N° 339

SÉNAT

SESSION ORDINAIRE DE 2011-2012

Enregistré à la Présidence du Sénat le 8 février 2012

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, ADOPTÉE PAR L'ASSEMBLÉE NATIONALE EN NOUVELLE LECTURE*, relative à la* **protection** *de l'***identité***,*

Par M. François PILLET,

Sénateur

(1) Cette commission est composée de : M. Jean-Pierre Sueur*, président ;* MM. Jean-Pierre Michel, Patrice Gélard, Mme Catherine Tasca, M. Bernard Saugey, Mme Esther Benbassa, MM. François Pillet, Yves Détraigne, Mme Éliane Assassi, M. Nicolas Alfonsi, Mlle Sophie Joissains*, vice-présidents ;* Mme Nicole Bonnefoy, MM. Christian Cointat, Christophe-André Frassa, Mme Virginie Klès*, secrétaires ;* MM. Jean-Paul Amoudry, Alain Anziani, Philippe Bas, Christophe Béchu, Mmes Nicole Borvo Cohen-Seat, Corinne Bouchoux, MM. François-Noël Buffet, Gérard Collomb, Pierre-Yves Collombat, Jean-Patrick Courtois, Michel Delebarre, Félix Desplan, Christian Favier, Louis-Constant Fleming, René Garrec, Gaëtan Gorce, Mme Jacqueline Gourault, MM. Jean-Jacques Hyest, Jean-René Lecerf, Jean-Yves Leconte, Antoine Lefèvre, Roger Madec, Jean Louis Masson, Jacques Mézard, Thani Mohamed Soilihi, Hugues Portelli, André Reichardt, Alain Richard, Simon Sutour, Mme Catherine Troendle, MM. André Vallini, René Vandierendonck, Jean-Pierre Vial, François Zocchetto.

Voir le(s) numéro(s) :

Sénat : Première lecture : **682** (2009-2010), **432**, **433** et T.A. **126** (2010-2011)
Deuxième lecture : **744** (2010-2011), **39**, **40** et T.A. **9** (2011-2012)
Commission mixte paritaire : **237**, **238**, T.A **56**
Nouvelle lecture : **332** et **340** (2011-2012)

Assemblée nationale (**13**ème législ.) : Première lecture : **3471**, **3599** et T.A. **713**
Deuxième lecture : **3887**, **4016** et T.A. **798**
Nouvelle lecture : **4223**, **4229** et T.A. **838**

S O M M A I R E

Pages

LES CONCLUSIONS DE LA COMMISSION DES LOIS

La commission des lois, réunie le mercredi 8 février 2012 sous la présidence de **M. Jean-Pierre Sueur, président**, a procédé à l'examen du **rapport** de **M. François Pillet** et **du texte** qu'elle propose pour la **proposition** de **loi** n° **332** (2011-2012), adoptée par l'Assemblée nationale en nouvelle lecture, relative à la **protection de l'identité.**

M. François Pillet, rapporteur, a salué le fait que l'Assemblée nationale, en apportant à l'utilisation du fichier central biométrique de la population française créé par la proposition de loi, un certain nombre de restrictions, ait pris conscience de la nécessité d'en limiter l'usage à la seule lutte contre l'usurpation d'identité et rapproché ainsi sa position de celle du Sénat.

Il a cependant constaté que les garanties juridiques que les députés avaient substituées aux garanties techniques définitives et irréversibles adoptées par le Sénat, ne levaient pas toutes les inquiétudes, en raison des imperfections qu'elles présentaient.

Surtout, il a rappelé que rien n'empêcherait qu'elles soient levées rapidement s'il était décidé d'étendre les possibilités d'usage du fichier central biométrique. Or, comme la Commission nationale de l'informatique et des libertés l'a rappelé à plusieurs reprises, en particulier devant la commission des lois, la constitution d'un fichier biométrique aussi puissant que celui prévu par la proposition de loi doit s'accompagner de garanties solides et pérennes, qui interdisent l'utilisation de la base centrale pour un autre objet que celui pour lequel elle a été créée.

Pour l'ensemble de ces raisons la commission des lois a rétabli, à son initiative, la garantie technique du « *lien faible* », qu'elle avait défendue dès la première lecture du texte, et qui présente l'avantage d'être irréversible et d'assurer ainsi une très grande efficacité à la lutte contre l'usurpation d'identité, sans rien céder de l'exigence absolue de protection des libertés publiques.

Elle a par ailleurs conservé la limitation à deux du nombre d'empreintes digitales enregistrées sur la base centrale, introduite par l'Assemblée nationale, conformément à la décision du Conseil d'État relative au passeport biométrique.

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

Mesdames, Messieurs,

Le Sénat est appelé à examiner en nouvelle lecture, après l'Assemblée nationale, la proposition de loi relative à la protection de l'identité, présentée par nos collègues Jean-René Lecerf et Michel Houel.

Cette nouvelle lecture intervient après l'absence d'adoption conforme par les deux chambres des conclusions de la commission mixte paritaire.

Cette dernière était pourtant parvenue à établir un texte commun sur l'unique article restant en discussion (article 5), en reprenant le dispositif proposé par le Sénat.

Toutefois, le Gouvernement a souhaité que l'Assemblée nationale, qui avait été saisie la seconde de ce texte d'origine sénatoriale, examine, en premier, le texte résultant des travaux de la commission mixte et il a proposé aux députés d'adopter un amendement inversant totalement le sens des conclusions de la commission mixte paritaire, puisqu'il rétablissait le texte de l'Assemblée nationale pourtant écarté par la majorité des membres constituant la CMP.

Le Sénat, contraint de se prononcer par un même vote sur l'amendement et le texte, les a rejetés, afin, comme l'y invitait le rapporteur de la commission mixte paritaire, notre collègue, Mme Virginie Klès, de réaffirmer son attachement au système du « *lien faible* » qu'il défend depuis le début de l'examen de cette proposition de loi.

Les fichiers dits à « *lien faible* » et les fichiers à « *lien fort* »

Dans son principe, le dispositif des fichiers à « *lien faible* » consiste à associer un même numéro, compris par exemple entre 1 et 6 000, à l'identité et aux empreintes d'une personne, sans créer de lien direct entre l'identité et les empreintes. Sur une population de 60 millions de personnes, chaque numéro correspondrait à 10 000 personnes. Une empreinte renvoie donc à un numéro, qui renvoie lui-même à 10 000 noms[1]. Ainsi, tout se passe comme si 10 000 empreintes étaient rangées dans un tiroir portant un numéro de 1 à 6 000, les 6 000 identités correspondant dans un second tiroir portant le même numéro, et les 10 000 visages dans un troisième tiroir portant lui aussi le même numéro.

[1] *Ce dispositif a notamment été exposé par M. le Pr Ari Shamir, lors de la 31e conférence des commissions de protection des données personnelles et de la vie privée (réunion des CNIL mondiales) à Madrid en novembre 2009.*

Il y a alors deux façons de constituer la base :

- attribuer les numéros au hasard, ce qui est l'option la plus simple. Celle-ci ne présente aucune difficulté technique et n'est, pour cette raison, pas susceptible de faire l'objet d'un brevet ;

- créer les numéros à partir des empreintes digitales des intéressés afin de rendre possible de recréer le bon numéro sur présentation de l'empreinte. Concrètement, il s'agit « *d'écrire* » l'empreinte sous la forme d'un unique nombre compris entre 1 et 1 milliard, et de ne retenir, pour l'inscrire dans la base, que les trois, quatre ou cinq derniers chiffres. Ceci évite qu'une image de l'empreinte soit enregistrée physiquement dans la base (en revanche elle l'est sur la carte d'identité). Ce dernier procédé a été breveté par la SAGEM.

L'identification d'un individu par ses seules empreintes digitales à travers la base est impossible, puisqu'une série d'empreintes renvoie à 10 000 individus.

En revanche, la détection d'une tentative d'usurpation d'identité est garantie à presque 100% puisque, dans une population de 60 millions de français, il y a très peu de chance que les empreintes du fraudeur soient dans le même « *tiroir* » que celle de la personne dont il tente d'usurper l'identité.

Le dispositif des fichiers dits à « *lien fort* » consiste à associer de manière univoque une identité et une biométrie. Lorsque l'on connaît l'une on est donc en mesure de retrouver l'autre, ce qui permet l'utilisation de ce fichier pour retrouver l'identité d'une personne inconnue à partir, par exemple, de ses seules empreintes digitales.

Examinant le texte en nouvelle lecture, les députés ont rétabli l'ensemble des modifications qu'ils lui avaient apportées, à l'initiative du Gouvernement, au cours de la deuxième lecture.

Ces modifications s'inscrivent certes dans le sens défendu depuis le début par le Sénat : accepter la constitution d'un fichier biométrique pour la lutte contre l'usurpation d'identité, mais réserver son usage à cette seule lutte contre l'usurpation d'identité.

Sans doute la décision du Conseil d'État relative au passeport biométrique[1] ainsi que les prises de position de la CNIL le 25 octobre 2011 ne sont pas étrangères à cette inflexion récente de la position du Gouvernement et des députés.

Pour autant, même ainsi amendé, le texte issu des travaux de l'Assemblée nationale reste inconciliable avec les principes qui ont guidé le Sénat dans l'examen de cette proposition de loi.

En effet, la création d'un fichier biométrique de la totalité de la population française, fichier inédit « *des gens honnêtes* », impose au législateur, compte tenu des risques phénoménaux qu'un mésusage ferait courir à l'ensemble de nos concitoyens, de l'assortir de garanties absolues et inaltérables.

[1] *CE, n° 317827, 26 octobre 2011,*

Or, à la quasi unanimité, les sénateurs ont souhaité apporter, avec le dispositif du « *lien faible* » des garanties définitives et irréversibles, tandis que la majorité à l'Assemblée nationale s'est contentée, en rétablissant son système de « *lien fort* » de garanties légales, dont on sait, avec l'exemple du fichier national automatisé des empreintes génétiques (FNAEG), qu'en matière de fichiers, elles se lèvent facilement, morceau par morceau.

Il convient, par conséquent, de revenir à la rédaction proposée par le Sénat et la commission mixte paritaire. Elle seule prend en compte les risques que présente ce fichier de soixante millions de français, et permet, en y apportant la meilleure garantie qui soit, d'en tirer pleinement parti pour lutter contre l'usurpation d'identité, son unique objet.

I. LES GARANTIES PROPOSÉES PAR L'ASSEMBLÉE NATIONALE DEMEURENT INSUFFISANTES COMPTE TENU DE LA NATURE DU FICHIER MIS EN PLACE

A. LA PRISE EN COMPTE PARTIELLE, PAR LES DÉPUTÉS, DES RISQUES DE MÉSUSAGE DU FICHIER

À l'initiative du Gouvernement, les députés ont adopté en deuxième lecture et rétabli lors de leur examen des conclusions de la CMP et en nouvelle lecture, un ensemble de dispositions supprimant le système du « *lien faible* » mis en place par le Sénat, pour revenir à un « *lien fort* », établissant une corrélation univoque entre les données d'état civil d'un individu et ses données biométriques enregistrées dans le fichier central.

Ils ont assorti ces dispositions de garanties juridiques censées réserver l'usage de la base centrale à la seule lutte contre l'usurpation d'identité.

À cette fin, ils ont précisé que l'identification d'un individu par les empreintes digitales contenues dans la base ne serait possible que :

- pour l'établissement des titres d'identité ou de voyage ;

- la poursuite de certaines infractions liées à l'usurpation d'identité ;

- sur réquisition du procureur de la République pour établir l'identité d'une personne décédée inconnue dans une catastrophe naturelle ou un accident collectif.

L'interconnexion des données biométriques de la base centrale avec tout autre fichier nominatif serait aussi interdite.

La liste des infractions relatives à l'usurpation d'identité, pour lesquelles la consultation de la base serait autorisée, soit sous le contrôle du procureur de la République, en cas de crime ou délit flagrant (article 55-1 du code de procédure pénale) ou dans le cadre d'une enquête préliminaire (article 76-2 du même code), soit sous celui du juge d'instruction, dans le cadre d'une commission rogatoire (article 154-1 du même code), comprendrait :

- l'usurpation d'identité proprement dite (article 226-4-1 du code pénal) ;

- l'escroquerie en général (article 313-1 et 313-2 du même code) ;

- le délit de révélation de l'identité d'un agent des services spécialisés de renseignement (article 413-13 du même code) ;

- le délit de substitution de nom dans un document officiel (article 433-19 du même code) ;

- l'usurpation d'identité lorsqu'elle peut conduire à l'engagement de poursuite pénale contre la victime (article 434-23 du même code) ;

- le faux, la détention et l'usage de faux, y compris dans une écriture publique (articles 441-1 à 441-4 du même code) ainsi que l'obtention indue de documents administratifs la déclaration mensongère ou l'usage, l'attestation ou l'établissement de certificats inexacts ou falsifiés (articles 441-6 et 441-7 du même code) ;

- l'usurpation d'identité dans le cadre d'infractions routières ou pour la communication d'information relative au permis de conduire ou à la circulation des véhicules (articles L. 225-7, L. 225-8 et L. 330-7 du code de la route), ainsi que la déclaration de fausse identité ou de fausse adresse aux agents assermentés chargés de constatés les infractions en matière de police du transport ferroviaire (article L. 2242-5 du code des transports) ;

- la délivrance d'extraits du casier judiciaire d'un tiers ou leur modification par l'usage d'un faux nom ou d'une fausse qualité (article 781 du code de procédure pénale).

L'utilisation de la base de données devrait être, sous peine de nullité, mentionnée et spécialement motivée au procès-verbal.

Une mention ajoutée à l'article 55-1 du code de procédure pénale exclurait les recherches d'identification à partir des traces de personnes inconnues (à l'exception de l'identification d'une personne décédée inconnue, expressément prévue par la présente rédaction de l'article 5 de la proposition de loi).

Enfin, le texte proposé par l'Assemblée nationale prévoit explicitement que l'identification d'une personne à partir de ses empreintes digitales puisse avoir lieu sans son assentiment, au titre des actes d'instruction qui peuvent être accomplis par l'officier de police judiciaire avec l'autorisation expresse du juge d'instruction.

L'ensemble de ses limitations d'accès ou d'utilisation de la base centrale ne concerne que l'identification par les empreintes digitales et ne porte pas sur les autres données enregistrées dans le fichier central.

Prenant en compte l'annulation, par la décision du Conseil d'État précitée, de la disposition du décret n° 2008-426 du 30 avril 2008 modifiant le décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques, qui prévoyait l'enregistrement et la conservation dans la base centrale des huit empreintes du demandeur de titre, les députés ont modifié l'article 5 de la présente proposition de loi, à l'initiative du Gouvernement, pour préciser que seules les deux empreintes inscrites sur la carte d'identité biométrique devraient être conservées dans la nouvelle base centrale. Cette modification aurait dû s'accompagner, par coordination, d'une modification à l'article 2. Il n'en a rien été.

B. DES AMÉNAGEMENTS QUI NE LÈVENT PAS TOUTES LES INQUIÉTUDES VOIRE EN SUSCITENT DE NOUVELLES

1. Une limitation à l'usurpation d'identité qui n'est pas avérée

Le rapporteur de la commission des lois de l'Assemblée nationale défend le dispositif du « *lien fort* » associé à certaines garanties légales en faisant valoir que la limitation de l'utilisation du fichier biométrique de la population française à la seule lutte contre l'usurpation d'identité devrait dissiper toute crainte sur les mésusages de la base centrale.

Cependant, quand bien même de telles garanties seraient pérennes et irréversibles – ce qui n'est malheureusement pas le cas –, **d'ores et déjà le dispositif proposé déborde le strict cadre de l'usurpation d'identité, ce qui ouvre la voie à d'autres empiètements, à l'avenir, afin d'étendre peu à peu le périmètre de l'utilisation du fichier central biométrique de la population française**.

a) Le recours au fichier central pour des enquêtes qui ne présentent pas forcément de lien avec une usurpation d'identité

La liste des infractions pour lesquelles la consultation de la base centrale est autorisée devrait, en principe ne porter que sur des délits d'usurpation d'identité. Toutefois, plusieurs des infractions visées ne présentent pas de lien direct avec ce délit, ou sont bien plus générales que ce seul délit, ce qui autoriserait les forces de police à faire usage du fichier alors qu'aucune usurpation d'identité n'est en cause.

Il en est ainsi du délit de révélation de l'identité d'agent des services spécialisés de renseignement[1] : l'identité de l'auteur de l'infraction n'est pas en cause. De la même manière, on peut légitimement se demander ce que le faux en écriture publique qui ne porte pas sur l'identité d'une personne a à voir avec l'usurpation d'identité[2] ou ce que l'escroquerie a à voir avec l'usurpation d'identité, lorsque le délinquant ne se présente pas sous une fausse identité, mais qu'il agit, sous sa véritable identité, par des manœuvres frauduleuses[3].

Le rapporteur de l'Assemblée nationale a d'ailleurs lui-même proposé par un amendement d'autoriser l'utilisation de la base pour l'identification d'un cadavre par ses empreintes digitales, ce qui ne présente aucun lien avec l'objet initial de la proposition de loi : il a ainsi indiqué la méthode pour étendre l'usage de la base centrale à d'autres fins. Une fois le fichier créé, et à défaut d'une garantie technique qui rende impossible son utilisation pour autre chose que la lutte contre l'usurpation d'identité, il suffira d'une modification législative pour en étendre l'usage à d'autres fins.

b) L'accès aux données de la base centrale en dehors des procédures prévues

Le dispositif adopté par l'Assemblée nationale vise à mettre en place deux verrous : la limitation stricte des infractions susceptibles de fonder un recours au fichier ; l'interdiction d'utiliser ce fichier, même pour ces infractions, pour identifier une personne inconnue à partir des traces qu'elle aurait laissé. Il s'agit dans ce dernier cas d'interdire l'usage de la base centrale à des fins de recherche criminelle.

Pour autant, votre rapporteur s'interroge sur la portée exacte de cette dernière interdiction.

En effet, il note tout d'abord que la rédaction proposée par l'Assemblée nationale à l'article 5 crée un article 99-5 au code de procédure pénale qui vise justement à autoriser l'officier de police judiciaire agissant sous le contrôle du juge d'instruction à tenter d'identifier une personne sans son assentiment. Un tel assentiment n'est aucunement prévu pour la procédure normale d'identification proposée par l'Assemblée nationale, qui impose seulement l'information de l'intéressé sur l'utilisation de la base centrale : le mentionner expressément, dans la division du code de procédure pénale qui traite des pouvoirs d'enquête du juge d'instruction, vise à autoriser l'identification de l'intéressé sans qu'il en soit informé, c'est-à-dire sans qu'il ait été mis à même de prouver son identité et donc de lever le cas échéant, sans recours à la base centrale, les soupçons qui peuvent peser sur son identité. Ce dispositif fait basculer d'une logique de vérification d'une identité sur laquelle pèse des soupçons, à une logique d'identification dans le cadre d'une recherche criminelle.

---

[1] *Art. 413-13 du code pénal*
[2] *Art. 441-1 du code pénal.*
[3] *Art. 313-1 du code pénal.*

Surtout, votre rapporteur jugerait nécessaire que soit clarifiée l'articulation entre les pouvoirs limités d'accès à la base centrale définis aux articles 5 du présent texte et à la nouvelle rédaction proposée pour l'article 55-1 du code de procédure pénale et les pouvoirs généraux que les magistrats chargés de l'enquête tiennent des articles 60-1, 60-2, 99-3 et 99-4 du même code pour obtenir des documents numériques ou accéder à des informations contenues dans des fichiers nominatifs. L'accès à la base centrale biométrique en vertu de ces dernières dispositions est-il bien interdit en vertu de la nouvelle rédaction proposée pour les premiers articles cités ?

c) La question non résolue de l'utilisation de la base par les services spécialisés, hors de tout contrôle judiciaire

Votre rapporteur constate qu'aucune réponse n'a été apportée par le Gouvernement ni par le rapporteur de la commission des lois de l'Assemblée nationale à la question qu'il posait en deuxième lecture sur l'accès à la base centrale ouvert par l'article 7 *bis* A du présent texte aux services en charge de la lutte contre le terrorisme.

Dans le cadre du système à « *lien faible* » proposé par le Sénat, cet accès s'opérait à droit constant, puisqu'il conservait aux services en charge de la lutte contre le terrorisme l'accès aux actuels systèmes de gestion des cartes nationales d'identité et de passeports que leur ouvre actuellement l'article 9 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, sans leur donner les moyens d'identifier une personne à partir de ces traces biométriques.

En effet, actuellement, les services en charge de la lutte contre le terrorisme ne peuvent utiliser les données biométriques des détenteurs de titre contenues dans les fichiers pour identifier un individu à partir de ces seuls éléments. Le fichier de gestion des passeports « *TES* »[1] l'exclut expressément. Quant au fichier de gestion des cartes nationales d'identité, les empreintes digitales des intéressés n'y sont simplement pas enregistrées[2].

Loin de maintenir le droit en vigueur, le système à « *lien fort* » prôné par les députés étend considérablement les pouvoirs des services chargés de la lutte contre le terrorisme, puisque, faute de l'exclure, il leur permet d'accéder à la base dans l'exercice de leur mission, hors de tout contrôle d'un juge, et les autorise donc à en faire usage pour identifier une personne à partir de ses seules empreintes digitales ou par reconnaissance faciale.

Il ne peut être argué, pour restreindre cet usage, des limitations prévues à l'article 5 du présent texte, puisque la disposition spéciale déroge à la disposition générale et que l'article 7 *bis* A ouvre aux agents de ces services spécialisés, un accès sans limitation particulière à la base centrale biométrique.

---

[1] *Article 19 du décret n° 2005-12726 du 30 décembre 2005 relatif aux passeports.*
[2] *Article 8 du décret n° 55-1397 du 22 octobre 195 instituant la carte nationale d'identité.*

Renvoyer à un décret ne sera pas forcément suffisant, dans la mesure où il appartient au législateur, lorsque des libertés publiques sont en jeu, épuiser sa compétence.

Ce problème posé par le système à « *lien fort* » ne se posait pas avec le système à « *lien faible* ». Faute d'adopter ce dernier, il aurait été nécessaire que les députés modifient en conséquence la proposition de loi pour encadrer l'accès au fichier central par les services spécialisés et éviter ainsi une lacune dans le système de garanties légales qu'ils entendaient mettre en place.

*

Qu'il s'agisse de l'accès au fichier dans les cas non prévus par le texte ou de celui de l'accès ouvert aux services chargés de la lutte contre le terrorisme, les garanties prévues par l'Assemblée nationale paraissent ainsi incomplètes ou insuffisamment précises. Une telle imprécision pose inévitablement la question de la constitutionnalité du dispositif, alors qu'il appartient au législateur de définir avec précision les garanties légales nécessaire à l'exercice ou la protection des libertés publiques.

2. Une levée de l'interdiction des procédés de reconnaissance faciale ?

Le Sénat avait soumis l'image numérisée du visage enregistrée dans la base avec les autres données personnelles, à la même garantie technique que les empreintes digitales, celle du « *lien faible* ». Il avait aussi expressément exclu, conformément à la position de la commission nationale de l'informatique et des libertés, l'utilisation de tout procédé de reconnaissance faciale.

Les députés sont revenus sur cette rédaction. Certes, ils ont exclu que l'image numérisée du visage enregistrée dans la base biométrique puisse être utilisée par l'autorité de délivrance des titres d'identité ou de voyage pour identifier le demandeur d'un titre.

En revanche, ils n'ont apporté aucune précision sur les autres utilisations qui pourraient être faite de la base, par exemple, dans le cadre d'une consultation judiciaire opérée sur le fondement des articles 60-1, 60-2 et 99-3 et 99-4 du code de procédure pénale. **Dans le silence de la loi, devra-t-on considérer qu'un juge d'instruction pourrait demander à ce qu'une personne, dont le visage a été enregistré par une caméra de surveillance soit identifiée à partir des images numérisées dans le fichier central biométrique, ce qui reviendrait à valider ponctuellement des dispositifs de reconnaissance faciale** ?

3. Les risques liés au piratage du fichier

L'opportunité de créer un fichier central, regroupant la totalité de la population française, sur le modèle du « lien fort », qui lie de manière univoque identité et biométrie, doit aussi être examinée sous l'angle des risques, pour la sécurité des personnes, d'un piratage par des personnes mal intentionnées de la base centrale.

Le fichier ainsi constitué, qui portera à terme sur l'ensemble des Français et inclura leurs données biométriques, sera l'un des plus sensibles qui soient. Il est absolument nécessaire qu'il fasse l'objet des dispositifs de sécurité techniques les plus exigeants.

Toutefois si d'aventure, ce fichier était victime d'une tentative de piratage, il serait préférable pour la sécurité des citoyens français, qu'il soit conçu sur le modèle du « *lien faible* », plutôt que sur celui du « *lien fort* », afin que les auteurs du piratage ne disposent pas d'une base associant de manière univoque, l'état civil, le visage, les empreintes digitales et le domicile de l'ensemble de la population française.

II. LA NÉCESSITÉ DE RÉTABLIR DES GARANTIES TECHNIQUES DÉFINITIVES ET IRRÉVERSIBLES

A. LA PERTINENCE ET LA SOLIDITÉ DU DISPOSITIF DU « LIEN FAIBLE *»*

Il a été longuement répondu, lors des précédentes lectures du texte, aux arguments selon lesquels le système du « *lien faible* » ne serait ni mûr technologiquement, ni efficace pour lutter contre l'usurpation d'identité.

La technique du « *lien faible* » est connue depuis plusieurs années par la communauté scientifique des mathématiciens, des cryptologues et des informaticiens. Elle ne pose pas, s'agissant de la seule constitution du fichier central, de difficulté technique supérieure à celle d'une base biométrique à lien fort reposant sur une population de plusieurs dizaines de millions d'individus[1].

Par ailleurs, le système du « *lien faible* » repose sur la dissuasion, et une dissuasion si efficace, à plus de 99,9 % de chances de détecter la fraude, qu'elle équivaut à celle du système à « *lien fort* ». Il n'interdit pas, pour le délinquant fou ou inconscient qui aurait malgré joué sa liberté à 99,9 % de chances de perdre, que les services de police utilisent les données dont ils disposent, au moment de son interpellation, pour les confronter avec celles enregistrées dans leurs fichiers de police, ou celles contenues dans la base centrale pour resserrer rapidement le cercle des suspects, procéder à quelques vérifications – sans même avoir toujours besoin de déranger pour ce faire les intéressés – et identifier enfin le fraudeur.

---

[1] *Il existe même une façon de construire la base biométrique tellement simple qu'elle n'est pas brevetable. L'entreprise MORPHO, ex SAGEM, propose certes une façon plus raffinée de construire la base, mais cette technologie, qui repose sur un procédé breveté de codification de l'empreinte digitale n'a rien d'incontournable.*

B. LE REFUS, TRÈS MAJORITAIRE EN EUROPE, DES FICHIERS BIOMÉTRIQUES DE POPULATION À « LIEN FORT *»*

Les adversaires du dispositif du « *lien faible* » tirent parfois argument de ce qu'aucun pays ne l'a mis en œuvre pour conclure imprudemment à son inefficience.

Votre rapporteur souligne que raisonner ainsi revient très exactement à poser le problème à l'envers : c'est parce que presqu'aucune démocratie occidentale n'a souhaité créer un fichier central biométrique de la population qu'aucune n'a eu à se poser la question du fichier à « *lien faible* ».

L'Allemagne refuse tout fichier central biométrique par principe, le Royaume-Uni a récemment refusé de le mettre en place et la Belgique, pourtant si avancée dans les cartes d'identité électroniques n'a pas non plus eu besoin de mettre en place un tel fichier central. Quant aux Pays-Bas, leur ministre de l'intérieur, M. Piet Hein Donner, a annoncé, en avril dernier, que les six millions d'empreintes digitales enregistrées dans une base centrale dans le cadre du passeport biométrique seraient toutes effacées !

Seul Israël vient récemment de décider sa mise en œuvre, après un débat nourri et malgré une contestation très forte de cette solution. On doit cependant relever que la situation sécuritaire en Europe n'a rien à voir avec celle de l'État d'Israël.

Ainsi semble-t-il qu'au moins en Europe, la position la plus majoritaire soit celle qui refuse la mise en place d'un fichier central biométrique. Bien loin de jouer au détriment du système à « *lien faible* », ce constat étaie sa pertinence, face à un système de fichier central biométrique à « *lien fort* », qui paraît de plus en plus opposé aux standards européens applicable en la matière.

C. LA NÉCESSITÉ DE FAIRE PRIMER LES GARANTIES TECHNIQUES IRRÉVERSIBLES, CONFORMÉMENT À LA PRISE DE POSITION DE LA CNIL EN FAVEUR DU « LIEN FAIBLE *» POUR LE FICHIER CENTRAL BIOMÉTRIQUE*

L'audition récente de la présidente de la CNIL, le 14 décembre 2011, par notre commission des lois, après le vote du texte par les députés a une nouvelle fois permis de rappeler le soutien de cette institution au dispositif proposé par le Sénat.

Interrogée par notre collègue Jean-René Lecerf, auteur de la présente proposition de loi, sur les deux options défendues par nos deux assemblées, Mme Isabelle Falque Pierrotin, présidente de la CNIL, a indiqué : « *Sur la carte d'identité biométrique, nous avions considéré que la création d'une base centrale était disproportionnée au regard de l'objectif de sécurisation des titres. Si toutefois la base centrale est constituée, la meilleure garantie contre les utilisations détournées serait la garantie technique, celle du lien faible.*

L'Assemblée nationale et le Gouvernement semblent s'orienter vers une autre garantie, celle qui consiste à réduire, par la loi, les finalités d'accès à la base. Cependant, nous savons qu'une fois un fichier constitué il est toujours possible d'étendre ses finalités de consultation. C'est pourquoi la CNIL est inquiète : les restrictions juridiques seront toujours moins efficaces que les restrictions techniques, qui rendent impossibles l'utilisation de la base à des fins détournées »[1].

Les propos de la présidente de la CNIL posent les termes du débat.

Le fichier dont il est question sera le fichier central biométrique de la totalité de la population française. À quelles conditions et avec quelles garanties, la lutte contre l'usurpation d'identité peut-elle justifier la mise en place d'un instrument aussi puissant – et aussi dangereux qu'il est puissant ?

Et, surtout, c'est là tout l'objet de l'article 5, faut-il que ces garanties soient techniques et irréversibles ou peut-on se contenter de garanties juridiques, alors qu'une loi pourra demain modifier les finalités d'usage de la gigantesque base biométrique ainsi constituée ?

Votre commission constate que le dispositif proposé par l'Assemblée est loin de lever toutes les inquiétudes que la création d'une base centrale biométrique peut susciter et qu'il présente encore, à ce stade des travaux parlementaires, un certain nombre de lacunes.

Par ailleurs, reposant uniquement sur des garanties juridiques, il ne présente pas la même solidité que la garantie technique du « *lien faible* » définitive et irréversible, qui seule répond à l'exigence que votre commission a placé au cœur de sa réflexion sur ce texte : trouver un juste équilibre entre le souci de l'efficacité et l'impératif absolu de protection des libertés publiques.

Pour l'ensemble de ces raisons, à l'initiative de son rapporteur, votre commission a adopté un **amendement** rétablissant l'article 5 dans la rédaction adoptée par le Sénat en deuxième lecture, en y intégrant toutefois la limitation à deux du nombre d'empreintes digitales enregistrées dans la base centrale, que les députés ont prévue, conformément à la décision du Conseil d'État du 26 octobre 2011 précitée. Par coordination, votre commission a adopté un **amendement** inscrivant la même limitation à l'article 2, qui bien qu'adopté conforme par les deux chambres a été rappelé pour procéder à cette coordination, dans la liste des données enregistrées dans la carte d'identité.

*

* *

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

---

[1] *Texte de l'audition consultable à l'adresse suivante : http://www.senat.fr/compte-rendu-commissions/20111212/lois.html.*

EXAMEN EN COMMISSION

Mercredi 8 février 2012

_____

EXAMEN DU RAPPORT

M. François Pillet, rapporteur. – Nous sommes amenés à examiner une nouvelle fois cette proposition de loi, après le rejet par l'Assemblée nationale du texte commun auquel était parvenue la commission mixte paritaire. En nouvelle lecture, les députés en ont inversé le sens.

Certes, ils se sont rangés à notre avis en réservant le fichier à la lutte contre l'usurpation d'identité : c'est un progrès notable. Mais s'ils ont ainsi retrouvé l'esprit général du texte du Sénat, ils n'en ont pas adopté la lettre. Leur texte est en fait inconciliable avec les principes que nous avons constamment défendus. Il s'agit pourtant, fait exceptionnel, de recueillir les données biométriques de toute une population !

L'Assemblée nationale a pris en compte les risques de mésusage du fichier, mais n'a voulu les prévenir que par des garanties juridiques : l'identification d'un individu grâce aux empreintes digitales contenues dans la base ne pourra se faire que pour l'établissement de titres d'identité ou de voyage, ou dans le cadre de la poursuite d'infractions liées à l'usurpation d'identité, sur réquisition du procureur de la République. Mais la liste des infractions concernées est longue.

Ce texte n'apaise pas nos inquiétudes mais, bien au contraire, en suscite de nouvelles. Tout d'abord, je viens de le dire, il serait possible de recourir au fichier dans le cadre d'enquêtes sur des infractions dont le lien avec l'usurpation d'identité est ténu, voire inexistant : délit de révélation de l'identité d'un agent des services spécialisés de renseignement, faux en écritures publiques, même lorsque celles-ci ne portent pas sur l'identité d'une personne, escroquerie, même lorsque l'escroc ne se dissimule pas sous une fausse identité.

En outre, l'accès à la base serait possible en dehors des procédures prévues. Le texte ne s'articule pas avec les dispositions du code de procédure pénale qui accordent aux magistrats instructeurs le droit d'obtenir des documents numériques ou d'accéder à des informations contenues dans des fichiers normatifs. Le texte des députés ne semble pas interdire qu'ils aient mutuellement accès à la base centrale des données biométriques en vertu de ces dispositions. En outre, les services spécialisés – notamment ceux qui sont chargés de la lutte contre le terrorisme – pourraient y avoir accès hors de tout contrôle judiciaire, puisque le texte ne l'exclut pas ; or le choix du lien fort étend considérablement les possibilités offertes par le fichier.

Sur l'utilisation de certains éléments biométriques et notamment de l'image numérisée du visage, on relève la même ambiguïté. Dans le silence de la loi, les juges d'instruction pourraient demander qu'une personne dont le visage a été filmé par une caméra de surveillance, par exemple, soit identifiée grâce aux données du fichier, ce qui reviendrait à valider les dispositifs de reconnaissance faciale. Le progrès des techniques est tel que l'on peut identifier quelqu'un même à partir d'une image qui paraît inutilisable à des profanes.

Il ne faut pas sous-estimer non plus les risques liés au piratage : une telle éventualité serait catastrophique.

Voilà pourquoi les garanties juridiques ne suffisent pas : il faut des garanties techniques, qui rendent le fichier éternellement inutilisable à d'autres fins que celles prévues par la loi. On dit qu'en prévoyant un fichier à lien faible, le législateur en confierait l'élaboration à une entreprise déterminée, mais c'est faux : il existe des façons de mettre en œuvre le lien faible non brevetables. On prétend aussi qu'un tel fichier serait inefficace. Au contraire, il permettrait de lutter contre l'usurpation en amont : l'usurpateur aurait 99 chances sur 100 de se faire prendre au moment où il tenterait d'obtenir de faux papiers. Mieux vaut un risque infime d'usurpation d'identité et aucun risque pour les libertés publiques, que le contraire !

Sous prétexte qu'aucun pays n'a adopté le lien faible, on le juge inefficace, mais c'est prendre les choses à l'envers : presque aucune démocratie occidentale n'a créé de fichier biométrique de sa population ! L'Allemagne s'y refuse, invoquant explicitement son passé, ainsi que le Royaume-Uni et la Belgique, pourtant très avancée dans la mise en place de cartes d'identité électroniques. Le ministre de l'intérieur des Pays-Bas a annoncé en avril que les 6 millions d'empreintes digitales recueillies pour l'établissement de passeports biométriques seraient effacées. Seul Israël a instauré un fichier à lien fort, mais le contexte est tout autre.

Je citerai pour conclure la présidente de la Cnil : « Sur la carte d'identité biométrique, nous avions considéré que la création d'une base centrale était disproportionnée au regard de l'objectif de sécurisation des titres. Si toutefois la base centrale est constituée, la meilleure garantie contre les utilisations détournées serait la garantie technique, celle du lien faible. L'Assemblée nationale et le Gouvernement semblent s'orienter vers une autre garantie, celle qui consiste à réduire, par la loi, les finalités d'accès à la base. Cependant, nous savons qu'une fois un fichier constitué, il est toujours possible d'étendre ses finalités de consultation. C'est pourquoi la Cnil est inquiète : les restrictions juridiques seront toujours moins efficaces que les restrictions techniques, qui rendent impossible l'utilisation de la base à des fins détournées. »

Mme Virginie Klès. – Je suis en parfait accord avec M. le rapporteur. J'ai pu constater hier, lors de la cinquième journée parlementaire sur la sécurité où il a beaucoup été question de cybercriminalité, combien il est facile pour des hackers de pénétrer des fichiers : nous en avons des exemples tous les jours, à Bercy, à la CIA, etc. Le fichier que proposent les députés serait une bombe à retardement, mise à disposition de n'importe quel groupe terroriste. Je serais désolée que la France fût la première à s'engager dans cette voie.

M. Jean-René Lecerf. – Je serai bref, car c'est la quatrième fois que le Sénat se penche sur ce texte. Au risque d'être solitaire, je ne serai pas solidaire de l'avis de mon collègue et ami M. Pillet. Avec un fichier à lien faible, si l'usurpateur est le premier à se faire recenser, il sera impossible de le confondre. Soit on créera un fichier à lien fort, soit on n'en créera pas du tout, et le problème de l'usurpation d'identité restera entier.

M. Jean-Yves Leconte. – Que le fichier soit à lien fort ou à lien faible, si l'usurpateur est le premier à demander des papiers, sa fausse identité sera inscrite dans le marbre.

Mme Virginie Klès. – Il s'agirait d'une identité fictive et non pas usurpée. Car dans dix ans, tout le monde sera recensé dans la base.

M. Jean-René Lecerf. – J'ai souvent dit que j'étais prêt à changer d'avis dans dix ans.

Mme Virginie Klès. – Il sera trop tard !

Examen des amendements

Article 2

M. François Pillet, rapporteur. – Je vous soumets un amendement qui fixe à deux le nombre d'empreintes digitales recueillies, comme l'a proposé l'Assemblée nationale et conformément à la règle édictée par le Conseil d'Etat pour le passeport biométrique.

L'amendement n° 2 est adopté, ainsi que l'article 2 dans la rédaction issue des travaux de la commission.

Article 5

M. François Pillet, rapporteur. – Je vous propose ici de rétablir le lien faible.

L'amendement n° 1 rectifié est adopté, ainsi que l'article 5 et la proposition de loi dans la rédaction issue des travaux de la commission.

La commission a adopté les amendements suivants :

Article 2			
Auteur	**N°**	**Objet**	**Sort de l'amendement**
M. PILLET, rapporteur	2	Coordination	**Adopté**
Article 5			
Auteur	**N°**	**Objet**	**Sort de l'amendement**
M. PILLET, rapporteur	1 rect	Rétablissement de la garantie du lien faible	**Adopté**

TABLEAU COMPARATIF

___

Texte adopté par le Sénat en deuxième lecture ___ **Proposition de loi relative à la protection de l'identité**	Texte adopté par l'Assemblée nationale en deuxième lecture ___ **Proposition de loi relative à la protection de l'identité**	Texte adopté par l'Assemblée nationale en nouvelle lecture ___ **Proposition de loi relative à la protection de l'identité**	Texte élaboré par la commission en vue de l'examen en séance publique ___ **Proposition de loi relative à la protection de l'identité**
.....	.....	.....	.....
Article 2	Article 2	Article 2	Article 2
[Pour coordination]	*[Pour coordination]*	*[Pour coordination]*	*[Pour coordination]*
La carte nationale d'identité et le passeport comportent un composant électronique sécurisé contenant les données suivantes :	La carte nationale d'identité et le passeport comportent un composant électronique sécurisé contenant les données suivantes :	La carte nationale d'identité et le passeport comportent un composant électronique sécurisé contenant les données suivantes :	*(Alinéa sans modification).*
1° Le nom de famille, le ou les prénoms, le sexe, la date et le lieu de naissance du demandeur ;	1° Le nom de famille, le ou les prénoms, le sexe, la date et le lieu de naissance du demandeur ;	1° Le nom de famille, le ou les prénoms, le sexe, la date et le lieu de naissance du demandeur ;	1° *(Sans modification).*
2° Le nom dont l'usage est autorisé par la loi, si l'intéressé en a fait la demande ;	2° Le nom dont l'usage est autorisé par la loi, si l'intéressé en a fait la demande ;	2° Le nom dont l'usage est autorisé par la loi, si l'intéressé en a fait la demande ;	2° *(Sans modification).*
3° Son domicile ;	3° Son domicile ;	3° Son domicile ;	3° *(Sans modification).*
4° Sa taille et la couleur de ses yeux ;	4° Sa taille et la couleur de ses yeux ;	4° Sa taille et la couleur de ses yeux ;	4° *(Sans modification).*
5° Ses empreintes digitales ;	5° Ses empreintes digitales ;	5° Ses empreintes digitales ;	5° Deux de ses empreintes digitales ;
6° Sa photographie.	6° Sa photographie.	6° Sa photographie.	6° *(Sans modification).*
Le présent article ne s'applique pas au passeport délivré selon une procédure d'urgence.	Le présent article ne s'applique pas au passeport délivré selon une procédure d'urgence.	Le présent article ne s'applique pas au passeport délivré selon une procédure d'urgence.	*(Alinéa sans modification).*
.....	.....	.....	.....

Texte adopté par le Sénat en deuxième lecture ___	Texte adopté par l'Assemblée nationale en deuxième lecture ___	Texte adopté par l'Assemblée nationale en nouvelle lecture ___	Texte élaboré par la commission en vue de l'examen en séance publique ___
Article 5	Article 5	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.	I. — Afin de préserver l'intégrité des données requises pour la délivrance du passeport français et de la carte nationale d'identité, l'État crée, dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, un traitement de données à caractère personnel facilitant leur recueil et leur conservation.	~~I.~~ — Afin de préserver l'intégrité des données requises pour la délivrance du passeport français et de la carte nationale d'identité, l'État crée, dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, un traitement de données à caractère personnel facilitant leur recueil et leur conservation.	Afin de préserver l'intégrité des données requises pour la délivrance du passeport français et de la carte nationale d'identité, l'État crée, dans les conditions prévues par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, un traitement de données à caractère personnel facilitant leur recueil et leur conservation.
Ce traitement de données, mis en oeuvre par le ministère de l'intérieur, permet l'établissement et la vérification des titres d'identité ou de voyage dans des conditions garantissant l'intégrité et la confidentialité des données à caractère personnel ainsi que la traçabilité des consultations et des modifications effectuées par les personnes y ayant accès.	Ce traitement de données, mis en œuvre par le ministère de l'intérieur, permet l'établissement et la vérification des titres d'identité ou de voyage dans des conditions garantissant l'intégrité et la confidentialité des données à caractère personnel ainsi que la traçabilité des consultations et des modifications effectuées par les personnes y ayant accès.	Ce traitement de données, mis en œuvre par le ministère de l'intérieur, permet l'établissement et la vérification des titres d'identité ou de voyage dans des conditions garantissant l'intégrité et la confidentialité des données à caractère personnel ainsi que la traçabilité des consultations et des modifications effectuées par les personnes y ayant accès.	*(Alinéa sans modification).*
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 1° à 4° 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.	**Alinéa supprimé.**	**Alinéa supprimé.**	L'enregistrement des deux 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 1° à 4° 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.
La vérification de l'identité du demandeur s'opère par la mise en relation de l'identité alléguée et des autres données mentionnées aux 1° à 6° de l'article 2.	L'identification du demandeur d'un titre d'identité ou de voyage ne peut s'y effectuer qu'au moyen des données énumérées aux 1° à 5° de l'article 2.	~~L'identification~~ du demandeur ~~d'un titre d'identité ou de voyage ne peut s'y effectuer qu'au moyen des~~ données ~~énumérées~~ aux 1° à ~~5°~~ de l'article 2.	La vérification de l'identité du demandeur s'opère par la mise en relation de l'identité alléguée et des autres données mentionnées aux 1° à 6° de l'article 2.
Le traitement ne comporte pas de dispositif de reconnaissance faciale à partir	**Alinéa supprimé.**	**Alinéa supprimé.**	Le traitement ne comporte pas de dispositif de reconnaissance faciale à partir

Texte adopté par le Sénat en deuxième lecture ___	Texte adopté par l'Assemblée nationale en deuxième lecture ___	Texte adopté par l'Assemblée nationale en nouvelle lecture ___	Texte élaboré par la commission en vue de l'examen en séance publique ___
des images numérisées du visage qui y sont enregistrées.			des images numérisées du visage qui y sont enregistrées.
	Il ne peut y être procédé au moyen des deux empreintes digitales recueillies dans le traitement de données que dans les cas suivants :	~~Il ne peut y être procédé au moyen des deux empreintes digitales recueillies dans le traitement de données que dans les cas suivants :~~	**Alinéa supprimé.**
	1° Lors de l'établissement des titres d'identité ou de voyage ;	~~1° Lors de l'établissement des titres d'identité ou de voyage ;~~	1° **Supprimé.**
	2° Dans les conditions prévues aux articles 55-1, 76-2 et 154-1 du code de procédure pénale ;	~~2° Dans les conditions prévues aux articles 55-1, 76-2 et 154-1 du code de procédure pénale ;~~	2° **Supprimé.**
	3° Sur réquisition du procureur de la République, aux fins d'établir, lorsqu'elle est inconnue, l'identité d'une personne décédée, victime d'une catastrophe naturelle ou d'un accident collectif.	~~3° Sur réquisition du procureur de la République, aux fins d'établir, lorsqu'elle est inconnue, l'identité d'une personne décédée, victime d'une catastrophe naturelle ou d'un accident collectif.~~	3° **Supprimé.**
	Aucune interconnexion au sens de l'article 30 de la loi n° 78-17 du 6 janvier 1978 précitée ne peut être effectuée entre les données mentionnées aux 5° et 6° de l'article 2 de la présente loi contenues dans le traitement prévu par le présent article et tout autre fichier ou recueil de données nominatives.	~~Aucune interconnexion au sens de l'article 30 de la loi n° 78-17 du 6 janvier 1978 précitée ne peut être effectuée entre les données mentionnées aux 5° et 6° de l'article 2 de la présente loi contenues dans le traitement prévu par le présent article et tout autre fichier ou recueil de données nominatives.~~	**Alinéa supprimé.**
	II *(nouveau)*. — L'article 55-1 du code de procédure pénale est complété par un alinéa ainsi rédigé :	~~II. — L'article 55-1 du code de procédure pénale est complété par un alinéa ainsi rédigé :~~	II. — **Supprimé.**
	« Si les nécessités de l'enquête relative aux infractions prévues aux articles 226-4-1, 313-1, 313-2, 413-13, 433-19, 434-23, 441-1 à 441-4, 441-6 et 441-7 du code pénal, aux articles L. 225-7, L. 225-8 et L. 330-7 du code de la route, à l'article L. 2242-5 du code des transports et à l'article 781 du présent code l'exigent, le traitement de	~~« Si les nécessités de l'enquête relative aux infractions prévues aux articles 226-4-1, 313-1, 313-2, 413-13, 433-19, 434-23, 441-1 à 441-4, 441-6 et 441-7 du code pénal, aux articles L. 225-7, L. 225-8 et L. 330-7 du code de la route, à l'article L. 2242-5 du code des transports et à l'article 781 du présent code l'exigent, le traitement de~~	

Texte adopté par le Sénat en deuxième lecture ___	Texte adopté par l'Assemblée nationale en deuxième lecture ___	Texte adopté par l'Assemblée nationale en nouvelle lecture ___	Texte élaboré par la commission en vue de l'examen en séance publique ___
	données créé par l'article 5 de la loi n° du relative à la protection de l'identité peut être utilisé pour identifier, sur autorisation du procureur de la République, à partir de ses empreintes digitales, la personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis ou tenté de commettre une de ces infractions. La personne en est informée. Cette utilisation des données incluses au traitement susvisé doit être, à peine de nullité, mentionnée et spécialement motivée au procès-verbal. Les traces issues de personnes inconnues, y compris celles relatives à l'une des infractions susvisées, ne peuvent être rapprochées avec lesdites données. »	~~données créé par l'article 5 de la loi n° du relative à la protection de l'identité peut être utilisé pour identifier, sur autorisation du procureur de la République, à partir de ses empreintes digitales, la personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis ou tenté de commettre une de ces infractions. La personne en est informée. Cette utilisation des données incluses au traitement susvisé doit être, à peine de nullité, mentionnée et spécialement motivée au procès-verbal. Les traces issues de personnes inconnues, y compris celles relatives à l'une des infractions susvisées, ne peuvent être rapprochées avec lesdites données. »~~	
	III *(nouveau)*. — Le second alinéa de l'article 76-2 du même code est ainsi rédigé : « Les trois derniers alinéas de l'article 55-1 sont applicables. »	~~III. Le second alinéa de l'article 76-2 du même code est ainsi rédigé :~~ ~~« Les trois derniers alinéas de l'article 55-1 sont applicables. »~~	III. — **Supprimé.**
	IV *(nouveau)*. — Le second alinéa de l'article 154-1 du même code est ainsi rédigé : « Les trois derniers alinéas de l'article 55-1 sont applicables. »	~~IV. Le second alinéa de l'article 154-1 du même code est ainsi rédigé :~~ ~~« Les trois derniers alinéas de l'article 55-1 sont applicables. »~~	IV. — **Supprimé.**
	V *(nouveau)*. — La sous-section 1 de la section 3 du chapitre Ier du titre III du livre Ier du même code est complétée par un article 99-5 ainsi rédigé : « *Art. 99-5*. — Si les nécessités de l'information relative à l'une des infractions mentionnées au dernier alinéa de l'article 55-1	~~V. La sous-section 1 de la section 3 du chapitre Ier du titre III du livre Ier du même code est complétée par un article 99-5 ainsi rédigé :~~ ~~« *Art. 99-5*. Si les nécessités de l'information relative à l'une des infractions mentionnées au dernier alinéa de l'article 55-1~~	V. — **Supprimé.**

Texte adopté par le Sénat en deuxième lecture ___	Texte adopté par l'Assemblée nationale en deuxième lecture ___	Texte adopté par l'Assemblée nationale en nouvelle lecture ___	Texte élaboré par la commission en vue de l'examen en séance publique ___
	l'exigent, l'officier de police judiciaire peut, avec l'autorisation expresse du juge d'instruction, utiliser le traitement de données créé par l'article 5 de la loi n° du relative à la protection de l'identité pour identifier une personne à partir de ses empreintes digitales sans l'assentiment de la personne dont les empreintes sont recueillies. »	~~l'exigent, l'officier de police judiciaire peut, avec l'autorisation expresse du juge d'instruction, utiliser le traitement de données créé par l'article 5 de la loi n° du relative à la protection de l'identité pour identifier une personne à partir de ses empreintes digitales sans l'assentiment de la personne dont les empreintes sont recueillies. »~~	
.....	.....	.....	.....