

# **Biométrie : une sécurité accrue au détriment des libertés individuelles ?**

**Abstract** : Biométrie, Titres d'identité, Vie Privée, Traitement des données, fichiers

## **CHAPITRE 1 BIOMETRIE : UNE SECURITE ACCRUE AU DETRIMENT DES LIBERTES INDIVIDUELLES ?**

<b>I) UNE CONTRAINTE INTERNATIONALE</b>	<b>4</b>
A) UNE REPOSE A L'EXIGENCE INTERNATIONALE ET COMMUNAUTAIRE DE DOCUMENTS D'IDENTITE SECURISES	4
B) UNE REPOSE FRANÇAISE SUPERFETATOIRE ?	6
<b>II) UNE GENERALISATION COMPORTANT DES RISQUES IMPORTANTS POUR LES LIBERTES PERSONNELLES</b>	<b>7</b>
A) LA SYSTEMATISATION DE « LA LOGIQUE DES TRACES »	7
B) LA CONFUSION IDENTIFICATION - AUTHENTIFICATION	10
<b>CONCLUSION</b>	<b>11</b>

**« Science sans conscience n'est que ruine de l'âme ». Rabelais.**

Le principal objectif d'une utilisation à grande échelle des techniques biométriques est de parvenir à une véritable authentification des personnes et non plus seulement à une simple identification.

En effet, les techniques biométriques, à la différence d'autres (comme la carte d'identité classique) ayant les mêmes finalités mais permettant seulement de mesurer ou vérifier **ce que l'on possède** (carte, badge...) **ou ce que l'on sait** (mot de passe...), permettent la mesure et la reconnaissance de **ce que l'on est**. On passe ainsi avec elles, **de la simple identification** de l'utilisateur, qui consiste à associer une identité à une personne, **à une véritable authentification** de ce dernier, qui permet de confirmer l'identité proclamée ou au contraire de l'infirmier : on obtient ainsi une sécurité accrue et une diminution des risques de fraude à l'identité. Cette importante augmentation de la sécurité apportée par la biométrie conduit aujourd'hui les autorités à faire entrer cette technique dans une nouvelle ère : celle de son usage par le grand public avec d'une part, l'adoption du Règlement communautaire du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques (Règl. (CE) n° 2252/2004) et d'autre part, la présentation « officielle » en France du programme INES (Identité Nationale Electronique Sécurisée). Le premier texte concerne les passeports et les documents de voyage ; le second est pour sa part, présenté comme un projet global qui vise les passeports et cartes d'identité nationales.

Cependant, ces projets ont également un autre « but », une conséquence un peu moins visible, qui est la création de grandes bases de données nationales et européennes contenant toutes les nouvelles informations ainsi recueillies. Par exemple, dans le cadre de la mise en place en France de la future Carte d'Identité Nationale Electronique Sécurisée, le ministère de l'Intérieur compte centraliser et stocker les données de la carte dans trois grands fichiers. Plus généralement ces projets devraient mener à de nouveaux types de fichage des individus, encore plus précis et permettre tout à la fois le renouvellement et le développement des données déjà existantes dans les fichiers actuels de Police et du Gouvernement.

Comme le souligne Rabelais, et comme l'histoire nous l'a montré, les innovations techniques et leurs intérêts pour l'humanité ne dépendent que de l'utilisation qui en est faite. Dès lors on peut se demander si le simple fait de détenir les capacités techniques permettant une utilisation

généralisée de la biométrie doit forcément nous conduire à une mise en place effective de celle-ci ?

En effet, l'utilisation de la biométrie, en elle-même pose de nombreux problèmes philosophiques, sociologiques et politiques qui sont d'autant plus exacerbés lorsque les données biométriques sont massivement stockées dans des fichiers centralisés. Ces constatations font dès lors apparaître une confrontation entre deux intérêts divergents : d'une part la volonté de sécuriser toujours plus les rapports entre les individus, et d'autre part la nécessaire protection de la vie privée.

Ainsi, et pour ce qui est du niveau national, la Commission Nationale Informatique et Liberté (CNIL) ainsi que des associations de protection des droits de l'Homme se sont dites « préoccupées » par la « constitution de bases centrales, par la traçabilité possible par les empreintes de nos concitoyens et par les autres usages éventuels »<sup>1</sup> de ces fichiers à des fins policières. Pour appuyer ses craintes elle a, entre autres, cité et dénoncé à nouveau les dérives telles que celles qui ont résulté de l'utilisation en 2004 de fichiers de police comme le STIC<sup>2</sup> qui, à cause « d'informations erronées ou trop vieilles », ont bloqué l'embauche de candidats à des postes de sécurité. Ainsi, la CNIL a vérifié pour 254 requérants les renseignements inscrits dans le STIC et a constaté des « erreurs » pour 67 d'entre eux, soit « dans 26 % des cas »<sup>3</sup>. Cette remarque fait ressortir l'un des principaux problèmes en matière de traitements informatisés de données personnelles via des bases de données : il faut en permanence s'assurer de l'exactitude des données ainsi collectées et organisées afin d'éviter des conséquences néfastes.

Face à la multiplication des sources de données qui va se produire avec la généralisation de la biométrie dans les titres d'identité et aux interconnexions qui ne manqueront pas d'avoir lieu, la moindre erreur pourra se répercuter en de nombreux endroits, multipliant par la même les atteintes aux droits des individus. Cette généralisation de l'usage de la biométrie dans les titres d'identité qui se profile résulte en grande partie d'une contrainte internationale (I) qui ne doit

---

<sup>1</sup> Article de Patricia Tourancheau dans le Journal Libération, « La nouvelle carte d'identité met la puce à l'oreille de la Cnil », <http://www.liberation.fr/>, 21 Avril 2005.

<sup>2</sup> Système de traitement des infractions constatées : le STIC est un gigantesque fichier recensant toutes les informations concernant les personnes mises en cause dans des procédures judiciaires, ainsi que celles de leurs victimes. Le traitement vise les enquêtes ouvertes pour les crimes, les délits et les six catégories de contraventions de 5<sup>o</sup> classe.

<sup>3</sup> Vie-privée.org: Fédération Informatique et Libertés, « Fichage policier : 25% d'erreurs, mais que fait la police ? », <http://www.vie-privée.org/>, 13 Janvier 2003.

cependant pas faire perdre de vue que cette technique comporte des risques importants pour la protection des droits des individus et les libertés personnelles (II).

### ***I) Une contrainte internationale***

Souhaitant mieux contrôler les flux migratoires, notamment suite aux attentats qui ont frappé leur territoire, les autorités américaines ont adopté une série de mesures permettant de contraindre, indirectement, les pays étrangers à adopter les mêmes standards qu'eux en matière de titre d'identités (passeports à lecture optique et inclusion à terme de données biométriques dans les documents d'identité). L'Europe a ainsi engagé, de manière quelque peu contrainte, un programme visant à réformer et standardiser les titres d'identité dans les différents pays membres en y incluant des données biométriques. Face à cette généralisation annoncée de l'usage de la biométrie dans les titres d'identité, apparue en réponse à l'exigence communautaire et internationale de documents d'identité sécurisés, et du fait de ses obligations communautaires (A), la France s'est, elle aussi, lancée dans le développement de ces techniques au niveau national avec notamment le futur système de carte nationale d'identité biométrique mais aussi l'emploi de cette technique dans de nombreux autres titres d'identité, projets qui semblent dépasser les exigences communautaires (B).

### **A) Une réponse à l'exigence internationale et communautaire de documents d'identité sécurisés**

Suite aux attentats terroristes du 11 septembre 2001 aux Etats-Unis, des discussions ont été menées au niveau international et national pour rendre les documents de voyage (passeports et visas) plus sûrs. En mai 2003, l'Organisation Internationale de l'Aviation Civile a ainsi adopté un plan pour l'intégration d'éléments d'information biométriques dans les passeports et autres documents de voyage lisibles par des machines<sup>4</sup>. On peut penser cependant que ces discussions ont été quelque peu unilatérales car, in fine, les Etats-Unis ont « contraint » les pays à adopter des titres d'identité biométriques si ceux-ci souhaitent continuer à pouvoir entrer sur le territoire Américain sans visa.

---

<sup>4</sup>International Civil Aviation Organization (ICAO), « ICAO Recommendation on Biometrics », <http://www.icao.int/>, Mai 2003.

Parallèlement, mais aussi parce que des abus ont été découverts en matière de visas, l'Union Européenne a décidé, à l'occasion du sommet d'Athènes de juin 2003, de créer un « Système d'information sur les Visas » (VIS)<sup>5</sup>. Le VIS permettra d'améliorer la mise en oeuvre de la politique commune de visas, la coopération consulaire entre les représentations des Etats signataires des accords de Schengen et la consultation préalable à l'octroi d'un visa. Afin d'assurer une efficacité maximum pour ce projet, le Conseil Européen a demandé à la Commission, dans une déclaration en date du 25 mars 2003, « *de présenter des propositions visant à accroître l'interopérabilité des bases de données européennes et d'envisager la création de synergies entre les systèmes d'information actuels et futurs (SIS II, VIS et EURODAC)* »<sup>6</sup>.

Ainsi, saisi pour avis sur ce projet, le groupe de l'article 29 pour la protection des données, dans son avis du 11 août 2004<sup>6</sup>, a reconnu la légitimité de la finalité de l'insertion des éléments biométriques en vue de vérifier l'identité du détenteur du titre tout en soulignant la nécessité de garanties techniques en matière de sécurité et de fiabilité. En revanche, le groupe a exprimé les plus grandes réserves, notamment en ce qui concerne la proportionnalité, face à une solution qui conduirait à la conservation, dans des bases de données, de données biométriques relatives à tout étranger demandeur d'un visa ou d'un titre de séjour à des fins de contrôles ultérieurs des immigrants illégaux (en particulier ceux ne disposant d'aucun document), quand ces données seraient de telle nature qu'elles porteraient sur des éléments dont toute personne laisse des traces dans la vie quotidienne.

Prenant en compte les réserves émises par le G29, le Conseil a adopté le 13 Décembre 2004 le Règlement (CE) 2252/2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres<sup>7</sup>. Par ce texte, le Conseil souhaite généraliser au niveau des Etats membres l'introduction de données biométriques dans les titres d'identité mais aussi dégager au sein de l'Union européenne une approche cohérente en ce qui concerne les identificateurs ou les données biométriques pour les documents des ressortissants de pays tiers, les passeports des citoyens de

---

<sup>5</sup> Liberty & Security, « La proposition de système d'information sur les visas (VIS) renforce la sécurité et facilite les déplacements dans l'UE », <http://www.libertysecurity.org/>, 14 Mars 2005.

<sup>6</sup> Groupe de l'article 29 pour la protection des données, « Avis n° 7/2004 sur l'insertion d'éléments biométriques dans les visas et titres de séjour en tenant compte de la création du système d'information Visas (VIS) », <http://europa.eu.int/>, 11 Août 2004.

<sup>7</sup> Conseil de l'Union Européenne, règlement N° 2252/2004 « établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres », <http://europa.eu.int/>, 13 Décembre 2004.

l'Union et les systèmes d'information VIS et SIS II<sup>8</sup>. Dans cet objectif, le règlement se limite à l'harmonisation des éléments de sécurité, y compris les identificateurs biométriques, des passeports et des documents de voyage délivrés par les Etats membres en laissant le soin aux législateurs nationaux de désigner des autorités et des organismes habilités à consulter les données présentes sur le support de stockage des documents.

Suite à l'adoption de ce règlement, et se conformant à leurs obligations européennes, certains pays de l'Union, dont la France, ont d'ores et déjà entamé les démarches nécessaires à la mise en conformité de leurs titres d'identité.

## **B) Une réponse Française superfétatoire ?**

Suite notamment au règlement européen du 13 décembre 2004 imposant aux Etats membres de se doter à leur tour de titres d'identité biométriques, la France s'est lancée dans un projet visant à réformer en profondeurs les titres d'identité nationaux, projet qui va bien plus loin que ce qui est initialement imposé par ce règlement. En effet, ce dernier ne vise que les passeports et exclut explicitement les cartes d'identité ; son article 3 dispose expressément que : « *Ce règlement ne s'applique pas aux cartes d'identité délivrées par les Etats membres* »<sup>9</sup>.

Pour le moment, la face la plus visible de cette nouvelle politique est sans nul doute le projet de carte d'identité électronique. Ce programme ambitieux vise quatre objectifs :

- Fusionner, simplifier et sécuriser les procédures de demande de passeport et de carte nationale d'identité (CNI).
- Améliorer la gestion de ces titres dans de nouvelles applications.
- Délivrer des titres hautement sécurisés conformes aux exigences internationales.
- Offrir aux citoyens les moyens de prouver leur identité sur Internet et de signer électroniquement, afin de favoriser le développement de l'administration électronique.

---

<sup>8</sup> Europa, « Schengen: passer du SIS au SIS II », <http://europa.eu.int/>, 1<sup>er</sup> Juin 2005.

<sup>9</sup> Article 3 du Règlement (CE) N°2252/2004 du Conseil établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, <http://europa.eu.int/eur-lex/>, 13 Décembre 2004.

Si on en croit les annonces faites par le ministère de l'Intérieur, cette nouvelle carte sera obligatoire, payante et contiendra des données biométriques (empreintes digitales et image faciale). Concrètement, sa mise en place implique un fichage de tous les français et la création de bases de données nationales. Notons également qu'il est prévu que cette carte soit lisible sans contact.

Les projets en cours, et les futures applications envisagées pour la biométrie dans les titres d'identité démontrent que cette technologie employée à des fins d'identification et d'authentification est promise à un avenir certain. Cependant, les différentes consultations menées auprès des citoyens qui seront demain les acteurs de cette technologie font ressortir que l'usage des données biométriques, s'il n'est pas correctement encadré et contrôlé comporte des risques importants pour la vie privée de chacun et la protection des droits<sup>10</sup>.

## ***II) Une généralisation comportant des risques importants pour les libertés personnelles***

Le développement constant des technologies biométriques et la généralisation de leur usage en matière de titres d'identité conduit à développer une systématisation de la « logique des traces » (A) ce qui entraîne corrélativement un affaiblissement de l'espace public anonyme et induit une confusion entre l'identification et l'authentification (B).

### **A) La systématisation de « la logique des traces »**

La systématisation de la logique des traces est rendue possible avant tout par la nature même des données biométriques (1) qui permettent plus que toute autre un suivi précis et une identification certaine des individus. Cependant, un autre élément s'ajoute et vient renforcer cette possibilité : la volonté des autorités d'équiper les titres d'identité contenant de telles données de puces sans contact (2) permettant une lecture à distance des données. Cette lecture pourrait éventuellement se faire à l'insu du détenteur.

---

<sup>10</sup> V. E-juristes, « Encadrement et risques de la biométrie », <http://www.e-juristes.org>, 27 Février 2004.

## 1) Les données biométriques

L'information biométrique, parce qu'elle signe une réalité biologique qui nous appartient en propre, est plus appropriée que toute autre à une identification certaine des individus. Ce risque de la systématisation de la logique des traces est l'un des principaux que la CNIL a mis en exergue face à la biométrie : les éléments biométriques laissant des traces lui paraissent plus dangereux que les autres.

Comme le souligne avec beaucoup de justesse la CNIL, une donnée telle que l'empreinte digitale est en effet particulièrement dangereuse : nous laissons des traces de notre passage sans le vouloir sur toutes les surfaces non lisses que nous touchons. C'est entre autre pour cette raison que la CNIL s'est toujours opposée à la constitution d'une base de données centralisée de telles données biométriques qui induit la systématisation de « *la logique des traces* »<sup>11</sup> (ADN, empreintes vocales, digitales...) et conduit au développement de méthodes de recherches et d'identification des traces humaines à grande échelle d'où découle une progressive disparition du droit à l'oubli. Le fait que la biométrie soit présentée au grand public comme un remède universel propre à terrasser plusieurs maux comme le terrorisme, la fraude, le vol d'identité, l'atteinte à la vie privée... ne doit pas faire oublier à ce dernier que les données biométriques constituent un « *identifiant intime, unique et universel* » qui rend très facile le croisement des données provenant de multiples sources et le « traçage » des individus.

Ces craintes sont encore renforcées par le fait que les données de ces nouvelles formes de titre d'identité sont stockées dans des puces électroniques qui sont souvent de type « sans contact », c'est à dire permettant une lecture à distance, qui pourrait éventuellement se faire à l'insu du détenteur.

---

<sup>11</sup> Commission Nationale Informatique et Liberté, extrait du 22e rapport d'activité 2001 chapitre 3 : "un siècle de biométrie", <http://www.cnil.fr/>, 2002.



## 2) La carte munie d'une puce « sans contact »

Les nouveaux titres d'identité contenant des données biométriques seront tous équipés d'une puce électronique dans laquelle seront stockées l'identité du porteur, plus les données biométriques numérisées. Seulement, il ne s'agira pas de n'importe quel type de puce, le plus souvent les titres ainsi créés utiliseront une puce dite « sans contact »<sup>12</sup>. Cette puce présente pour principale caractéristique de permettre une lecture à distance de ces données, c'est à dire sans avoir à l'insérer dans un dispositif de lecture.

Ceci étant expliqué, on voit immédiatement les risques immenses qui apparaissent pour la protection de la confidentialité des données stockées sur la puce : une lecture de ces informations pourrait parfaitement s'effectuer à l'insu du titulaire. Ainsi, concernant la future carte d'identité issue du projet INES, Côme Jacquemin, représentant du Syndicat de la Magistrature, a déclaré « *Ce qu'on nous prépare, c'est un « Navigo » d'identité* » (référence faite au très controversé titre de transport électronique mis en place par la RATP qui contient lui aussi le même type de puce)<sup>13</sup>. Le système de puce sans contact pour la carte INES, comme celui du système Navigo, est conçu pour conserver les données relative à son utilisation : on parle pour ces données de « données virtuelles » ou bien encore de « données de trafic » ou « données associées ». Elles indiquent quand et à quel endroit un individu a été en contact avec le système ; généralisant par la même un peu plus la logique de trace. La banalisation des contrôles d'identité rendue possible par une telle puce constitue le point d'orgue de la systématisation de la logique des traces. Pour sa part, le ministère de l'Intérieur a justifié ce choix d'une puce sans contact en expliquant que le « sans contact » **serait plus facile à utiliser** (lors de contrôles de masse dans des aéroports par exemple) et **s'userait** moins.

Outre ces risques latents auxquels chacun songe face au développement actuel de ces techniques, il convient également de prendre conscience qu'au-delà de la systématisation de la logique des traces et de la disparition de l'espace public anonyme de nouveaux problèmes, et risques très

---

<sup>12</sup> Article de Stéphane Foucart dans le Journal Le Monde, "Polémique sur la carte d'identité électronique", <http://www.lemonde.fr/>, 28 Mai 2005.

<sup>13</sup> Association Souriez vous êtes filmés, "NAVIGO - TECELY : même combat : Les cartes numériques de transports à Paris et à Lyon vues par les Big brother Awards", <http://souriez.info/>, 15 Janvier 2003.

particuliers émergent, du fait que la biométrie conduit à une confusion entre l'identification et l'authentification des individus.

## B) La confusion identification - authentification

Dans un procédé de contrôle de l'identité d'une personne : l'identification est le fait de communiquer son identité alors que l'authentification, elle, est le fait d'apporter la preuve de l'identité que l'on a communiquée dans la phase d'identification<sup>14</sup>. Le parfait exemple de ce processus en deux temps est le couple identifiant (ou « login ») et mot de passe que l'on doit fournir dans de nombreux cas pour accéder à certaines ressources<sup>15</sup>. Dans ce cas précis, en entrant son login on s'identifie et avec le mot de passe on s'authentifie.

Face à ce schéma traditionnel, la biométrie a tendance à confondre le login et le mot de passe<sup>16</sup>: alors que la solution classique requiert la validation des deux paramètres, les procédés biométriques n'en demandent trop souvent qu'un seul. La disparition de la distinction entre identification et authentification qu'engendre la biométrie est propre à créer des risques particuliers aux conséquences importantes.

Cette confusion, que certains voient comme une simplification, mène d'autres personnes à déclarer que « l'utilisation de la biométrie comme moyen d'authentification dans le cadre d'une politique de sécurisation d'un système d'information est à déconseiller ».

Parmi les grands problèmes posés à l'heure actuelle par la biométrie de ce point de vue, on peut évoquer le fait que « *l'usurpation d'une donnée biométrique est réalisable par des techniques d'ores et déjà diffusées et accessibles* » mais surtout, « *une donnée biométrique ne se révoque pas quand elle est compromise* »<sup>17</sup>. Ce dernier problème mérite une attention toute particulière : chaque personne possède un jeu de données biométriques uniques, si elles sont usurpées par un

---

<sup>14</sup> Mag Securs (Magazine Européen de la Sécurité Informatique), « Authentification ou Identification ? » <http://www.mag-securs.com/>, Décembre 2003.

<sup>15</sup> Djamila Mahmoudi (PhD, collaboratrice au département Corporate Information and Technology de Swisscom AG), "Biométrie et Authentification", <http://sawww.epfl.ch/>, 2000.

<sup>16</sup> Jean-Marc Manach, "Un expert auprès du gouvernement dénonce les fausses promesses de la biométrie", <http://www.transfert.net/>, Octobre 2003.

<sup>17</sup> Jean-Marc Manach, « Un expert auprès du gouvernement dénonce les fausses promesses de la biométrie », <http://www.transfert.net/>, Octobre 2003.

tiers qui s'en sert non seulement le détenteur légitime aura beaucoup de mal à prouver l'usurpation mais en plus, s'il y arrive, ses données seront jugées inutilisables car falsifiées ; dès lors par quoi les remplacer ?

Ces nouveaux problèmes particuliers apparaissant avec la confusion entre identification et authentification ainsi que les risques posés par la systématisation de la logique des traces et les questions engendrées par l'affaiblissement de l'espace public anonyme sont autant de dangers pour la protection des droits des individus. Il convient de prendre en compte ces risques le plus vite possible pour tenter d'y apporter une réponse satisfaisante avant la mise en oeuvre de tous les projets actuellement annoncés. De plus, outre ces problèmes strictement liés à l'instauration de la biométrie dans les titres d'identité, un autre se pose en ce qui concerne le coût lié à cette instauration : celui-ci va en effet induire un certain nombre d'inégalités dont il ne faut pas ignorer les conséquences. Ainsi, au niveau de l'aménagement local (installation des systèmes dans les communes), on peut penser que seules les communes importantes auront dans un premier temps les moyens de mettre en oeuvre ces dispositifs en local pour leurs usagers. Bien qu'il soit prévu de procéder à la mise en place d'unités mobiles permettant de partager cette ressource entre plusieurs communes, les maires des plus petites se sont cependant farouchement opposés au projet<sup>18</sup>. Dans le même esprit, les pays occidentaux sont tous sur le point de se doter d'une carte électronique ce qui va, dans les transports internationaux, accentuer les différences de traitement déjà existantes : ainsi le citoyen d'un pays doté d'une carte électronique voyagera partout où il le souhaite avec un minimum d'entraves puisqu'il pourra se soumettre sans peine à tous les types de contrôle même les plus sécurisés, alors que les voyageurs originaires d'un pays non doté d'un tel système (notamment par manque de moyens financiers) devront surmonter toutes les tracasseries administratives (sûrement encore accrues avec la biométrie) renforçant encore son sentiment de subir une inégalité de traitement.

## **Conclusion**

Face aux proportions que la biométrie est en train de prendre dans le développement de titres d'identité utilisés au quotidien par tous les citoyens et face également aux risques de dérives très

---

<sup>18</sup> Philippe Crouzillacq , « Les maires de France s'opposent au projet de carte d'identité électronique », <http://www.01net.com/>, 10 Juin 2005

concrets qu'elle pourrait engendrer, la garantie d'une protection forte des droits des individus doit être apportée au plus vite. Les futurs utilisateurs (contraints) ont montré par leurs questions et leurs propositions, lors de chaque consultation sur ce sujet, que la protection des droits doit être la préoccupation première face à de tels systèmes; ils vont même jusqu'à se demander pour certains s'il ne vaudrait pas mieux renoncer purement et simplement à ces projets dont personne n'imagine encore toutes les conséquences à plus ou moins long terme sur la vie privée de chacun. Une chose est sûre, la protection nécessaire ne pourra passer que par des contrôles stricts et complets à chaque stade du développement de ces projets; lesquels devront être menés en toute transparence par les organismes nationaux et européens pour la protection des droits. Ces organes semblent, à l'heure actuelle, constituer les derniers remparts permettant d'assurer à chacun la protection de ses droits légitimes face à ces nouvelles méthodes de fichage généralisé via la biométrie.