

26<sup>e</sup> Conférence internationale sur la vie privée et la protection des données personnelles  
Wroclaw, 14-16 septembre 2004

Session : Droit à la vie privée et protection de la sécurité publique

Intervention de M. François GIQUEL,  
Commissaire, Commission Nationale de l'Informatique et des Libertés, Franc

Dès 1986, à la suite d'une vague d'attentats sur son territoire, la France s'était dotée d'une législation contre le terrorisme prévoyant notamment la centralisation des poursuites pénales en matière de crimes et délits liés au terrorisme, des juridictions spécialisées pour les juger et des pouvoirs de police judiciaire plus étendus que dans les autres domaines. Mais les événements du 11 septembre aux Etats-Unis, et d'autres impératifs intérieurs, comme la lutte contre toutes les formes de délinquance ont conduit les pouvoirs publics à renforcer la protection de la sécurité publique.

Plusieurs lois ont ainsi été votées depuis trois ans, et de nombreuses dispositions réglementaires ont été prises, comportant notamment la création ou l'extension de divers fichiers informatiques, afin d'assurer le suivi toujours plus précis de populations toujours plus nombreuses, ce qui a posé en termes plus aigus que jamais les problèmes de la protection des données personnelles.

Dans ce contexte sensible, la Commission nationale de l'informatique et des libertés a bien entendu été amenée à prendre part au débat public et à rappeler les garanties fondamentales qui, selon elle, devaient être instaurées pour assurer un juste équilibre entre le respect de la vie privée et des libertés individuelles et les impératifs de sécurité publique. Si toutes ses préoccupations n'ont pas été prises en considération, un certain nombre d'entre elles ont été comprises et admises.

C'est ce que j'essayerai de montrer rapidement dans le premier point de cette intervention, à seule fin d'illustrer par l'exemple français une problématique à laquelle mes homologues ont tous été confrontés. Dans un second temps, je tenterai d'exposer les nouveaux défis, les problématiques particulières auxquelles nous devons faire face aujourd'hui du fait de la dimension désormais mondiale des questions de sécurité.

## **I. LA REPONSE FRANÇAISE**

### **1. Une utilisation plus large des fichiers de police judiciaire**

Une première loi, intervenue en 2001 (loi « relative à la sécurité quotidienne ») a autorisé la consultation des fichiers de police judiciaire dans le cadre de certaines enquêtes administratives destinées à vérifier la moralité des personnes candidates ou exerçant des fonctions ou des missions de sécurité ou de défense, ou encore des activités les conduisant à accéder à des zones protégées(ex : centrales nucléaires, zones d'aéroports...) ou à utiliser du

matériel ou des produits dangereux , et ce « dans la stricte mesure exigée par la protection de la sécurité des personnes et la défense des intérêts fondamentaux de la nation ».

La CNIL n'a pas été consultée sur ces dispositions mais lors des avis rendus en 1998 et en 2000 sur le fichier national de police judiciaire STIC, géré par le ministère de l'intérieur, elle avait pris position sur la question , exprimant de sérieuses réserves sur la possibilité de consulter un tel fichier dans le cadre de missions de police administrative, dès lors qu'en particulier ces consultations portaient sur des procédures judiciaires en cours, ce qui lui paraissait contraire au secret de l'enquête et de l'instruction. Le législateur n'a pas suivi la CNIL.

En 2003, une nouvelle loi (dite loi pour la sécurité intérieure) a considérablement élargi la possibilité de consulter les fichiers de police judiciaire à des fins d'enquêtes administratives, en particulier pour l'instruction des demandes d'acquisition de la nationalité française, des demandes de délivrance et de renouvellement des titres relatifs à l'entrée et au séjour des étrangers, des demandes d'autorisation de port d'armes ainsi que la nomination et la promotion dans les ordres nationaux.

La CNIL a fait connaître sa position au Gouvernement et au Parlement, dès l'ouverture du débat parlementaire, estimant que ces dispositions soulevaient, sur plusieurs points, des questions graves au regard des principes généraux de la protection des données personnelles.

La Commission a ainsi réaffirmé son opposition à une utilisation administrative des fichiers de police judiciaire, sauf dans des cas exceptionnels, et appelé l'attention sur les risques de dérives graves et d'atteinte aux libertés individuelles et droits des personnes susceptibles d'en résulter, de tels fichiers n'étant pas conçus pour faire ainsi office de casiers judiciaires et ne comportant pas en particulier les garanties nécessaires pour permettre le respect effectif du droit à l'oubli, notamment en cas d'amnistie ou d'acquiescement. Des affaires récentes (licenciements abusifs à la suite de la consultation de fichiers de police judiciaire) ont montré que malheureusement ces risques sont bien réels et peuvent être aggravés dès lors que ces fichiers ne sont pas correctement mis à jour.

## **2. Des fichiers de police mieux encadrés**

Si la CNIL n'a pu obtenir satisfaction sur cette utilisation administrative des fichiers de police, elle a pu en revanche faire valoir auprès du Parlement, dans le cadre d'auditions, ses observations et propositions sur la nécessité d'inscrire dans la loi certaines garanties jugées par elle indispensables s'agissant de fichiers nationaux de police.

En effet, un certain nombre de garanties ont été inscrites pour la première fois dans la loi ; il en est ainsi en particulier :

- du contrôle de l'autorité judiciaire sur ces fichiers,
- de la limitation de la durée de conservation des informations, en particulier en fonction du degré de gravité de l'infraction et de l'âge de la personne mise en cause,
- du renforcement du principe de la mise à jour, voire, dans certaines conditions, de l'effacement des données concernant les personnes mises en cause et les victimes ;
- de l'encadrement des échanges de données réalisés dans le cadre des engagements internationaux, avec des organismes de coopération internationale en matière de

- police judiciaire ou des services de police étrangers devant présenter un niveau de protection des données suffisant ;
- de l'assouplissement des procédures de droit d'accès indirect aux fichiers de police, qui s'exerce en France, par l'intermédiaire d'un des magistrats de la CNIL. Désormais, après accord du responsable du fichier, les informations enregistrées dans un fichier de police peuvent être communiquées à la personne concernée,.

Saisi de la loi, **le Conseil constitutionnel a considéré que l'ensemble des garanties que ce texte offre en matière de création et d'utilisation des fichiers de police « est de nature à assurer, entre le respect de la vie privée et la sauvegarde de l'ordre public, une conciliation qui n'est pas manifestement déséquilibrée ».**

La modification de la loi française de protection des données, intervenue récemment (loi du 6 août 2004), maintient un contrôle préalable de la CNIL sur toute création de fichier intéressant la sécurité publique, la défense et la sûreté de l'Etat ou comportant l'utilisation de données biométriques.

### **3. Un accès élargi des services de police aux fichiers informatiques existant dans d'autres secteurs**

Egalement introduites en 2001 mais renforcées en 2003, différentes mesures (dont certaines ont d'ailleurs été préparées bien avant les événements du 11 septembre) visent à faciliter par des liaisons informatiques l'accès direct des services de police judiciaire à un certain nombre de fichiers de données à caractère personnel (tout particulièrement les fichiers des opérateurs de télécommunications et des fournisseurs d'accès à internet) .

Ces mesures, ont, pour certaines (données de connexion) fait l'objet de consultations de la CNIL.

La loi de 2001 a ainsi obligé les fournisseurs d'accès à conserver les données de connexion à internet, pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, tout en précisant que les données conservées ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées. La durée de conservation a été fixée par la loi à un an maximum, alors que la CNIL avait proposé que la durée de conservation des données de connexion soit limitée à trois mois.

La loi a aussi prévu la possibilité pour l'autorité judiciaire de prescrire le déchiffrement de données cryptées, saisies ou obtenues au cours d'une enquête ou d'une instruction.

Par ailleurs, les règles de procédure pénale ont été modifiées de façon à permettre tout d'abord à tout officier de police judiciaire, au cours d'une perquisition, d'accéder par un système informatique implanté sur les lieux où se déroule la perquisition, à des données intéressant l'enquête en cours et stockées dans le dit système ou dans un autre système informatique et d'en faire copie.

En outre, sur demande de l'officier de police judiciaire qui peut intervenir par voie télématique ou informatique, les organismes publics ou les personnes morales de droit privé, à l'exception des églises et groupements à caractère religieux, philosophique, politique,

syndical et des organismes de presse, sont tenus de mettre à sa disposition les informations utiles à la manifestation de la vérité, à l'exception de celles protégées par un secret prévu par la loi, contenues dans le ou les systèmes informatiques ou traitements de données nominatives.

De même, il peut être fait obligation aux opérateurs de télécommunications, sur réquisition du procureur de la République, de conserver pendant une durée ne pouvant excéder un an, le contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs, ces informations devant être tenues à disposition par voie télématique ou informatique.

Ces nouvelles dispositions, en permettant un accès direct et en ligne aux fichiers, élargissent considérablement les possibilités d'interrogation des fichiers informatiques par les services de police.

#### **4. La création de nouveaux fichiers ou l'extension de fichiers existants**

Dans les trois dernières années, la loi a permis la création de nouveaux fichiers spécialisés de police et l'extension de certains de ceux qui existaient déjà.

- Il en est ainsi en particulier, du fichier national des empreintes génétiques.

A sa création, ce fichier recensait uniquement les empreintes génétiques de personnes définitivement condamnées pour des infractions graves présentant un caractère sexuel. La liste de ces infractions a été élargie une première fois par la loi pour la sécurité quotidienne de 2001 à des infractions à caractère terroriste ou d'atteinte contre les biens, puis une seconde fois, par la loi de 2003, au point de changer la nature même du fichier, conçu à l'origine pour faciliter l'identification et la recherche des auteurs des infractions sexuelles et qui, aujourd'hui, concerne la quasi-totalité des crimes et des délits d'atteinte aux biens ou aux personnes ainsi que les trafics.

En ce qui concerne les personnes concernées, le fichier a connu une évolution comparable : devant, à l'origine, recenser uniquement les empreintes génétiques de personnes condamnées définitivement, les modifications résultant de la loi de 2003 permettent désormais d'inclure au fichier l'empreinte génétique des personnes mises en examen (alors que jusqu'à présent leur empreinte génétique pouvait seulement faire l'objet d'une comparaison avec le contenu du fichier sans conservation).

Consultée sur le décret d'application de la loi, la CNIL a estimé que l'importance de cette double extension du champ d'application du fichier nécessitait des garanties sérieuses destinées à prévenir tout enregistrement non contrôlé, erroné ou abusif des personnes et tout usage d'un tel fichier à des fins étrangères à celles pour lesquelles il a été constitué. Elle a ainsi obtenu un certain nombre de garanties parmi lesquelles une réduction de la durée maximale de conservation des informations relatives aux personnes mises en cause, fixée à vingt-cinq années au lieu des quarante prévues à l'origine .

La CNIL avait précédemment obtenu que les empreintes génétiques inscrites dans le fichier ne puissent être réalisées que sur la partie non codante de l'ADN, garantie désormais inscrite dans la loi.

- En mars 2004, dans le cadre d'une loi portant adaptation de la justice aux évolutions de la criminalité, le législateur a souhaité créer un fichier central comportant l'adresse des auteurs de certaines infractions à caractère sexuel afin de prévenir le renouvellement des infractions concernées et de faciliter l'identification de leurs auteurs, en faisant ainsi obligation à ces personnes de justifier de leur adresse une fois par an et de déclarer leurs changements d'adresse au gestionnaire du fichier ou au commissariat de police ou à la brigade de gendarmerie de son domicile.

Bien que non saisie, la CNIL a fait part au Pparlement de ses préoccupations sur trois aspects de la création de ce fichier :

- le caractère automatique de l'inscription et la durée uniforme de la durée de conservation des informations nominatives enregistrées, fixée à quarante ans, sans que soient pris en considération, notamment, la nature de l'infraction commise, l'âge de son auteur au moment des faits et la gravité de la mesure ou de la décision prononcée à son encontre ;

- l'extrême sensibilité des informations enregistrées dans le fichier, qui appelait des garanties voisines de celles qui entourent le fonctionnement du casier judiciaire national automatisé, aussi bien pour la saisie des informations que pour l'accès au fichier ;

- la possibilité pour les autorités administratives d'avoir accès à ce fichier pour « *l'examen des demandes d'agrément concernant des activités ou professions impliquant un contact avec des mineurs* », la Commission considérant que cet accès à des fins purement administratives n'était pas cohérent avec la finalité judiciaire de ce fichier .

Sur ces trois points, la Commission a pu obtenir, comme pour les autres fichiers de sécurité publique, que les garanties minimales qui doivent selon elle accompagner toute création de fichier de ce type, soient inscrites dans la loi (durées de conservation graduées selon la gravité de l'infraction, procédure d'effacement des données notamment en cas d'acquiescement, mesures de sécurité renforcées pour l'accès au fichier, restrictions d'accès pour les autorités administratives). En outre, comme tout autre fichier elle devra bien entendu être consultée sur les modalités de fonctionnement de ce fichier.

## II. LES NOUVEAUX DEFIS

Je souhaiterais évoquer maintenant deux dossiers qui me paraissent particulièrement significatifs de la dimension mondiale que prennent aujourd'hui les questions de sécurité : les transferts de données sur les passagers et la biométrie.

### 1. L'accès aux bases de données de réservation des compagnies aériennes (APIS-PNR).

Comme on le sait, la législation antiterroriste américaine a prévu de manière unilatérale l'obligation pour toute compagnie aérienne assurant des vols à destination des Etats-Unis de donner, sur demande, aux services de contrôle aux frontières américaines, accès aux données de réservation de leurs passagers dits "Passenger Name Record" (PNR). Cette disposition s'est très rapidement transformée en une réglementation relative à l'accès direct

des autorités américaines aux systèmes globaux de réservation aérienne, peu importe leur localisation dans le monde.

Je ne referai pas ici l'historique de cette affaire dont l'aboutissement dans les relations entre l'Europe et les Etats Unis conduit actuellement à un double recours du Parlement européen devant la Cour européenne de justice, d'une part contre le Conseil (les Gouvernements des Etats membres) portant sur l'accord international passé et d'autre part contre la Commission européenne portant sur sa décision d'adéquation qui pourrait aboutir à une renégociation. On connaît la position des commissaires à la protection des données réunis dans le groupe dit "de l'article 29" à l'égard de cette affaire.

Je voudrais à ce stade tirer quelques enseignements pour nos réflexions à venir qui montrent des possibilités d'évolution d'ores et déjà très concrètes dans un sens favorable à la protection des droits des personnes et à l'établissement de solutions plus proportionnées et respectueuses des droits.

- Aux Etats Unis, certains des projets les plus attentatoires aux libertés fondés sur ces données, tel CAPPS II, ont été abandonnés quelques semaines après l'accord Europe USA alors même que celui ci avait permis de tester ce système.

- La communication des données de réservation exigées par le Canada ou l'Australie correspond à des schémas différents et plus mesurés; l'Australie, par exemple ne souhaite conserver aucune donnée sauf celles relatives aux personnes qui auront fait l'objet d'une vérification particulière. Ces approches différentes montrent qu'un certain débat s'instaurera nécessairement sur les solutions ou s'est d'ores et déjà instauré.

- Les autorités indépendantes en charge de la protection des données ont parmi leurs exigences demandé que les compagnies aériennes communiquent elles mêmes les données expurgées de celles qui ne doivent pas être communiquées en remplacement de la solution initialement retenue par les autorités américaines consistant à accéder directement aux systèmes de réservation avec les mêmes droits que les compagnies aériennes. Nous observons depuis quelques semaines, contrairement à il y a seulement quelques mois, un vif intérêt des compagnies européennes pour l'approche prônée par les commissaires qui d'ailleurs pourrait être mise en oeuvre avant la fin de l'année.

Ces évolutions dans un espace de temps très rapide montrent qu'il convient de pousser plus loin l'analyse et de continuer à oeuvrer pour inciter à des solutions plus appropriées et proportionnées, voire à reposer la question en des termes nouveaux, d'autant que, sans préjuger des décisions de la Cour Européenne de Justice, l'accord passé entre les Etats Unis et l'Europe a une durée de 3 années et demie.

A vrai dire, cette affaire aurait dû être posée en termes de sûreté des transports aériens plutôt qu'en termes de flux transfrontières de données et d'adéquation comme elle l'a été jusqu'à maintenant.

Dès lors il aurait peut être été possible, il est sans doute encore possible de répondre aux préoccupations de sûreté du transport aérien, d'abord par le renforcement de la coopération



policière, et, si un accès aux listes de passagers est nécessaire, ce qui paraît parfaitement légitime, il pourrait l'être d'une manière beaucoup moins disproportionnée.

## 2. Le développement du recours aux techniques biométriques

Au plan européen, des initiatives ont été lancées pour systématiser l'introduction de données biométriques dans les visas, les titres de séjour et les passeports et à mettre en place un système commun d'information sur les visas (VIS) qui permettrait de recenser dans une base unique les demandes et les refus de visas.

Ces projets soulèvent des questions de première importance au regard des principes de protection des données personnelles et nécessitent aujourd'hui des prises de positions communes de la part de l'ensemble des autorités de protection des données.

L'avis du groupe de l'article 29 du 11 août 2004 doit à cet égard être particulièrement salué comme constituant une première initiative significative en ce sens. Cet avis peut se résumer ainsi :

1- le traitement des données biométriques est susceptible d'avoir de très fortes répercussions sur les droits fondamentaux des personnes concernées et ce d'autant plus qu'il porterait sur des éléments dont les personnes laissent des traces dans la vie quotidienne (empreintes digitales en particulier) ;

2- le groupe reconnaît la légitimité de la finalité de l'insertion proposée de la photo et des empreintes digitales dans une puce sans contact en vue d'établir un lien plus fiable entre le visa ou le titre de séjour et son titulaire (vérification de l'identité). Cependant :

- cette finalité doit être précisée dans la réglementation trop vague sur ce point,
- sa mise en oeuvre suppose que soient traitées une série de questions relatives à la fiabilité et à la sécurité des systèmes qui seront retenus :
  - sécurité du processus de collecte et d'insertion (contre fraude à l'identité, erreurs, captation, signature électronique etc),
  - garanties lorsque la personne ne dispose pas des éléments biométriques en cause,
  - haute fiabilité des systèmes et garanties contre les faux rejets,
  - mesures contre l'accès à l'insu de la personne ou par des personnes non autorisées (chiffrement des données dans la puce et protection par un code personnel du porteur).

3 - le groupe a aussi exprimé de sérieuses réserves, au regard du principe de proportionnalité et de l'accroissement des risques d'usage à d'autres fins, en ce qui concerne la conservation souhaitée par le Conseil des données biométriques dans des bases de données au delà de la période nécessaire aux contrôles légaux pour la délivrance des documents, à leur production et à de leur remise aux demandeurs lorsque le choix s'est porté sur des éléments biométriques dont la personne laisse des traces dans la vie quotidienne. Cette conservation est présentée comme nécessaire en l'état dans le cadre du contrôle des immigrants illégaux (en particulier ceux qui ne disposent d'aucun document).

Le groupe a ainsi souhaité avoir communication des études pouvant justifier les exigences impérieuses en matière de sécurité ou d'ordre public qui imposeraient une telle approche et

savoir si des approches alternatives ont été ou pourraient être étudiées qui ne présenteraient pas les mêmes risques

4- Sur les autres orientations exprimées par le Conseil en ce qui concerne la base de données européenne des visas/titre de séjour, à partir desquelles la Commission doit préparer une proposition de cadre juridique, le groupe s'est exprimé sur différents points:

- nécessité d'une évaluation précise des finalités envisagées qui sont très larges,
- interrogation sur la centralisation européenne de certaines données, notamment sur les personnes hébergeant ou prenant en charge les frais d'hébergement des étrangers,
- difficultés majeures en matière d'accès par des pays tiers,
- information des étrangers sur leurs droits,
- restriction de la durée de conservation des données à 5 ans maximum et non minimum,
- mesures de sécurité.

La CNIL suit pour sa part d'autant plus attentivement les travaux conduits au plan européen qu'une loi intervenue à la fin de l'année 2003<sup>1</sup> a réformé de façon substantielle les procédures de vérification des identités lors de la délivrance des visas et lors du contrôle aux frontières en généralisant le recours aux techniques biométriques, et que le ministère de l'Intérieur étudie actuellement un projet de carte d'identité électronique intégrant les empreintes digitales.

S'agissant de l'intégration de données biométriques dans les visas et les titres de séjour, la loi française prévoit que les empreintes digitales des ressortissants étrangers, non ressortissants d'un État membre de l'Union européenne, pourront être relevées, mémorisées et faire l'objet d'un traitement automatisé non plus seulement dans les cas de demandes de délivrance d'un titre de séjour de plus de 3 mois<sup>2</sup> et d'étrangers en situation irrégulière ou faisant l'objet d'une mesure d'éloignement du territoire français, mais également dans les cas **de demandes de visas** ou encore d'étrangers qui, ayant été contrôlés à l'occasion du franchissement de la frontière en provenance d'un pays tiers, ne seront pas munis des titres nécessaires ou ne rempliront pas les conditions d'entrée sur le territoire .

La CNIL, saisie pour avis du projet de loi, avait estimé que la mémorisation et le traitement de données issues des empreintes digitales, compte tenu des caractéristiques de l'élément d'identification physique retenu et des usages possibles des bases de données qui pourraient ainsi être constituées, ne pouvaient être admis que s'ils étaient justifiés par des exigences impérieuses en matière de sécurité ou d'ordre public et que si des garanties appropriées (durée de conservation limitée, accès restreint aux données par des personnels habilités, mesures d'effacement) étaient prises pour assurer le respect des droits et libertés individuelles, et ce d'autant plus que ces bases de données d'empreintes digitales seraient susceptibles de concerner à court terme plusieurs millions de personnes.

Elle a aussi estimé que la loi devrait clairement indiquer les finalités pour lesquelles il pourra être procédé à des traitements automatisés d'empreintes digitales des étrangers et que ses modalités d'application sur lesquelles la CNIL devra être consultée devront préciser notamment les modalités d'habilitation des personnes pouvant accéder aux informations, la

---

<sup>1</sup> loi du 24 novembre 2003 relative à l'immigration

<sup>2</sup> Disposition intervenues en 1997 non encore appliquée



durée de conservation et les conditions de mise à jour des informations enregistrées ainsi que l'exercice de leur droit d'accès par les personnes concernées<sup>3</sup>.

Je ne traiterai pas plus en détail de ces questions qui font par ailleurs l'objet d'une session parallèle dans le cadre de cette conférence tant en effet les questions sont multiples. Qu'il me soit cependant permis de poursuivre la réflexion engagée par deux réflexions d'ordre général complémentaires.

- Pour légitimes que soient les motifs de conservation des empreintes digitales, le risque est grand que ces données puissent servir ultérieurement à d'autres fins.
- Les travaux menés au plan mondial pour la standardisation des technologies et des applications en cause, fortement poussés par les industriels du secteur, conduisent nécessairement à ce que ces applications concernent à terme la planète entière. Mais dès lors, ne pourront-elles pas aussi être facilement à la disposition de régimes non démocratiques ? Ces dernières préoccupations font d'ailleurs écho aux questions soulevées par le Conseil de l'Europe dans un rapport d'étape sur la biométrie soumis actuellement à consultation.

Force est de constater que l'opinion publique s'intéresse peu à ces questions et serait même rassurée par l'adoption des techniques biométriques et la conservation de leurs empreintes digitales pour garantir leur identité.

Mais n'y a-t-il pas des périodes, des sujets, sur lesquels il nous revient, commissaires à la protection des données, de faire progresser le débat public, en particulier par une contribution directe aux études et réflexions qui font actuellement défaut et qui devraient pourtant être conduites, pour évaluer clairement la justification de l'emploi, dans ces domaines, des techniques biométriques et le recours de moyens alternatifs moins attentatoires aux libertés ?

Il me paraît ainsi, qu'au-delà de ce rendez vous annuel, un renforcement de la coopération entre autorités de protection des données sur ces sujets serait particulièrement opportun.

## Conclusions

---

<sup>3</sup> Ces réserves de principe ont aussi été rappelées expressément par la CNIL lors des premières observations qu'elle a adressées au ministère de l'Intérieur sur la carte d'identité électronique. Ce projet de refonte des titres d'identité consisterait à remplacer la carte d'identité actuelle par une carte à microprocesseur qui, dans le cadre du développement de l'administration électronique, pourrait être utilisée pour accéder à des téléservices. Cette carte pourrait comporter les empreintes digitales, susceptibles d'être conservées dans une base centrale, comme d'ailleurs les photographies. La CNIL a en conséquence demandé au ministère de l'Intérieur qu'un argumentaire précis lui soit fourni en particulier sur les finalités et les modalités selon lesquelles seraient utilisées les données biométriques, qu'il s'agisse de leur consultation par lecture directe de la carte d'identité ou de la conservation, dans une base de données centrale, des empreintes digitales. Il faut rappeler que la CNIL, lorsqu'elle s'est prononcée en 1986 sur le projet de carte d'identité infalsifiable, s'était attachée à obtenir toutes garanties de nature à éviter que la délivrance de ces nouveaux titres ne puisse conduire à un contrôle généralisé des individus et à la constitution d'un fichier national de population. Elle avait en particulier obtenu du ministère de l'Intérieur l'assurance qu'aucun fichier national d'empreintes ne serait constitué, les relevés d'empreintes n'étant conservés que dans les dossiers manuels détenus par les préfectures.

Dans la recherche du point d'équilibre entre sécurité et libertés, nous devons être guidés par deux préoccupations majeures dans le domaine du traitement de l'information de nature policière: la recherche de proportionnalité dans toutes les dimensions des projets d'une part et, d'autre part, la mise en œuvre, de toutes les garanties de protection des données nécessaires pour assurer un fonctionnement des fichiers, qui soit pleinement respectueux des valeurs et principes qui fondent nos sociétés démocratiques.