

**Audition de Monsieur Guy CANIVET
Premier Président de la Cour de Cassation**

18 MAI 2005

Tout en m'appuyant sur les éléments du dossier que la CNIL m'a adressé, je ferai les observations suivantes.

I. Le contexte du projet

1. Le contexte géographique

L'introduction de la biométrie dans les documents d'identité répond à la volonté de réguler la circulation des individus sur un espace géographique donné. Cette problématique s'inscrit à la fois dans un cadre national, européen et mondial.

Sur le plan national, les éléments d'informations ne manquent pas. Comme le montre la consultation du site Internet de la CNIL, la question biométrique n'est pas nouvelle. Cette instance a ainsi déjà rendu des avis divers relatifs à l'introduction de la photographie numérisée ou des empreintes digitales sur un certain nombre de documents. Il est encore trop tôt pour mesurer les changements qu'entraînera le projet préparé par le Ministère de l'Intérieur par rapport à la situation existante.

Au niveau européen, deux textes de référence abordent les usages de la biométrie : la directive de 1995 et le règlement de 2004. Quelques pistes de réflexions concernant l'usage de ces technologies pour réguler et contrôler les flux migratoires sont également esquissées dans le programme de La Haye qui a été récemment publié.

Enfin, la question biométrique se comprend également dans une perspective internationale, puisque l'objectif que poursuivent les différents Etats est d'appréhender les déplacements des individus à une échelle mondiale.

Les normes d'une portée mondiale auxquelles nous devons nous référer sont celles de l'Organisation de l'Aviation Civile Internationale (OACI). En effet, les recommandations de cette autorité pèsent lourdement sur les législations nationales et les conventions internationales en vigueur.

Par ailleurs, nous ne pouvons pas aborder cette question dans sa globalité sans faire mention des dispositions en vigueur aux Etats-Unis. Nos compatriotes qui se sont rendus récemment dans ce pays ont pu constater qu'il était impossible d'entrer sur le sol américain sans se soumettre à un relevé d'empreintes et bientôt il nous faudra un passeport biométrique. Les normes prises par la première puissance mondiale établissent des standards que les autres Etats seront contraints de suivre dans l'édification des documents d'identité.

2. Le contexte normatif

Le champ normatif aussi doit être étudié sous l'angle national et international. Au plan mondial, les conventions et les recommandations internationales peuvent avoir une portée obligatoire ou indicative. En Europe, certains textes s'imposent, d'ores et déjà, aux Etats-membres (règlement 2004). D'autres éléments de référence sont également contenus dans l'article 8 de la convention européenne des droits de l'homme et dans la jurisprudence de la CEDH. Les législations des grands ensembles régionaux ont une incidence directe ou indirecte sur les évolutions réglementaires dans les autres pays dans la mesure où elles constituent des cadres de références susceptibles d'influencer les décisions des gouvernements.

Au niveau national, il convient d'étudier les changements qu'introduit le nouveau dispositif INES par rapport à la situation existante. L'obligation de posséder une carte d'identité (voire de la porter toujours sur soi) et de se soumettre à un relevé d'empreintes sont deux éléments nouveaux qui prêtent à réflexion. On peut se demander quelles seront les sanctions qui seront prévues à l'encontre des citoyens qui refuseraient ces contraintes.

3. Le contexte culturel

Dans le paysage des grandes démocraties, certains pays sont, par tradition, plutôt hostiles au recours aux documents d'identité obligatoires et à la constitution de fichiers centraux recensant la totalité de la population. C'est notamment le cas de la Grande-Bretagne qui n'a jamais connu de carte d'identité sauf en période de guerre. L'actualité récente a, d'ailleurs, montré l'ampleur des difficultés que rencontrait le gouvernement de Tony Blair pour imposer un tel document.

A l'inverse, d'autres Etats, à l'image de la France, se situent culturellement dans une tradition de contrôle de la population.

Enfin, la position de méfiance des anciens pays rattachés au bloc soviétique pour l'intensification des contrôles d'identité s'explique à travers l'étude de l'histoire récente. Leurs habitants gardent encore en mémoire le souvenir du système communiste. Ils ne sont pas prêts à concéder ces nouvelles libertés récemment acquises.

Ces éléments sont loin d'être négligeables dans cette problématique. Les incursions de l'Etat dans la sphère individuelle seront ressenties différemment selon les cultures nationales des pays considérés.

Il faut aussi prendre en compte les différences entre l'opinion publique, ce qu'elle perçoit en matière de liberté individuelle, et l'opinion des intellectuels.

II. La méthode d'appréciation

En première analyse, on peut essayer d'identifier les restrictions de liberté induites par le projet INES et les avantages attendus.

- **Les restrictions de liberté** liées à la concrétisation du dispositif présenté par le Ministère de l'Intérieur sont de quatre ordres :

- **Une intrusion de l'Etat dans la sphère personnelle et dans la sphère des libertés**
Collecter, classer et conserver des données personnelles et même corporelles en vue de les exploiter, cela touche à la dignité humaine, à l'intégrité du corps humain, et ce n'est pas non plus sans conséquence sur les libertés individuelles.
- **Un coût social non négligeable**
La société tout entière supportera les conséquences d'une intensification des techniques de contrôle.
- **Un coût économique important**
L'édition des documents d'identité et la construction et l'entretien d'une base centrale recensant les données biométriques de tous les citoyens français représente un investissement lourd sur le long terme. Paradoxalement, plus le système offrira de garanties pour le citoyen, plus celui-ci sera onéreux pour le contribuable. Par ailleurs, la carte d'identité sera désormais payante. Même si le prix annoncé par le Ministère de l'Intérieur devrait être relativement modéré, ce choix n'est pas neutre socialement.
- **Un processus irréversible**
Une fois que le dispositif sera lancé, il sera très difficile de revenir en arrière. Or, aujourd'hui personne n'est en mesure de prédire les usages qui pourront être faits de l'ensemble des données collectées. Dans ce domaine, il serait donc prudent d'appliquer le « principe de précaution ».

- **Les avantages attendus** par le Ministère de l'Intérieur sont les suivants :

- **un renforcement de la sécurité ;**
- **une simplification des démarches administratives ;**
- **une sécurisation des transactions commerciales en ligne** (signature électronique).

Dès lors quelle peut être la démarche d'appréciation ?

1. Examen des finalités

Les promoteurs du projet doivent nous apporter plus d'informations sur les finalités, notamment sur l'ampleur des menaces qui justifient le déploiement d'un tel dispositif. Terrorisme, maîtrise des flux migratoires, lutte contre le terrorisme sont les principaux motifs invoqués par les autorités pour défendre ce projet, mais ils ne sont pas suffisamment étayés pour que nous puissions juger de la pertinence de la réponse apportée par l'Etat.

Il faudrait vérifier ce que l'administration recherche dans le renforcement des contrôles, quels sont les gains attendus.

On peut également se demander pourquoi l'autorité publique souhaite intervenir dans la sphère commerciale en étendant l'usage de la signature électronique, qui sera contenue dans la puce, aux transactions marchandes. Dans une économie libérale, il appartient aux opérateurs privés de mettre en œuvre les mesures nécessaires pour sécuriser ces opérations.

Au-delà des fins « primaires » annoncées par l'administration, on peut se demander si le projet ne poursuit pas d'autres finalités secondaires, imaginaires ou réelles

Enfin, il y a comme une sorte de finalité « systémique » : avec ce dispositif, en effet, se développe une logique de fichage général de la population, alors qu'auparavant, l'Etat ne conservait que les empreintes biométriques des individus suspects ou jugés potentiellement criminogènes en raison de leurs antécédents.

2. Examen de l'utilité

D'un point de vue technique, il faut s'assurer que les choix réalisés par le Ministère de l'Intérieur sont les plus pertinents par rapport aux objectifs que l'Etat souhaite atteindre. Cela nécessite un examen technique par des spécialistes. N'étant pas un expert sur la question, je ne peux me prononcer sur le sujet.

Une question se pose également concernant la validité des procédures administratives qui encadreront l'utilisation de la future base centrale (contrôle des accès, traçabilité des utilisateurs, séparation des fichiers...).

3. Examen de la nécessité

On peut aussi se demander si les moyens technologiques proposés sont absolument indispensables pour parvenir aux objectifs annoncés. Ne peut-on y arriver par d'autres procédés ? Le Québec, par exemple, recommande de ne pas recourir à l'exploitation d'un fichier biométrique sans avoir examiné l'ensemble des alternatives existantes (cf. *La biométrie au Québec : les principes d'application pour un choix éclairé*. Juillet 2002). Pour l'instant, ces justifications ne sont pas présentes dans le projet INES. Toutefois, le Ministère de l'Intérieur apportera probablement des précisions à ce sujet.

De même, l'introduction de la carte d'identité électronique et sécurisée va-t-elle réellement simplifier les démarches administratives ? La création d'un fichier unique et centralisé de la carte d'identité et des passeports facilitera-t-elle réellement les procédures d'identification ?

4. Examen de la proportionnalité

Le principe de proportionnalité est bien connu des commissaires de la CNIL. Il est explicitement rappelé dans la Convention Européenne. Les intrusions dans la vie privée induites par ce projet sont-elles réellement proportionnées aux fins qui lui sont assignées ? Par exemple, la présence d'un autre identifiant biométrique, en plus de la photographie du porteur numérisé dans la puce, se

justifie-t-elle au regard des objectifs annoncés ? De même, faut-il un double stockage, dans la carte et dans la base centrale ?

Il faut aussi tenir compte des externalités liées à ce dispositif. Les promoteurs du projet se sont-ils assurés que le fichier central ne pourrait être utilisé à d'autres fins que celles qui ont été annoncées par le Ministère de l'Intérieur ? On peut ainsi craindre que certains opérateurs privés ne demandent à leurs clients de produire des preuves biométriques de leurs identités pour les transactions courantes (abonnement téléphonique, crédit à la consommation...). Les banques, les sociétés de crédits et les opérateurs téléphoniques pourraient ainsi contraindre le citoyen à délivrer des informations biométriques confidentielles et personnelles dès lors que ces éléments existent.

Enfin, à partir du moment où le dispositif est mis en place, le risque de détournement des données biométriques pour la constitution de fichiers privés n'est pas à exclure. En effet, la collecte de ces informations ne nécessite pas un accord tacite de l'individu que ce soit pour la photo, le relevé de l'iris ou les empreintes digitales.

5. Examen des garanties

Les garanties annoncées par le Ministère de l'Intérieur sont-elles suffisantes au regard des enjeux soulevés par la biométrie ? Outre les procédures prévues pour réguler la gestion du fichier et la traçabilité de ses utilisateurs, quel est le contenu des dispositions prévues pour permettre au citoyen l'accès au fichier ? Sur ce point, les indications générales contenues dans le document de présentation du projet INES ne me semblent pas suffisamment étayées pour le moment.

III. Les trois grands points d'interrogation

- Dans le cadre du projet INES, le citoyen aura la double obligation de porter une carte d'identité obligatoire et de délivrer ses empreintes biométriques pour établir ce document. Or, ce niveau de contrainte est sans équivalent dans les autres grandes démocraties. C'est une grande question.

- Puisque chaque carte d'identité sera pourvue d'une puce contenant les informations biométriques de son porteur, on peut se demander s'il est véritablement nécessaire de constituer des fichiers centraux pour améliorer l'efficacité des contrôles.

Le Ministère de l'Intérieur a annoncé que le dispositif intégrerait plusieurs bases de données centralisées contenant différents types de données (l'une pour les empreintes digitales, l'autre pour la photographie...) tout en précisant que ces fichiers seraient reliés entre eux. Selon quelles modalités s'organiseront l'interopérabilité et l'interconnexion entre ces différentes bases ? Là encore, ce point demeure en suspens.

- Enfin, le fichier serait accessible à tous « les services publics de sécurité » selon la terminologie employée par les promoteurs du projet. Cette définition vague englobe-t-elle également les services qui traitent des infractions mineures ou d'ordre économique et fiscal, par exemple ? Là encore, le document de présentation du projet INES reste pour le moins évasif.

En définitive, le système peut être plus ou moins contraignant. Il faut une approche pragmatique et non dogmatique, encore moins idéologique, sur ce dossier en mettant en perspective les éléments mesurables et en évaluant les réponses apportées par le projet INES.

*

* *

En réponse aux diverses questions qui ont été posées, M.. Canivet a apporté les précisions suivantes.

1. Je ne pense pas que l'introduction de ce nouveau dispositif pourrait avoir pour conséquence une augmentation importante des contrôles d'identité en France. Au contraire, je pense que la généralisation de cette nouvelle carte d'identité aboutira à une simplification des contrôles qui dès lors deviendront moins nécessaires. En effet, la carte d'identité hautement sécurisée sera le document unique que le porteur devra présenter pour justifier son identité. Toutefois, celui qui n'est pas en mesure de présenter cette pièce à un agent sera, *de facto*, en état d'infraction puisqu'il contreviendra à l'une des dispositions du projet : l'obligation de détenir une carte d'identité.

En revanche, l'extension croissante des finalités attribuées aux fichiers centraux montre qu'en ce domaine, les garanties apportées par la loi sont vite levées. Ainsi, le dispositif Tracfin ne visait à vérifier que des transactions financières douteuses ne servaient pas à blanchir le produit du trafic de stupéfiants. Progressivement, les usages ont bien évolué, puisque désormais toute personne ayant effectué un an de prison effectuant des transactions d'un certain montant fera l'objet d'un contrôle par Tracfin.

De la même façon, une fois que la base centrale existera, on peut imaginer que le champ des usages autorisés va rapidement croître. A partir du moment où l'outil existe, il est dans la nature de l'administration d'en exploiter toutes les potentialités, y compris celles qui sont porteuses de risques pour les libertés des citoyens. En effet, toute bureaucratie secrète une volonté de contrôle sur les individus. Toutes les potentialités des techniques existantes sont mises à disposition pour satisfaire ce but. Cela constitue indéniablement un enseignement de la sociologie administrative. Si la menace terroriste est réelle, l'administration se sert également de la sensibilisation particulière de l'opinion à ce danger pour empiéter sur le terrain des libertés individuelles et prendre des mesures qui auraient été auparavant rejetées.

Toutefois, nous pouvons imaginer un système de garanties permettant d'éviter que l'utilisation de la base centrale ne soit dévoyée pour des usages qui n'avaient pas été initialement prévus par la loi. Par exemple, plus le système est centralisé et intrusif, plus l'autorité en charge de le réguler doit disposer de moyens conséquents, afin de remplir pleinement sa mission. Il faut également prévoir des garanties judiciaires pour les citoyens afin qu'ils puissent bénéficier de recours possibles.

2. L'Etat doit-il constituer de tels fichiers ? Il m'apparaît difficile de donner une réponse définitive sur le sujet. Je n'ai pas encore suffisamment d'éléments précis sur le projet INES pour me faire une opinion.

3. Certains choix techniques posent des questions importantes : par exemple, la puce contenue dans la future carte d'identité pourrait être lisible sans que cela nécessite un contact physique avec un lecteur, c'est-à-dire que l'individu pourrait être identifié à son insu et ses déplacements, « tracés » par les autorités. A partir du moment où nous collectons des données sans consentement de l'intéressé, nous nous exposons à ce type d'exploitation. Faut-il prévoir ces dérives possibles ou interdire le recours à cette technologie ? Je ne suis pas sûr de la réponse à apporter à cette question.

Par ailleurs, laisser la possibilité à un individu de refuser de délivrer ses empreintes biométriques peut constituer un frein. Prenez l'exemple du service militaire. Les objecteurs de conscience ont fini par être admis par la société qui a trouvé des moyens alternatifs (service civil) plutôt que de les mettre en prison.

De la même façon, si un citoyen ne souhaite pas donner ses empreintes biométriques pour établir une nouvelle carte d'identité, l'Etat doit lui proposer une solution alternative.

4. S'il y a bien quelque chose d'irréversible dans le progrès technique, toutefois, nous devons essayer d'en réguler au mieux les effets. C'est précisément le rôle d'une autorité administrative indépendante comme la CNIL.

5. Il convient d'identifier les risques potentiels liés à l'introduction de ce nouveau dispositif et d'évaluer les solutions les plus pertinentes pour limiter ces incidences négatives.

Par exemple, concernant le relevé de l'Iris, il faut avoir la certitude que ces informations seront utilisées à des seules fins d'identification et non pour obtenir des éléments sur l'état de santé de l'individu (consommation de stupéfiants, maladies...).

Il faut envisager les conséquences les plus intrusives et les plus condamnables de ce projet et prendre en compte l'ensemble des risques potentiels même s'ils ne sont, pour l'heure, pas encore avérés.

C'est une manière de prendre en compte le principe de précaution.