente proposition de loi et **l'article 9** porte le gage.

B. LA POSITION DE VOTRE COMMISSION

1. Limiter l'usage du fichier biométrique à la seule lutte contre la fraude à l'identité, en doublant les garanties juridiques de garanties matérielles

L'utilisation du fichier central biométrique dans le cadre de recherches criminelles, pour identifier une personne uniquement à partir des empreintes retrouvées sur le lieu d'un crime, pose problème : les impératifs de

la sécurité publique peuvent-ils justifier les restrictions apportées à l'exercice de la liberté individuelle et au respect de la vie privée ? À terme, ce fichier pourrait porter sur l'ensemble de la population française, ce qui constitue, par rapport aux fichiers de police actuels, un changement d'échelle sans précédent. En effet, contrairement aux fichiers précités, l'enregistrement dans la base biométrique sera indistinct et ne portera pas exclusivement sur des personnes faisant l'objet d'une suspicion légitime.

À l'initiative de son rapporteur, votre commission a considéré que le fichier étant constitué, conformément à l'intention des auteurs de la proposition de loi, pour permettre de lutter contre la fraude à l'identité, il convenait d'en limiter l'usage à cette seule finalité et interdire toute utilisation à des fins de recherche criminelle.

Elle a adopté à cette fin un **amendement** de son rapporteur, à **l'article 5**, doublant les garanties juridiques apportées à l'utilisation du fichier d'une garantie matérielle, la constitution de la base biométrique selon la technique dite du « *lien faible* » précédemment décrite, qui rend concrètement impossible l'identification d'une personne uniquement à partir de ses empreintes digitales ou de l'image numérique de son visage, tout en permettant de détecter les fraudes éventuelles à l'identité.

Par un autre **amendement** de son rapporteur au même article votre commission a par ailleurs précisé que la traçabilité des consultations et des modifications effectuées dans le fichier doit être assurée.

2. Encadrer les vérifications d'identité effectuées à partir des données biométriques

À l'initiative de son rapporteur, votre commission a adopté un **amendement** (**article 5 *bis***) traduisant la recommandation formulée par la CNIL selon laquelle le recours à des dispositifs de reconnaissance biométrique est légitime dès lors que les données biométriques sont conservées sur un support dont la personne a l'usage exclusif. La vérification de l'identité du possesseur du titre doit être effectuée à partir des données inscrites sur ce document ou dans sa puce électronique. En cas de doute sérieux sur cette identité ou sur l'altération possible du titre, la base centrale pourrait être consultée.

Votre commission a par ailleurs restreint l'accès aux empreintes digitales enregistrées sur le composant électronique aux seuls agents habilités à cet effet.

3. Renforcer les autres instruments de lutte contre la fraude documentaire

Constatant que les solutions simples formulées en 2005 par sa mission d'information sur la nouvelle génération de documents d'identité et la

fraude documentaire n'avaient pas toujours été mises en œuvre, la commission des lois a adopté un **amendement** de son rapporteur (**article 5** ***ter***) prévoyant la mise en place d'un fichier susceptible de renseigner les administrations et certains opérateurs économiques habilités sur le statut valide ou non du titre d'identité présenté. Ce dispositif, conçu sur le modèle en vigueur pour les chèques irréguliers (fichier national des chèques irréguliers – FNCI), fournira aux particuliers et aux entreprises, qui n'ont pas le droit d'effectuer un contrôle de l'identité par les empreintes digitales, un instrument efficace pour savoir si le titre qui leur est fourni est bien valide.

Votre commission a par ailleurs adopté deux **amendements** identiques de MM. Jean-René Lecerf et Bernard Frimat (**article 7** *bis*), prévoyant que lorsque le juge ordonne l'annulation d'un acte d'état civil frauduleux en raison d'une usurpation d'identité, et la transcription de cette annulation dans l'acte de naissance de la victime, il précise, dans le dispositif de sa décision, le motif de cette annulation. Ceci doit permettre de distinguer, sur l'acte de naissance, les mentions rectifiées qui sont personnelles à la victime et celles qui résultent de l'usurpation d'identité.

Enfin, à **l'article 7**, votre commission a mis en cohérence les quantums de peines d'emprisonnement et d'amende initialement prévus.

4. Donner à l'usager la pleine maîtrise de la fonctionnalité d'identification électronique de la carte d'identité et éviter que ceux qui la refusent soient évincés de certains services

À l'initiative de son rapporteur votre commission a apporté, par un **amendement à l'article 3**, deux garanties supplémentaires pour l'usage de la fonction optionnelle d'identification et de signature électronique de la carte nationale d'identité.

En premier lieu, elle a prévu que le titulaire de la carte reste maître des données d'identification qu'il communique à l'occasion de l'utilisation de cette fonctionnalité. En effet, les situations où il est nécessaire de s'identifier totalement dans les échanges en ligne sont rares et il est souhaitable que l'intéressé décide lui-même des informations qu'il communique.

En second lieu, afin de conserver à la fonctionnalité électronique son caractère optionnel et éviter qu'elle devienne un instrument d'exclusion, elle a prévu que ceux qui n'en disposerait pas ou ne souhaiterait pas l'utiliser ne puissent se voir refuser l'accès à un service ou une transaction commerciale ou administrative. Ceux-ci devront donc continuer à rester accessible à chacun dans les conditions du droit actuel.

*

* *

Votre commission a adopté la proposition de loi **ainsi rédigée**.

EXAMEN DES ARTICLES

Article premier

Preuve de l'identité

Le présent article tend à poser le principe selon lequel 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 suffirait à en justifier.

Il reprend en cela une règle déjà énoncée à l'article 78-3 du code de procédure pénale, ainsi qu'aux articles premiers des textes instituant la carte nationale d'identité[1] et le passeport français[2].

Regrouper ces dispositions dans l'article premier de ce texte, qui vise à poser le socle législatif des principes applicables à la protection de l'identité est opportun.

Votre commission a adopté l'article premier **sans modification**.

Article 2

Données inscrites sur la puce électronique des cartes nationales d'identité et des passeports

Le présent article détermine les données enregistrées sur la puce électronique de la carte nationale d'identité et du passeport sécurisé.

Il s'agira des données d'état civil du titulaire du titre (nom de famille et d'usage, prénoms, sexe, date et lieu de naissance), de la mention de son domicile, et de certaines données biométriques (taille, couleur des yeux, empreintes digitales, photographie du visage).

À l'exception des empreintes digitales, la plupart de ces données sont d'ores et déjà imprimées sur les titres d'identité actuels[3] : la puce électronique du passeport biométrique contient une image numérisée des empreintes digitales de deux doigts de son titulaire, afin de permettre aux services compétents de s'assurer que le porteur du titre en est bien le titulaire légitime.

---

[1] *Article premier du décret n° 55-1397 du 22 octobre 1955 instituant la carte nationale d'identité.*

[2] *Article premier du décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports.*

[3] *La CNI ne mentionne toutefois pas la couleur des yeux de son titulaire, ce qui est en revanche le cas du passeport.*

Le choix du nombre d'empreintes digitales enregistrées sur le support électronique ne relève pas nécessairement du domaine de la loi. Il obéit toutefois à l'exigence de proportionnalité des moyens déployés aux fins poursuivies, ce qui impose à l'autorité réglementaire de ne retenir que le nombre strictement nécessaire à la vérification de l'identité du porteur du titre.

La directive européenne relative au passeport biométrique impose deux empreintes au minimum et le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports, se limite à ce nombre. Toutefois, huit empreintes au total sont enregistrées dans la base centrale. Le ministère de l'intérieur justifie ce choix par le fait que les performances des systèmes biométriques décroissent avec l'augmentation de la taille de la population de référence. Ainsi, pour 50 millions d'individus, le taux d'erreur est de 4 % avec 2 doigts et tombe à 0,16 % avec 8 doigts.

Votre commission a adopté l'article 2 **sans modification**.

Article 3

Utilisation optionnelle de la CNI à des fins d'identification sur les réseaux de communication électronique et de signature électronique

L'article 3 tend à rendre possible l'enregistrement, sur la carte nationale d'identité électronique, de données permettant à son titulaire de s'identifier sur les réseaux de communication électroniques et de mettre en œuvre sa signature électronique.

Une telle fonctionnalité ne pourrait toutefois être mise en place qu'à la demande du titulaire de la carte. Selon les explications apportées par M. Raphaël Bartolt, directeur de l'agence nationale des titres sécurisés, la carte d'identité contiendra deux puces, l'une réservée à la vérification de l'identité du porteur au moyen de ses empreintes digitales (puce dite « *régalienne* »), qui ne pourrait être lue que par les autorités habilitées à procéder à un contrôle d'identité, l'autre réservée à la fonctionnalité mise en place par le présent article (puce « *vie quotidienne* »), qui pourrait être lue par des dispositifs diffusés dans le commerce et raccordés à un ordinateur personnel.

- Un dispositif qui vise à apporter au commerce et à l'administration électronique plus de sécurité.

La plus grande part des transactions effectuées en ligne ne requièrent pas l'identification précise de l'acheteur : le paiement suffit. Toutefois, dans certains cas, l'identification de l'une des parties peut être nécessaire pour garantir le paiement, éviter l'utilisation frauduleuse du titre de paiement d'un tiers, s'assurer de la capacité de l'intéressé à contracter ou à consulter le service en ligne ou lui imputer une obligation particulière.

Des dispositifs existent d'ores et déjà, qui permettent de sécuriser la transaction : certification électronique, données personnelles de connexion comme un mot de passe ou un code particulier, double confirmation de la

transaction par l'envoi d'un e-mail sur l'adresse personnelle de l'intéressé, signature électronique[1]…

La signature électronique

« *Le développement du commerce électronique est subordonné à l'existence de garanties sur la sécurité des transmissions de données et des paiements en ligne. Grâce à un système de chiffrement appliqué au message transmis, sans que ce dernier soit nécessairement lui-même chiffré, la signature électronique constitue une réponse au problème, car elle garantit l'authenticité et l'intégrité des données, ainsi que l'identité du signataire. Si la confidentialité est requise, il faut chiffrer le contenu du message.*

« De façon générale, le chiffrement consiste à rendre le texte d'un message illisible pour qui ne détient pas la clé de déchiffrement. Dans les systèmes de chiffrement symétriques, une seule clé sert à la fois à chiffrer et à déchiffrer les données. Elle doit être gardée secrète par les parties intéressées pour que la sécurité de l'information soit garantie. L'inconvénient principal réside dans le fait que l'expéditeur et le destinataire doivent convenir à l'avance de la clé et disposer d'un canal sûr pour l'échanger.

« Telle est la raison pour laquelle se développent depuis quelques années des systèmes de signature électronique reposant sur des algorithmes de chiffrement asymétriques où chaque utilisateur dispose de deux clés, une clé publique et une clé privée. Ces deux clés sont elles-mêmes créées à l'aide d'algorithmes mathématiques. Elles sont associées l'une à l'autre de façon unique et sont propres à un utilisateur donné. Un message chiffré à l'aide d'un algorithme asymétrique et d'une clé privée, qui constitue l'un des paramètres de l'algorithme, ne peut être déchiffré qu'avec la clé publique correspondante, et inversement. La clé publique doit donc être connue de tous, tandis que la clé privée reste secrète, la carte à puce semblant être le meilleur support de stockage des clés privées. Lorsque l'algorithme de chiffrement asymétrique est utilisé seulement pour créer la signature électronique, les mêmes clés, privée et publique, sont utilisées, mais seulement pour vérifier l'authenticité et l'intégrité du message.

« Contrairement à la signature manuscrite, la signature numérique, composée de chiffres, de lettres et d'autres signes, ne comporte aucun élément permettant de l'attribuer à une personne donnée. Chaque utilisateur doit donc établir avec certitude l'identité de ses correspondants. Telle est la raison pour laquelle on recourt à des services de certification, souvent désignés comme « tiers de certification », qui disposent de la confiance de chacun et qui garantissent l'appartenance d'une signature à une personne. Comme le destinataire utilise la clé publique de l'expéditeur pour vérifier la signature électronique de ce dernier, la vérification suppose que le tiers certifie au destinataire que la clé publique qu'il utilise correspond bien à la clé privée de l'expéditeur signataire et que ce dernier est bien celui qu'il prétend être. Les tiers de certification délivrent donc des certificats d'authentification contenant, d'une part, divers renseignements sur la personne dont on souhaite vérifier l'identité (nom, prénom, date de naissance...), d'autre part, sa clé publique. Ces certificats sont généralement réunis dans des bases de données mises en ligne sur le réseau Internet, ce qui permet à chacun d'y accéder facilement.

« La signature numérique constitue donc un bloc de données créé à l'aide d'une clé privée ; la clé publique correspondante et le certificat permettent de vérifier que la signature provient réellement de la clé privée associée, qu'elle est bien celle de l'expéditeur et que le message n'a pas été altéré. »

Rapport de la mission d'information sur la nouvelle génération de documents d'identité, préc., p. 79-80

La fonctionnalité proposée par le présent article se substituerait, pour ceux qui l'utiliseraient, aux dispositifs précédents.

---

[1] *L'article 1316-4 du code civil, créée par la loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, reconnaît à la signature électronique la même valeur qu'à la signature matérielle de l'intéressé. Il précise qu'elle « consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État ».*

Son intérêt est évident : non seulement l'authentification électronique par la carte d'identité bénéficiera d'un fort degré de confiance, mais elle pourra être mise en œuvre facilement, puisqu'il suffira de connecter la carte à un lecteur électronique raccordé à l'ordinateur. Elle évitera en outre aux intéressés d'avoir à multiplier les codes de connexion ou les mots de passe.

Un système comparable, mis en place en Belgique à partir de 2004, a rencontré un grand succès, puisque la carte électronique a été diffusée à plus de neuf millions d'exemplaires.

Ce dispositif pourrait constituer, à l'avenir, un élément clé du développement de l'administration numérique et des services en ligne mis en place par l'État ou les collectivités territoriales au profit des citoyens.

Un point doit être souligné : si la puce « *vie quotidienne* » apportera une sécurité renforcée à certaines communications électroniques, celle-ci sera moindre que la sécurisation de l'identité permise par la puce régalienne : ni l'identification sur les réseaux de communication électronique, ni la signature électronique ne reposeront sur l'authentification de l'utilisateur de la carte par ses empreintes digitales.

- Des garanties nécessaires

M. Sébastien Huyghe, commissaire de la CNIL, a souligné lors de son audition que l'utilisation de la fonctionnalité d'identification ou de signature électronique impliquerait, techniquement, la mise en œuvre de certificats électroniques, enregistrés dans la puce « *vie quotidienne* », qui pourraient contenir un grand nombre de données à caractère personnel (noms, prénoms, sexe, date et lieu de naissance, adresse e-mail, adresses de résidences successives, photographie du titulaire, signature manuscrite numérisée, *etc.*).

C'est pourquoi il a jugé nécessaire de mettre en place des mécanismes de divulgation partielle des données, car l'utilisation de services en ligne ne nécessite pas systématiquement l'identification précise des personnes ou la communication de l'ensemble des données contenues dans les certificats. Ne seraient alors divulguées, au cours de la communication électronique, que les seules informations requises, selon la nature du service en ligne, pour assurer les vérifications préalables utiles à sa mise en œuvre (lieu de résidence, âge, nationalité, *etc.*).

Reprenant cette recommandation, votre commission a adopté un **amendement** de son rapporteur, prévoyant qu'à chaque utilisation de la carte, son titulaire décide des données transmises par voie de communication électronique.

La simplification des démarches en ligne et l'amélioration de leur sécurité que devrait autoriser le système proposé est opportune. Toutefois sauf à rendre pratiquement obligatoire, un dispositif juridiquement optionnel, il faut veiller à ce que nul ne puisse se voir refuser l'accès à un service donné ni opposer un refus de vente pour le seul motif qu'il ne possède pas une carte d'identité incluant la fonction d'identification électronique. À défaut, comme

l'ont souligné MM. Alain Grimfeld et Jean-Claude Ameisen, respectivement président et membre du comité consultatif national d'éthique (CCNE), une fonctionnalité conçue pour faciliter la vie des citoyens pourrait devenir paradoxalement un instrument d'exclusion. Votre commission a pour cette raison adopté un **amendement** de son rapporteur interdisant que l'accès aux transactions ou services en ligne puisse être conditionné à l'utilisation de la fonctionnalité d'identification électronique de la carte.

Votre commission a adopté l'article 3 **ainsi modifié**.

Article 4

Contrôle des documents d'état civil fournis à l'appui d'une demande de délivrance de CNI ou de passeport

Le présent article vise à prévoir que les agents chargés du recueil ou de la délivrance des titres d'identité procèdent, si nécessaire, à la vérification des données d'état civil apportées par le demandeur du titre – lequel en est informé – auprès des officiers d'état civil dépositaires de ces actes. Un décret en Conseil d'État préciserait les conditions dans lesquelles cette vérification s'opérerait.

Ce dispositif vise à répondre à l'une des défaillances majeures de la chaîne de l'identité : la facilité avec laquelle les fraudeurs peuvent obtenir des copies ou des extraits d'actes d'état civil d'autres personnes pour les produire ensuite, falsifiés, à l'appui d'une demande de titre d'identité au nom de l'intéressé. Prévoir que l'administration vérifie, en tant que de besoin, auprès de l'officier d'état civil dépositaire de l'acte, que la copie est conforme ou qu'elle a été délivrée à la bonne personne devrait permettre de rendre plus difficile la fraude initiale à l'identité.

D'ores et déjà l'administration s'est engagée dans cette voie, puisque le décret n° 2004-1159 du 29 octobre 2004[1], puis, plus récemment, le décret n° 2011-167 du 10 février 2011[2], autorisent les services compétents à faire procéder à cette vérification pour les dossiers qu'elles instruisent, sans limiter cette possibilité aux seuls titres d'identité.

Ces dispositions réglementaires et la disposition législative sont donc convergentes, le présent article faisant toutefois obligation aux services de procéder à la vérification en tant que de besoin, alors que le décret n'ouvre qu'une faculté.

Votre commission a adopté l'article 4 **sans modification**.

---

[1] *Décret n° 2004-1159 du 29 octobre 2004 portant application de la loi n° 2002-304 du 4 mars 2002 modifiée relative au nom de famille et modifiant diverses dispositions relatives à l'état-civil.*

[2] *Décret n° 2011-167 du 10 février 2011 instituant une procédure de vérification sécurisée des données à caractère personnel contenues dans les actes de l'état civil.*

Article 5

Fichier central biométrique des cartes nationales d'identité et des passeports

Le présent article autorise la **création d'un fichier central contenant l'ensemble des données requises pour la délivrance du passeport et de la carte nationale d'identité**, notamment celles qui seront inscrites sur le composant électronique de ces titres d'identité (état civil du titulaire, données biométriques, domicile).

Ce fichier serait créé dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Dans la mesure où il inclura des données biométriques, il relèvera de l'article 27 de cette loi qui impose qu'il soit autorisé par décret en Conseil d'État, pris après avis motivé et publié de la CNIL, ce que prévoit d'ailleurs l'article 6 du présent texte.

Les finalités assignées au fichier sont doubles :

- préserver l'intégrité des données requises pour la délivrance des passeports et CNI ;

- permettre l'établissement et la vérification des titres dans des conditions garantissant l'intégrité et la confidentialité des données personnelles des demandeurs de titre.

En l'absence d'autres précisions, il reviendrait au pouvoir réglementaire de décider comment sera constituée cette base de données. Or, un tel choix est susceptible de permettre ou non des usages différents de ceux initialement prévus.

Il n'existe actuellement pas de fichier biométrique central aussi important que celui prévu par le présent article. Seul le fichier TES de gestion des passeports biométriques, précédemment présenté[1], s'en approche. Votre rapporteur observe que le texte qui l'a institué rend possible son utilisation pour d'autres buts que la seule lutte contre la fraude documentaire, comme la lutte contre le terrorisme. Certes, dans ce dernier cas, une disposition expresse du texte créant le fichier rend les services compétents destinataires des informations qu'il contient. Cependant, même en l'absence d'une telle disposition, l'autorité judiciaire a toujours la possibilité de demander à utiliser le fichier à des fins d'enquête.

Un tel usage d'une base biométrique nationale portant sur toute la population française est-il ou non légitime, alors que cette base n'est initialement créée que pour améliorer la lutte contre la fraude à l'identité ? La possible utilisation d'un fichier de cette ampleur à des fins d'investigation policière assure-t-elle une conciliation équilibrée et proportionnée entre les exigences de protection de la liberté individuelle et de respect de la vie privée et les impératifs de sécurité publique ?

---

[1] Cf. supra*, au II)A) de l'exposé général.*

À l'initiative de son rapporteur, votre commission a jugé nécessaire d'exclure toute possibilité d'utilisation du fichier biométrique central à des fins de recherche criminelle, par l'identification d'une personne à partir des ses données biométriques, et d'en limiter l'usage à la seule lutte contre la fraude documentaire.

Or, ainsi qu'il a été précisé dans l'exposé général, les garanties qui peuvent être apportées en la matière sont de deux ordres : juridiques et matérielles. Un **amendement** de votre rapporteur, adopté par la commission, propose de doubler les garanties juridiques par des garanties matérielles, afin de rendre l'utilisation du fichier pour identifier une personne à partir de ces seules empreintes digitales juridiquement et techniquement impossible.

Il prévoit que la base biométrique qui sera créée soit conçue selon la technologie des bases biométriques dites « *à lien faible* », déjà évoquée par la mission d'information de la commission des lois sur la nouvelle génération de documents d'identité et la fraude documentaire[1], qui constitue la garantie matérielle la plus solide, puisqu'elle interdit qu'un lien univoque soit établi entre une identité civile et les empreintes digitales de l'intéressé.

Plusieurs dizaines ou centaines de milliers d'empreintes sont associées à plusieurs dizaines ou centaines de milliers d'identités sans qu'un lien soit établi entre une de ces empreintes et l'une de ces identités. Nul ne peut en conséquence être identifié à partir de ses seules empreintes digitales, ce qui interdit l'utilisation du fichier à des fins de recherche criminelle, en l'absence d'autres indices impliquant l'intéressé.

En revanche, cette technologie permet de s'assurer de l'identité d'un individu, par la comparaison entre l'identité qu'il allègue et les éléments biométriques associables à cette identité. Les chances pour qu'un individu qui souhaiterait usurper l'identité d'une autre personne possède des empreintes biométriques correspondant à celles susceptibles d'être associées à l'identité en cause sont en effet très faibles et inférieures à 1 %. L'usurpation devient impossible, car trop risquée.

Ce dispositif assure donc le respect de la finalité unique pour laquelle la création du fichier est demandée, garantir la fiabilité des documents d'identité et la lutte contre la fraude, en empêchant toute utilisation à d'autres fins.

Constatant que le présent article excluait que l'identification d'une personne puisse être effectuée par un dispositif de reconnaissance faciale, votre commission a par ailleurs jugé souhaitable de faire bénéficier le visage de la même garantie que les empreintes digitales en prévoyant que l'image numérisée du visage ne soit pas liée par un lien univoque à l'identité de l'intéressé, ce qui interdit matériellement toute identification d'une personne par reconnaissance faciale.

---

[1] *Rapport de la mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire,* op. cit.*, p. 65.*

Enfin, elle a ajouté aux garanties juridiques relatives au fonctionnement du fichier une exigence de traçabilité des consultations et des modifications effectuées par les personnes y ayant accès.

Votre commission a adopté l'article 5 **ainsi rédigé**.

Article 5 bis *(nouveau)*

Modalités du contrôle d'identité à partir du titre d'identité

Le présent article, qui résulte d'un **amendement** du rapporteur, adopté par la commission, vise à éviter que la base centrale soit utilisée systématiquement pour authentifier l'identité du détenteur du titre d'identité.

La vérification d'identité ne s'effectuerait qu'à partir des données imprimées sur la carte ou inscrite dans la puce électronique. Ainsi l'intéressé conserverait la maîtrise de ses données biométriques, puisqu'elles ne seraient liées de manière univoque à son identité que sur le titre biométrique qu'il a en sa possession (dans la base centrale à lien faible, les identités ne seraient pas liées de manière univoques aux biométries). Cette disposition traduit une recommandation constante de la CNIL, qui considère légitime le recours à des dispositifs de reconnaissance biométrique pour s'assurer de l'identité d'une personne, dès lors que les données biométriques sont conservées sur un support dont la personne à l'usage exclusif[1].

Le présent article réserve toutefois la possibilité pour les agents chargés d'effectuer le contrôle d'identité de consulter la base centrale, en cas de doute sérieux sur l'identité alléguée ou s'ils constatent que le titre est susceptible d'avoir été falsifié, contrefait ou altéré. Le fichier central ayant pour finalité de permettre la détection des fraudes, son utilisation dans de telles circonstances est opportune.

Enfin, à l'initiative de son rapporteur, votre commission a souhaité limiter aux seuls agents habilités à cet effet, la possibilité de lire les empreintes digitales inscrites sur le titre d'identité pour s'assurer qu'elles correspondent à celles du porteur du titre. En dehors de contrôles d'identité effectués par ces agents habilités, nul ne pourrait être contraint, pour prouver son identité, de présenter ses empreintes digitales pour qu'elles soient comparées à celles enregistrées sur la carte d'identité ou le passeport.

Votre commission a adopté l'article additionnel 5 *bis* **ainsi rédigé**.

Article 5 ter *(nouveau)*

Information sur la validité des titres d'identité présentés

Le présent article, issu d'un **amendement** du rapporteur adopté par la commission, tend à autoriser la consultation, par les administrations publiques et certains opérateurs économiques spécialement habilités, à consulter le

---

[1] *CNIL, délibération n° 2007-368 du 11 décembre 2007 portant avis sur un projet de décret en Conseil d'État modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques.*

fichier central pour s'assurer de la validité ou non du titre d'identité qui leur est présenté.

Ce dispositif s'inspire de celui applicable, avec le fichier national des chèques irréguliers (FNCI), aux chèques perdus et volés. Ceux auxquels ils sont présentés aux fins de paiement peuvent ainsi connaître leur statut et refuser de les encaisser s'ils sont déclarés non valides. Il traduit une recommandation formulée par la mission d'information de la commission des lois sur la nouvelle génération de documents d'identité et la fraude documentaire[1], qui n'avait jamais été mise en œuvre.

Votre commission a adopté l'article additionnel 5 *ter* **ainsi rédigé**.

Article 6

Modalités réglementaires d'application

Le présent article précise que les modalités d'application de la proposition de loi, dont les modalités et la date de mise en œuvre de la fonctionnalité d'identification électronique prévue à l'article 3, seront fixées par décret en Conseil d'État pris après avis de la CNIL.

Il s'agit là, en ce qui concerne la création du fichier prévu à l'article 5, de l'application de l'article 27 de la loi précitée « *informatique et libertés* » qui prévoit que les fichiers portant sur l'identification ou l'authentification d'une personne à partir de données biométriques doivent être autorisés par décret en Conseil d'État pris après avis de la CNIL.

Le texte d'application devra en particulier préciser, conformément aux dispositions de l'article 29 de la loi précitée :

- la dénomination et la finalité du traitement ;

- le service auprès duquel s'exerce le droit d'accès de l'intéressé à ces données personnelles ;

- les catégories de données à caractère personnel enregistrées ;

- les destinataires ou catégories de destinataires habilités à recevoir communication de ces données ;

- le cas échéant, les dérogations à l'obligation d'information de l'intéressé sur la finalité et les modalités d'utilisation du fichier.

Votre commission a adopté l'article 6 **sans modification**.

Article 7

(art. 323-1, 323-2 et 23-3 du code pénal)

Dispositions pénales

Le présent article tend à aggraver la répression pénale des infractions d'accès, d'introduction, de maintien frauduleux dans un système de traitement

---

[1] *Rapport de la mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire,* op. cit.*, p. 48.*

automatisé de données à caractère personnel, d'entrave à son fonctionnement ou de modification ou de suppression frauduleuse des données qu'il contient, lorsque ces faits sont commis à l'encontre d'un système de traitement automatisé mis en œuvre par l'État.

Ces infractions sont actuellement punies de peines d'emprisonnement de deux à cinq ans et de peines d'amende de 30 000 à 75 000 euros. Ces peines seraient portées à cinq ans et 300 000 euros d'amende.

Votre commission a souhaité maintenir une cohérence entre le quantum des peines d'emprisonnement et d'amende encourues. Elle a adopté un amendement de son rapporteur ramenant l'amende à 75 000 euros.

Votre commission a adopté l'article 7 **ainsi modifié**.

Article 7 bis *(nouveau)*
Indication, dans les rectifications d'actes d'état civil consécutives à une usurpation de ce motif

Le présent article, qui résulte de l'adoption de deux amendements identiques de MM. Jean-René Lecerf et Bernard Frimat, apporte une solution à la difficulté à laquelle les personnes victimes d'usurpation d'identité se trouvent confrontées lorsqu'elles obtiennent, par jugement, l'annulation des actes d'état civil passés par l'usurpateur sous leur identité et la transcription de cette annulation en marge de leur acte de naissance.

Les règles de conservation intégrale des mentions portées à l'état civil, interdit de faire disparaître purement et simplement les mentions correspondant aux actes annulés. Le dispositif du jugement décidant l'annulation est porté en marge sans autre indication, ce qui ne permet pas de distinguer l'annulation dont la cause est l'usurpation de l'annulation pour un motif propre à la personne.

Le présent article résout cette difficulté en imposant que, lorsqu'un acte est annulé par le juge sur le fondement d'une usurpation d'identité, le dispositif du jugement dont la transcription est ordonnée à l'état civil, fasse référence à l'usurpation, ce qui permettra, à l'avenir, de distinguer entre les mentions portées en marge des registres d'état civil, celles qui ont pour cause la fraude et les autres.

Votre commission a adopté l'article 7 *bis* **ainsi rédigé**.

Articles 8 et 9
Application de la loi et gage

L'article 8 prévoit respectivement l'application du texte sur tout le territoire de la République et l'article 9 correspond au gage financier de la loi.

Votre commission a adopté ces articles **sans modification**.

*

* *

Votre commission a adopté la proposition de loi **ainsi rédigée**.

EXAMEN EN COMMISSION

Mercredi 13 avril 2011

M. François Pillet, rapporteur. – La fraude à l'identité recouvre notamment le vol de documents authentiques, la falsification d'un ou de plusieurs éléments de documents authentiques, la contrefaçon c'est-à-dire la reproduction totale de documents, l'obtention frauduleuse de documents authentiques, ou l'usage frauduleux de documents empruntés ou volés à un tiers.

Les données sur l'usurpation d'identité fournies aux médias par le Credoc n'ont pas été scientifiquement établies. Le chiffre de 210 000 cas a été obtenu en suivant une méthode unanimement critiquée : les enquêteurs ont interrogé 2 000 personnes, la question portant sur dix années -« avez-vous depuis 1999 été victime d'une usurpation d'identité ou d'un usage frauduleux de vos données personnelles ? » - et la réponse a été multipliée par la population française puis divisée par dix années. Le résultat est d'une fiabilité douteuse. Même s'il ne dispose pas encore des outils statistiques nécessaires, l'Observatoire national de la délinquance et de la réponse pénale a, quant à lui, fourni une évaluation plus précise du phénomène à partir de l'état 4001 transmis par les gendarmeries et les commissariats. Cette évaluation fait apparaître, pour 2009, 13 900 faits de fraude documentaire ou d'identité. La direction des affaires criminelles et des grâces indique qu'il y a eu cette année-là 11 627 condamnations pour de tels faits.

Au plan humain et personnel, il en résulte pour les victimes des situations parfois dramatiques ; les conséquences sont graves aussi pour l'État et les opérateurs économiques. Jusqu'à présent, les réponses apportées ont été parcellaires. M. Lecerf, dans le rapport de la mission d'information sur les titres d'identité de 2005, soulignait que la fraude documentaire profite des défaillances de la chaîne de l'identité. Toutes les garanties de sécurité ne sont pas réunies. Les moyens de détection de la fraude doivent être améliorés. Notre collègue avait préconisé des solutions simples, toutes n'ont pas été mises en œuvre.

Comment assurer une meilleure sécurité ? Qu'apporte la biométrie ? Comment protéger des données personnelles aussi sensibles que les données biométriques ? Quelle est la fiabilité des nouveaux systèmes ? La biométrie peut avoir trois usages. Elle peut servir à l'identification dans le cadre de recherches criminelles : tel est l'objet des fichiers automatisés des empreintes digitales et génétiques. Elle peut être utilisée pour contrôler l'accès à certains lieux, réservés aux personnes dont les empreintes ou le visage ont été reconnus. Enfin, elle permet de s'assurer que l'identité de celui qu'on contrôle est bien celle qu'il allègue.

Aucun des projets de loi rédigés sur le sujet par les gouvernements successifs n'ont finalement été présentés au Parlement. En particulier, le projet d'identité nationale électronique sécurisée (Ines) n'a pas abouti. Il fusionnait les procédures de délivrance et de gestion de la carte d'identité et du passeport ; un fichier central d'identité était créé. Il n'y a jamais eu de suite.

Le passeport biométrique a toutefois été mis en place, conformément à nos engagements internationaux et européens. Cependant, le décret, je le rappelle, fait l'objet de critiques. Il a été contesté devant le Conseil d'État, lequel ne s'est pas encore prononcé.

Il n'y a pas de modèle commun en Europe : la carte d'identité est facultative en Allemagne, elle n'existe pas au Royaume-Uni, elle est obligatoire en Espagne, en Belgique ; la collecte des empreintes est facultative en Allemagne, elle n'existe pas au Royaume-Uni, elle est obligatoire en Espagne, en Italie.

Le sujet engage aussi des enjeux économiques, industriels : la sécurisation des échanges électroniques est un marché ; les collectivités, les administrés paient le coût de ces titres biométriques. Les entreprises françaises, en pointe sur ce domaine, veulent investir le marché français.

Il convient de concilier les libertés individuelles et la sécurité publique. Pour la CNIL, « les données biométriques ne sont pas des données personnelles comme les autres ». Elle n'a pas émis de contre-indication à l'usage des données biométriques mais elle recommande de veiller à une proportionnalité entre les objectifs, les moyens mis en œuvre, les atteintes possibles aux libertés individuelles.

Mes amendements sont inspirés par le rapport Lecerf de 2005. Le législateur doit encadrer la finalité du fichier pour en éviter le détournement. L'utilisation de la biométrie n'est pas contestée si l'intéressé conserve la maîtrise des données servant à son identification. L'expérience du passeport biométrique n'a pas soulevé de difficultés.

Faut-il un fichier central des identités biométriques ? Pour protéger les identités, il faut une banque de données grâce à laquelle on puisse vérifier les données sur une carte d'identité qui pourrait être falsifiée et détecter les usurpateurs. Le fichier est bien l'élément de lutte le plus efficace.

Quelle finalité assigner à ce fichier ? C'est le cœur du débat. Une base d'empreintes digitales peut être exploitée pour vérifier qu'une seule personne n'a pas deux identités ; mais aussi, pour identifier un criminel d'après les empreintes laissées sur la scène de crime. Obtenir une identité à partir d'une empreinte, grâce à un fichier général, pose cependant un problème de libertés publiques. La proposition de loi tend à créer un fichier consacré à la gestion et la sécurisation des titres et je proposerai par amendement de le limiter à cet objet.

Comment ? Les garanties juridiques, comme le respect de la loi informatique et libertés et l'autorisation d'accès au fichier délivrée par un magistrat, ne sont pas suffisantes. Le rapport Lecerf recommandait des garanties matérielles. Sur le plan informatique, une première solution est celle du lien unidirectionnel. Si le lien est unidirectionnel entre l'identité et la donnée biométrique, on ne peut interroger la base qu'à partir de l'identité. Mais le lien peut à tout moment être rendu bidirectionnel, si le législateur change d'avis. C'est pourquoi nous avons retenu une autre technique, celle du lien faible. Les données concernant une personne ne sont pas stockées dans un casier réservé à elle seule. Si chaque casier comprend 100 000 personnes, l'identification à partir d'une donnée biométrique devient impossible. Une empreinte relevée sur une scène de crime ne désignera pas une personne, mais une liste de 100 000 noms. En revanche, il est possible de confondre

un usurpateur en confrontant ses empreintes et celles correspondant à l'identité usurpée.

M. Jean-Pierre Sueur. – Le fichier ne pourra être utilisé par la justice pénale.

M. François Pillet, rapporteur. – Non. Il aura un objet unique, sécuriser les identités. Le fichier des empreintes génétiques est surexploité par rapport à la volonté initiale du législateur. Donc, je vous propose d'introduire cette garantie technique à l'article 5. Pour le reste, je vous propose de suivre M. Lecerf.

M. Jean-René Lecerf, auteur de la proposition de loi. – Il y a six ans, la commission des lois m'a lancé sur le sujet en me confiant une mission que j'ai assurée avec M. Charles Guené, portant sur la fraude documentaire. Nous avions intitulé notre rapport *Identité intelligente et respect des libertés*. Mais depuis 2005, il ne s'est rien passé. Nous avions accéléré la remise du rapport afin de ne pas être devancés par le projet de loi Ines. La technologie était alors préhistorique et la France était en avance sur les autres pays européens, mais elle a aujourd'hui pris un retard considérable. Les entreprises françaises sont en pointe mais elles ne vendent rien en France, ce qui les pénalise à l'exportation par rapport aux concurrents américains.

Le nombre des usurpations d'identité croît sans cesse. Le gouvernement a estimé que le travail du Credoc n'était pas fiable, mais la méthode des enquêteurs est similaire à celle des instituts de sondage. La question – restrictive – a abouti à 210 000 réponses positives. Le ministère, lui, n'a pas de données sur la question puisqu'il n'y a pas d'incrimination spécifique pour usurpation d'identité ; celle-ci est généralement suivie d'escroquerie – mais toute escroquerie ne commence pas par une telle usurpation.

Il s'agit d'un sport très facile à pratiquer. Je me demande pourquoi certains délinquants persistent à braquer des banques quand il est si simple d'usurper une identité. Une poubelle sur dix contient les éléments suffisants pour s'attribuer l'identité d'un membre du foyer. On y trouvera de quoi demander un document d'état civil, à partir duquel on obtiendra une vraie-fausse carte d'identité. Grâce à celle-ci on ouvrira un compte bancaire, que l'on approvisionnera faiblement. On demandera un prêt ; on l'obtiendra et c'est un autre qui le remboursera. Et tout cela quasiment sans risque ! S'il n'y a pas 210 000 usurpations d'identité aujourd'hui, il y en aura beaucoup plus avant longtemps. L'usurpation d'identité sur Internet est également en croissance continue.

Les conséquences sont sans gravité lorsque l'identité est imaginaire ou appartient à une personne décédée, mais calamiteuses quand il s'agit d'une personne vivante dont l'identité est volée et revendue, peut-être à dix personnes… La victime ne pourra plus quitter le territoire. Elle ne pourra plus se marier, elle est réputée l'être déjà. Elle sera condamnée pour autrui, son nom sera porté au casier judiciaire national. Des individus ont aussi pu travailler dans les aéroports, près des avions, avec une fausse identité. La victime sera privée de chéquier, elle subira une interdiction bancaire. Dans certains cas, tout cela se termine par un suicide.

La réponse la plus judicieuse est la biométrie. M. Guené et moi-même avons rencontré en 2005 des parlementaires américains qui nous ont dit : si vous n'avez pas de passeport biométrique, vous n'entrerez plus aux États-Unis. Les

empreintes digitales sont inscrites sur une puce dans la carte d'identité, et l'Imprimerie nationale qui confectionne les passeports pourrait aussi bien fabriquer des cartes d'identité biométriques qui règleraient le problème de l'usurpation d'identité. Le système le plus élémentaire est la biométrie sans base centrale : le douanier, le gendarme, le responsable d'une agence bancaire peut comparer les empreintes de la personne et celles gravées dans le titre d'identité. Cette comparaison autorise une authentification, non une identification, puisque la personne peut avoir d'autres identités.

Mais comme la multiplication des identités est fréquente dans les entreprises terroristes, par exemple, nous voulons aller plus loin : le douanier, le gendarme doivent être certains que la personne est bien celle à qui la carte a été délivrée ; et que cette personne n'est pas enregistrée sous d'autres identités. Alors on peut parler d'identification.

Or pour cela, il faut une base de données. Il revient au législateur d'en définir l'étendue, l'utilisation, l'architecture. Une base à lien faible sert à vérifier l'unicité de l'identité d'une personne. Sera-t-il possible d'identifier des personnes âgées désorientées, des enfants perdus ? En tout cas, l'utilisation dans le cadre des enquêtes criminelles est écartée. L'objectif visé est de mettre un terme aux usurpations d'identité sans méconnaître les libertés publiques. En 2005, l'argument essentiel contre ce type de fichier était qu'il aurait interdit, entre 1940 et 1944, la fabrication de fausses identités. C'était la seule objection.

Le ministère de l'intérieur sera tenté d'aller au-delà. Précisément, bâtir un système à lien faible nous assure que jamais le fichier ne pourra être exploité à d'autres fins que la vérification d'identité.

Le Gouvernement souhaite aussi qu'en option, figure sur la carte d'identité une seconde puce portant la signature électronique de la personne, autorisant l'authentification à distance, ce qui remplacerait le recours à des sociétés commerciales.

M. Bernard Frimat. – Comment, si un rapprochement vous conduit à un tiroir de 100 000 noms, pouvez-vous conclure à l'usurpation ?

M. François Pillet, rapporteur. – Par la confrontation de l'identité alléguée, des empreintes digitales susceptibles d'y correspondre et de celles de l'usurpateur : le croisement des informations conduit éventuellement à une alerte à l'usurpation. La police ne pourra utiliser le fichier que si elle dispose déjà d'autres renseignements, mais non si elle dispose uniquement d'une empreinte. Nous ne voulons pas laisser derrière nous une bombe : c'est pourquoi nous créons un fichier qui ne peut être modifié.

M. Yves Détraigne. – Le phénomène des usurpations d'identité s'accroîtra dans l'avenir.

M. Jean-Jacques Hyest, président. – L'usurpation est plus rentable que le trafic de drogue !

M. Yves Détraigne. – Il faut vivre avec son temps. Nous avions présenté, Mme Escoffier et moi-même, une proposition de loi sur la protection de la vie privée face à l'essor du numérique. Car les petits génies de l'informatique, les *hackers*, se

font fort de voler l'identité des personnes comme de pénétrer dans les ordinateurs centraux de Bercy. Mais notre rapporteur a raison de ne pas nous proposer une solution qui autoriserait tous les recoupements.

M. Jean-Pierre Sueur. – Je rends hommage à MM. Pillet et Lecerf qui montrent un extrême respect des libertés. Nous y sommes tous attachés, comme à la sécurité publique.

Vous excluez totalement que dans le cours d'une enquête criminelle, la police sous le contrôle de la justice puisse avoir recours à ce fichier, me semble-t-il.

M. François Pillet, rapporteur. – Elle a accès à d'autres fichiers, pas à celui-là. Elle consulte le fichier des empreintes digitales et génétiques qui comprend des données relatives à ceux qui ont été condamnés ou impliqués dans des affaires criminelles.

M. Jean-Pierre Sueur. – La tentation existera et je prends acte de votre position : le seul délit que le fichier servira à détecter est l'usurpation d'identité.

M. François Pillet, rapporteur. – La tentation existe déjà ! Le ministère de l'intérieur n'est pas d'accord avec mon amendement à l'article 5. Mais j'ai souhaité vous le proposer.

M. Jean-Pierre Sueur. – Je m'y rallie.

M. Jean-René Lecerf. – La question posée par notre collègue Sueur est la question centrale. C'est à nous, le législateur, de décider et, par exemple, d'ajouter les protections juridiques afin de détecter toute exploitation indue de cet outil. La traçabilité de l'utilisateur du fichier est possible, il suffit de présenter ses empreintes digitales.

Ce que déplore le ministère de l'intérieur, c'est le choix du lien faible, qui interdit tout retour en arrière, tout changement de cap.

M. Bernard Frimat. – L'Assemblée nationale amendera …

M. Jean-Pierre Sueur. – Et la vertu sénatoriale n'y résistera pas.

M. Jean-Paul Amoudry. – La loi du 1er juillet 2010 de lutte contre le surendettement a créé un fichier positif, une centrale de crédit en fait, qui comprendra les noms de 30 à 40 millions de personnes. Cela pose un problème de protection des données. Je suis le délégué de la Cnil au comité qui travaille sur ce futur fichier. Le seul moyen d'identification qui ait été jugé possible est le numéro de sécurité sociale, dont l'usage jusqu'à présent était réservé à la sécurité sociale. Le montage est d'une invraisemblable complexité. Si un titre d'identité sécurisé était mis en service rapidement, cela serait très utile pour la centrale de crédit !

M. Jean-Jacques Hyest, président. – Le numéro de sécurité sociale est le numéro Insee, très facile à recomposer…

M. Jean-Paul Amoudry. – Mais il est protégé et ne peut être utilisé dans d'autres domaines que celui de la sécurité sociale.

EXAMEN DES AMENDEMENTS

Article 3

M. François Pillet, rapporteur. – Si nous inscrivons dans le texte une option de seconde puce, il est bon de veiller à ce que le titulaire de la carte reste maître des données qu'il choisit de transmettre. C'est l'objet de l'amendement n° 6.

L'amendement n° 6 est adopté.

M. François Pillet, rapporteur. – L'amendement n° 8 veille à ce que les administrations et les sociétés commerciales ne puissent refuser une prestation à qui refuse l'identification électronique, que nous créons comme une simple faculté.

L'amendement n° 8 est adopté. L'article 3 est adopté dans la rédaction issue des travaux de la commission.

Article 5

M. François Pillet, rapporteur. – L'amendement n° 9 vise à renforcer la protection juridique en organisant une traçabilité des consultations du fichier.

L'amendement n° 9 est adopté.

M. François Pillet, rapporteur. – Pour créer le fichier biométrique à lien faible, la technologie existe, il s'agit d'un brevet Sagem. La traçabilité du visage sera bientôt une réalité, il faut donc prévoir les mêmes garanties pour le visage et pour les empreintes digitales. Tel est l'objet de l'amendement n° 7.

L'amendement n° 7 est adopté.

L'article 5 est adopté dans la rédaction issue des travaux de la commission.

Article additionnel après l'article 5

M. François Pillet, rapporteur. – Le contrôle de l'identité doit se faire en circuit fermé, à partir du document lui-même.

L'amendement n° 3 rectifié bis est adopté et devient un article additionnel après l'article 5.

M. François Pillet, rapporteur. – L'amendement n° 4 tend à autoriser les administrations et certains opérateurs économiques à vérifier la validité de la carte d'identité présentée.

L'amendement n° 4 est adopté et devient un article additionnel après l'article 5.

Article 7

M. François Pillet, rapporteur. – L'amendement n° 5 tend à mettre en cohérence les quantums de peines et d'amendes.

M. Jean-René Lecerf. – Qui, curieusement, ne sont pas très élevés.

L'amendement n° 5 est adopté.

L'article 7 est adopté dans la rédaction des travaux de la commission.

Article additionnel après l'article 7

M. François Pillet, rapporteur. –Avis favorable aux amendements identiques n° 1 de M. Frimat et n° 2 de M. Lecerf. Lorsque la victime d'une usurpation d'identité parvient enfin au terme de son périple judiciaire, après tant d'années, ses documents d'état civil comportent des mentions telles que l'annulation d'un mariage contracté en réalité par l'usurpateur : le motif de la décision -l'usurpation dont elle a été victime- n'est pas mentionné, c'est une lacune. Je demande aux auteurs de rectifier leurs amendements pour remplacer le terme de « circonstance » par celui de « motif ».

M. Bernard Frimat. – Oui !

M. Jean-René Lecerf. – D'accord.

Les amendements n°s 1 rectifié et 2 rectifié sont adoptés et deviennent un article additionnel.

La proposition de loi est adoptée dans la rédaction issue des travaux de la commission.

Le sort des amendements examinés par la commission est retracé dans le tableau suivant :

Auteur	N°	Objet	Sort de l'amendement
Article 3 Utilisation optionnelle de la CNI à des fins d'identification sur les réseaux de communication électronique et de signature électronique			
M. PILLET, rapporteur	8	Interdiction de faire dépendre l'accès à un service de l'utilisation de la fonctionnalité électronique de la carte d'identité	**Adopté**
M. PILLET, rapporteur	6	Maîtrise, par l'intéressé, des données de la carte électronique faisant l'objet d'une transmission	**Adopté**
Article 5 Fichier central des CNI et des passeports			
M. PILLET, rapporteur	9	Traçabilité des consultations et modifications de la base centrale	**Adopté**
M. PILLET, rapporteur	7	Construction de la base centrale selon le modèle du "lien faible"	**Adopté**
Articles additionnels après l'article 5			
M. PILLET, rapporteur	3	Principe selon lequel le contrôle d'identité est effectué à partir des informations inscrites sur le titre d'identité	**Adopté**
M. PILLET, rapporteur	4	Fichier central de la validité des titres d'identité	**Adopté**

Auteur	N°	Objet	Sort de l'amendement
Article 7 Dispositions pénales			
M. PILLET, rapporteur	5	Harmonisation des peines d'emprisonnement et d'amende encourues	**Adopté**
Articles additionnels après l'article 7			
M. FRIMAT	1	Rectification de l'état civil des personnes victime d'usurpation d'identité	**Adopté avec modification**
M. LECERF	2	Rectification de l'état civil des personnes victimes d'usurpation d'identité	**Adopté avec modification**

ANNEXE
LISTE DES PERSONNES ENTENDUES

- M. Jean-René Lecerf, auteur de la proposition de loi

Ministère de la justice et des libertés

- M. François Capin-Dulhoste, sous-directeur de la justice pénale générale

- M. François Ancel, sous-directeur du droit civil

Ministère de l'intérieur

- **M. Laurent Marcadier**, conseiller affaires juridiques

- **M. Cyril Maillet**, conseiller technique

- **M. Laurent Touvet**, directeur des libertés publiques et des affaires juridiques (DLPAJ)

- M. Raphaël Bartolt, directeur de l'agence nationale des titres sécurisés (ANTS)

- **M. Gérard Bonningue**, responsable du département « Titres et identités » à l'agence nationale des titres sécurisés

- **M. Michel Bergue**, chef de mission pour la prévention et lutte contre la fraude documentaire

Conseil national des barreaux

- **M. Richard Sedillot**, avocat à la Cour, vice-président de la commission Libertés et Droits de l'homme

CNIL

- **M. Sébastien Huyghe**, député et commissaire de la CNIL

- M. Émile Gabrié, service des affaires juridiques

Observatoire national de la délinquance et des réponses pénales

- **M. Cyril Rizk**, responsable des statistiques

Ligue des droits de l'homme

- **M. Jean-Claude Vitran**

GIXEL (groupement professionnel des industries de composants et de systèmes électroniques)

- M. Didier Chaudun, Président du Gixel, Morpho

- Mme Marie Figarella, Gemalto

- M. Frédéric Trojani, Gemalto

- M. Pierre Aubry Imprimerie nationale

- M. Antoine Paoli, Imprimerie nationale

- M. Michel Bartosik, Inside Secure

- M. Bernard Didier, Morpho

- Mme Carole Pellegrino, Morpho

- M. Xavier Fricout, Oberthur

- M. Alban Feraud, Oberthur

- M. Philippe Lauri, SPS Technologies

- Mme Annick Alligier, ST Microelectronics

- M. Laurent Sourgen, ST Microelectronics

- M. Philippe Karnaugh, Thales

CCNE

- **M. Alain Grimfeld**, président

- M. Jean-Claude Ameisen

Contributions écrites

- **M. Jacques Pélissard**, président de l'association des Maires de France

- **M. Benoît Parlos**, délégué national à la lutte contre la fraude

TABLEAU COMPARATIF

___

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
	Proposition de loi relative à la protection de l'identité	**Proposition de loi relative à la protection de l'identité**
	Article 1er	Article 1er
	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.	*(Sans modification).*
	Article 2	Article 2
	La carte nationale d'identité et le passeport comportent un composant électronique sécurisé contenant les données suivantes :	*(Sans modification).*
	a) Le nom de famille, le ou les prénoms, le sexe, la date et le lieu de naissance du demandeur ;	
	b) Le nom dont l'usage est autorisé par la loi, si l'intéressé en a fait la demande ;	
	c) Son domicile ;	
	d) Sa taille et la couleur de ses yeux ;	
	e) Ses empreintes digitales ;	
	f) Sa photographie.	
	Les dispositions du présent article ne s'appliquent pas au passeport délivré selon une procédure d'urgence.	
	Article 3	Article 3
	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 oeuvre sa signature électronique.	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

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
		d'identification transmises par voie électronique.
Code de la consommation		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 service 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.
Art. L. 122-1. — Il est interdit de refuser à un consommateur la vente d'un produit ou la prestation d'un service, sauf motif légitime, et de subordonner la vente d'un produit à l'achat d'une quantité imposée ou à l'achat concomitant d'un autre produit ou d'un autre service ainsi que de subordonner la prestation d'un service à celle d'un autre service ou à l'achat d'un produit.		L'accès aux services d'administration électronique mis en place par l'Etat, 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.
Cette disposition s'applique à toutes les activités visées au dernier alinéa de l'article L. 113-2.		
Pour les établissements de crédit, les établissements de paiement et les organismes mentionnés à l'article L. 518-1 du code monétaire et financier, les règles relatives aux ventes subordonnées sont fixées par le 1 du I de l'article L. 312-1-2 du même code.		
Code monétaire et financier		
Art. L. 311-1. — Les opérations de banque comprennent la réception de fonds du public, les opérations de crédit, ainsi que les services bancaires de paiement.		
	Article 4	Article 4
	Les agents chargés du recueil ou de l'instruction des demandes de délivrance de la carte nationale d'identité ou du passeport font, en tant que de besoin, procéder à la vérification des données de l'état civil fournies par l'usager auprès des officiers de l'état civil dépositaires de ces actes dans des conditions fixées par décret en Conseil d'État.	*(Sans modification).*
	Le demandeur en est préalablement informé.	

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
	Article 5	Article 5
	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.	*(Alinéa sans modification).*
	Ce traitement, mis en oeuvre par le ministère de l'intérieur, permet l'établissement et la vérification des titres dans des conditions garantissant l'intégrité et la confidentialité des données à caractère personnel.	Ce traitement, mis en œuvre par le ministère de l'Intérieur, permet l'établissement et la vérification des titres 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'enregistrement des empreintes digitales et de l'image numérisée du visage du demandeur est réalisé de manière telle qu'aucun lien univoque ne soit établi entre elles, ni avec les données mentionnées aux *a* à *d* de l'article 2, et que l'identification de l'intéressé à partir de l'un ou l'autre de ces éléments biométriques ne soit pas possible.
	~~L'identification du demandeur ne peut s'y effectuer qu'au moyen~~ des données ~~énumérées~~ aux *a)* à ~~*e)*~~ de l'article 2.	La vérification de l'identité du demandeur s'opère par la mise en relation de l'identité alléguée et des autres données mentionnées aux *a* à *f* de l'article 2.
		Article 5 bis (nouveau)
		La vérification de l'identité du possesseur de la carte nationale d'identité ou du passeport est effectuée à partir des données inscrites sur le document lui-même ou sur le composant électronique sécurisé mentionné à l'article 2.
		Sont seuls habilités à procéder à cette vérification à partir des données mentionnées au *e* de l'article 2, les agents habilités à cet effet dans des

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
		conditions définies par décret en conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés. En cas de doute sérieux sur l'identité de la personne, ou lorsque le titre présenté est défectueux ou paraît endommagé ou altéré, la vérification d'identité peut être effectuée en consultant les données conservées dans le traitement prévu à l'article 5.
		Article 5 ter (nouveau) Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, définit les conditions dans lesquelles le traitement prévu à l'article 5 peut être consulté par les administrations publiques et certains opérateurs économiques spécialement habilités à cet effet, pour s'assurer de la validité de la carte nationale d'identité ou du passeport français présentés par son titulaire pour justifier de son identité.
	Article 6	Article 6
	Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, fixe les modalités d'application de la présente loi. Il définit notamment les modalités et la date de mise en oeuvre des fonctions électroniques mentionnées à l'article 3.	*(Sans modification).*
	Article 7	Article 7
Code pénal	~~Le code pénal est ainsi modifié :~~	**Alinéa supprimé.**
	~~1° L'article~~ 323-1 ~~est complété~~ par un alinéa ainsi rédigé :	Les articles 323-1, 323-2 et 323-3 du code pénal sont complétés par un alinéa ainsi rédigé :
Art. 323-1. — Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni		

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
de deux ans d'emprisonnement et de 30 000 euros d'amende.		
Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45 000 euros d'amende.		
	« Lorsque cette infraction a été commise à l'encontre d'un traitement automatisé de données à caractère personnel mis en oeuvre par l'État, la peine est portée à cinq ans d'emprisonnement et ~~300 000~~ euros d'amende. »	« Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à cinq ans d'emprisonnement et à 75 000 € d'amende. »
	~~2° L'article 323-2 est complété par un alinéa ainsi rédigé :~~	**Alinéa supprimé.**
Art. 323-2. — Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.		**Alinéa supprimé.**
	~~« Lorsque cette infraction a été commise à l'encontre d'un traitement automatisé de données à caractère personnel mis en oeuvre par l'État, la peine est portée à cinq ans d'emprisonnement et 300 000 euros d'amende. »~~	
	~~3° L'article 323-3 est complété par un alinéa ainsi rédigé :~~	**Alinéa supprimé.**
Art. 323-3. — Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende.		
	~~« Lorsque cette infraction a été commise à l'encontre d'un traitement automatisé de données à caractère personnel mis en oeuvre par l'État, la peine est portée à cinq ans d'emprisonnement et 300 000 euros d'amende. »~~	**Alinéa supprimé.**

Texte en vigueur	Texte de la proposition de loi	Texte élaboré par la commission en vue de l'examen en séance publique
___	___	___
		Article 7 bis (nouveau)
		Toute décision rendue en raison de l'usurpation d'identité dont une personne a fait l'objet et dont la transcription ou la mention sur les registres de l'état civil est ordonnée, doit énoncer ce motif dans son dispositif.
	Article 8	Article 8
	La présente loi est applicable sur l'ensemble du territoire de la République.	*(Sans modification).*
	Article 9	Article 9
	Les éventuelles conséquences financières résultant pour l'État de l'application de la présente loi sont compensées, à due concurrence, par la création d'une taxe additionnelle aux droits prévus aux articles 575 et 575 A du code général des impôts.	*(Sans modification).*