Note d'observations de la Commission nationale de l'informatique et des libertés concernant la proposition de loi relative à la protection de l'identité

Examinée en séance plénière le 25 octobre 2011

Depuis le début des années 2000, plusieurs projets de cartes d'identité biométriques et électroniques ont vu le jour. La Commission a ainsi été saisie par le ministère de l'intérieur de trois avant-projets de loi et s'est prononcée, en particulier en juillet 2008, sur un projet de loi relatif à la protection de l'identité. Celui-ci n'ayant pas été déposé sur le bureau de l'Assemblée nationale, la délibération n° 2008-306 du 17 juillet 2008 n'a pas été rendue publique.

A l'occasion du débat parlementaire en cours sur la proposition de loi n° 682 relative à la protection de l'identité, la CNIL estime nécessaire, conformément à ses missions générales de conseil et d'information prévues par l'article 11 de la loi « Informatique et Libertés », de faire connaître son analyse en la matière. La présente note d'observations, examinée en séance plénière de la Commission le 25 octobre 2011, s'appuie tout particulièrement sur les décisions qu'elle a déjà rendues s'agissant des passeports biométriques (délibération n°2007-368 du 11 décembre 2007), des cartes d'identité électroniques et biométriques (notamment délibération n° 2008-306 précitée), et plus généralement en matière de biométrie, d'administration électronique et de téléservices.

I. Les données biométriques sont des données particulièrement sensibles dont le traitement est strictement encadré par la loi

La Commission rappelle que **les données biométriques ne sont pas des données à caractère personnel « comme les autres »**. Elles présentent en effet la particularité de permettre à tout moment l'identification de la personne concernée sur la base d'une réalité biologique qui lui est propre, permanente dans le temps et dont elle ne peut s'affranchir. A la différence de toute autre donnée à caractère personnel, la donnée biométrique n'est donc pas attribuée par un tiers ou choisie par la personne : elle est produite par le corps lui-même et le désigne ou le représente, lui et nul autre, de façon immuable. Elle appartient donc à la personne qui l'a générée et tout détournement ou mauvais usage de cette donnée fait alors peser un risque majeur sur l'identité de celle-ci.

Cette spécificité des données biométriques a d'ailleurs conduit le Législateur à leur conférer une protection et un encadrement particuliers. La modification de la loi « Informatique et Libertés » intervenue le 6 août 2004 a ainsi renforcé le pouvoir de contrôle de la CNIL sur de tels traitements (autorisation préalable nécessaire), considérés comme présentant des risques particuliers au regard de la vie privée et des libertés individuelles.

La nécessité de prêter une attention particulière aux données biométriques doit être renforcée lorsque la biométrie utilisée est dite « à trace », comme les empreintes digitales par exemple. Celles-ci ont en effet la particularité de pouvoir être capturées et utilisées à l'insu des personnes concernées, comme par exemple à des fins d'usurpation d'identité.

Il en est de même pour les caractéristiques du visage. En effet, si celles-ci ne donnent pas lieu à dépôt de traces, l'association entre vidéoprotection et dispositifs de reconnaissance faciale aboutit à un résultat similaire en créant des traces informatiques en lieu et place des traces physiques laissées par les empreintes digitales.

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

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

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

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

II. Chargée d'appliquer la loi, la CNIL s'est déjà prononcée sur l'utilisation de la biométrie dans le cadre de la délivrance de titres d'identité

Sur la base de cette « grille de lecture », **la Commission s'est prononcée à de multiples reprises sur des projets de traitements biométriques** mis en œuvre dans le cadre de la délivrance de titres d'identité ou de voyage, tout particulièrement dans le cadre de son avis sur **les passeports biométriques**.

La finalité du système des passeports biométriques, autorisé par le décret n° 2005-1726 du 30 décembre 2005 modifié, **est uniquement d'ordre administratif**. Ce traitement a ainsi pour seul objectif de mieux sécuriser la délivrance de ces titres et en particulier de lutter contre la fraude à l'identité.

Pour atteindre cet objectif, le système des passeports biométriques repose sur deux éléments principaux, qui se retrouvent dans la proposition de loi actuellement examinée par le Parlement : la délivrance de passeports équipés de puces électroniques contenant des données biométriques (photographie et deux empreintes digitales) et la création d'une base de données centralisée contenant notamment les empreintes digitales de huit doigts des demandeurs de titre.

Dans son avis du 11 décembre 2007, la Commission a rappelé qu'elle a toujours considéré comme **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 dans un support individuel** exclusivement détenu par la personne concernée. Ainsi, la personne concernée, et elle seule, conserve la maîtrise de ses données biométriques qui restent sous sa responsabilité et ne peuvent pas être utilisées pour l'identifier à son insu.

La CNIL a ainsi relevé que l'insertion d'un composant électronique constitue une mesure efficace de protection contre la falsification ou la contrefaçon des documents dès lors qu'elle permet de s'assurer par des mécanismes cryptographiques de l'authenticité de la puce et de l'intégrité des données qu'elle contient. En outre, l'insertion d'éléments biométriques dans le composant est de nature à empêcher les possibilités d'usurpation d'identité dans la mesure où elle permet leur comparaison avec les empreintes présentées par la personne physique détentrice du titre.

C'est pourquoi **la Commission a estimé que l'introduction dans les titres d'identité et de voyage d'un composant électronique contenant des données biométriques est proportionnée par rapport à l'objectif de renforcement de la sécurité de l'établissement et de la vérification des titres**. En ce qui concerne spécifiquement les passeports, la législation européenne fait d'ailleurs obligation aux Etats membres de délivrer de tels passeports.

L'analyse de la Commission a cependant été différente en ce qui concerne la création de la base de données biométriques centralisée.

Tout d'abord, en ce qui concerne la finalité de ce traitement en base centrale, la Commission a rappelé que le traitement, sous une forme automatisée et centralisée, de données telles que les empreintes digitales, compte tenu à la fois des caractéristiques de l'élément d'identification physique retenu, des usages possibles de ces traitements et des risques d'atteintes graves à la vie privée et aux libertés individuelles en résultant, ne pouvait être admis que dans la mesure où des exigences en matière de sécurité ou d'ordre public le justifient.

Or, ce traitement étant constitué uniquement aux fins de faciliter et de sécuriser les procédures de délivrance des passeports, **la Commission a considéré que, si légitimes soient-elles, les finalités invoquées 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.

En outre, **la proportionnalité du traitement en base centrale des empreintes digitales des demandeurs de titre a fait l'objet de réserves de la part de la Commission**.

Celle-ci a ainsi rappelé que **la création d'une base centralisée de données biométriques de grande ampleur comporte des risques importants et implique des sécurités techniques complexes et supplémentaires**. En effet, un fichier est d'autant plus vulnérable, « convoité » et susceptible d'utilisations multiples qu'il est de grande dimension, qu'il est relié à des milliers de points d'accès et de consultation, et qu'il contient des informations très sensibles comme des données biométriques.

La CNIL a également souligné que **le recueil de huit empreintes digitales et leur conservation en base centrale ne résultaient pas des prescriptions du règlement communautaire relatif aux passeports.** Or, le nombre d'empreintes digitales enregistrées dans le traitement central revêt un aspect déterminant dans l'appréciation du caractère pertinent, adéquat et non excessif des données collectées au regard de la finalité du traitement. A cet égard, la Commission relève que le Conseil d'Etat, saisi de requêtes en annulation du décret relatif aux passeports, devrait se prononcer prochainement sur ce point.

Elle a enfin relevé qu'**un dispositif biométrique de lutte contre la fraude ne peut être pleinement efficace que si les documents d'état civil produits par les demandeurs pour se faire enregistrer dans le système sont fiables**. Or, aucune mesure particulière n'était prévue par le ministère de l'intérieur afin de sécuriser ces « documents sources ».

Au regard de l'ensemble de ces éléments, **la Commission a estimé que la conservation sous forme centralisée des huit empreintes digitales des demandeurs de passeport semblait disproportionnée au regard de l'objectif de lutte contre la fraude documentaire.**

III. Application de ces principes au cas de la proposition de loi relative à la protection de l'identité

La proposition de loi relative à la protection de l'identité reprend dans une large mesure le dispositif mis en œuvre dans le cadre des passeports biométriques ainsi que les précédents projets du ministère de l'intérieur relatifs aux cartes d'identité biométriques et électroniques. Plus précisément, elle poursuit trois objectifs principaux :

- garantir une meilleure fiabilité des cartes nationales d'identité et des passeports, en équipant ces titres de puces électroniques contenant des données biométriques (photographie et empreintes digitales) ;

- lutter contre la fraude à l'identité, en créant un traitement de données à caractère personnel pour faciliter le recueil et la conservation des données requises pour la délivrance de ces titres (données biométriques et autres données d'identification nécessaires à cette délivrance) ;

- offrir aux titulaires de cartes d'identité de nouveaux services tels que l'authentification à distance et la signature électronique.

1) Sur la légitimité de la délivrance de titres biométriques

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

La délivrance de tels documents doit cependant, selon la Commission, être assortie de garanties complémentaires. Celles-ci pourraient porter en premier lieu sur **l'âge minimal de collecte des identifiants biométriques** : pour la CNIL, la détermination de cet âge **n'est pas seulement un élément technique mais une question de principe** méritant un large débat. Pour préserver la dignité de la personne ainsi que pour garantir la fiabilité de la procédure, la Commission considère que la collecte et le traitement des empreintes digitales devraient être limités pour les enfants, par exemple en prévoyant une dispense de collecte pour les enfants de moins de douze ans, comme le prévoit d'ailleurs le droit communautaire en la matière.

En second lieu, la Commission estime que la comparaison entre la donnée biométrique enregistrée dans le composant et l'empreinte lue en direct sur un lecteur pourrait se faire dans la carte elle-même. La mise en œuvre de cette **technique**, dite **« *match on card* »**, serait

susceptible d'apporter une garantie supplémentaire à la protection des données à caractère personnel, en **évitant toute possibilité de copie externe**. D'autres mesures techniques et logiques doivent également être prévues afin d'assurer la sécurité de ces composants et des données à caractère personnel qui y sont contenues.

2) Sur la création de la base de données biométriques

Deux catégories de finalités peuvent être attribuées au traitement centralisé de données biométriques dans le cadre des documents d'identité et de voyage : soit le traitement a pour finalité la gestion des procédures administratives de délivrance des titres, et en particulier la lutte contre la fraude à l'identité, soit il s'agit un nouvel outil de police judiciaire. Ces deux finalités n'appellent pas les mêmes dispositifs techniques ni les mêmes garanties en matière de protection des données des personnes concernées.

Dans le cadre de la proposition de loi relative à la protection de l'identité, le système projeté a pour seul objectif de mieux sécuriser la délivrance de ces titres et en particulier de lutter contre la fraude à l'identité. Dès lors, il s'agirait uniquement de créer un fichier administratif, semblable au traitement déjà mis en œuvre relatif aux passeports biométriques, et en aucun cas de constituer un outil de police judiciaire à la disposition des services de police et de gendarmerie.

Il convient cependant de **s'assurer que le traitement créé ne peut être utilisé à d'autres fins** que la sécurisation de la délivrance des titres d'identité et de voyage, par exemple en le prévoyant expressément dans la loi. De même, l'interdiction de procéder à l'interconnexion avec tout autre traitement de données à caractère personnel, à l'exception des fichiers de passeports et de cartes d'identité volés ou perdus, pourrait être prévue dans le texte de la proposition de loi.

Il conviendrait également de **s'assurer qu'un tel système ne soit pas détourné de sa finalité** par un recours systématique aux réquisitions judiciaires, qui sont possibles sur tout traitement de données à caractère personnel en application des dispositions du code de procédure pénale. En effet, une consultation systématique du fichier aurait pour effet de le doter *de facto* d'une finalité de police judiciaire, qui constitue une finalité distincte.

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

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

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

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

Si une telle base centralisée de données biométriques était néanmoins envisagée, des garanties supplémentaires de nature à assurer la protection des données personnelles des citoyens français devraient être introduites.

Par exemple, **la limitation du nombre d'empreintes digitales enregistrées dans la base centrale** pour chaque personne pourrait être envisagée. La Commission considère en effet que la limitation à deux doigts constituerait une garantie matérielle contre le détournement de finalité du système, en empêchant les recherches en identification sur la base des empreintes digitales, tout en permettant de vérifier la correspondance entre l'identité revendiquée et les empreintes présentées. Comme indiqué précédemment, le Conseil d'Etat devrait d'ailleurs se prononcer prochainement sur la pertinence de l'enregistrement de huit empreintes digitales au regard de la finalité du traitement relatif aux passeports.

D'**autres mesures** permettraient également de limiter les possibilités d'utilisation de la base de données biométriques à la seule fin de lutte contre la fraude à l'identité. Ainsi de **l'absence de lien univoque entre les données biométriques enregistrées dans le traitement central et les données d'état civil** des personnes auxquelles ces données correspondent, ou de **l'interdiction expresse de procéder à des recherches en identification** sur la base des éléments biométriques enregistrées dans la base.

3) Sur la possibilité de mettre en œuvre des dispositifs de reconnaissance faciale : les réserves de la Commission

Si les remarques qui précèdent concernant la base centralisée de données biométriques valent tout autant pour les empreintes digitales que pour les photographies, la Commission relève que **les fonctionnalités d'identification des personnes, à partir de l'analyse biométrique de la morphologie de leur visage, revêtent un caractère particulier.**

En effet, la Commission considère que la mise en œuvre par l'Etat de dispositifs de reconnaissance faciale des personnes présente des risques importants pour les libertés individuelles, notamment dans le contexte actuel de multiplication du nombre des systèmes de vidéoprotection, de leur interconnexion et de leur interopérabilité. Dans ces conditions, **la CNIL exprime sa plus grande réserve sur la possibilité**, ouverte par la proposition de loi, **de recourir à de telles fonctionnalités** dans le cadre des demandes de titres d'identité et de voyage

Compte tenu de ces risques, il serait souhaitable de prévoir un cadre juridique spécifique et limité, propre à l'utilisation des technologies de reconnaissance faciale à des fins d'identification des personnes par l'Etat. En tout état de cause, la Commission estime que de tels traitements biométriques devraient faire l'objet d'expérimentations préalables, placées sous son contrôle.

4) Sur les fonctions électroniques de la carte nationale d'identité

La proposition de loi prévoit de nouvelles fonctionnalités de la carte nationale d'identité, qui permettra de s'authentifier en ligne et de signer électroniquement. La Commission considère que l'**objectif de simplification des démarches administratives en ligne et de développement du commerce électronique est tout à fait légitime**.

Cependant, de telles fonctions électroniques appellent des garanties particulières, dans la mesure où elles pourraient permettre la constitution d'un identifiant unique pour tous les citoyens français ainsi que la constitution d'un savoir public sur les agissements privés. C'est pourquoi le dispositif projeté doit empêcher la collecte excessive de données, le suivi des personnes sur internet ainsi que l'usurpation de l'identité numérique.

A cet égard, la Commission relève que **plusieurs garanties essentielles** sont prévues par la proposition de loi, comme par exemple **le caractère facultatif de sa détention pour bénéficier des téléservices** commerciaux ou de l'administration ou encore **le consentement des personnes au traitement de leurs données à des fins d'utilisation de téléservices**.

En outre, elle souligne que l'utilisation de téléservices impliquera nécessairement la mise en œuvre de certificats électroniques, enregistrés dans la puce à contact de la carte d'identité contenant 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.). Il apparaît dès lors nécessaire de s'assurer que seules les données personnelles nécessaires aux transactions électroniques sont communiquées lors de l'utilisation de ces téléservices.

Dans ces conditions, la Commission estime que de telles fonctionnalités doivent être accompagnées de la mise en place de **mécanismes dits de « divulgation partielle » ou « sélective »**, qui permettent de ne communiquer que les seules informations requises, selon la nature du téléservice, pour assurer les vérifications préalables utiles à la mise en œuvre de celui-ci (critère géographique, d'âge, etc.). Si la proposition de loi semble prévoir de tels mécanismes, il convient cependant de bien les distinguer, dans le texte, de la **nécessaire information, claire et préalable à toute transmission de données, des personnes concernées,** notamment sur la nature des informations communiquées au téléservice.

Par ailleurs, de telles fonctionnalités ne devraient pas permettre le suivi des personnes sur internet ou l'**exploitation par l'Etat d'informations sur les transactions privées effectuées par les citoyens**. Une telle interdiction serait utilement rappelée dans le texte prévoyant ces nouvelles fonctionnalités de la carte électronique. Des mesures techniques de nature à garantir l'impossibilité de tracer l'ensemble des transactions effectuées par les personnes, telles que l'inclusion d'autres certificats dans la puce électronique de la carte d'identité, l'utilisation de listes de révocation et non de serveurs de révocation, ainsi que la définition de politiques rigoureuses d'habilitation et de traçabilité au sein des organismes de certification, pourraient également être prévues.

Enfin, des mesures techniques de nature à garantir l'absence de constitution d'un identifiant unique (la création d'identifiants sectoriels spécifiques à chaque prestataire) ainsi que la sécurité des communications entre la carte d'identité et les lecteurs d'une part, entre la carte, les fournisseurs de téléservice et le tiers certificateur d'autre part, devraient également faire l'objet de spécifications techniques détaillées.

Isabelle FALQUE-PIERROTIN