

## Audition de M. Didier BIGO

**Maître de conférences des Universités à l'Institut d'Etudes Politiques de Paris**

**Chercheur associé au Centre d'Etude et de Recherche International (CERI)**

**11 MARS 2005**

**Du point de vue de la perspective historique**, on relève des flux et reflux quant à la volonté d'identifier, en fonction du contexte social et politique. Les deux évolutions peuvent d'ailleurs être simultanées. Mais les reflux ont uniquement lieu en période de mouvements populaires de résistance ou de promotion du droit comme limite aux pouvoirs de l'Etat ; ils ne viennent pas de la bonne volonté de l'Etat. Quant aux flux, ils sont très liés à la volonté classificatoire, à la volonté de savoir pour prédire l'avenir, de « savoir sans limite ». Chaque bureaucratie a toujours l'impression de ne pas savoir assez par rapport à ce qu'on lui demande.

Comme exemple de résistance populaire, on peut évoquer ici le « *Doom's day* ». En 1086, dans le cadre de la conquête de l'Angleterre, Guillaume le Conquérant a voulu recenser les biens des individus vaincus. Il s'agissait donc bien d'identifier pour contraindre, ce qui a fondé la résistance des individus et de l'Eglise. L'Eglise a accepté que les individus donnent leur nom de baptême, et non pas leur nom commun, ce qui a bloqué la volonté d'identification du pouvoir en place. Les débats actuels qui se tiennent en Grande-Bretagne sur l'identification par l'Etat et les cartes d'identité reposent en partie sur cet élément juridique. En Angleterre, le droit d'avoir une anonymité par rapport à l'Etat continue à exister, sur la base de la notion de *privacy*, comme sphère interdite à l'Etat. Face à cet argument, les tenants de la carte d'identité mettent en avant l'objectif de protéger la société, voire de protéger les plus faibles, ce qui peut aller à l'encontre de la *privacy*.

En France, les positions sont sensiblement différentes, sans doute parce que nous avons eu une Révolution réussie ; en conséquence, l'Etat, assimilé au peuple, y a un droit de savoir qui est plus facilement accepté mais il faut éviter le mésusage par un mauvais gouvernement. L'accent est ici mis sur le contrôle politique et la légitimité de l'action.

Alors, pourquoi identifier ? pour contraindre ? protéger ? savoir ? et dans quelles limites ? savoir tout ou seulement ce qui est utile à une action spécifique ? La tendance aujourd'hui est celle d'un savoir policier dans une logique d'anticipation du futur ; elle amène à vouloir savoir tout sur tout, avec la volonté de pouvoir réutiliser des informations qui ont été collectées dans un domaine spécifique, pour quelque chose qui n'est pas encore connu. Ce jeu sur le passé, présent et futur est un problème crucial. La question doit être posée à l'échelle européenne.

A l'échelle européenne, les tensions demeurent, dans le cadre notamment des discussions du groupe dit « de l'article 29 ». Le terme *privacy* n'a pas la même résonance philosophique et intellectuelle des deux côtés de la Manche. Ainsi, sur le point de savoir qui a le droit d'identifier, les ambiguïtés sont fortes au niveau européen dans les terminologies employées sur « les autorités nationales compétentes ». Elles masquent des différences cruciales dans les pratiques des régimes. Certaines autorités sont légitimes dans un Etat de droit : police judiciaire notamment. Mais il est plus difficile de l'admettre s'agissant des douanes ou des services de renseignement interne. Que dire des consultants privés, qui, parce qu'étant sous contrat public, peuvent avoir accès à un certain nombre de données ? Il faut savoir qu'en dépit des demandes répétées visant à obtenir une liste exhaustive des autorités nationales compétentes, certains pays ont des réticences fortes pour y répondre. Or à l'échelle européenne, ce ne sera plus l'Etat requis qui aura le droit d'accepter ou non la demande d'information, mais ce sera l'Etat requérant, en vertu du principe de coopération. Un Etat qui refusera de fournir l'information devra alors le justifier. Dans ces conditions, nous avons besoin d'une liste exhaustive des autorités compétentes ; dans le cas contraire, nous risquons de transférer des données cruciales dans des pays où les systèmes de protection ne sont pas structurés de la même manière que les nôtres. En Allemagne, par exemple, les services de renseignement interne ont le droit d'alimenter en données le système d'information Schengen. Aux Pays-Bas, un certain nombre de services de renseignement font appel aux services de police pour obtenir leurs informations.

Enfin, toujours au niveau européen, demeure le problème fondamental du contrôle : il faut insister sur la nécessaire séparation entre ceux qui sont acteurs du contrôle (d'identité) et ceux qui contrôlent les contrôleurs. Les administrations de police et de contrôle des étrangers doivent pouvoir avoir accès à la comparaison des données fournies par les individus sur leur identité et aux données enregistrées auparavant par les administrations, mais il faut une séparation nette entre les administrations chargées de vérifier la fiabilité des informations et le comportement des contrôleurs. Ce n'est pas le cas dans de nombreux pays. Il nous faudrait des instances indépendantes, pouvant être des commissions de contrôle des données, des médiateurs, et surtout des juges du siège pouvant intervenir rapidement.

La création d'une haute autorité, prévue par la loi anglaise, irait dans ce sens, à condition qu'elle ne soit pas désignée par le Ministère de l'Intérieur. Une opportunité existe à l'échelle européenne, avec l'Agence des droits fondamentaux. On devrait exiger qu'elle ait des pouvoirs de contrôle, sur l'ensemble du territoire européen, sur les fonctionnaires des Etats. Cette Agence est initialement destinée à la lutte contre les discriminations, mais la proposition a été faite par le groupe de recherches Challenge, qui représente 21 universités européennes, d'élargir son mandat en ne la soumettant pas au troisième pilier, en connectant ses pouvoirs d'investigation (sans lesquels elle ne serait qu'un troupe l'œil) avec ceux du médiateur et en réunissant l'agence des droits fondamentaux et la protection des données et surtout en obligeant les gouvernements à indexer le budget de l'agence sur l'allocation des fonds consentis à la sécurité (second et troisième piliers). Il serait souhaitable qu'un débat ait lieu au Parlement Européen sur cette question.

En indexant les montants versés pour la protection des données aux budgets dédiés à la sécurité à l'échelle européenne, on pourra peut-être un peu mieux contrôler ceux qui veulent encore plus nous contrôler au nom de la lutte contre le terrorisme et le crime, car s'ils ont plus de pouvoir il est fondamental qu'ils soient soumis eux-mêmes à plus de contrôles et ne puissent invoquer à tout moment l'urgence ou la raison d'Etat. La question des moyens financiers est bien souvent le point d'achoppement en matière de contrôle ; ils sont souvent très limités, y compris s'agissant de l'espace Schengen. Or des commissions de contrôle ont besoin de chercher elles-mêmes l'information, faute de quoi elles doivent recourir à l'intermédiaire de services de police.

### **Sur le plan technique, y a-t-il ou non une révolution dans l'identification ?**

On peut considérer que les technologies d'identification dépendent avant tout de l'ampleur de la circulation et du volume des échanges ; l'élargissement des sphères d'échange, et le contrôle des inconnus, dont l'étranger n'est qu'une partie, sont l'élément déterminant. En la matière, l'évolution historique est importante : on pense au maillage du territoire par les gendarmes. Les travaux de la Gendarmerie nationale font ressortir un maillage des personnes et des traces des personnes. La manière dont son système informatique évolue ne vise plus simplement à encadrer un territoire, mais aussi les points de passage des personnes. La volonté est de contrôler ce que les gens ont fait pour arriver là, avec la croyance que l'on pourra prédire où ils vont. Anticiper les mouvements futurs reste pourtant très délicat.

Pour ce qui est des capacités techniques à disposition, il faut appréhender les technologies mais aussi les usages culturels que l'on en fait. Une technologie disponible ne doit pas nécessairement être utilisée à son maximum (ce n'est pas parce que l'on a une voiture qui peut faire du 250 km./heure que l'on doit conduire à cette vitesse...). Or la tendance naturelle des bureaucraties est d'utiliser les capacités techniques au maximum : pourquoi me brider alors que les capacités techniques me permettent de faire plus ? Il faut par ailleurs insister sur les relations entre les professionnels de la politique et les professionnels de la sécurité. Les premiers jouent sur une gestion des peurs et des insécurités.

### **Pourquoi la biométrie ?**

Il est clair que le recours à la biométrie, c'est-à-dire à une caractéristique physique permanente et inaltérable du corps humain, comme technique identificatoire, a un aspect assez neuf quand ceci est relié à la gestion à distance par des bases de données. Le credo des administrations veut que « le corps ne peut pas mentir », il offre une certitude et un savoir objectif. Il y a comme un rêve bureaucratique de pouvoir se passer de l'individu et de son discours dans le processus d'identification et de communication des informations. Cela rejette toute médiation du langage et de l'individu. Ce n'est pas à l'individu de parler de soi, de dire son identité car ce serait par cette faille que peut se glisser la fraude. La biométrie met l'individu dans l'incapacité de dire son identité, de la circonscire, de la contextualiser et en ce sens elle est problématique. Les administrations croient qu'elles ont pour but d'objectiver ce que l'individu serait par son corps, si possible dans son tréfonds, et pas seulement en surface. Toute une série de narratifs laissent entendre que l'intervention de l'individu est associée à la fraude et au mensonge. Il faut bloquer ce type de suspicion bureaucratique masqué derrière la certitude scientifique.

Les identifiants biométriques contemporains ont une dimension systématique, qu'il apparaît difficile de modifier. Quid du permanent et de l'infalsifiable ? Le rapport à la structure du corps fait que les identifiants situés à la surface du corps sont plus facilement falsifiables, ce qui explique la tentative de toutes les technologies biométriques d'évoluer vers des paramètres non maîtrisés par

les individus, avec en outre un rapport aux traces laissés par des identifiants biométriques, dans une optique de recherche criminelle. On pense aux empreintes ADN, qui, au-delà de l'authentification, vise à l'identification. La photo est utile ponctuellement, mais pose problème dans la durée. Les empreintes digitales peuvent être dénaturées par des brûlures et les empreintes rétiniennes peuvent l'être par des lentilles. Aujourd'hui, la photo numérique, avec reconnaissance faciale, devient quelque chose de plus développé ; on trouve de tels dispositifs dans des aéroports, pour repérer la structure des visages grâce à un logiciel. Pour les citoyens, cette évolution semble anodine ; or les technologies sous-jacentes sont très différentes. Or ces technologies de reconnaissance faciale sont déjà à l'œuvre dans un certain nombre d'aéroports, sans aucune information du public.

La chaleur du corps est un moyen de plus en plus utilisé aux Etats-Unis, afin de repérer des températures anormales, provoquées par des émotions. Un programme du FBI a été mis en place à cet effet. Cela montre le rapport ambigu entre la certitude d'un savoir sur le corps (le corps ne ment pas) et un comportement dangereux, soit-disant révélateur d'une idée politique. On ne peut pas dériver les derniers du premier, malgré les discours intéressés des sociétés privées.

Quant à l'ADN, qui est un identifiant biométrique complexe à mettre en oeuvre, son utilisation reste limitée. En revanche, on peut le faire parler à la place de la personne. Des recherches sont en cours, au Japon notamment, permettant de faire la comparaison entre un identifiant génétique de masse – des maladies associées à un groupe ethnique, par exemple - et l'identifiant de certains individus. Ces techniques « désindividualisent » l'individu spécifique pour le réinsérer dans une population cible, avec laquelle il entretient un rapport de proximité indicielle. Sont ici en jeu les techniques de « profiling » et de proactivité policière. Il s'agit de créer des profils de risque, des populations cibles, à partir des statistiques fournies par les bases de données et sur la base d'informations sociologiques.

### **Les identifiants sont-ils devenus infalsifiables ?**

La fraude est de plus en plus difficile, mais chaque technologie voit émerger des contre-technologies, souvent à un faible coût. Pour les empreintes digitales, un système de colle permet de contourner les lecteurs optiques. Si l'argument est la simplification administrative (moins de personnel et plus de systèmes techniques), le niveau de fraude aux empreintes digitales sera considérable. Déjà, aux Etats-Unis, on voit apparaître, dans les aéroports, des files d'attentes particulières, fonction de catégories de personnes.

S'agissant des empreintes rétiniennes, on trouve des lentilles spécifiques, propres à contourner les systèmes. La fraude à l'ADN suppose pour sa part des technologies de piratage plus complexes, mises en œuvre non pas au niveau du contrôle, mais au niveau des originaux figurant dans les bases de données. S'il y a faiblesse des systèmes, c'est bien dans la conservation inaltérable des informations dans les bases de données. Plus la base de données est concentrée, plus le risque est grand d'une destruction accidentelle ou volontaire. Il apparaît que les réponses sont très variées selon les pays quant à la structure de la base de données, mais toujours au nom d'une plus grande fiabilité. Il est frappant de voir que des arguments identiques sont utilisés pour aboutir à des solutions différentes.

Le problème des techniques se pose aussi en termes d'**acceptabilité pour les personnes concernées**.

Sur ce plan, on ne saurait cependant faire abstraction de la forte pression provenant des entreprises privées qui proposent des systèmes de contrôle. Un argument extrêmement utilisé veut que les

contrôles de visa sont acceptés dès lors que les personnes ne sont pas touchées physiquement. Or les administrations sont souvent sensibles aux arguments fournis par leurs fournisseurs privés. Lors du Salon consacré au I-pod, on pouvait constater qu'un certain nombre d'argumentaires d'entreprises privées contaminaient le discours des services de police et de gendarmerie. On peut s'attendre à ce que les technologies liées à la rétine et à la morphologie faciale soient demain des technologies dominantes, car ne nécessitant pas de contact physique pour les contrôles. Avec les technologies actuelles, la nécessité du volontariat des individus reste obligatoire, ne serait-ce que pour la remise des échantillons initiaux. Il ne faut pas non plus tomber dans un certain fantasme, selon lequel tout pourrait se passer à l'insu des personnes. Quoi qu'il en soit, il existe des lieux précis de contrôle avancés : les aéroports sont un bon exemple, puisque les gens sont stoppés dans un flux en mouvement. De même, la rétine fonctionne bien dès lors qu'il faut faire accéder un nombre restreint de personnes à un lieu spécifique ; en revanche, cette technologie n'est pas utilisable pour des surveillances de masse dans des rues.

La participation volontaire de la personne est *de facto* médiatisée. Mais donner des identifiants est souvent un passage obligé pour obtenir des documents – une carte à puces par exemple. Il faut donc être très prudents quant aux éléments qui sont fournis. La carte comptabilise-t-elle les trajets ? Permet-elle ou non de suivre les mouvements ? Les Européens semblent très prudents sur ce point, mais les Américains sont plus ambitieux, désireux de tracer les mouvements des personnes, y compris *via* les cartes à puces.

En réalité, la question de l'acceptation importe moins que celle du droit d'accès et de correction des données à tout moment du processus.

Il semble également important de faire admettre aux administrations que les moyens qu'elles utilisent ne sont pas les seuls possibles, ce qui est loin d'être évident.

Concernant **la centralisation et l'usage des informations**, l'argument classique des gouvernements consiste à dire que l'identification est un outil simple, efficace, rapide pour prouver l'identité des « bons citoyens », qui permet d'éviter la multiplication des codes. Du coup, elle est assimilée à l'authentification. Il faut pourtant être prudent quant aux notions d'identification et d'authentification. Cette dernière correspond à des éléments techniques et pratiques, mais il faut veiller à ne pas exagérer la coupure entre les deux, parce que l'authentification concourt en partie à l'identification. Concernant l'argument de simplicité, je note qu'il est rare que les administrations suppriment les autres moyens de preuve. La carte d'identité est sans doute un moyen efficace de prouver son identité, mais un certain nombre d'enquêtes sociologiques montre que la production de carte nationale d'identité n'empêche pas le harcèlement policier répétitif à l'égard de jeunes d'origine étrangère. Le document est utile pour faire preuve de son bon droit, mais l'usage sociologique et culturel qui en est fait est déterminant. Enfin, la rapidité exige que des moyens appropriés (lecture optique) soient fournis aux services de police, avec le risque de la « pixelisation » des contrôles, qui autorise des contrôles en tout point du territoire. Mais pourra-t-on éviter le développement de l'authentification-identification dans la sphère para-publique et privée, c'est-à-dire une généralisation des logiques de contrôle, à toutes fins ?

En même temps, il faut bien voir que cela favorise la circulation rapide des individus. L'identifiant est une garantie de l'identité, il n'a pas que des aspects négatifs. La problématique vient de la corrélation qui peut être faite avec des fichiers centraux

En effet, il faut distinguer la carte d'identité classique, qui donne lieu à un narratif d'accompagnement sur les trajectoires et les mouvements, l'authentification, qui n'est que

momentanée, et la carte d'identification avec mémoire des mouvements précédents, qui vise à reconstituer le parcours d'un individu sans son intervention. Or entre une carte d'identité et une carte d'identification, l'écart est important. Il faut être prudent en matière de suivi des traces et de mise en mémoire. Quelle doit être la durée de leur conservation ? Quelles sont les raisons de cette mise en mémoire ?

C'est là qu'intervient la problématique de la base centrale. Celle-ci n'a de sens qu'à travers une logique policière d'interconnexion des données, recueillies pour des raisons initiales différentes, et conservées quasi-indéfiniment, afin d'être utilisées à d'autres fins par la suite. Il convient de s'interroger sur les fichiers proposés et les critères utilisés. Les fins de recherche policière peuvent être les indices des crimes passés – l'authentification –, mais aussi les comportements futurs – les profils d'identification. Les bases de données Europol servent fondamentalement à cela ; le but de cette institution est de constituer des profils et des groupes dangereux. Le danger est bien là, et non pas sur une éventuelle aide technique d'Europol à des enquêtes policières, qui est la bienvenue.

Des bases de données centrales sont aussi créées pour aboutir à des fichiers profilés ethniquement. Le discours sur la prévention est ancien, mais est devenu une justification permanente depuis les événements du 11 septembre. Le discours policier relayé par celui des services de renseignement sur l'anticipation des comportements des criminels terroristes, n'est pas une forme de savoir scientifique mais ce que l'on peut qualifier de dimension « astrologique » du discours, du type « nous pouvons connaître le futur », et qui a été décrit dans l'ouvrage de Philip K Dick « minority report », dimension astrologique qui est masquée par la technologie utilisée. Ces discours visant à prédire les comportements futurs à partir d'informations déterminant le corps sont dangereux, d'autant que cette justification se retrouve à tous les niveaux, dans la lutte anti-terroriste, dans la lutte contre l'immigration, dans la lutte contre la criminalité organisée, dans la diffusion des visas, passeports, cartes d'identité... Il y a là un continuum d'insécurité qui vise à englober toutes les dimensions. Le projet INES, dans son argumentaire, est assez révélateur de cela.

L'authentification renvoie à une forme de certitude, qu'on opposerait à l'identification. Cependant, de nombreux procédés d'authentification sont des procédés d'identification. Il convient donc d'être plus précis. Très souvent est mis en avant l'argument de la police scientifique et de la police judiciaire, à travers un rapport au passé, alors même que la cible est un rapport au futur, avec des logiques proactives.

Le projet français pose problème dans sa volonté d'instituer un fichier informatique centralisé, quand bien même il promet l'absence d'interconnexions. L'histoire des fichiers montre en effet que très souvent, l'interconnexion apparaît peu à peu pour des raisons d'ordre public. Dès que l'on crée un fichier informatique centralisé, on est forcément amené à l'utiliser à d'autres fins, quels que soient les engagements pris, à supposer qu'un gouvernement prenne dans ce domaine des engagements pour le futur. (Le paragraphe 2 du projet INES du ministère de l'intérieur laisse entendre que les textes européens visent les cartes d'identité, alors qu'ils ne concernent que les visas et passeports ; il y a là une ambiguïté, volontaire ou non, alors qu'il n'y a pas de texte européen précisant les modalités propres aux CNI).

Rappelons-nous que les registres de population ont une histoire en France, liée à Vichy. La création d'un registre national de population à l'échelle européenne serait un véritable problème. L'un des arguments avancés consiste à dire que l'incapacité à contrôler valablement les visas et les passeports implique la généralisation d'un document d'identification pour tous les Européens, certains ajoutant même qu'il fallait le faire avant que les Américains ne nous l'imposent dans la pratique.

Utiliser l'argument de la lutte anti-terroriste pour la constitution d'un registre de population est extrêmement discutable. En outre, de telles mesures passives ne vont pas changer quoi que soit ; mieux vaut mettre l'accent sur l'infiltration d'organisations clandestines pour lutter contre le terrorisme.

Quant aux arguments mettant en exergue une simplification de la vie du citoyen, ils paraissent bien faibles au regard des risques encourus. La Chambre des Lords, et en tout cas le *Joint Committee on Human Rights*, vient de considérer qu'il y avait risque par rapport à l'article 8 de la Convention européenne des droits de l'homme. Il faudrait étudier la compatibilité du projet français avec cet article 8, en particulier en cas de création d'un fichier central. L'absence de fichier central rendrait-elle la CNI plus acceptable ? Il est difficile de le dire en l'état du projet.

On peut faire valoir aussi, c'est un des arguments principaux du ministère de l'intérieur, qu'un contrôle local de l'identité, y compris avec une empreinte biométrique, ne permet pas de lutter contre l'usurpation de l'identité, tandis que la création d'un fichier central permettrait de lutter contre la fraude à l'émission de la carte. En l'absence de fichier central, la nouvelle carte d'identité n'apporterait finalement guère de progrès. L'objectif est non pas le zéro défaut, mais de donner un moyen supplémentaire aux forces de police pour éviter la détention par une même personne de plusieurs cartes d'identité.

Mais, s'il est vrai qu'un fichier central est un moyen de limiter les risques de fraude, on peut lui opposer l'argument de la proportionnalité. Et puis un fichier central peut-il supprimer toute forme de fraude ? Aucune étude technique ne permet de le dire. La fraude se fera au niveau du fichier central au lieu de se faire à l'échelle locale. Un fichier central n'évitera pas par lui-même les erreurs sur les lieux de naissance et les reconnaissances de filiation. On peut améliorer la sécurité anti-fraude, mais quelles seront les populations pénalisées ? Et dans quelle proportion ? Certains, issus d'anciennes colonies françaises, rencontreront des problèmes. Il convient de mesurer tous les effets de la mise en place d'un fichier central. Le fichier central crée un maillon supplémentaire, a priori plus efficace, mais la question porte surtout sur l'utilisation qui en sera faite, d'autant plus qu'avec l'adresse, on apporte une trace ou une possibilité de trace. Avec une base centrale, on peut supposer que les compagnies aériennes vont exiger le numéro d'identité des passagers ou que l'on conservera la trace de leurs passages, s'ils doivent « signer » chaque passage de leurs empreintes, alors qu'aujourd'hui, il n'existe pas de base centrale pour les passeports et que ceux-ci ne comportent pas d'identifiant biométrique. La question est philosophique : jusqu'où faut-il tracer les mouvements des individus ? Chacun a bien entendu son opinion sur le sujet.

Enfin, **sur le plan économique**, la dimension financière de tous ces projets, que ce soit en France, au Royaume-Uni ou en Allemagne, fait l'objet d'estimations très variables. Le fait est que peu d'économistes se sont impliqués dans ces recherches sur les problématiques de sécurité intérieure, peu de personnes ont travaillé sur ces questions, sans doute parce que les incitations sont insuffisantes pour que les chercheurs orientés sur l'économie de la défense entrent dans la branche de la sécurité. Les travaux dans ce domaine existent essentiellement aux Etats-Unis.

