IDENTIFICATION ET SURVEILLANCE DES INDIVIDUS

QUELS ENJEUX POUR NOS DÉMOCRATIES ?

Avec

Laurent Bonelli
Ayse Ceyhan
Vincent Denis
Vincent Dufief
Sébastien Laurent
Pierre Piazza
Sylvia Preuss-Laussinotte
Thierry Rousselin
Jérôme Thorel
Anastassia Tsoukala
Jean-Claude Vitran

Identification et surveillance des individus

Quels enjeux pour nos démocraties ?

**Christian Aghroum, Michel Alberganti, Laurent Bonelli, Ayse Ceyhan,
Vincent Denis, Vincent Dufief, Sébastien Laurent, Pierre Piazza, Sylvia
Preuss-Laussinotte, Thierry Rousselin, Jérôme Thorel, Anastassia
Tsoukala et Jean-Claude Vitran**

DOI : 10.4000/books.bibpompidou.1192
Éditeur : Éditions de la Bibliothèque publique d'information
Année d'édition : 2010
Date de mise en ligne : 17 janvier 2014
Collection : Paroles en réseau
ISBN électronique : 9782842461805

<http://books.openedition.org>

Édition imprimée

ISBN : 9782842461294
Nombre de pages : 96

Référence électronique

AGHROUM, Christian ; et al. *Identification et surveillance des individus : Quels enjeux pour nos démocraties ?* Nouvelle édition [en ligne]. Paris : Éditions de la Bibliothèque publique d'information, 2010 (généré le 02 février 2021). Disponible sur Internet : <<http://books.openedition.org/bibpompidou/1192>>. ISBN : 9782842461805. DOI : <https://doi.org/10.4000/books.bibpompidou.1192>.

© Éditions de la Bibliothèque publique d'information, 2010
Conditions d'utilisation :
<http://www.openedition.org/6540>

IDENTIFICATION ET SURVEILLANCE DES INDIVIDUS

QUELS ENJEUX POUR NOS DÉMOCRATIES ?

Avec

Laurent Bonelli
Ayse Ceyhan
Vincent Denis
Vincent Dufief
Sébastien Laurent
Pierre Piazza
Sylvia Preuss-Laussinotte
Thierry Rousselin
Jérôme Thorel
Anastassia Tsoukala
Jean-Claude Vitran

Identification et surveillance des individus

Quels enjeux pour nos démocraties ?

Actes du colloque organisé par la Bpi
le samedi 17 janvier 2009
dans la Petite Salle du Centre Pompidou

**Président
du Centre Pompidou**
Alain Seban

**Directrice générale
du Centre Pompidou**
Agnès Saal

**Directrice de la Bpi
par intérim**
Sophie Danis

**Responsable du pôle
Action culturelle
et communication**
Philippe Charrier

**Chef du service
Animation**
Emmanuèle Payen

**Chef du service
Édition/Diffusion**
Arielle Rousselle

Colloque
**Conception
et réalisation**
Marion Loire

Publication
Chargée d'édition
Virginie Leduc

Mise en page
Virginie Leduc

Catalogue disponible sur
<http://www.bpi.fr>, rubrique
Éditions de la Bibliothèque
publique d'information
Distribution numérique
par GiantChair.com

© Éditions de la Bibliothèque
publique d'information/Centre
Pompidou, 2010.
ISBN 978-2-84246-129-4
ISSN 1765-2782

Sommaire

- 4 Ouverture
Philippe Charrier

Histoire socio-politique de l'identification et de la surveillance

- 6 Histoire de l'identité en France
Vincent Denis
- 13 Du bertillonnage à l'Europe biométrique
Pierre Piazza
- 26 Faire l'histoire de la surveillance
Sébastien Laurent

Enjeux des politiques d'identification et de surveillance

- 33 Identité, identification et surveillance : enjeux à l'heure de la biométrie
Ayse Ceyhan
- 40 Table ronde
Animée par Michel Alberganti

Technologies d'identification, de surveillance et libertés individuelles

- 62 Technologies de sécurité et respect des droits
et libertés individuelles : quelles protections ?
Sylvia Preuss-Laussinote
- 70 Victimes et complices : les individus face aux technologies d'identification
et de surveillance
Thierry Rousselin
- 76 Table ronde
Animée par Michel Alberganti

Ouverture

Philippe Charrier*

Je vous souhaite la bienvenue au nom de la Bpi et du Centre Pompidou à cette journée consacrée à l'identification et la surveillance des individus. Aujourd'hui, vous serez filmé et enregistré. Ainsi, nos débats pourront être écoutés par d'autres, en d'autres lieux et à d'autres moments. La Bpi a la particularité d'ouvrir ses espaces et ses collections à tout un chacun, sans inscription. Elle enregistre systématiquement tous ses débats pour les mettre en ligne et les partager le plus largement possible. La Bpi résiste également aux sirènes de l'identification et elle en paie le prix en tant qu'institution. Sans identification, la connaissance de notre public, pour mieux le servir, se heurte à de nombreuses limites comme l'impossibilité d'effectuer des réservations. Or, ce système nous permettrait de résoudre efficacement la question de la file d'attente. Il s'agit d'un problème récurrent à la Bpi. Mais, la culture de l'établissement nous apprend que la gratuité et la liberté d'accès – principes qui font de la Bpi une bibliothèque ouverte et d'exception – risqueraient d'être rapidement menacées par l'identification. Si j'aborde cette question par l'intermédiaire de la Bpi : bibliothèque ô combien pacifique, c'est que la question de l'identification et de la liberté individuelle se posent souvent en terme d'opposition entre liberté et sécurité. N'y voyons pas le seul enjeu. Finalement, si nous nous laissons identifier si facilement, ne serait-ce pas moins par docilité que dans l'espoir d'être mené cahin-caha sur le chemin d'une socialisation croissante, une intégration toujours plus grande de l'humanité ? Il s'agit d'un grand point d'interrogation. Pardonnez ce questionnement un peu naïf d'un bibliothécaire.

Le colloque d'aujourd'hui nous entraînera bien au-delà de mon étroite interrogation corporatiste. Je tiens à vous remercier pour votre présence, à remercier nos intervenants ainsi que Marion Loire et l'équipe qui nous aidé à préparer ce colloque.

4
Ouverture

Note

* Responsable du pôle Action culturelle et communication à la Bpi. ↑

Histoire socio-politique de l'identification et de la surveillance

- 6 Histoire de l'identité en France**
Vincent Denis
- 13 Du bertillonnage à l'Europe biométrique**
Pierre Piazza
- 26 Faire l'histoire de la surveillance**
Sébastien Laurent

Histoire de l'identité en France

Vincent Denis*

Plus qu'une histoire de l'identité, je voudrais vous présenter quelques éléments de l'histoire de l'identification en France, ainsi qu'en Europe, du ^{xvi}^e siècle jusqu'au début du ^{xix}^e siècle, et plus particulièrement l'histoire de l'identification écrite que nous appelons, aujourd'hui, les papiers d'identité. Pour introduire mon propos, je voudrais vous raconter deux histoires d'identité et d'identification que je voudrais rapprocher. Au ^{xvi}^e siècle, dans un village des Pyrénées qui se trouve aujourd'hui en Ariège, se déroule l'affaire Martin Guerre, célèbre dans les annales judiciaires. C'est l'histoire d'un homme qui avait quitté son village pendant de nombreuses années pour devenir soldat. Il est revenu après huit ans d'absence et a repris sa place parmi les siens, notamment auprès de sa femme. Au bout de quelques années, plusieurs habitants mettent en doute son identité et affirment qu'il est un imposteur. S'engage alors un procès, resté célèbre, qui cherche à savoir s'il est le vrai Martin Guerre. Les témoignages des villageois, ses souvenirs, son accent, ses cicatrices, la manière dont il s'exprime, sont examinés. L'enquête va jusqu'à comparer ses sabots avec ses pieds. Les magistrats sont très partagés. Il est sur le point d'être blanchi quand revient le véritable Martin Guerre qui, évidemment, confond l'imposteur.

Il est nécessaire de faire un bond dans le temps pour l'autre histoire, fictive cette fois mais inspirée de faits réels. Il s'agit de l'histoire du colonel Chabert¹, imaginée par Balzac, qui se situe pendant la période de la Restauration, dans les années 1815-1830. Chabert, un colonel de l'armée de Napoléon, disparu pendant la campagne de Russie et déclaré mort, revient en France après la guerre. Sa femme s'est remariée entre-temps avec un riche aristocrate et Chabert ne va jamais pouvoir reconquérir son identité. En effet, Balzac met en scène un ordre du droit et de l'écrit contre lequel la parole de Chabert et même son corps ne pourront rien. Chabert finit sa vie dans un hospice sous un numéro de matricule anonyme.

6

Histoire de l'identité
en France

Que montre le rapprochement de ces deux histoires ? À l'époque de Martin Guerre, l'identité d'une personne ne repose pas sur des documents écrits ou légaux mais d'avantage sur les relations qu'il entretient avec les membres de sa communauté locale, familiale, professionnelle. Des relations que l'on pourrait qualifier d'interpersonnelles. À l'inverse, l'époque de Chabert voit triompher l'ordre de l'identification écrite, un ordre des papiers et des registres sans lequel il n'existe pas d'identification certaine. Entre ses deux épisodes, il s'est produit une grande mutation dans la société française. L'État, en tant que principal acteur, a contribué à mettre en place tout un ensemble de techniques d'identification écrite dont beaucoup forment la matrice actuelle, que nous connaissons bien aujourd'hui, notamment le passeport et la carte d'identité. Dans quelles circonstances s'est développé ce grand mouvement en faveur de l'identification écrite et l'identification à distance qui ont popularisé ces documents ? Quels étaient les documents utilisés ? Comment reconnaissait-on un individu ? Comment les populations en France ont-elles subi, accepté et se sont adaptées à cette grande transformation des codes de l'identité dont je vous ai montré quelques éléments ? La genèse de cette identification à distance repose sur l'écrit. Celle-ci s'est faite très largement en liaison avec le contrôle de la mobilité des personnes. Les

autorités, à l'époque moderne, ne cherchent pas à contrôler l'ensemble des mouvements de la population sur le territoire. Ils en seraient incapables. Il est plus juste d'affirmer que certains groupes, parce qu'ils sont mobiles, font l'objet de contrôles et de mesures d'identification particulières. Un certain nombre de secteurs ont motivé l'intervention des autorités qui ont cherché à leur imposer ces formes d'identification écrite.

Un des premiers moteurs de l'identification écrite a été la recherche de criminels et de prisonniers en fuite, dans un mouvement qui commence au ^{xiv}^e siècle et continue pendant l'Inquisition. Le deuxième groupe moteur de l'identification écrite sont les groupes de voyageurs qui, pendant les grandes épidémies, notamment de peste, sortaient des régions infestées et étaient soumis à des contrôles qui reposaient sur l'écrit. Il leur était imposé de porter ce que l'on appelait des « billets de santé » ou des « patentes de santé² ». Le recours à l'identification écrite est également stimulé par le développement de l'assistance et de la question sociale. À partir du Moyen Âge central, s'est produit ce que certains historiens ont appelé la « déconversion de la société féodale ». Un très grand nombre de personnes se retrouvait ainsi exclu des cadres du travail alors en place : les structures agraires ou corporatives comme l'artisanat. Ces populations, appelées les « inutiles au monde », se sont retrouvées surveillées, obligées, dans la mesure du possible, de s'insérer dans des cadres du travail. À partir du ^{xvi}^e siècle, les structures hospitalières ont commencé à se développer en Europe, et notamment en France avec l'arrivée de l'hôpital général au ^{xvii}^e siècle. Ces structures ont cherché à restreindre l'accès des ayants droit à leur service d'assistance en distinguant les étrangers des personnes issues du lieu qui en bénéficiaient. Des instruments de tri et de séparation qui reposent sur le contrôle des papiers sont alors mis en place entre les *outsiders* et les *insiders*.

7

Histoire de l'identité
en France

Un autre facteur de la mise en place de l'identification écrite a été celui d'une population capable de servir sur les navires de guerre et qui ont fait l'objet, plus particulièrement en France, de mesures très concrètes pour permettre leur contrôle. Pour l'armée de terre, il s'agissait d'éviter la désertion. Pour les « gens de la mer », il s'agissait d'éviter que ces individus ne se retirent des côtes au moment où ils pouvaient être mobilisés pour servir les opérations de l'armée royale. Le développement d'armées professionnelles a également joué un rôle important dans l'histoire de l'identification puisqu'il fallait payer ses membres et donc éviter les éventuelles escroqueries. Des systèmes de registres se sont ainsi mis en place à partir du ^{xviii}^e siècle.

Enfin, la fonction de contrôle des voyageurs aux frontières des États, que nous connaissons aujourd'hui notamment par l'intermédiaire des passeports, s'est développée très tardivement. Elle n'apparaît qu'à la fin du ^{xviii}^e siècle avec la Révolution française, le développement de l'État-nation et surtout la mise en place d'une séparation stricte entre une communauté nationale et les étrangers, qui n'existait pas avant cette époque. Dans cette histoire, le ^{xviii}^e siècle représente une étape majeure pour les questions qui nous intéressent et qui sont des questions contemporaines. Le siècle des Lumières a connu une accélération de ce mouvement vers l'identification

écrite et l'identification à distance. L'usage des papiers et le basculement vers ces nouveaux codes de l'identité s'affirment de manière très évidente dans le dernier siècle de l'Ancien Régime français, bien avant la Révolution française. Le siècle des Lumières coïncide aussi avec la multiplication de projets d'identification des populations. Ces projets reposent en particulier sur un couple technique composé des registres et du certificat d'identité portatif. En 1716, par exemple, l'administration militaire met en place des registres centralisés de tous les soldats de l'armée française et les installe à Versailles. À peu près à la même époque, un système de registres du même type est inventé pour tous les mendiants présents dans le royaume et qui seraient arrêtés par les forces de police. Les projets fleurissent à nouveau au milieu du XVIII^e siècle avec l'aggravation de la question sociale et la volonté de la part de la police d'identifier les populations pauvres, marginales ou laborieuses pour attribuer à chacun une place fixe, repérable, et les réincorporer dans les cadres d'une société dont le tissu social est en train, à leurs yeux, de se désagréger à cause de la mobilité sociale et géographique. À Paris, un officier de la maréchaussée, qui répondait au nom de Guillauté, a rédigé un projet tout à fait prodigieux, édité. Il s'agit d'un immense registre de toute la population parisienne, chaque habitant étant fiché. Ses fiches sont classées par famille, puis par immeuble, par rue, par quartier. Dans ces illustrations, Guillauté représente une vaste salle dont les murs sont recouverts de fichiers avec un plan gigantesque de la ville et des tiroirs où les commis de la police pourraient puiser l'information dont ils auraient besoin à propos d'un individu. Guillauté avait aussi inventé une sorte de machine : une sorte de roue fixée dans le mur qui faisait tourner les fichiers pour diminuer l'espace de stockage. Il s'agit bien sûr d'un projet imaginaire, d'une utopie policière qui n'a jamais vu le jour. Mais elle indique des potentialités étonnamment modernes.

Une autre innovation considérable au XVIII^e siècle réside en la banalisation d'une technique de signalement : la description de l'apparence physique. Jusque-là, il s'agissait d'une pratique réservée aux « réprouvés » tels que les prisonniers, criminels, esclaves mais aussi les soldats considérés comme des fugitifs en puissance. En dehors de ces cas, il était considéré comme indigne de prendre le signalement de quelqu'un. Tout change à partir du XVIII^e siècle puisque cette description physique envahit les certificats, les passeports se multiplient pour devenir une pratique administrative banale. Une évolution qui s'achève au début du XIX^e siècle où la pratique est généralisée. À cette époque, sous Napoléon, même les permis de chasse comportent un signalement, ce qui aurait été inimaginable un ou deux siècles auparavant. L'irruption du corps dans l'identification est due à l'identification à distance. En effet, certaines institutions policières : la police de Paris, les institutions pénales, l'administration des galères, qui se trouvent dans certains ports français, puis les bagnes ou encore l'administration militaire, se dotent de vastes jeux de registres qui concentrent des données sur des personnes qu'elles veulent surveiller ou retrouver et qui se cachent sous une fausse identité – les soldats s'ils deviennent déserteurs, des mendiants ou des vagabonds qui se seraient échappés d'un lieu de répression. Elles enregistrent le nom et le signalement de chacun. Une nouvelle ambition apparaît : la volonté

de retrouver par le corps et le signalement un individu recherché même s'il se cache sous une fausse identité. L'administration militaire installée à Versailles – siège du gouvernement – compile des listes de déserteurs avec leur signalement d'après des informations qu'elle reçoit des différents régiments. Ces listes sont compilées dans un grand volume que l'on appelle « livre des déserteurs » qui est envoyé après impression aux principales cours de justice, aux polices des grandes villes et aux ports. Ce travail de l'administration permet donc de comparer à des centaines de kilomètres les suspects qui peuvent être arrêtés et le signalement des déserteurs que cette administration a accumulé. Le travail des employés du bureau des déserteurs à Versailles est tout à fait fascinant. Les prisons et les magistrats leur adressent parfois directement des signalements écrits d'hommes arrêtés à Toulouse ou à Marseille et qu'ils comparent avec leur propre registre. Ces employés inaugurent l'identification par comparaison au signalement de personnes qui ne sont jamais physiquement présentes devant eux, des personnes qu'ils n'ont jamais vues, mais auxquelles ils peuvent attribuer une identité simplement en comparant des descriptions physiques. Il s'agit encore d'une pratique compliquée et difficile mais c'est à ce moment-là, je crois, qu'elle apparaît, et elle est amenée à se développer par la suite.

Je voudrais maintenant vous parler des documents d'identification qui existaient à l'époque. Cette période moderne des ^{xvii}^e-^{xviii}^e siècles correspond véritablement à ce que l'on pourrait appeler un « âge du registre ». Qu'il s'agisse de criminels, de prisonniers, de soldats, de voyageurs donc, les identités des personnes sont enregistrées, c'est-à-dire littéralement inscrites dans des cahiers, des gros volumes tenus par les embryons de l'administration centrale ou municipale. Se pose assez vite le problème du classement des identités sous cette forme, notamment avec la multiplication des registres et de leurs volumes. Pour exemple, un registre central des mendiants, de tous les hôpitaux généraux du royaume est mis sur pied en 1724. Les quelques commis en charge de la gestion du registre reçoivent toutes les semaines des dizaines de signalements. La question de la méthode de classement – problème majeur pour cette administration – se pose. Comment retrouver l'identité d'une personne à partir des données disponibles ?

À partir de la fin du ^{xvii}^e siècle apparaît un autre support, plus souple que le registre : la fiche ou le dossier. Ainsi, plusieurs documents séparables sont actualisables et reclassables à volonté. En France, ce système de fichiers semble apparaître dans les archives de l'administration des galères sous Louis XIV. Les geôliers ont créé quelque chose de tout à fait astucieux. Ils ont construit de petites boîtes dans lesquelles ils ont entreposé des cartons avec l'identité de chaque galérien. Dans le cas où un galérien changeait de bateau, sa fiche changeait de boîte, chaque boîte correspondant à une galère différente. La fiche amovible offre une gestion beaucoup plus souple que les anciens registres. Au milieu du ^{xviii}^e siècle, Joseph Demery, un officier de police chargé de la librairie à Paris, donc de la censure, possède un fichier pour son usage personnel, étonnamment moderne, composé de fiches pré-imprimées sur plusieurs centaines d'écrivains, libraires, imprimeurs, colporteurs qu'il est chargé de surveiller. La fiche ne supprime le registre que vers le milieu

du xix^e siècle. En 1830, le préfet de police de Paris, Gisquet, met sur fiches les sommiers judiciaires – listes de condamnés qui existaient déjà dans l'administration policière parisienne mais qui étaient jusque-là entreposées dans des registres. Un deuxième aspect est la multiplication des documents d'identité portatifs. Il ne s'agit que d'une simple feuille dont une seule face est imprimée. À l'époque moderne, il existe une multitude de documents portatifs remis par une autorité qui indique l'identité de leurs porteurs. Parmi les plus anciens, il faut mentionner les insignes qui étaient des jetons, des médailles, que devaient porter de façon visible dès la fin du Moyen Âge les pèlerins, les colporteurs, les coursiers diplomatiques, les pauvres autorisés à mendier dans une ville ou encore les voyageurs qui voulaient entrer dans une ville pendant une épidémie de peste. Les documents sur papier se multiplient à l'époque moderne, surtout à partir du xvi^e siècle, sans doute parce qu'ils permettent d'indiquer plusieurs informations et que l'usage du papier, qui est une invention récente en Occident, se démocratise. Ainsi se multiplient des documents comme les passeports, certificats, etc. Leur forme évolue lentement mais cette évolution s'accélère au xviii^e siècle. Des formulaires imprimés apparaissent peu à peu pour devenir la règle au début du xix^e siècle. Les passeports étaient jusqu'alors très souvent collectifs et deviennent individuels. En France, les passeports se standardisent sous la Révolution française. En 1792, on définit un premier formulaire uniforme. Mais c'est sous l'administration napoléonienne, en 1807, que le modèle suivant est créé. Il s'agit du passeport à souches, réputé infalsifiable notamment grâce à l'utilisation d'encres spéciales, d'un papier qui réagit chimiquement si on tente d'effacer l'encre, des filigranes pour permettre la reconnaissance. Donc, l'histoire du passeport moderne commence, je crois, avec ce passeport. Avec la multiplication des documents s'opère une démultiplication des supports, une spécialisation, en particulier à la fin du xviii^e siècle. Les feuilles sont remplacées par d'autres inventions, comme le livret que l'on appelle aussi « petit cahier », instaurées dans les années 1770 pour les ouvriers et qui est promis à un grand avenir. En effet, nos passeports contemporains sont des livrets comportant un certain nombre de pages qui permettent l'accumulation des visas. À la même époque est inventé le support de la carte, que l'on appelait encore « cartouche » au début du xviii^e siècle. Ce terme, à l'origine du terme « carton », vient de l'italien *cartoccio*. Les soldats avaient ainsi sur eux des « cartouches de congés ». Sous la Révolution française, il y a tout un système de cartes de sûreté réservées à la population masculine des grandes villes, en particulier Paris. Sous une forme extrêmement condensée, elles permettent d'avoir des informations sur l'identité du porteur. Leur forme est petite et plus solide que la feuille de passeport et il s'agit en fait de l'ancêtre de notre carte d'identité, que l'on peut avoir sur soi en permanence. Enfin, sous la Révolution française, l'identification de l'individu est prise en charge par l'État. Jusqu'en 1789, presque tout le monde pouvait délivrer un passeport ou un certificat à un individu, depuis le curé de paroisse jusqu'au roi lui-même. Depuis la Révolution, ce sont les municipalités qui, seules, ont le droit de distribuer les passeports avec ce qui deviendra les préfectures. Bientôt, elles s'appuieront sur les registres de l'état civil qui leur seront confiés à partir de 1792. L'employé de mairie devient alors la première autorité en matière d'identité. Il s'agit d'une rupture majeure dans l'histoire de l'identification

en France puisque l'État est désormais le garant de l'identité de chacun qu'il atteste par des registres d'état civil et des passeports officiels qu'il délivre. Il ne faudrait pas conclure que l'histoire de l'identification est celle de progrès continus, du triomphe annoncé de l'identification écrite et de la prise en charge presque totalitaire de chaque individu d'un État omniscient où tout le monde serait fiché ou enregistré. En effet, le témoignage oral demeure un élément important, sinon essentiel, encore au XIX^e siècle. Pour obtenir un passeport, il suffit de se présenter avec un ou deux témoins dignes de foi, donc des habitants des lieux. On sait que près des mairies, il est notoire que des aubergistes aient fréquemment à attester l'identité de tous leurs clients. Ce sont toujours les mêmes personnes que l'on voit inscrites sur les registres de police, moyennant quelques pièces. Les employés et la police s'inquiètent peu de savoir qui est réellement ce voyageur qui demande un passeport. Les documents qui autorisent à circuler en France sont facilement délivrés. Les bases de l'identification écrite restent donc fragiles.

L'histoire des papiers d'identité est aussi celle de l'incertitude et de la fraude à cette époque. Au XIX^e siècle, la maréchaussée emprisonne des individus, manifestement suspects d'être des repris de justice parce qu'à l'époque les condamnés étaient marqués. Ces derniers n'hésitent pas à déclarer leur identité mais prétendent avoir purgé leur peine. Lorsqu'on écrit au tribunal qui est censé les avoir jugés, il est impossible de retrouver leur sentence. Alors, que faire d'eux ? Dans d'autres cas, ce sont des imposteurs. Louis Le Roger³, jeune soldat pauvre, harcèle de lettres la veuve d'un grand aristocrate parisien en déclarant être un enfant naturel de son mari, ce qui est totalement invérifiable. Il est arrêté par la police qui prend très au sérieux ce genre d'affaire et parvient sans peine à démolir l'identité qu'il prétend être la sienne. Il prétendait notamment avoir reçu une éducation cachée. En revanche, la police est incapable de prouver qui il est. Il n'est donc pas rare de trouver dans les prisons des individus qui n'ont pas d'identité certaine. L'enfermement est d'ailleurs considéré comme le meilleur moyen de leur faire retrouver la mémoire. Louis Le Roger s'en tient d'ailleurs à ses prétentions. Il finit par mourir en prison, tué par ses codétenus à qui il refusait de parler parce qu'il s'estimait justement aristocrate. Cet épisode montre, en définitive, l'impuissance des autorités à identifier le prisonnier avec certitude et donc la nécessité de s'en remettre à ses déclarations. Cette histoire est aussi celle de la fraude. Au lendemain de mesures royales pour imposer aux soldats des cartouches de congés standardisées, apparaissent des faux, plus ou moins habiles, que le Roi doit punir de galère. À mesure que les papiers se démultiplient au XVIII^e siècle, ils deviennent des documents que l'on s'échange, que l'on revend, que l'on falsifie. C'est le cas notamment au sein des populations pauvres qui sont menacées de contrôle pour lutter contre le vagabondage et la mendicité et utilisent ce procédé pour échapper à la police. L'échange se fait dans les tavernes, dans les auberges, sur les routes. Par exemple, un pèlerin français en route pour Saint-Jacques-de-Compostelle et dont nous avons gardé le journal, raconte comment une fois arrivé en Espagne, il a donné son passeport à un français déserteur qui désirait rentrer en France. D'autres titres, comme les permissions de mendier, font l'objet de véritables trafics. Dans le Paris du XVIII^e siècle, la police découvre des

réseaux parfaitement organisés associant des écrivains publics qui fabriquent des faux documents et des pauvres, en particulier des veuves sont envoyées dans les églises pour quêter avec ces documents. À l'époque napoléonienne, tous ceux qui désirent échapper au service militaire dans les armées françaises usent de subterfuges très divers pour entrer dans la clandestinité, mais souvent avec la complicité d'employés municipaux et préfectoraux. Plutôt que de brûler volontairement la mairie et l'état civil comme certains l'ont fait à cette époque, ils préfèrent falsifier ou altérer discrètement les registres de l'état civil, en changeant l'âge par exemple. Une autre technique réside dans la fuite et la cache derrière une fausse identité ou un faux passeport, notamment en se procurant des formulaires vierges, en volant des cachets ou en fabriquant des faux. L'État et les faussaires s'engagent alors dans une course de vitesse à la technologie qui se poursuit encore. Les faussaires ont compris que les autorités ne cherchaient pas à contrôler l'identité mais les signes d'authenticité des papiers qui leur sont propres.

Pour conclure, je souhaite insister sur l'importance de l'époque moderne dans la genèse de certaines pratiques contemporaines d'identification ; en témoigne l'apparition de mesures presque biométriques autour du signalement. Toutes ces mesures butent sur un certain nombre d'imperfections. On ne peut donc pas exagérer le rôle de ces administrations. Cette époque correspond à l'entrée des Français dans l'âge moderne d'une identification écrite qui repose sur ces documents.

Notes

* Maître de conférences en histoire à l'université Paris-I. ↑

1. *Colonel Chabert*, 1^{re} éd. 1832. ↑

2. Documents nominatifs qui permettaient d'établir officiellement l'absence de risque d'épidémie. Preuve de la bonne santé des voyageurs et du passage par les régions non infectées. ↑

3. DENIS, Vincent, « Imposteurs et policiers au siècle des Lumières », *Politix*, 2006/2, n° 74, p. 11-30. Voir [l'article](#). ↑

12

Histoire de l'identité
en France

Du bertillonnage à l'Europe biométrique♦

Pierre Piazza*

Avec l'essor du bertillonnage¹ à la préfecture de police de Paris, une véritable rupture va prendre forme en France, à partir du dernier tiers du XIX^e siècle, en matière de rationalisation des techniques policières d'identification érigeant le corps des individus en objet de savoir. Ce processus de rationalisation est d'ailleurs déjà à l'œuvre avant même ce tournant majeur de la III^e République, comme a pu l'analyser précisément Vincent Denis² dans son ouvrage *Une histoire de l'identité. France, 1715-1815*³. Le bertillonnage est notamment fondé sur la mesure de certaines parties du squelette humain, le relevé de stigmates inscrits à même la peau, le perfectionnement des clichés photographiques (face/profil) réalisés par les fonctionnaires de police et l'amélioration des modes de rédaction du signalement reposant désormais sur une description « scientifique » du visage⁴. Il va progressivement contribuer à affranchir les forces de l'ordre des « hasards de l'empirisme » en matière d'identification des personnes. Avec le bertillonnage se dessine aussi la mise en place de fichiers de police sans cesse plus volumineux contenant notamment des informations sur les données corporelles de catégories d'individus de plus en plus nombreuses et diverses : délinquants et criminels récidivistes, mendiants et vagabonds, aliénés retrouvés sur la voie publique, étrangers faisant l'objet d'une mesure d'expulsion du territoire, personnes soupçonnées d'espionnage, anarchistes, etc.

À partir du début du XX^e siècle, l'émergence de savoirs et de savoir-faire sans cesse davantage sophistiqués sur les méthodes de classement des empreintes digitales (notamment grâce aux recherches menées par le Britannique Sir Francis Galton⁵ et l'Argentin Juan Vucetich⁶) conduira également à la constitution d'immenses fichiers dactyloscopiques par d'innombrables services de police à travers le monde⁷. Ces fichiers auront pour objectif d'identifier plus rigoureusement les délinquants et criminels, les migrants ou même l'ensemble de la population dans certains pays qui s'orienteront vers la mise en place d'un Office national d'identification dactyloscopique. Cette rationalisation des techniques policières d'identification va aussi permettre aux forces de l'ordre d'identifier avec plus de certitude les individus par le papier *via* des modes de rédaction du signalement moins approximatifs, en incluant les empreintes digitales dans les documents d'identité, en normalisant les clichés photographiques qu'ils contiennent, en standardisant et homogénéisant la forme et le contenu de ces documents, en développant des techniques destinées à empêcher leur falsification ou encore en établissant un lien étroit entre les informations contenues dans les titres d'identité et celles que conservent les pouvoirs publics dans des fichiers centralisés.

Lorsque l'on porte un regard de nature socio-historique sur le développement et la rationalisation sans cesse accrue des procédures de mise en carte des individus, on constate la récurrence d'un double phénomène. L'exemple de la carte nationale d'identité le révèle pleinement. C'est à la fois un outil qui a pu favoriser à travers le temps, tant dans la pratique que symboliquement, un resserrement des allégeances aux valeurs de l'État-nation. En effet, c'est en manipulant quotidiennement ce « type d'instrument d'État » matérialisant une « appartenance commune » que chaque citoyen a pu être amené à éprouver la « nation » dans son for intérieur comme une dimension essentielle de sa

13

Du bertillonnage à
l'Europe biométrique

propre identité. Mais parallèlement à cette dimension « intégratrice », s'en est constamment greffée une autre qui renvoie à des logiques policières de contrôle et de surveillance ayant notamment eu pour effet de stigmatiser certaines catégories de la population : création d'un carnet anthropométrique des nomades à partir de 1912 pour mieux contrôler, suivre à la trace et réprimer les personnes dont la non sédentarisation est perçue comme un véritable danger⁸ ; apposition de la mention « Juif » sur les cartes de citoyens de confession juive sous Vichy ayant alors directement servi à favoriser leur persécution ; instauration de la carte nationale d'identité en 1955 à des fins de surveillance des Français musulmans d'Algérie⁹. La biométrie est véritablement héritière de ces premières entreprises policières d'identification prenant le corps des individus pour cible. Tendant actuellement de plus en plus à s'imposer parmi les acteurs publics en charge des questions de sécurité comme une technologie incontournable, elle renvoie à des procédés qui, en vue de savoir avec une quasi-certitude qui est qui, permettent de transformer certaines caractéristiques physiques, physiologiques ou comportementales propres à chacun (empreintes digitales, empreintes palmaires, ADN¹⁰, iris, rétine, reconnaissance faciale, etc.) en une empreinte numérique qui est exploitable informatiquement.

Ces dernières années, cette technologie a surtout donné lieu à l'essor de deux types de dispositifs dans le champ de la sécurité : la constitution de bases de données biométriques (de plus en plus vastes constituées à l'échelon national et supranational) et l'introduction de puces contenant des données biométriques dans des titres d'identité ou de voyage¹¹. Donnons ici quelques exemples qui montrent combien ces deux types de dispositifs biométriques se sont considérablement développés ces dernières années. En France, institué par un décret du 8 avril 1987, le FAED (Fichier automatisé des empreintes digitales) a été le premier fichier national biométrique, commun à la police nationale et à la gendarmerie, à devenir opérationnel en 1994. Il enregistre et conserve notamment les empreintes digitales de l'ensemble des personnes mises en cause dans une procédure pénale pour crime ou délit. Plus de trois millions d'individus y sont aujourd'hui fichés. Quant au FNAEG (Fichier national automatisé des empreintes génétiques), il a été créé par une loi du 17 juin 1998. Initialement déployé à des fins de répression des infractions sexuelles, ce fichier d'empreintes génétiques est néanmoins progressivement devenu, surtout depuis la loi du 18 mars 2003 sur la sécurité intérieure, un véritable « outil d'identification criminelle généraliste ». Pratiquement tous les crimes et délits peuvent actuellement donner lieu à un génotypage en France et le FNAEG contient le profil génétique de plus de 1,2 millions de personnes¹². Néanmoins, les impératifs d'identification criminelle ne constituent pas les seuls motifs du recours des autorités françaises à la biométrie. Les technologies biométriques sont aussi de plus en plus systématiquement employées à des fins d'identification des étrangers. Une disposition de la loi du 26 novembre 2003 relative à la maîtrise de l'immigration a instauré le relevé et le traitement automatisé des empreintes digitales des demandeurs de visa. La France a mis en place (par un décret du 2 novembre 2007) un traitement biométrique intitulé VISABIO qui fait suite aux expérimentations menées depuis 2004 par les ministères de l'Intérieur et des Affaires étrangères

dans le cadre du programme BIODEV¹³ (autorisé par un décret du 5 octobre 2004). Ce dispositif vise surtout à permettre aux autorités de savoir quelle est l'identité des étrangers en cas de contrôle et d'éviter à ces derniers toute possibilité de dissimuler qui ils sont et si une mesure d'éloignement est décidée à leur rencontre.

VISABIO s'articule au projet VIS (*Visa identification System*) que le Conseil de l'Union européenne a résolu, par une décision du 8 juin 2004, de mettre en place très prochainement. Le VIS devrait devenir l'un des plus grands fichiers biométriques centralisé au monde dans lequel pourront être stockées les dix empreintes digitales de millions d'individus (entre 70 et 100 millions) non européens susceptibles de pénétrer dans l'espace Schengen ou d'y transiter¹⁴. Au niveau européen, ce dispositif s'ajoute au fichier biométrique EURODAC¹⁵ (*EUROpean DACtylographic system*). Institué en décembre 2000, il est devenu opérationnel trois ans plus tard. Cette base de données biométrique permet de collecter, à des fins de comparaison, les empreintes digitales des immigrants illégaux et de tout étranger de plus de quatorze ans amené à déposer une demande d'asile. L'Europe souhaite aussi introduire des données biométriques dans une nouvelle version du SIS (*Système d'information Schengen*) : le SIS II. Il convient également d'évoquer la mise en réseau à l'échelon européen, au nom de l'application du principe de disponibilité de l'information¹⁶, des fichiers biométriques (empreintes digitales et ADN) constitués par les États membres *via* le Traité de Prüm qui, signé en 2005, a été intégré dans le cadre législatif de l'UE en 2007.

Depuis les attentats du 11 septembre 2001, les technologies biométriques ont encore trouvé d'autres champs d'application en raison de la pression exercée par les États-Unis sur l'UE. En effet, dans le cadre de la guerre déclarée contre le terrorisme, la mise en place par les autorités américaines à l'entrée de leur territoire de programmes de contrôles biométriques des personnes en provenance d'États tiers (notamment le *Patriot Act* et le *US-VISIT*¹⁷) a fortement incité les États de l'UE à délivrer des passeports biométriques à leurs ressortissants. Par un règlement du 13 décembre 2004, la Commission européenne a déterminé les normes biométriques à intégrer dans les passeports et les documents de voyage délivrés par les États membres de l'UE. Enfin, ces dernières années, de nombreux pays ont aussi mis en place ou projeté d'instaurer pour leurs citoyens des cartes nationales d'identité biométriques. Par exemple en France, le projet INES (*Identité nationale électronique sécurisée*) a fait l'objet en 2005 d'un débat national organisé par le Forum des droits sur l'internet, même s'il a ensuite été suspendu, en particulier en raison de l'ampleur des résistances qu'il avait suscitées et des difficultés pour le ministère de l'Intérieur d'en démontrer l'impérieuse nécessité¹⁸. Depuis quelques années, on assiste donc à un essor considérable de la biométrie, modalité *high tech* officiellement érigée au rang de solution indispensable en matière de sécurité au nom de l'efficacité de la lutte contre des risques, menaces et dangers présentés comme étant principalement en lien avec l'intensification de la circulation des individus à l'échelle planétaire. Cette application des dispositifs biométriques à des populations sans

15

Du bertillonage à
l'Europe biométrique

cesse plus larges pose pourtant quelques problèmes de taille auxquels on voudrait ici s'intéresser en insistant tout particulièrement sur les initiatives prises récemment par l'UE.

Tout d'abord, évalue-t-on suffisamment les risques susceptibles de résulter du recours de plus en plus massif aux technologies biométriques avant de s'orienter dans cette voie ? Parallèlement, organise-t-on, en toute transparence, de nombreux et importants débats, tant au niveau des instances politiques nationales qu'européennes, avant que la décision de s'orienter vers une généralisation de l'emploi des technologies biométriques ne soit arrêtée ? Régulièrement présentée par les responsables politiques, en vue de justifier son absolue nécessité, comme une « solution miracle » pour révéler l'identité des individus, la biométrie ne constitue pas une technologie totalement fiable. Le Groupe de l'article 29 (groupe des autorités européennes sur la protection des données) et, en France, le Comité consultatif national d'éthique pour les sciences de la vie et de la santé ont, concernant les passeports, par exemple dénoncé la fragilité des transmissions des données biométriques réalisées à partir des puces intégrées dans ces documents et les conséquences majeures induites par ce phénomène en matière de « confidentialité¹⁹ ». De plus, les taux d'erreurs à l'enregistrement et de fausses acceptations lors de la réalisation des contrôles ne sont jamais nuls et varient plus ou moins fortement notamment en fonction du type d'identifiant biométrique mobilisé²⁰. Ainsi que le pointe encore le G 29, la possibilité de retrouver les données d'un individu dans une base biométrique diminue proportionnellement à l'augmentation du nombre de données qu'on traite dans cette même base²¹. Selon lui, un tel problème se posera tout spécialement avec la mise en œuvre du vis qui sera, du fait des lourdeurs de sa gestion, certainement à l'origine de conséquences dommageables pour les individus. De plus, parce qu'il « n'existe pas de littérature scientifique démontrant de manière irréfutable que la technologie dactyloscopique est suffisamment fiable en ce qui concerne soit les enfants, soit les personnes âgées²² » et qu'il est impossible de relever correctement les empreintes digitales de près de 5 % d'individus (en raison notamment de divers handicaps²³), le G 29 estime que le protocole du vis ne pourra pas concrètement s'appliquer chaque année à près d'un million de demandeurs de visas, qui encourront donc toujours le risque d'être injustement stigmatisés du fait de limites techniques²⁴. Ce point de vue est partagé par le CEPD (Contrôleur européen à la protection des données²⁵). Soulignant par exemple que la mise en œuvre du sis II pose surtout le problème de la fiabilité de la biométrie, il considère qu'elle est surestimée. À l'appui de son propos, le CEPD évoque notamment cet exemple qui illustre parfaitement l'ampleur des risques pouvant résulter de la croyance en la toute-puissance de cette technologie en matière de preuve identitaire dans le cadre d'investigations policières :

« En juin 2004, un avocat de Portland (États-Unis) a été emprisonné pendant deux semaines parce que le FBI avait établi que ses empreintes digitales correspondaient à des empreintes trouvées dans le cadre des attentats de Madrid (sur un sac plastique ayant contenu le détonateur). Il a finalement été établi que la technique de comparaison était défaillante et avait entraîné une erreur d'interprétation²⁶. »

16

Du bertillonage à
l'Europe biométrique

La plupart des autorités de protection des données nationales et européennes, ainsi que nombre de chercheurs en sciences sociales s'intéressant de par le monde aux enjeux de l'identification des personnes²⁷, pointent la nature « sensible » des données biométriques²⁸ et la multitude de problèmes qu'engendre l'extension récente au sein de l'UE de bases de données biométriques centralisées de plus en plus volumineuses : faiblesse du régime de protection des données à caractère personnel, risques d'atteinte à des droits considérés comme fondamentaux (notamment le droit à l'oubli ou à la présomption d'innocence) et à la vie privée²⁹, possible stigmatisation de certaines catégories d'individus³⁰, dangers liés à la consolidation de logiques de « traçabilité » et de « profilage » des personnes³¹, etc. Malgré la quantité et l'importance de ces problèmes, l'UE s'engage inexorablement dans le déploiement de « solutions biométriques » en matière de sécurité sans que ne soient toujours sérieusement appréciées l'ensemble des incidences néfastes que peut produire la mise en place d'un véritable système de surveillance numérique des personnes. Ainsi, concernant le vis, Émile Gabrié a rigoureusement étudié la manière dont la Commission Européenne a mis en place « sa » propre expertise de ce dispositif (non publicisée) et il en tire la conclusion suivante :

« Cette expertise a pour principale motivation de légitimer les positions de la Commission sur le vis, et indirectement celles du Conseil. La méthodologie retenue est ainsi employée dans ce but : elle consiste à étudier les effets de quatre *scenarii* possibles, afin de comparer leurs opportunités et d'en dégager la mesure la plus avantageuse et équilibrée. Notre hypothèse de simple instrumentalisation de l'expertise, menée dans le seul but de légitimer les arbitrages déjà retenus par les acteurs dominants, n'est pas fondée sur des présupposés. Elle s'appuie notamment sur le fait que cette expertise n'était ni obligatoire ni demandée ou souhaitée par aucune autre institution : la Commission en est la seule initiatrice et elle seule a décidé de mener cette étude. De plus, aucun des *scenarii* comparés dans ce travail n'a fait l'objet ne serait-ce que d'une allusion, tout au moins dans les documents officiels, de la part des autres acteurs, ni même du Conseil qui a pourtant impulsé le processus. Apparemment, ces trois autres possibilités ont donc été imaginées ou invoquées par les rédacteurs de ce travail dans le seul but d'appuyer la mise en place du vis telle que retenue par la Commission, par la mobilisation d'un registre d'expertise³². »

17

Du bertillonage à
l'Europe biométrique

S'il se pose avec acuité au niveau supranational, l'enjeu de la rigueur des procédures mises en œuvre en vue d'évaluer les incidences générées par le vis ; il apparaît tout aussi problématique à l'échelon national. Cet extrait particulièrement révélateur d'une délibération de la CNIL³³ portant sur BIODIV l'atteste en 2007 :

« La Commission avait demandé, dans ses délibérations n° 04-075 du 5 octobre 2004 et n° 2005-313 du 20 décembre 2005 sur le traitement BIODEV, qu'une étude approfondie soit conduite, de façon indépendante et selon une méthodologie précisément définie, sur les expérimentations menées. Tout en se félicitant de la démarche progressive qui a été adoptée, la Commission souligne que les expérimentations conduites semblent l'avoir été de façon plus limitée que prévu. Outre l'abandon, dès BIODEV II, du "visa électronique" à puce, le nombre de consulats équipés pour la biométrie fin 2006 est resté sensiblement inférieur à ce qui était programmé par BIODEV II (25 sur 40), de sorte que la base centrale alimentée depuis mars 2005 ne contenait, en décembre 2006, que 100 000 visas biométriques [en total cumulé depuis mars 2005], soit 2,80 % du total des visas émis pour la période considérée [150 000 en mai 2007]. Elle relève également que le nombre de postes équipés dans les points de contrôle aux frontières est resté en deçà des prévisions. De surcroît, deux des modalités principales du fonctionnement du traitement n'ont pas été expérimentées : la consultation des bases centrales par les agents consulaires afin de prévenir les usurpations d'identité, et les contrôles à l'intérieur du territoire, à la différence de ce qui était prévu par le décret du 20 décembre 2005. Enfin, bien qu'un certain nombre d'éléments d'appréciation et des bilans partiels aient été fournis, l'évaluation d'ensemble prévue à l'article 8 du décret n° 2004-1266 du 25 novembre 2004 n'a pas été réalisée. La CNIL ne dispose donc pas d'une étude indépendante, globale, reposant sur des critères et des objectifs bien identifiés³⁴. »

18

Du bertillonage à
l'Europe biométrique

Pour Alex Türk, président de la CNIL, l'essor considérable de la biométrie est symptomatique d'une « vague sécuritaire technologique » qui caractérise actuellement les politiques de l'UE et dont les fondements reposent sur le « mythe du contrôle absolu par l'instrument informatique ». Il précise néanmoins que « considérée comme la panacée en matière d'identification et d'authentification, alors même qu'elle n'a jamais fait l'objet d'une évaluation officielle, concertée sur le plan international, la biométrie se développe aujourd'hui massivement, et prend une part de plus en plus importante dans les processus d'identification administrative, sans qu'aucune réflexion réelle n'ait été conduite sur les conséquences à l'égard des personnes des erreurs d'identification biométrique³⁵. »

Ce phénomène apparaît d'ailleurs d'autant plus inquiétant qu'il s'accompagne souvent d'un processus décisionnel qui manque véritablement de transparence. En 2005, le CEPD indiquait par exemple au sujet de la proposition de règlement du Parlement européen et du Conseil relatif au vis sur laquelle il était amené à se prononcer :

« Quel que soit l'intérêt de la biométrie à certains égards, son utilisation généralisée aura un impact majeur sur la société et devrait faire l'objet d'un débat large et ouvert. Le CEPD doit constater que ce débat n'a pas vraiment eu lieu avant l'élaboration de la proposition³⁶. »

Il convient d'ailleurs de rappeler que, dès 2004, la CE avait habilement décidé de créer une ligne budgétaire relative au VIS pour, en quelque sorte, placer le Parlement européen devant le fait accompli avant qu'il ne devienne codécisionnaire avec le Conseil sur les questions relatives à « l'Espace de liberté, de sécurité et de justice » (comme le préoyaient les dispositions du traité d'Amsterdam). De même, la création du SIS II par le biais d'un règlement et d'une décision a eu pour effet d'exclure du processus législatif les parlements nationaux et l'opinion publique des pays directement concernés par ce dispositif. Ce « déficit démocratique » peut être considéré comme d'autant plus inquiétant que l'idée de confier à terme la gestion du SIS II à une « agence gestionnaire autonome » inquiète nombre d'États membres : ils considèrent dangereuse cette option consistant à rendre responsable une telle structure des données sensibles intéressant la sûreté de l'État, la défense et la sécurité publique. Il est possible d'évoquer la manière dont le traité de Prüm a pu être transposé dans le cadre juridique de l'UE, qui apparaît encore très révélatrice de ce déficit démocratique. Si ce traité a été dans un premier temps signé par sept États membres (Allemagne, Autriche, Belgique, Espagne, France, Luxembourg et Pays-Bas), il a ensuite été demandé aux vingt autres pays de l'UE de l'accepter en bloc, sans disposer de la possibilité de participer à la détermination des mesures ayant initialement présidé à son élaboration. De plus, le processus décisionnel particulier emprunté (rappelant celui de l'intergouvernementalité de Schengen) a limité le rôle du Parlement européen³⁷. Comme le CEPD a pu le souligner :

« [Il est] fâcheux que l'on ait suivi cette procédure car cela conduit à ignorer totalement la nécessité d'un processus législatif démocratique et transparent puisque les facultés, déjà très limitées, instituées par le troisième pilier ne sont pas respectées³⁸. »

19
Du bertillonage à
l'Europe biométrique

Enfin, alors que l'échange et la consultation automatisée entre États de données relatives aux empreintes digitales et aux profils ADN des individus renvoient à des interrogations fondamentales concernant la protection des données, plusieurs parlements nationaux ont ratifié le traité de Prüm dans l'urgence, sans organiser de véritables débats, comme en Espagne³⁹. Dans d'autres cas, ces débats ont été réduits à leur plus simple expression : ainsi, en Allemagne, la discussion et le vote n'ont duré en tout que trente minutes⁴⁰. De même, en décembre 2007, la CNIL demandera aussi à ce que, du fait des graves atteintes à la vie privée et aux libertés individuelles à laquelle pouvait, à ses yeux, conduire l'institution en France du passeport biométrique soit organisé un débat démocratique hexagonal dans le cadre du Parlement⁴¹. Elle ne sera pas entendue sur ce point, et le décret relatif au passeport biométrique adopté par le ministère de l'Intérieur français (le 30 avril 2008) ne prendra aucunement en considération nombre des « réserves » que cette institution avait formulé pour souligner le caractère potentiellement liberticide de ce dispositif.

Le deuxième point important auquel je souhaite m'intéresser concerne le respect des principes juridiques fondamentaux de « proportionnalité » et de « finalité ». La directive 95/45/CE du 24 octobre 1995 (sur la protection

des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données) s'appuie surtout sur ces deux principes que tout dispositif européen de collecte et d'échange de ces données se doit impérativement de respecter.

« Les États membres prévoient que les données à caractère personnel doivent être :

- collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités [...] ;
- adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement⁴². »

On constate pourtant que les fichiers biométriques déployés par l'UE posent de sérieux problèmes d'application en la matière et constitue un exemple particulièrement significatif de mise en forme concrète du concept de « continuum de l'(in)sécurité » au sein de l'UE qui, dans le discours politique/policier, relie les questions relatives à l'immigration avec la lutte contre la criminalité et le terrorisme⁴³.

La Convention Schengen avait officiellement pour but de favoriser la libre circulation des personnes au sein de l'espace Schengen. En contrepartie, afin que la concrétisation de cet objectif n'aboutisse pas sur un véritable « déficit de sécurité », elle avait décidé de mettre en place des « mesures d'accompagnement » destinées à harmoniser, et à renforcer le contrôle exercé lors du franchissement par une personne des frontières externes de l'espace Schengen. Parmi ces mesures, le sis occupait une place prédominante : il constituait en quelque sorte la clef de voûte de toute la construction Schengen⁴⁴. Le sis devait servir à préserver l'ordre et la sécurité publique en facilitant, *via* une procédure automatisée entre États Schengen, un échange constant et rapide d'informations (concernant notamment les personnes recherchées aux fins d'arrestation) afin de renforcer la coopération policière et judiciaire en matière pénale. Parallèlement, le sis devait permettre d'assurer l'application des dispositions portant sur la libre circulation des personnes. Il représentait donc aussi un dispositif que l'on consultait par exemple dans le cadre des procédures de délivrance des visas et des titres de séjour, car il comprenait des informations relatives aux personnes privées du droit d'entrer sur le territoire d'un des États Schengen. Ces renseignements sont signalés aux fins de non admission pour des motifs tels que l'interdiction de pénétrer sur le territoire en raison d'un statut dérogeant aux règles nationales en matière d'immigration. Surtout depuis l'adoption par les États membres du plan global de lutte contre l'immigration clandestine et la traite des êtres humains (février 2002) et du plan d'action concernant la gestion des frontières extérieures (juin 2002), le sis a été amené à jouer un rôle particulièrement important dans la gestion par l'UE des flux migratoires. Avec le sis II contenant des données biométriques, le but jusqu'alors poursuivi semble changer radicalement de nature. Si l'objectif du sis « première génération » se limitait essentiellement à l'ex-

exploitation de données personnelle à des fins de non admission de certains individus sur le territoire des États membres, le sis II servira à l'échange d'informations pour le contrôle des personnes (et également des objets) *via* notamment une « mise en relation » des signalements qu'il contient lorsque cela répond à un « besoin opérationnel manifeste ». De plus, il est prévu que de nouvelles autorités disposeront d'un possible accès à certaines données du sis II : autorités compétentes en matière d'asile et habilitées à octroyer le statut de réfugié (accès aux données relatives à l'immigration) ; EUROPOL⁴⁵ (accès aux signalements relatifs à l'extradition, la surveillance discrète et les documents volés à des fins de saisie) et EUROJUST⁴⁶ (accès aux données relatives à l'extradition et à la localisation). Enfin, les données du sis II pourront être connectées avec les bases de données d'INTERPOL⁴⁷ (pour les passeports volés, détournés, égarés ou invalidés). Si le CEPD a pu indiquer sa difficulté à comprendre quelles étaient les véritables intentions des autorités européennes lors de la création du sis II, du fait de l'absence d'exposer les motifs dans les textes officiels instituant ce dispositif inédit⁴⁸ ; il est pourtant assez facile de comprendre la nouvelle tendance qui se dessine depuis peu. Les autorités, précédemment évoquées, auront la possibilité de consulter les données biométriques du sis II pour obtenir des informations utiles à la poursuite de leurs propres objectifs. Ces derniers répondent cependant à des logiques complètement étrangères à celles invoquées initialement pour justifier l'institution du sis. D'instrument de lutte contre la « délinquance transfrontalière » et d'accompagnement de la liberté de circulation des individus, le sis risque rapidement se transmuter en un instrument d'enquête d'envergure, voire en un véritable instrument policier de surveillance (les données biométriques autorisant et facilitant une extension des recherches sur les personnes) appliqué à des champs bien plus vastes : immigration, mais aussi criminalité organisée et terrorisme⁴⁹.

21

Du bertillonage à
l'Europe biométrique

Un processus identique se constate à propos d'EURODAC. Dans la lignée de ce qu'avaient suggéré les conclusions du Conseil « Justice et affaires intérieures » du 13 juin 2007, la Commission européenne a proposé – en septembre 2009 – de permettre aux services répressifs des États membres et à EUROPOL d'accéder à certaines données d'EURODAC. Elle a notamment considéré que cela permettrait de combler une lacune en matière de lutte antiterroriste. Soutenue par des États membres comme l'Allemagne, la France ou encore le Royaume-Uni, cette proposition a cependant été vivement critiquée par le Haut commissariat des Nations Unies pour les réfugiés et la Commission nationale consultative des Droits de l'homme. Ces derniers ont dénoncé un non respect du principe de proportionnalité et un détournement de la finalité d'EURODAC, d'autant plus inquiétant à leurs yeux qu'il risque de favoriser des pratiques policières stigmatisantes à l'encontre des demandeurs d'asile déjà particulièrement vulnérables en les érigeant, au détriment de l'application du principe de la présomption d'innocence, en une véritable population suspecte par nature⁵⁰.

De même, le CEPD a officiellement contesté la légitimité d'une telle mesure au regard des principes définis par la Charte des droits fondamentaux de l'UE, et a notamment indiqué :

« Il est clair que les instruments proposés par la Commission constituent une ingérence dans la vie privée. Leur utilité et leur nécessité sont cependant loin d'être démontrées : leur nécessité devrait être prouvée en apportant des preuves convaincantes de l'existence d'un lien entre les demandeurs d'asile et le terrorisme ou la grande criminalité. Or, les propositions n'établissent nullement ce lien⁵¹. »

Ajoutons que les États membres se servent de plus en plus de la base d'EURODAC pour comparer les données dactyloscopiques qu'elle contient (sur les demandeurs d'asile) avec les empreintes digitales qu'ils prélèvent sur les migrants irréguliers appréhendés à l'intérieur de leur territoire, afin de rendre plus performantes leurs politiques d'expulsion. Cette base biométrique ne sert donc plus uniquement à la gestion des procédures relatives aux demandeurs d'asile (afin de déterminer l'État membre qui doit être responsable de l'examen d'une demande d'asile conformément au Règlement de Dublin), mais elle devient un instrument de plus en plus décisif dans les politiques de lutte contre l'immigration irrégulière. À tel point qu'en 2007, la Commission européenne a d'ailleurs préconisé que les données dactyloscopiques des étrangers arrêtés en situation irrégulière sur le territoire d'un État membre soient, dans un avenir proche, directement stockées dans cette base⁵².

Le projet de création du vis s'inscrit encore pleinement dans une telle logique. La volonté de rendre le vis « interopérable⁵³ » avec le SIS II et EURODAC – qui ont néanmoins des finalités différentes – et de permettre l'accès des services répressifs au vis (alors que cette base de donnée n'a pas été initialement pas pensée comme un outil de nature répressive) pose la question de la remise en cause de la « proportionnalité » de ce dispositif – eu égard à l'objectif qui lui était initialement assigné : la mise en place d'une politique commune en matière de visas⁵⁴. Le vis va surtout devenir un outil utile permettant d'identifier biométriquement les « clandestins » qui ont pénétré légalement sur le territoire d'un des États membres, mais qui ont par la suite prolongé leur séjour alors que leur visa était expiré⁵⁵. Par conséquent, comme le précise Serge Slama :

« La préoccupation est tout autant de vérifier les identités en cas de contrôle sur le territoire et d'empêcher toute entrave à une mesure d'éloignement par dissimulation de l'identité ou du pays d'origine⁵⁶. »

Le respect du principe de proportionnalité par le Traité de Prüm apparaît tout aussi problématique. En effet, comment être certain que les dispositions instituées en la matière sont en adéquation avec l'objectif poursuivi (lutte contre la criminalité transfrontière et le terrorisme), et absolument indispensables pour y parvenir dans la mesure où aucune évaluation des dispositifs d'échange d'ADN et d'empreintes digitales entre États membres n'a jamais été effectuée sur une large échelle pour le déterminer ? Cet enjeu est encore pleinement au cœur de la mise en œuvre du passeport biométrique par certains États membres. Ainsi, alors

que le Règlement européen de décembre 2004 prévoyait d'introduire, dans la puce que contient ce document, la photographie numérisée et deux empreintes digitales de son titulaire, le ministère de l'Intérieur français a décidé d'étendre ce nombre d'empreintes à huit et de conserver l'ensemble de ces données biométriques dans une base centralisée, ce qui peut apparaître disproportionné au regard des finalités officiellement avancées pour justifier un tel dispositif (rendre plus aisées les procédures d'établissement, de délivrance, de renouvellement, de remplacement et de retrait des passeports et prévenir, détecter et réprimer leur falsification et leur contrefaçon)⁵⁷.

Notes

♦ L'auteur a souhaité réintituler son intervention. Titre original : « Du papier à la biométrie : identifier les individus ». ↑

* Maître de conférences en sciences politiques à l'université de Cergy-Pontoise. Il est spécialiste de l'histoire des dispositifs étatiques de l'identification des individus tels que les cartes d'identité, les fichiers et la biométrie. Il a notamment dirigé avec Xavier Crettiez (professeur en sciences politiques à l'université de Versailles-Saint-Quentin-en-Yvelines et à l'Institut d'Études Politiques de Paris) un ouvrage intitulé *Du papier à la biométrie, identifier les individus* (Les Presses de Sciences Po, 2006). Il a également publié *Une histoire nationale de la carte d'identité*, aux éditions Odile Jacob, en 2004. ↑

1. Alphonse Bertillon (1853-1914) a inventé l'anthropométrie judiciaire, appelée « système Bertillon » ou « bertillonage ». son système d'identification sera mis en œuvre à la Préfecture de police de Paris à partir des années 1880, et sera ensuite utilisé dans de nombreux pays. Voir le « projet Bertillon » (dirigé par Ilse ABOUT et Pierre PIAZZA) mis en ligne sur [Criminocorpus](#). ↑

2. Voir la communication « Histoire de l'identité en France ». ↑

3. Seyssel, Champ Vallon, 2008. ↑

4. Martine KALUSZYŃSKI, « Alphonse Bertillon et l'anthropométrie » in Alain FAURE et Philippe VIGIER (éd.), *Maintien de l'ordre et polices en France et en Europe au XIX^e siècle*, Paris, Créaphis, 1987, p. 269-285 ; Pierre PIAZZA, « La fabrique bertillonienne de l'identité. Entre violence physique et symbolique », *Labyrinthe*, 6, 2000, p. 33-50 ; Ilse ABOUT, « Les fondations d'un système national d'identification policière en France (1893-1914). Anthropométrie, signalements et fichiers », *Genèses*, 54, 2004, p. 28-52. ↑

5. Francis Galton (1822-1911), homme de science britannique. Il est notamment l'inventeur d'une méthode d'identification des individus par les empreintes digitales. (<http://galton.org/>) ↑

6. Juan Vucetich (1858-1925), fonctionnaire de police argentin à l'origine d'un système de classification des empreintes digitales. Il a surtout œuvré au développement de la dactyloscopie en Amérique du Sud. Voir notamment Pierre PIAZZA, *Histoire de la carte nationale d'identité*, Odiles Jacob, Paris, 2004. ↑

7. Simon A. COLE, *Suspect identities: A History of Fingerprints and Criminal Identification*, Cambridge (Mass.), Harvard University Press, 2002. ↑

8. Henriette Asséo, « La gendarmerie et l'identification des "nomades" (1870-1914) » in Jean-Noël LUC (éd.), *Gendarmerie, État et société au XIX^e*, Paris, Publications de la Sorbonne, 2002, p. 301-311 ; Pierre PIAZZA, « Au cœur de la construction de l'État moderne. Sociogenèse du carnet anthropométrique des nomades », *Les Cahiers de la sécurité intérieure*, 48, 2^e trimestre 2002, p. 207-227 ; Emmanuel FILHOL, « La loi de 1912 sur la circulation des "nomades" (Tsiganes) en France », *Revue européenne des migrations internationales*, 23, 2, 2007, p. 135-158. ↑

9. Voir sur ces aspects, Pierre PIAZZA, *Histoire de la carte nationale d'identité*, Paris, Odile Jacob, 2004. ↑

10. Acide DésoxyriboNucléique. ↑

11. Voir notamment Colin J. BENNETT et David LYON (éd.), *Playing the Identity Card. Surveillance, Security and Identification in Global Perspective*, Londres/New-York, Routledge, 2008. ↑

12. Pour une analyse plus globale du développement des fichiers de sécurité publique en France ces dernières années : Pierre PIAZZA, « L'extension des fichiers de sécurité publique », *Hermès*, 53, 2009, p. 69-74. ↑

13. Sylvie CRAIPEAU, Gérard DUBEY et Xavier GUCHET, *L'expérimentation BIODEV : du contrôle à distance au macro-système technique*. Rapport final de recherche GET (Groupe des Écoles des Télécommunications) / INT (Institut National des Télécommunications), avril 2006. ↑

14. Dennis BROEDERS, « The New Digital Borders of Europe. EU Databases and the Surveillance of Irregular Migrants », *International Sociology*, 22, 1, 2007, p. 71-92. ↑

15. Irma VAN DER PLOEG, « *The Illegal Body: "EURODAC" and The Politics of Biometric Identification* », *Ethics and Information Technology*, 1, 4, 1999, p. 295-302 ; Evelien BROUWER, « *EURODAC: its Limitations and Temptations* », *European Journal of Migration and Law*, 4, 2, 2002, p. 231-247 ; Jonathan P. AUS, « *Supranational Governance in an "Area of Freedom, Security and Justice": EURODAC and the Politics of Biometric Control* ». University of Sussex, Sussex European Institute, Sussex European Institute working paper n° 72, 2003. ↑
16. Didier BIGO, Willy BRUGGEMAN, Peter BURGESS et Valsamis MITSILEGAS, « Principe de disponibilité des informations », 5 mars 2007. (<http://www.libertysecurity.org/article1377.html>) ↑
17. *United States Visitor and Immigrant Status Indicator Technology*. Ensemble de mesures de sécurité qui commence aux bureaux de délivrance de visas du Département d'État du pays d'où l'on part, jusqu'aux procédures de départ et d'arrivée aux États-Unis. L'objectif est de vérifier l'identité des voyageurs à chaque étape. ↑
18. Pierre PIAZZA, « Les résistances au projet INES », *Cultures & Conflits*, n° 64, 2007, p. 65-75 ; Clément LACOUETTE-FOUGÈRE, *Les métamorphoses d'INES. Trajectoire d'un programme public innovant : la carte nationale d'identité électronique*, mémoire de Master Recherche politique et société en Europe, Institut d'études politiques de Paris, 2008. ↑
19. Comité Consultatif National d'Éthique pour les Sciences de la Vie et de la Santé, Biométrie, données identifiantes et droits de l'homme, avis n° 98, 2007. ↑
20. Bernadette DORIZZI, « Les taux d'erreurs dans le recours aux identifiants biométriques », in Ayse CEYHAN et Pierre PIAZZA (éd.), *L'identification biométrique*, Paris, Presses de la MSH (à paraître au troisième semestre 2010). ↑
21. Avis n° 7/2004 (11 août 2004) du G 29 sur le vis. ↑
22. Avis n° 3/2007 (1^{er} mars 2007) du G 29 sur le vis. ↑
23. Le premier rapport officiel d'inspection du groupe de coordination de contrôle d'EURODAC (juillet 2007) souligne que pas moins de 6 % des empreintes digitales contenues dans cette base biométrique n'ont pas pu être exploitées du fait de leur mauvaise qualité. ↑
24. Sur ces aspects, voir l'avis n° 3/2007 (1^{er} mars 2007) du G 29 sur le vis. ↑
25. Institution indépendante créée par le règlement (CE) n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données. ↑
26. Avis du CEPD sur le sis II, 19 avril 2006. ↑
27. Voir notamment le réseau « Identinet » coordonné par Jane CAPLAN et Edward HIGGS du Saint Anthony's College (Université d'Oxford) : <http://identinet.org.uk/> ↑
28. Dans un rapport rendu public au début de l'année 2005, le Comité consultatif institué par la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel tenait déjà à apporter les précisions suivantes à propos de la biométrie : « L'application de la biométrie soulève d'importantes questions en matière de droits de l'homme. L'intégrité du corps humain et la manière dont il est utilisé par la biométrie constituent un aspect de la dignité humaine [...] Une fois que cette technique aura été adoptée à grande échelle, un développement irréversible, porteur d'effets imprévisibles, pourrait être amorcé. C'est pour cela qu'il convient d'appliquer le principe de précaution qui, selon les circonstances, impose une certaine retenue. » Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques, février 2005. ↑
29. Avis n° 3/2005 (30 septembre 2005) du G 29 sur le passeport biométrique. ↑
30. Notamment les individus à qui seront accordées des « exemptions » à l'enrôlement biométrique : avis du CEPD sur le passeport biométrique en date du 26 mars 2008. ↑
31. Voir la lettre du 30 novembre 2004 adressée par le G 29 au président du Conseil de l'UE. ↑
32. Émile GABRIÉ, *Biométrie et visas : l'établissement d'un dispositif d'identification et de contrôle des étrangers en Europe. Illustrations européennes de l'emploi de nouvelles technologies policières*, Mémoire de DEA, Université Paris Dauphine, 2005, 146 p. ↑
33. Commission nationale de l'informatique et des libertés. ↑
34. CNIL, Délibération n° 2007-195 du 10 juillet 2007 portant avis sur le projet de décret pris pour l'application de l'article L. 611-6 du Code de l'entrée et du séjour des étrangers et du droit d'asile, portant création d'un traitement automatisé de données à caractère personnel relatives aux ressortissants étrangers sollicitant la délivrance d'un visa et modifiant la partie réglementaire de ce même code. ↑
35. Alex TÜRK, « La difficile quête d'un équilibre entre impératifs de sécurité publique et protection de la vie privée », entretien réalisé par Pierre PIAZZA, *Cultures & Conflits*, 76, 2009. ↑
36. CEPD, avis sur la proposition de règlement concernant le vis, 23 juillet 2005. ↑
37. Thierry BALZACQ, Didier BIGO, Sergio CARRERA et Elspeth GUILD, *Security and the Two-Level Game : the Treaty of Prüm, the EU and the Management of Threat*, CEPS Working Document, n° 234, janvier 2006. ↑
38. Avis du CEPD sur le traité de Prüm, 4 avril 2007. ↑
39. Jacques ZILLER, *Le Traité de Prüm. Une vraie-fausse coopération renforcée dans l'espace de sécurité, de liberté et de justice*, European University Institute Working Papers, Law n° 2006/32. ↑
40. Elspeth GUILD et Florian GEYER, « *Getting local : Schengen, Prüm and the dancing procession*

of Echternach. *Three paces forward and two back for EU police and judicial cooperation in criminal matters* », CEPS Journal, 5 décembre 2006. ↑

41. CNIL, avis sur le projet de décret permettant la délivrance des nouveaux passeports biométriques, 11 décembre 2007. ↑

42. Directive 95/45/CE du 24 octobre 1995. ↑

43. Valsamis MITSILEGAS, « Contrôle des étrangers, des passagers, des citoyens : surveillance et antiterrorisme », *Cultures & Conflits*, 60, 2005, p. 185-197. ↑

44. Didier BIGO, *Polices en réseaux. L'expérience européenne*, Presses de Science Po, 1996. ↑

45. *EUROpean POLice office*. ↑

46. Unité de coopération judiciaire de l'Union européenne. ↑

47. *INTERnational POLice*. ↑

48. CEPD, avis sur le sis II, 19 avril 2006. ↑

49. Thierry BALZACQ, « *The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies* », *Journal of Common Market Studies*, 46, 1, 2008, p. 75-100 ; Sylvia PREUSS-LAUSSINOTTE, « L'élargissement problématique de l'accès aux bases de données européennes en matière de sécurité », *Cultures & Conflits*, 74, 2009, p. 82-90. ↑

50. Voir le rapport d'information n° 2155 déposé par la Commission des affaires européennes sur la deuxième phase de mise en œuvre du régime d'asile européen commun, Assemblée nationale, J.O., 15 décembre 2009. ↑

51. CEPD, avis sur la proposition modifiée de Règlement du parlement européen et du Conseil concernant la création du système d'EURODAC (...) et la proposition de décision du Conseil relative aux demandes de comparaison avec les données d'EURODAC présentées par les services répressifs des États membres et EUROPOL à des fins répressives, 10 avril 2010. ↑

52. Dennis BROEDERS, « Le virage biométrique dans la "lutte contre l'immigration clandestine" de l'Union européenne : l'établissement d'un contrôle migratoire intérieur "2.0" » in Ayse CEYHAN et Pierre PIAZZA (éds.), *L'identification biométrique*, Paris, Édition de la MSH (à paraître au troisième semestre 2010). ↑

53. Voir la communication de la Commission européenne sur le « renforcement de l'efficacité et de l'interopérabilité des bases de données européennes dans le domaine de la Justice et des Affaires Intérieures et sur la création de synergies entre ces bases », 24 novembre/2005, COM (2005) 597 final. ↑

54. CEPD, *Opinion of the European Data Protection Supervisor*, Bruxelles, 20 janvier 2006. ↑

55. Michael SAMERS, « *An Emerging Geopolitics of "Illegal" Immigration in the European Union* », *European Journal of Migration and Law*, 6, 1, 2004, p. 23-41. ↑

56. Serge SLAMA, « Politique d'immigration: un laboratoire de la frénésie sécuritaire » in Laurent Mucchielli (éd.), *La Frénésie sécuritaire. Retour à l'ordre et au contrôle social*, Paris, La Découverte, 2008, p. 64-76. ↑

57. Plus généralement sur quelques enjeux relatifs à la mise en œuvre du passeport biométrique par le ministère de l'Intérieur en France : Pierre PIAZZA, « La mise en œuvre du passeport biométrique en France : quelques réflexions sur les modes d'action du ministère de l'Intérieur », BlogClariss, 31 mai 2008 : (<http://groupeclaris.wordpress.com/2008/05/31/la-mise-en-oeuvre-du-passeport-biometrique-en-france-quelques-reflexions-sur-les-modes-d%E2%80%99action-du-ministere-de-l%E2%80%99interieur/>). ↑

Faire l'histoire de la surveillance

Sébastien Laurent*

Je voudrais vous présenter quelques réflexions générales et historiques autour de la question de la surveillance. Au préalable, je partirai de deux idées générales. Elles sont relativement admises ou assez fréquemment diffusées et répandues dans les médias. Mes prédécesseurs ont déjà démontré qu'elles étaient en partie imparfaites.

La première idée serait que l'État, les pouvoirs publics, le gouvernement, seraient une forme de figure cyclopéenne qui surveillerait en permanence nos moindres faits et gestes. Il s'agit là d'une idée que l'on peut interroger mais qui est courante.

La deuxième idée tient au fait que nous connaissons actuellement en Europe, du moins dans la France « post-11 septembre », une période qui marquerait l'apogée contemporain de la surveillance. Il serait dangereux de laisser croire que ce phénomène ne débute qu'à notre époque. La tâche ingrate mais quasiment fonctionnelle de l'historien, dans ce genre d'événements, est de rappeler à la fois la profondeur historique du phénomène, mais aussi d'apporter quelques éléments d'analyse.

Je me situerai dans une perspective très panoramique et générale, dans une réflexion de long terme. Qu'est-ce que j'entends par surveillance ? Il s'agit évidemment de la surveillance des individus – ou la surveillance collective des individus – par les autorités publiques. Je précise les autorités publiques car il existe bien des phénomènes de surveillance privée par des acteurs privés et au bénéfice d'intérêts privés. Je les laisse de côté car il s'agit d'un autre cas de figure. De même, quelle est la nature de cette surveillance ? Elle est finalement assez variée. Je me concentrerai sur la surveillance qui concerne les comportements d'individus au regard du droit puisque c'est ce qui légitime, dans un État démocratique, la capacité à surveiller les individus. Ce peut être une surveillance basée sur le comportement des individus ou sur leurs opinions religieuses ou politiques.

26

Faire l'histoire de
la surveillance

Vincent Denis l'a rappelé, la société de l'Ancien Régime dans laquelle s'inscrivent les phénomènes de surveillance et d'identification est une société caractérisée par des éléments prémodernes dans lesquels les contraintes collectives pèsent fortement sur les individus. L'interconnaissance, cette surveillance de tous, sous le regard de tous, dans des communautés de petite taille, est assez prédominante. Ceci explique en partie le faible investissement des organisations centrales dans la surveillance ou alors un investissement qui est fait en général sur des catégories délictueuses ou spécifiques – comme l'inscription maritime, les militaires. Il s'agit alors de microsurveillance ou d'autosurveillance mise en place par la communauté elle-même, mais qui en fait est extrêmement imparfaite. Néanmoins, ce contexte fait naître le phénomène de surveillance au sein de notre société.

D'autre part, un basculement s'opère autour des XVIII^e et XIX^e siècles avec la naissance de « l'opinion ». Il ne s'agit pas d'une opinion publique à proprement parler mais de l'opinion d'une catégorie de la bourgeoisie et de certaines élites nobiliaires qui vont ouvertement déjouer la censure et

commencer à émettre un certain nombre de critiques vis-à-vis des autorités religieuses et politiques. À cette même époque, dans le contexte de la lieutenance générale de la mairie de Paris, naissent les premiers efforts en matière de surveillance des opinions politiques. Puis, il y a l'apparition et la naissance véritable sur un plan philosophique de l'individu. Ceci constitue un point tout à fait important. Une chose est d'identifier par des signes pratiques et des dispositifs techniques l'individu, une autre est de considérer, du point de vue des autorités, qu'elles soient religieuses ou politiques, que l'individu existe au sens contemporain du terme. Une véritable mutation de la civilisation s'opère, qui touche un certains nombres de pays occidentaux. Cet événement se concrétise par la délimitation, au XIX^e, siècle de ce que l'on va appeler les libertés individuelles par le droit – la fixation dans des textes à valeur constitutionnelle, des textes de loi, d'un certain nombre de garanties publiques qui sont apportées aux individus. Ce basculement va être un facteur explicatif de la disparition de la société archaïque de l'Ancien Régime vers une société moderne fondée sur l'individu et les garanties qui sont apportées à ses individus.

Un dernier point est important : l'émergence de la politique moderne au sens contemporain du terme. L'introduction de mécanismes de représentations politiques et la naissance d'idéologies vont venir contester la base de la société d'Ancien Régime. Il s'agit de l'introduction du suffrage censitaire limité à une élite en France entre 1815 et 1830, puis du suffrage universel en 1848, et en 1870. Par étapes, de nouvelles couches de la société entrent dans l'ordre de l'expression politique. De ce point de vue, l'enracinement du suffrage universel marque l'entrée des masses dans la vie politique et pose inévitablement de nouvelles questions en termes de surveillance de l'opinion politique. Sous la Restauration, avec la naissance du suffrage censitaire, naît la « surveillance de l'esprit public » avec des méthodes nouvelles et plus précises – que Pierre Karila-Cohen¹ a montré dans un très bel ouvrage². La montée en puissance des idéologies contestatrices que sont les idéologies libérales et démocratiques vont se traduire par la naissance et le renforcement des appareils de surveillance. Le point à conserver à l'esprit est que les II^e et III^e Républiques n'ont pas remis en cause les dispositifs légaux, pratiques et administratifs de surveillance des individus, tant à l'égard du comportement que des opinions politiques. La police politique républicaine est un héritage direct dans ses cadres et ses mécanismes de fonctionnement de la police politique du Second Empire. Dès les origines, pas tant sous la I^{re} ou la II^e République, mais sous la III^e République ce phénomène se traduit par un régime de surveillance. C'est un point qui me paraît important, il constitue un élément de continuité avec les régimes précédents.

Quelles sont alors les transformations d'ordre pratique du point de vue de la réalisation des tâches de surveillance ? Au XIX^e siècle, des activités de surveillance publique apparaissent, qui connaissent un développement important. Des organes administratifs de surveillance vont être créés. Le Premier et surtout le Second Empire créent une police politique, la « police spéciale », ayant pour fonction non pas de surveiller les individus au regard du droit commun mais de surveiller et de collationner leurs opinions religieuses

et politiques. Ce dispositif est complété par la mise en place de services de renseignements militaires qui n'effectuent pas seulement des tâches de collecte militaire ou technique mais aussi un travail de surveillance politique à l'intérieur comme à l'extérieur du territoire.

Le dernier point à aborder tient à la grande diversité des acteurs de la surveillance. En la matière, le XIX^e siècle voit la naissance d'organes spécialisés avec des tâches précisément délimitées, essentiellement constitués d'un corps de policiers et de militaires en petit nombre. Cependant, l'État montre une certaine incapacité à organiser de façon rationnelle cette surveillance. Ainsi, des corps subalternes de l'administration qui effectuent un travail quotidien (les eaux et forêts, les douanes, les postiers par exemple) se voient confier des tâches de surveillance politique auprès des administrés à des échelles tout à fait différentes – les travaux récents sont clairs à cet égard. Finalement, aucune conception d'ensemble ne se dégage en matière de surveillance des individus et de rationalisation de son fonctionnement. La réalité historique déjoue ici tous les fantasmes panoptiques. De multiples chevauchements existent entre ces différents corps de fonctionnaires, y compris parmi ceux d'entre eux spécialisés dans la surveillance. Un second élément tient aux rivalités politiques qui déclenchent au XIX^e siècle les premières « guerres des polices ».

Je voudrais revenir maintenant sur quelques éléments plus concrets. L'activité de surveillance ou d'identification n'est pas une activité continue dans son intensité et dans le temps. Comme le montre Patrick Weil³, en matière de surveillance des étrangers et de politique de l'immigration, des poussées xénophobes sont apparues. Cependant, l'État lui-même, a présenté des velléités de surveillance des individus. Ainsi, au cours des XIX^e et XX^e siècles, de véritables régimes de surveillance se sont constitués : la Convention, le Premier et le Second Empire, l'époque de Vichy et de l'Occupation, etc. Il existe, en outre, d'autres éléments discriminants liés aux temps de paix ou de guerre. En temps de guerre, la surveillance doit être plus ample et l'investissement étatique en la matière est d'autant plus fort. En tant de paix, des périodes de tension ou de crise se présentent, caractérisées par des moments particulièrement importants de surveillance des individus. Dans son livre, Vincent Denis montre que la Régence est une période de basculement. La fin des années 1880, dans un contexte de tensions nationales et nationalistes en France, correspond à un autre moment de paix mais aussi d'accroissement de l'effort de surveillance. Ainsi, il existe une forte discontinuité de l'effort de surveillance, même en temps de paix.

Quels sont alors les moyens mis à disposition de l'État pour le fonctionnement des divers dispositifs de surveillance ? Peuvent être cités des éléments d'ordre technique : des fichiers, des moyens d'identification. En amont, il existe des moyens humains, dont certains se révèlent très anciens : discussions, interrogatoires dans un cadre légal ou non, avec ou sans violence, techniques d'infiltrations policières, subornations de témoins, chantages, filatures, etc. De multiples techniques de renseignements humains constituent ainsi quotidiennement le cœur des pratiques de surveillance. L'autre point à retenir tient finalement à l'ancienneté des pratiques. Dans le Paris du XVIII^e siècle,

autour de 1730, une première poussée de surveillance clandestine d'opinions se déclenche, y compris des opinions populaires. À cette époque, environ 300 à 350 « mouches » –des espions dans la lieutenance générale de police de Paris – effectuent un travail de collecte des opinions de la population parisienne, mais non de l'élite.

D'autre part, les moyens techniques mis à disposition suscitent des interrogations quant à l'existence de ruptures technologiques en la matière au cours de l'histoire. Finalement, y a-t-il un âge technique de la surveillance ? Les moyens techniques employés dans les pratiques de surveillance n'ont-ils pas introduit une forme de rupture dans la nature même de la surveillance ? Je laisse à des spécialistes et à des hyper contemporanéistes le soin de trancher cette question. Je voudrais juste rappeler que l'utilisation de moyens techniques par les organes de surveillance est extrêmement précoce. L'histoire des techniques et des moyens d'information et de communication le montre : les administrations se sont rapidement investies, financièrement et techniquement, dans leur usage – le cas de la biométrie présenté par Pierre Piazza le montre bien. Le télégraphe électrique date de 1837, les câbles sous-marins des années 1860, le téléphone (1879), la TSF (1895), le satellite, puis l'Internet sont autant de jalons dans une même tendance. L'émergence de tous ces moyens scande pour les premiers le cours du XIX^e siècle. À chaque innovation technologique, l'État en investit les contenus. Dans le cas de la France, le ministère de l'Intérieur a rapidement opéré un véritable monopole au niveau des télécommunications : le développement des réseaux de télégraphe électriques avant de nationaliser le téléphone dans les années 1880. Le ministère de la Marine et de la Guerre a encouragé les transferts de technologies de la TSF depuis l'Italie et la Grande-Bretagne. Ceci illustre clairement l'usage militaire de ces techniques de surveillance. En outre, tous ces moyens techniques servent finalement à accumuler un très grand nombre de données.

29

Faire l'histoire de
la surveillance

Pour autant, qui dit accumulation de données ne dit pas efficacité dans le traitement et la capacité d'expertise de ces dernières. Il s'agit là d'un problème central que les spécialistes du renseignement connaissent bien. Un analyste américain avait dit, dès 1973 :

« Nous sommes aujourd'hui dans une ère de surveillance de masse grâce aux moyens d'interceptions satellitaires. Cependant, nous sommes ignorants de la capacité et de la qualité de traitement de l'information individuelle dans ce type de renseignement. »

Ce qu'il avait appelé la « surveillance de masse » pose un certain nombre de questions éthiques et politiques, mais cela ne signifie pas pour autant que la surveillance de masse produise des données réellement exploitables et donc une surveillance effective.

J'aimerais pour finir soulever quelques questions concernant ce travail de surveillance, fortement enraciné dans des régimes démocratiques. Je souhaiterais notamment évoquer la question du rapport des autorités politiques à

la légalité. De ce point de vue, je voudrais signaler l'exception française en la matière. Elle réside dans le caractère extrêmement tardif avec lequel les autorités parlementaires ont été saisies de la question des services de renseignements. Ce n'est qu'en 2007 qu'une loi a créé un dispositif permettant aux parlementaires de contrôler les activités des services de renseignements. Une telle pratique avait pourtant été inventée sous le régime républicain de 1848. L'Assemblée constituante avait alors mis en place des commissions de contrôle parlementaire pour les fonds secrets. Ce dispositif a fonctionné jusqu'au Second Empire. Ce n'est que dans les années 1970 que l'opposition centriste, puis communiste dans les années 1980, a essayé de mettre en place, en vain, une instance de contrôle parlementaire sur les organes de renseignements. Ce sera chose faite en 2007, dix à quinze ans après l'Allemagne, l'Italie et à la plupart des grandes démocraties libérales, y compris dans certains pays de l'Europe de l'Est. Cela traduit la volonté du pouvoir exécutif de ne pas tolérer cette immixtion sur ce qui relève du domaine réservé de l'État. Malgré tout, quelques progrès en matière d'encadrement d'un certain nombre de techniques de surveillance se constatent. La [loi de 1978](#) qui crée la Commission nationale informatique et libertés [CNIL], a quand même permis l'encadrement de pratiques qui relevaient jusque-là d'un pouvoir réglementaire non contrôlé. Le [rapport Bauer](#) de décembre 2008 en a encore apporté l'illustration. La loi de 1978 a mis en place deux grands principes. L'administration doit déposer une procédure d'autorisation dès qu'elle veut créer un fichier, que se soit un fichier de surveillance ou un simple fichier administratif. Dans la perspective qui nous intéresse, il est évident que les fichiers de surveillance sont très concernés. Le rapport Bauer a montré que l'on avait redécouvert des fichiers qui avaient échappés à la vigilance. On voit donc bien que se maintiennent des pratiques clandestines de fichage par l'administration elle-même. Un second exemple réside dans la [loi de 1991](#) visant à encadrer les écoutes administratives et judiciaires. Là aussi, on a créé une autorité administrative indépendante du point de vue de l'histoire longue de la démocratie libérale. Pour une fois, en comparaison avec d'autres démocraties libérales, la France n'a pas été la dernière. La Belgique a adopté un dispositif réglementaire similaire, il y a un an. Ainsi, la loi précédemment mentionnée autorise un certain nombre d'administrations, notamment l'administration des douanes, le service des renseignements douaniers, à procéder à ce que l'on appelle des « livraisons contrôlées ». La loi autorise ainsi l'infiltration de réseaux de la criminalité organisée et l'utilisation du trafic de drogue pour procéder ensuite à des arrestations au sein du « milieu ». Il faut ajouter que toutes ces pratiques de surveillance, progressivement et de façon incomplète, tendent non pas à se placer sous le régime de la loi mais à se voir imposer un certain nombre de contraintes par des normes écrites. *A contrario*, l'administration a développé pendant deux siècles des pratiques, non pas véritablement illégales mais que l'on pourrait juger aujourd'hui scandaleuses car la question de leur justification tant sur un plan philosophique que politique n'a pas été débattue ou même abordée.

Pour conclure, le phénomène de surveillance des individus est une pratique ancienne avec laquelle la démocratie dans le monde et notamment la République en France a toujours composé. Ceci me paraît être un point tout

à fait important. D'autre part, un progrès mesuré de l'encadrement juridique de cette pratique s'est opéré au cours des siècles. Il est évident que le cadre national est totalement dépassé par certaines pratiques d'identification. Malgré l'existence d'un discours public valorisant la publicité et la transparence de l'action publique, il subsiste toujours un espace secret au sein de l'appareil d'État. Je l'ai appelé dans mes travaux « l'État secret »⁴, qui vit et se nourrit du travail quotidien et très ancien de la surveillance.

Notes

* Maître de conférences habilité en histoire contemporaine à l'université Michel-de-Montaigne de Bordeaux et également maître de conférences à Sciences-Po Paris. Il est un spécialiste de l'histoire du renseignement aux XIX^e et XX^e siècles. Il a dirigé de nombreux ouvrages sur le renseignement, notamment : *Politiques de l'ombre. État, renseignement et surveillance en France* (Paris, Fayard, 2009), *Politiques du renseignement* (Presses universitaires de Bordeaux, « Espace public », 2009), *Secrets d'État, pouvoirs et renseignement dans le monde contemporain* (Armand Colin, 2005) et *Archives « secrètes », secrets d'archives ? Historiens et archivistes face aux archives sensibles*, (CNRS Éditions, 2003). ↑

1. Maître de conférences en histoire contemporaine à l'université Rennes-II-Haute Bretagne. ↑

2. *L'État des esprits. L'invention de l'enquête politique en France (1814-1848)*, Rennes, PUR, 2008. ↑

3. Directeur de recherche au CNRS. ↑

4. *Politiques de l'ombre. État, renseignement et surveillance en France* (Paris, Fayard, 2009). ↑

Enjeux des politiques d'identification et de surveillance

- 33** **Identité, identification et surveillance : enjeux à l'heure de la biométrie**
Ayse Ceyhan

- 40** **Table ronde**
Animée par Michel Alberganti

Identité, identification et surveillance : enjeux à l'heure de la biométrie

Ayse Ceyhan*

Les systèmes biométriques produisent un changement paradigmatique au regard de l'identité, en faisant du corps et des données personnelles les nouvelles sources d'identité et d'identification. Comment les concepts d'identification, de surveillance et d'identité évoluent-ils à l'heure de la biométrie ? Quelles conséquences est-il possible d'en tirer concernant les modalités du « vivre ensemble », de la confiance des uns vis-à-vis des autres, et des citoyens vis-à-vis des autorités et institutions ? Ma présentation sera donc conceptuelle et s'appuiera sur quelques exemples récents. Comme le disait Emmanuel Kant, « une observation sans concept est vide, et un concept sans observations est également vide ». Les concepts dont je vais parler sont anciens, cependant, ils prennent un sens différent selon le contexte dans lequel ils sont employés. Parmi les caractéristiques les plus saillantes de ce dernier à l'heure actuelle, on peut citer la transformation de la sécurité en un enjeu politique global, son traitement par des technologies de pointe comme la biométrie¹, et l'utilisation des données personnelles comme l'élément stratégique de ces technologies entraînant une intrusion sans précédent dans la vie privée des individus.

Je voudrais commencer ma démonstration par un retour sur la notion de biométrie. Cette dernière est investie de plusieurs définitions. J'aimerais mettre l'accent sur les dispositifs biométriques comme la collection informatique des mesures biologiques, génétiques ou comportementales uniques à un individu ; et leur analyse par des méthodes statistiques et mathématiques afin de vérifier, d'authentifier l'identité d'une personne et/ou lui attribuer une identité reconnaissable. Lorsqu'on parle du rapport de la biométrie à l'identité, deux notions sont généralement déployées : l'authentification et l'identification. L'authentification est le processus de certification qui permet d'associer une identité à une personne qui prétend procéder à une action. Elle permet de vérifier que la personne qui prétend détenir une carte d'identité, une carte d'entrée, une carte d'accès ou qui entreprend une action sur Internet est bien le titulaire ou l'auteur de l'échange en question. Quant à l'identification, elle est le processus d'assignation et d'attestation d'une identité reconnaissable à un individu. L'identification est donc à la fois procédurale et relationnelle. Elle se fait de plusieurs façons. On pense d'abord à la façon administrative, c'est-à-dire à la certification, effectuée par les services de l'État, qui se concrétise par l'attribution d'une carte d'identité ou d'un passeport. Quant au monde numérique, elle se fait par l'association de codes : code PIN, mot de passe, code d'accès et données personnelles. Mais l'aspect le plus important de l'identification est l'assignation d'une identité à travers les rapports interactifs tant au niveau individuel qu'au niveau social. L'identité est une notion difficile à cerner, car elle n'est jamais fixe et donnée définitivement. Elle est en permanence en (re)construction. Même si la biométrie est fondée sur la mesure des parties inchangeables du corps par les technologies de capture des empreintes digitales, de l'iris ou de la rétine, au-delà de la construction technologique de l'identité, elle touche à la question de l'identité relationnelle. Dans cette relation, interviennent non seulement l'individu et les autorités qui capturent ses empreintes, mais aussi la technologie.

33

Enjeux à l'heure
de la biométrie

Je voudrais désormais parler de ce que j'entends par surveillance. De nos jours, nous sommes dans un monde où les processus d'identification et de surveillance commencent à aller de pair, et parfois vont jusqu'à se confondre. La surveillance se caractérise, par une attention systématique portée aux données personnelles obtenue à travers l'observation des itinéraires, des interactions, de la mobilité du corps de l'individu dans le but de gérer, de discipliner, de contrôler et de prévoir de futurs ou possibles comportements à risques. Dans cette configuration, que devient l'identité ? Actuellement, l'identité n'est plus envisagée dans son acceptation multiple et mouvante, mais elle est assignée d'une fonction d'attestation de certitude, voire même de fixité. Rappelons que la recherche d'une identité fixe est une préoccupation très ancienne. Elle a toujours intrigué les philosophes, les sociologues même si elle fut examinée sous des appellations différentes. La question classique qui a intrigué tout le monde depuis le début était de savoir s'il était possible de reconnaître et figer l'identité des choses et des êtres de manière définitive. Ainsi, dès les présocratiques tels que [Parménide](#), la philosophie a été affectée par la question de la conciliation entre mêmeté et changement. Pour les uns comme Parménide, il est difficile de penser le changement : « L'être est un continu éternel. » Pour les autres comme [Héraclite](#), selon la célèbre formule dont il est l'auteur : « On ne peut entrer deux fois dans le même fleuve. » Tout est en perpétuel mouvement. La question de savoir comment envisager l'identité du moi dans le temps, comment s'identifier et identifier l'autre, a toujours préoccupé les historiens, les philosophes, les sociologues.

En fait, l'identité est un concept difficile à définir de façon synthétique. Elle englobe plusieurs éléments. Comme le dit Erik Erikson² : « L'identité est à la fois conscience et processus. Elle est à la fois le moi ou le soi, un processus et une relation. » Du point de vue psychologique, elle constitue la subjectivité de l'individu ; du point de vue philosophique, elle est liée au lien permanent unissant mêmeté et différences. La pensée de [Paul Ricoeur](#) peut apporter un éclairage intéressant sur ce sujet. Elle distingue deux pôles de l'identité ; « l'identité *idem* » ou « identité *mêmeté* », et identité *ipse*. Si l'on applique cette formule à l'identification biométrique, « l'identité *idem* » peut renvoyer à l'information contenue sur les gènes d'un individu, la partie inchangée du corps comme par exemple l'empreinte de la rétine, de l'iris, de la main. Toutefois Ricoeur rappelle qu'on ne peut pas se contenter de définir l'identité seulement à travers « l'identité *idem* ». Il faut penser à « l'identité *ipse* », qui est la définition du soi par rapport à soi-même, et par rapport à l'autre reconnu dans son altérité – concept cher à [Levinas](#). Ricoeur nous invite, à juste titre, à intégrer le rapport à l'autre, le relationnel et le sensible dans la définition même de l'identité. Or, les systèmes biométriques, par leur focalisation sur l'identification de l'individu à travers les parties interchangeables du corps réduisent l'identité à l'*idem*, sans un lien direct avec l'*ipse*.

La biométrie introduit un changement paradigmatique au processus d'identification. L'identité n'est plus assignée par certification, même si les éléments biométriques sont intégrés dans la puce de la carte d'identité. Elle n'est plus représentée seulement par une carte. La société n'aura plus de rôle

à jouer dans le processus d'identification d'un individu. L'identification par l'intermédiaire d'un tiers semble, quant à elle, amenée à disparaître. Avec la biométrie, le corps et ses parties inchangeables fourniront la principale source pour l'attestation de l'identité d'un individu. Quel est donc la nature de ce corps qui attestera dorénavant de l'identité des individus ? Il ne s'agit plus de la représentation du corps anatomique et médicalisé du XIX^e siècle mais du corps comme information qui se transforme en données numériques. Le corps est objectivé, réduit à des paramètres informatiques et naturels, donc inaltérables. Dans les systèmes biométriques actuels et dans leurs interconnexions avec les systèmes de surveillance, le corps est source d'information et générateur de flux de données doubles. Ces systèmes s'opèrent par l'abstraction des parties du corps de leur assise territoriale et leur réassemblage dans des bases de données sous forme de données doubles. Comme exemple de base de données où les données sont réassemblées de la sorte, nous pouvons penser aux fichiers de police nationale, aux fichiers de police au niveau européen ou aux fichiers utilisés par les compagnies d'aviation. Cette transformation du corps en données et sa circulation comme données doubles affectent évidemment l'ontologie du corps, qui ne se décline que comme flux d'informations. Ce processus s'accompagne également de la déterritorialisation et de la dématérialisation de l'identité. L'identité ne s'établit plus par une nomination de la puissance publique, mais elle se reconnaît sur le corps transformé en un code numérique. Peut-on donc considérer la biométrie comme une donnée personnelle au sens de la loi européenne de 1995, par exemple ?

Il s'agit d'une question qui a été d'actualité pendant longtemps et qui a généré pas mal de débats et d'interrogations. Pour ce qui est de mon propos, je vais juste faire une allusion, de manière rapide, à ce qu'est une donnée personnelle. Il s'agit d'une information qui vous permet de vous identifier, de vous reconnaître directement ou indirectement. Évidemment, nous connaissons des données personnelles très classiques : le nom, le prénom, la date de naissance, l'adresse postale ; mais il y a d'autres données personnelles, créées à l'heure de la société d'information et de l'informatique comme l'adresse IP, l'adresse électronique, le numéro de sécurité sociale, le numéro de carte de crédit, l'empreinte digitale, l'ADN et la photo d'identité. La photo d'identité, par exemple, est-elle une donnée personnelle ? Beaucoup de débats ont eu lieu sur le sujet. Je signalerais que l'OACI³ et la CEE ont proposé de la reconnaître comme une donnée personnelle. Les images captées par la vidéosurveillance ont également fait l'objet de discussions pour savoir si elles devaient être considérées comme des données biométriques personnelles. La CEDH⁴ a répondu par l'affirmative, refusant ainsi au Royaume-Uni l'autorisation de divulguer l'enregistrement vidéo d'une personne qui souhaitait se suicider. Dans un contexte où se propage un système d'identification à partir de l'empreinte des parties non changeables du corps qui se transforment en données personnelles. Deux types de données personnelles peuvent être distingués, en dehors des données personnelles classiques. Il s'agit, dans un premier temps, des données biométriques et, dans un second temps, des données personnelles créées à partir de la narration de l'intime et du relationnel sur Internet.

35

Enjeux à l'heure
de la biométrie

Internet est un dispositif fondamental dans la création de l'identité digitale car il promet de produire un nouveau type d'identité grâce à l'e-gouvernement, c'est-à-dire l'utilisation de l'information digitale et des technologies de communication dans l'espace public et l'espace des services par le gouvernement et les citoyens. À un autre niveau, des informations, liées à la sphère intime des individus, circulent sur les blogs et les sites comme *Facebook*. La somme de ces informations crée une identité digitale. Pour autant, il s'agit de données narrées, situées, avancées, publicisées dans des situations spécifiques et des contextes spécifiques d'échanges, d'amitié, de contacts ou d'achats. Elles ne doivent donc être valides que dans le contexte particulier dans lequel elles sont créées. Or, actuellement, il est possible d'assister à un phénomène nouveau de combinaison de plusieurs données de ce type, à leur extraction du contexte particulier au sein duquel elles ont été créées, à leur échange, voire même leur vente. Le droit à la protection de notre vie privée est ainsi violé. La description de cette évolution permet de faire ainsi un lien entre identification et surveillance.

La surveillance renvoie à la collecte et au traitement des données à des fins d'anticipation et de prévention de futurs risques. Nous sommes dans un contexte où toute sorte d'information peut devenir source de surveillance. Il ne s'agit pas seulement de l'information biométrique, de données personnelles au sens classique de toute information collectée par des acteurs publics ou privés, mais aussi transnationaux sur la vie, l'itinéraire, l'information, les achats, les goûts, la lecture des individus, etc. Nous vivons dans un monde où notre identité – ou notre identification et surveillance – se fait par des acteurs publics mais aussi par des acteurs privés transnationaux dont nous ne connaissons même pas l'existence. À cet égard, nous pouvons nous référer aux fichiers informatiques des compagnies d'aviation appelées PNR⁵, qui collectent et gardent la trace de toutes les informations que nous donnons aux agences de voyage lorsque nous réservons un billet d'avion ou un billet de train. Il est utile de rappeler que quatre compagnies privées dans le monde s'occupent de la collecte, de la conservation, de l'échange et de l'envoi de ces données aux autorités qui le leur demandent, et en particulier les autorités américaines (*The Department of Homeland Security*). Ainsi, lors d'une réservation sur Internet ou dans une agence de voyage, nos données personnelles les plus classiques mais aussi les informations que nous rentrons dans ce processus de réservation sont collectées, transformées, standardisées, conservées. En même temps, des profils sont conservés à partir de ces données pour leur capacité à devenir des personnes à risque. Une nouvelle procédure d'autorisation de voyage pour se rendre aux États-Unis a été instaurée le 12 janvier 2009. Cette procédure s'appelle l'ESTI⁶. Ce système concerne les 22 pays bénéficiaires du programme d'exemption de visas, dont la France, auxquels s'ajoutent huit pays asiatiques. Désormais, avant d'embarquer pour un voyage à destination des États-Unis ou en transit par le pays, il faudra obtenir une autorisation de voyage ESTA auprès du *Department of Homeland Security*. Avant même l'achat des billets, il faudra entrer des informations sur Internet (nom, adresse, date de naissance, numéro et référence de passeport, etc.), fournir les informations concernant le(s) voyage(s) (nom de la compagnie aérienne, numéro du vol, adresse de séjour aux États-Unis, motif

du voyage, etc.) et attendre la réponse du *Department of Homeland Security*. La réponse peut être quasi immédiate si l'autorisation est accordée. Mais l'autorisation peut se trouver être en instance, voire refusée. Ce dispositif constitue un bon exemple du « profilage de l'individu », dans un contexte anodin comme un voyage. Le *Department of Homeland Security* fait une opération de « *profiling*⁷ » : en fonction du risque que représente l'individu, il est autorisé ou non à se rendre aux États-Unis. Les autorités américaines soulignent qu'il n'y a aucune « *expectation of privacy* » au moment de l'utilisation du système ESTA. Or, nous ne pouvons contrôler les informations personnelles et les données que nous fournissons. Nous ne pouvons savoir où elles vont ; ce qu'elles deviennent, ni comment le « *profiling* » est établi. Nous pouvons juste les réactualiser si nous voulons repartir aux États-Unis dans les deux ans qui suivent, car ces autorisations ne sont valables que deux ans. Ceci soulève évidemment un grave problème de confiance sur le plan des relations internationales, et constitue une entrave majeure à la liberté de circulation. Pour autant, le processus de mise en place de ce système d'identification et de surveillance des individus n'est pas un phénomène nouveau et il existe une historicité de ce mouvement.

[Michel Foucault](#) en avait parlé dans ses écrits. Selon lui, les technologies de sécurité répondent à des mesures statistiques, des mises en service d'événements probables, des regroupements, des comparaisons, des calculs de coûts, tous participant au traitement de l'aléatoire. En se référant aux travaux du philosophe et sociologue Zygmunt Bauman⁸, il est possible de dire que l'aléatoire représente bien ou caractérise assez justement la société dans laquelle nous vivons. La dimension aléatoire du comportement des individus dans notre société est générée par de multiples facteurs : la mondialisation, la transnationalisation, la multiplication des identités, l'existence d'une société virtuelle, etc. Parallèlement, les technologies de sécurité qui se propagent, s'appuyant sur les données biométriques des individus et les données personnelles, participent à ce traitement de l'aléatoire, de l'incertitude qui, en contre coup, devient l'horizon dans lequel s'inscrit l'utilisation de ces mêmes technologies. Ces évolutions traduisent donc une « érosion de la confiance » dans les sociétés contemporaines. Cette dernière renvoie à un concept mouvant. Certains comme Bauman diront qu'il s'agit d'un moyen de réduire la complexité sociale – et souvent de façon irrationnelle – permettant ainsi de gérer des situations de déficit d'informations, de connaissances. D'autres penseurs, comme James Coleman, affirmeront *a contrario* que la confiance est un comportement rationnel qui nous pousse à coopérer avec les autres et les institutions. Toutefois, un autre concept est plus pertinent pour situer cette question : celui de sécurité ontologique, c'est-à-dire le sentiment de sécurité en permanence et la reconnaissance d'un environnement, d'une connaissance, d'une relation ou même d'une idée. Nous avons l'impression de vivre un moment de crise de sécurité ontologique d'où le recours à des technologies de certitude comme les technologies biométrique ou les technologies de surveillance.

Nous devrions nous interroger sur la perméabilité des sociétés aux technologies de sécurité et sur la question de leur acceptabilité. Cette dernière

est une question difficile à exposer en peu de temps car il s'agit d'une notion relative dépendant des contextes, des cultures, des moyens d'information dont dispose une société. Dans notre problématique, elle est évidemment liée au concept de protection de la vie privée, voire de la vie intime. La question de l'acceptabilité est difficile à saisir, néanmoins des études ont été faites sur le sujet. J'ai eu l'occasion de participer à l'une de ces études à l'université Queens au Canada. Celle-ci examinait l'attitude de citoyens de plusieurs pays dont la France, les États-Unis, le Mexique, l'Allemagne, le Royaume-Uni, la Hongrie et d'autres, face aux technologies de sécurité. L'étude⁹ a été publiée sous la direction du sociologue David Lyon qui travaille sur les questions de surveillance et d'identification. Concernant la France, jusqu'à l'adoption du passeport biométrique, les Français n'étaient pas très nombreux à connaître la biométrie comme moyen d'identification. On parlait de la biométrie seulement comme moyen d'identification policière et non comme un moyen d'identification des individus. Les Français connaissent mieux le GPS, par exemple. Ils sont 54 % à le connaître contre 24 % qui disent connaître la biométrie. Ces chiffres sont antérieurs à l'adoption du passeport biométrique. D'autre part, les Français ne connaissent pas la législation concernant la protection des données. Ils font confiance à l'État pour les protéger et ne connaissent pas bien l'existence de la CNIL. En outre, les Français interrogés semblent ne pas considérer les lois sécuritaires et les mesures de surveillance comme intrusives. Seulement 41 % des Français craignent que ces mesures ne le deviennent. Pour des raisons historiques, ils sont favorables à la carte d'identité. Toutefois, l'acceptabilité est une question très relative et mouvante. Ce genre d'études, d'enquêtes ne donnent l'image que d'un moment particulier.

38

Enjeux à l'heure
de la biométrie

En conclusion, je voudrais terminer en soulevant quelques questions. Quel est l'impact de la biométrie en tant que technologie de sécurité (j'intègre les technologies d'identification et de surveillance) ? J'ai identifié trois domaines mais la question peut être élargie. Concernant la police et le travail des policiers au quotidien – je m'adresse aux différentes polices et corps de gendarmerie : commissariats, aéroports, aérobares, ou centres de traitement des informations –, quel est l'impact de la biométrie sur leur travail ? Quel est l'impact sur l'organisation des rapports au sein même de la police ou des agences de sécurité ? Quel est l'impact de la biométrie sur l'antiterrorisme ? On voit bien que dans beaucoup de rapports mais aussi de projets de loi, la biométrie est strictement liée à l'antiterrorisme et proposée comme un moyen. Quelle en est son efficacité ? Quelle est l'influence des nouvelles technologies de sécurité sur la confiance des individus les uns envers les autres, sur le « vivre ensemble », sur la confiance envers les systèmes informatiques et du e-gouvernement qui se développe de plus en plus ? Quel impact ces mêmes technologies ont-elles sur les libertés et les droits fondamentaux, en particulier le droit à la protection de l'intimité ou de l'intime ? Comment protéger l'information personnelle ? Comment être maître de l'information personnelle ? Quelle est la confiance des individus vis-à-vis de la protection des données ou d'autres institutions que ce soit au niveau européen ou au niveau mondial ?

Public : J'ai une question méthodologique. Vous semblez limiter la question des enjeux pour la démocratie à la question de l'intimité. Le reste, vous l'abandonneriez à la police, à l'antiterrorisme et à des rapports sociaux numérisés sous voie de contrôle. Mais, est-ce que l'expression publique n'est pas une expression qui devrait rester libre sans vraiment avoir de rapport avec une numérisation à vocation coactive ou coercitive ?

Ayse Ceyhan : Dans la précipitation, il a semblé que je limitais la question de la démocratie à la question de l'intime. Évidemment, je suis d'accord avec cette question. Je pense qu'il faut la pousser en dehors des cadres qui sont instaurés par ces systèmes, à la libération de l'expression publique par n'importe quel moyen, que ce soit l'écriture ou la voix. Mais il faut aussi prévoir des espaces de transgression à ces limites. Comment alors opérer cette transgression ? La démocratie, me semble-t-il, prévoit aussi la liberté de transgresser sans entraver la liberté de l'autre. Comment pouvoir s'exprimer, comment pouvoir s'identifier ? Comment pouvoir identifier l'autre ? Comment ne pas refuser l'émergence de multiples formes d'identité et pourquoi être obligé de reconnaître la position d'une certaine identité à l'autre ? Ce sont des questions qui sont liées au problème que vous soulevez. Ce dernier est très vaste mais je suis d'accord sur le fond avec la critique que vous avez formulée.

Notes

* Maître de conférences à Sciences-Po Paris et directrice du programme « Sécurité–Technologie–Société » et du Groupe d'études et d'expertises sécurité et technologies (www.geest.msh-paris.fr). Elle est spécialiste des technologies de sécurité, notamment de la biométrie. ↑

1. Ayse CEYHAN, « *Technologization of Security : Management of Uncertainty and Risk in the Age of Biometrics* », *Surveillance & Society*, n° 5(2), 2008. ↑

2. Psychanalyste américain d'origine allemande (1902-1994). ↑

3. Organisation de l'aviation civile. ↑

4. Cour européenne des Droits de l'homme. ↑

5. *Personal Name Register*, en français : partage des données relatives aux passagers. [voir [accord pnr 2007](#)] ↑

6. *Electronic System for Travel Information*. [[informations](#)] ↑

7. Processus appelé « profilage » en français qui consiste à réaliser un portrait psychologique d'un individu en examinant des données et en les comparant à des statistiques. ↑

8. Enseignant en philosophie et en sociologie à l'université de Varsovie, Zygmunt Bauman fuit la Pologne en 1968, lors des persécutions antisémites. Il s'exile en Angleterre où il devient sociologue à l'université de Leeds. Il possède la double nationalité. Son œil vif se porte sur les nouveaux moyens de communication comme la télé-réalité. « Le concept de l'exclusion, de l'éphémère et de la célébrité dérisoire est une métaphore du monde dans lequel nous vivons aujourd'hui. » ↑

9. Ayse CEYHAN, « *Privacy in France in the age of security and information technologies* », *Privacy, Surveillance and the Globalization of Personal Information*, sous la direction de David LYON, Mc Gill-Queen's University Press, 2010. ↑

39

Enjeux à l'heure
de la biométrie

Table ronde : Enjeux des politiques d'identification et de surveillance

Animée par Michel Alberganti*

Michel Alberganti : Les enjeux des politiques en matière de surveillance et d'identification relèvent d'une question qui paraît évidente et qui en réalité ne l'est pas tant, dans la mesure où ces questions sont très rarement présentes dans le débat politique. Les exemples sont multiples, dont le dernier remonte à l'élection présidentielle suivie de la campagne législative pendant laquelle ces thèmes n'ont pas du tout été abordés. Dans les médias, ces sujets sont traités de façon relativement évidente, bâtis sur un consensus national assez fort : davantage de surveillance serait le gage d'une meilleure sécurité de tous. On imagine très mal les risques qui peuvent être associés à ce type de développement. Or, on se trouve dans une période particulière où de nombreuses technologies sont venues renforcer les techniques de surveillance. Le développement de l'informatique, des réseaux et d'internet, donne une place à part entière à ces capteurs multiples que sont la biométrie, les caméras de vidéosurveillance, la géolocalisation, les puces RFID et demain sans doute bien plus. Tous ces capteurs sont traités aujourd'hui avec des systèmes informatiques de plus en plus puissants et complexes, avec des bases de données de plus en plus énormes et des systèmes informatiques capables d'extraire de l'information de ces données numériques. La situation change et un débat politique devrait s'inspirer ou tirer des leçons de cette évolution technologique, pour reconsidérer la façon la société veut vivre vis-à-vis de ces sujets. Dans une démocratie, la population doit être à la fois au courant et être un acteur de cette décision. Christian Aghroum, commissaire divisionnaire et chef d'un organe de l'Office central de lutte contre la criminalité liée aux

technologies de l'information et de la communication, peut juger à la fois de l'évolution de ces technologies et des politiques liées à la surveillance et à la sécurité. Jean-Claude Vitran, animateur du groupe de travail « Libertés et technologie de l'information » à la Ligue des droits de l'homme prendra également la parole, ainsi que Laurent Bonelli, maître de conférences à l'université Paris-X-Nanterre et membre du centre d'étude sur les conflits.

Christian Aghroum : Qu'est-ce qu'un office central ? Dans notre organisation, il s'agit d'un service de police judiciaire. Sur la base des renseignements à vocation judiciaire qui lui sont adressés par les services de police et de gendarmerie pour déterminer les infractions, rechercher les auteurs et les déférer à la justice, l'OCLIC monte des enquêtes à caractère national et international. Nous venons en renfort à d'autres services et notre compétence s'étend à tout le territoire national. Nous avons donc une mission à vocation opérationnelle dans des domaines qui couvrent l'ensemble de la cybercriminalité, liée aux technologies de l'information et des télécommunications, tout particulièrement au piratage de données. Le vol de données individuelles, le vol de données à l'intérieur des sociétés et des entreprises est le grand sport à l'échelle nationale et internationale. Votre biométrie, votre nom, votre identité numérique intéressent tout le monde. Il nous appartient d'en protéger ses frontières et barrières. Nous avons ensuite la charge de la formation des acteurs qui vont travailler sur toutes les infractions facilitées par ces technologies nouvelles. Elles évoluent jour après jour : la cyberpédopornographie, le cybertrafic de stupéfiants, le cyberterrorisme (qui est d'ailleurs un peu un fantasme). Les terroristes

se servent d'outils normaux, d'outils modernes de communication, et le cyberterrorisme est encore autre chose – mais il s'agit d'un autre débat.

Notre organisme compte une soixantaine de personnes. Nous disposons de plusieurs outils à vocation nationale comme les plateformes de signalement de contenus illicites, le site [Info escroquerie](#) sur Internet. Nous sommes amenés à développer une activité stratégique puisque nous assistons, conseillons notre ministère et participons à l'élaboration de lois et de décrets dès lors qu'il y a matière à avancer juridiquement.

Michel Alberganti : Pourriez-vous nous dire ce que vous constatez en matière de surveillance ? Que se passe-t-il aujourd'hui de votre point de vue ? Comment percevez-vous la situation ?

Christian Aghroum : L'une de nos premières constatations tient au fait que l'identité intéresse tout le monde. On peut mettre en cause plusieurs phénomènes. Le taux de pénétration des ordinateurs et d'Internet dans les foyers français est de plus en plus important. C'est une très bonne chose. Je m'applique à croire et à dire qu'Internet est un dispositif qui s'inscrit au sein de la vie réelle et non dans un univers virtuel. L'univers internet peut certes paraître distant, mais n'est pourtant que l'expression de ce que l'on vit au quotidien.

D'autre part, nous voyons apparaître depuis quelques années deux phénomènes assez pénalisants pour notre action, la libre circulation des uns et des autres et, à mon sens, pour les libertés individuelles. Le premier est celui de l'anonymisation. Il est très utile, très efficace de circuler

sur Internet de manière anonyme. Une des vocations de l'outil est de permettre la création d'une autre identité, de vivre une autre vie. C'est très bien en soi. Par contre, ces outils d'anonymisation compliquent considérablement notre travail dès lors que l'on aura à chercher, à surveiller et identifier des individus criminels ou délinquants. Notre tâche est ainsi considérablement compliquée. Ceci constitue un premier handicap, compliquant considérablement la compréhension que nous pouvons avoir des identités criminelles dans cet univers de libre circulation de l'information et démultipliant ainsi le nombre des victimes potentielles – tel est le cas avec la cyberpédopornographie. En outre, la montée en puissance des outils de sécurisation et, parallèlement, de piratage constitue une autre source d'inquiétudes. Les données échangées et conservées doivent l'être selon des formes réglementaires. La France, de concert avec l'Union européenne, impose une conservation des données d'un an, non pas aux particuliers mais aux fournisseurs d'accès et autres. En Europe, les fournisseurs d'accès doivent les conserver entre six mois et deux ans selon les directives. Par contre, rien n'encadre « l'absence de droit à l'oubli » sur Internet. Dès lors que votre image, votre photo, votre vidéo ou une insertion quelconque ira circuler sur Internet vous concernant, il y a très peu de chances de la faire disparaître. Bien sûr, s'il s'agit d'une infraction à caractère pénal dont vous êtes victime et si le site qui l'héberge est installé en France, nous pourrions être en mesure de retirer ce site illicite ou son contenu du réseau internet. Par contre, cela n'empêchera pas x ou y de conserver la photo d'une nageuse connue et de très haut niveau, qui a fait la gloire de la France, et dont les photos circulent toujours. Il s'agit

d'un risque véritable. Le risque de piratage est tout aussi évident. Conserver des données est une bonne chose, mais il faut savoir les conserver de manière sécurisée et permettre qu'elles ne soient pas acquises, piratées, récupérées par n'importe qui, dans n'importe quelles conditions pour un usage non bénéfique. Au niveau des entreprises, cette problématique renvoie au vol de données. Celui-ci va alors contrarier le secteur de la recherche et du développement, et imposer de gérer les contraintes de l'espionnage industriel. Suivant la même perspective, le développement d'outils jusqu'alors réservés aux services du renseignement et qui sont maintenant à disposition de tous, peut susciter également des inquiétudes. Presque tout un chacun est muni d'un téléphone portable qui lui permet de communiquer dans le monde entier, de prendre des photos, des vidéos, d'enregistrer des gens à leur insu. La détention par la quasi-totalité de la population de ce type d'appareil va générer des complications considérables. Elle conduit à l'heure actuelle au développement d'un nouveau type de délinquance. Des menaces, que l'on ne connaissait pas, commencent à apparaître sur Internet : le racket, par exemple (devoir donner une somme d'argent pour ne pas voir sa photo diffusée sur le Réseau). Peu à peu, la frontière s'effrite entre vie privée et vie publique, dans des proportions que l'on n'imaginait peut-être pas il y a dix ou vingt ans.

Un autre risque réside dans la multiplication du « flicage » *via* Internet. Il est nécessaire de rappeler qu'être policier est un métier, encadré par des lois, des règlements, une déontologie. Néanmoins, des abus peuvent survenir, qu'il est nécessaire d'éradiquer.

Dans un État comme le nôtre, nous ne pouvons nous permettre d'avoir une police dans laquelle chacun ne respecte ni les lois, ni les règles, ni la déontologie. Nous avons une police des polices pour repérer les abus, et des magistrats pour les sanctionner. Par contre, nous assistons à une démultiplication du « flicage » sur le Réseau. Ainsi sommes-nous tous, potentiellement, devenus des « flics » d'Internet par la possibilité qui nous est offerte de taper dans Google le nom de notre voisin ou la personne que l'on va recruter. Nous nous retrouvons à chercher de l'information que nous n'aurions pu détenir auparavant. Sommes-nous en état de la vérifier et d'en contrôler l'exactitude de son contenu ? De notre côté, la recherche d'informations à laquelle nous procédons se fait de manière ciblée sur telle ou telle personne, dans tel ou tel cas, dans tel ou tel type d'enquête, que ce soit en police de renseignement ou en police judiciaire. Pour autant, cette information est vérifiée et impose d'autres vérifications par la suite. À présent, le contenu informatif simple que l'on peut découvrir sur Internet va poser de vrais problèmes à l'avenir en termes de recrutement de personnel, de frontières entre vie privée et vie publique, entre vie professionnelle et vie intime, et un réel problème en termes de « droit à l'oubli ». Par exemple, vous avez 18 ans, et vous êtes étudiant. Dans une soirée étudiante, vous faites ce que l'on a tous déjà plus ou moins fait dans ce type de manifestations : vous vous lâchez ! Quelques photos et vidéos sont prises et sont diffusées sur Internet. À 35 ans, vous vous présentez aux élections de votre village ou à un poste. On vous ressortira cette image que vous aurez montrée à 18 ans et vous serez jugé toute votre

vie là-dessus. À mon sens, il existe un risque, pour cette nouvelle génération de subir un tel abus et pour la génération suivante d'être contrainte à plus de puritanisme.

D'autres questions peuvent se poser. Auparavant, nous connaissions des agences privées de recherche : des détectives privés. Or, nous voyons apparaître des entreprises de conseil en entreprise, de recherche de renseignements, rassemblées sous le vocable d'« intelligence économique ». Elles aident l'entreprise à ne pas être agressée, attaquée, à ne pas faire l'objet de piratage industriel et aussi à procéder au recrutement de ses salariés. Ces entreprises peuvent avoir une attitude très agressive. Dans quelque temps, un encadrement de ces entreprises d'intelligence économique sera nécessaire. Va-t-on vers plus d'État ? Je suis convaincu, au contraire, que nous nous orientons vers une société dans laquelle une place plus grande sera accordée aux dispositifs technologiques. Je ne suis pas sûr que ce soit la meilleure direction à prendre. Si la technologie nous conduit à abandonner l'homme dans le dispositif de surveillance, le dispositif d'identification, nous allons passer complètement à côté de ce qu'est la réalité de notre société. L'homme doit rester le maître des technologies. Pour autant, nul affolement : la France ne se dirige pas vers un système du type « *Big Brother* ».

Malgré tout, nous ne devons pas aller trop loin dans la mise en place de ce dispositif technologique à des fins sécuritaires. Cela pourrait nous conduire à des errements. En effet, nous pouvons miniaturiser, de plus en plus, le support de l'identité : la possibilité d'implantation de puces RFID sous la peau des individus en

est un exemple. Je n'aime guère une telle perspective. Pour autant, des besoins existent en matière de reconnaissance de l'identité chez certains types d'individus. À l'heure actuelle, si un individu n'est ni délinquant ni criminel, il n'a jamais eu à prélever son ADN ou son empreinte digitale. Il ne sera donc jamais identifié, en cas de décès par exemple. Cette situation vaut pour certains SDF. Ceci peut être déploré. Des personnes meurent ainsi dans l'anonymat le plus complet. Néanmoins, cette part d'anonymat, accordée aux uns et aux autres, est peut-être une meilleure option que l'implantation d'une puce sous chacune de nos peaux qui devrait nous conduire à vivre ou à être surveillé de trop près.

Michel Alberganti : Merci beaucoup, Christian Aghroum. Je vais passer la parole à Jean-Claude Vitran¹, qui a pris position très récemment contre le projet « EDVIGE », sur le profilage des citoyens dans la paranoïa sécuritaire.

Jean-Claude Vitran : Aujourd'hui, de nombreux sociologues répètent que les citoyens étaient plus libres sous le septennat de Georges Pompidou qu'aujourd'hui. Ils répètent aussi que depuis plus d'une dizaine d'années, la surveillance des citoyens s'est particulièrement intensifiée. Avant d'aller plus loin, je voudrais quand même préciser que la Ligue des droits de l'homme n'est pas systématiquement contre toute forme de contrôle social. Ainsi, dirai-je simplement que les « droits-de-l'homme » ne sont pas « jusqu'au-boutistes ». Nous pensons que les systèmes de surveillance sont nécessaires, par exemple pour la fermeture des portes du RER ou pour la circulation sur les autoroutes. Des fichiers sont aussi nécessaires pour

établir des statistiques, pour faire des prévisions. Pour vous éclairer plus précisément sur ce point, je reviendrai en quelques mots sur le fichier national automatisé des empreintes génétiques, le FNAEG². Il était à l'origine destiné au fichage des délinquants sexuels. En 1998, nous avons approuvé la constitution de ce fichier. À l'époque, il concernait environ 1 500 délinquants. Aujourd'hui, le rapport du groupe sur les fichiers de M. Alain Bauer³, a dénombré un million de personnes fichées. Quelle en est la raison ? Cette situation est due à des contournements. De modifications en modifications – en 2001 puis en 2003 et en 2004 – présentées comme essentielles à la protection de la sécurité nationale, presque tous les crimes ont été intégrés (sauf les délits financiers par exemple). Toutes les données de ces suspects justiciables sont conservées de vingt-cinq à quarante ans. N'importe qui peut donc avoir son ADN collecté, simplement pour un chapardage ou de simples soupçons. Ces contournements successifs nous ont amenés à combattre ce fichier. La Ligue des droits de l'homme est inquiète sur de nombreux points. Tout d'abord, dans le dépliant de présentation est mentionnée la phrase suivante : « [...] L'État ou d'autres institutions publiques ou privées ont toujours cherché à identifier et à surveiller les citoyens. » Il a été souligné le fait que l'on commençait déjà sous Louis XIV à faire des petites fiches pour les galériens. Dans les années 1800-1810, Foucher était devenu le champion du fichage. À présent et depuis quelques années, nous assistons à une démultiplication du phénomène, due à l'emballlement de la micro-informatique et à l'apparition du microprocesseur, en novembre 1971. Il a permis la miniaturation des systèmes numériques.

Nous sommes passés, à ce moment-là, de l'artisanat à l'industrie du renseignement et du fichage.

Le second point de mon argumentation concerne les décisions ayant trait à la surveillance et au fichage, prises sans débat parlementaire. EDVIGE⁴ est l'archétype de l'exemple en la matière. Un arrêté a promulgué ce fichier, le 28 juin 2009, sans débat parlementaire. Le STIC⁵ contient les noms de 30 millions de personnes. Parmi elles, 5 millions ont été condamnés. Pour les autres, il s'agit de suspects ou de témoins qui peuvent le rester pendant trente ans. En outre, le STIC a été révélé au public plusieurs années après sa création. C'était un fichier de police tenu secret. Son existence a été connue de la Commission nationale de l'informatique et des libertés (CNIL) en 2003, alors que le fichier était opérationnel depuis les années 1995-1997. En 2006, le rapport de la commission Bauer révélait l'existence de 34 fichiers de police. Aujourd'hui, il en existe 45 et demain 57 sachant que 12 sont en cours d'étude. Pourquoi ce type de fichier connaît-il une telle croissance exponentielle ? Le troisième point concerne l'accès des citoyens à leurs propres données. La loi de 1978 prévoit un droit d'accès et de rectification aux données collectées. Faire cette démarche ressemble au parcours du combattant. Vous vous engagez pour plusieurs mois, voire plusieurs années, pour obtenir satisfaction. Quelquefois, alors que ce sont vos propres données personnelles, il vous est simplement dit que cela ne vous regarde pas. Le quatrième point se rapporte à la concomitance entre l'État et le secteur marchand. L'État veut profiler le citoyen pour avoir la paix sociale et anticiper le mécontentement ainsi que le secteur

marchant, pour faire le maximum de valeur ajoutée, de business. Tous les alibis et les prétextes sont bons : la sécurité, la commodité, le confort, la qualité de vie, le snobisme et même l'utilisation de certaines déviances. Tous les mensonges et toutes les compromissions sont utilisés. Le secteur marchand a besoin de l'État. Il fait pression sur la législation ; on l'a vu avec les OGM par exemple – pour légitimer ces systèmes toujours plus liberticides. Leurs intérêts sont convergents. Les marchés de la surveillance et du fichage sont porteurs d'une forte valeur ajoutée. Les États ont besoin de croissance, de développement économique, de juguler le chômage. Le secteur de la sécurité représente 17,5 milliards d'euros en 2006 et connaît une progression moyenne de 20 % par an. Voilà les raisons qui nous préoccupent et qui nous font dire que la démocratie est malade.

Pourtant, les barrières existent contre ce phénomène. La première renvoie au principe de finalité. Dans quel but un système ou un fichier est-il constitué ? Quelle est sa destination ? Ensuite le principe de proportionnalité peut également être cité. Les données collectées doivent être strictement nécessaires au but recherché, selon l'article 8⁶ de la Déclaration des droits de l'homme et du citoyen de 1789. La loi ne doit établir que des peines strictement et évidemment nécessaires. Ainsi, le principe de proportionnalité doit être fondé sur un besoin impérieux et notamment proportionné au but légitime recherché. Je voudrais également évoquer la liberté de conscience. Ce point est clairement défini par les articles 10⁷ et 11⁸ de la Déclaration des droits de l'homme et du citoyen de 1789. Ils existent des domaines

qui relèvent exclusivement de la sphère privée – l'orientation sexuelle, la santé, les opinions religieuses – et n'ont aucune raison de figurer dans une base de données.

Pour terminer, je propose de nous pencher sur la nanotechnologie. Elle est prometteuse d'un avenir radieux pour l'humanité selon les scientifiques et les industriels, ce qui est certainement vrai. Mais cette technologie est porteuse d'interrogations sérieuses sur l'intégrité de l'homme et les possibilités coercitives et liberticides. Tous les organismes qui réfléchissent sur le sujet – la CNCDH⁹, la CNIL, le COMETS¹⁰) attirent l'attention des pouvoirs publics et de la société civile sur les dangers éventuels de cette technologie, la liberté des citoyens. Sans un réflexe citoyen, les Droits de l'homme risquent d'être réduits à néant.

Michel Alberganti : Merci Jean-Claude Vitran. Je passe la parole à Laurent Bonelli¹¹, qui est commentateur régulier en matière de sécurité, mais aussi d'antiterrorisme.

Laurent Bonelli : Je travaille depuis un certain nombre d'années sur la sécurité urbaine, et plus récemment, dans le cadre de plusieurs contrats collectifs pour la Commission européenne, sur des questions liées à l'antiterrorisme en Europe. Une part des résultats de ces recherches a été publiée dans l'ouvrage que j'ai dirigé, avec Didier Bigo et Thomas Deltombe, *Au nom du 11 septembre*, qui essaie précisément de faire le point sur les récentes évolutions législatives, policières, judiciaires, militaires, etc., dans la plupart des démocraties occidentales.

Pour revenir à l'intitulé de la table ronde, je crois que l'on ne peut comprendre les enjeux présents des

politiques d'identification et de surveillance que par un retour sur le passé. Les exposés¹² très éclairants sur l'histoire sociopolitique de l'identification et de la surveillance montraient notamment qu'il existe très tôt une volonté de savoir des gouvernants. Celle-ci se décline de deux manières. Une attention toute particulière est d'abord portée à tout ce qui pourrait troubler l'ordre politique et social. Cela a donné lieu à la création de services dévolus à des missions de surveillance, des « mouches » jusqu'aux renseignements généraux, qui s'intéressaient à l'activité sociale, économique, politique, religieuse du pays¹³. La deuxième version reste beaucoup plus discrète : l'espionnage. Il n'existe pas de démocratie occidentale qui n'ait pas de service d'espionnage, c'est-à-dire de collecte agressive de l'information. Il s'agit d'une dimension qui, dans une certaine mesure, est constitutive de l'État, puisque les différences qui existent entre les régimes démocratiques et les régimes autoritaires ne sont pas déterminantes, à ce niveau.

En ce qui concerne la surveillance traditionnelle, vous vous doutez bien que les services de renseignements et les services policiers ou militaires qui en ont la charge entretiennent un rapport particulier à la question de la violence politique. C'est elle qui vient en effet, le plus fortement et le plus visiblement, troubler l'ordre social et politique du pays. Je parle de violence politique, non pas de terrorisme. Certains sont terroristes pour un pays, réfugiés politiques dans le pays voisin et aucun groupe clandestin ou armé ne s'est jamais revendiqué comme groupe terroriste. Ils se considèrent, selon les cas, comme l'avant-garde du prolétariat, des soldats de l'Islam, des combattants nationalistes ou de la

liberté, etc. Or, la lutte antiterrorisme va précisément recouvrir les deux logiques de surveillance politique et d'espionnage dont je parlais. C'est au nom de la première que seront menées des réformes structurelles ou législatives, qui en réalité favorisent et étendent la surveillance politique et l'espionnage. Il ne faut pas croire que l'antiterrorisme soit la seule source de légitimité des services de renseignement.

Mais revenons aux enjeux contemporains de l'antiterrorisme. On peut sérier un certain nombre de dynamiques. Les attentats du 11 septembre 2001 ont souvent été présentés comme l'année zéro, le point de remise en question, des politiques antiterroristes. Tout aurait changé avec la chute des tours jumelles. Or, il ressort de l'enquête collective que dans l'immense majorité des pays occidentaux, la continuité l'emporte. Ce qui ne signifie pas qu'il n'y ait pas de nouveautés. Parmi celles-ci, la stratégie adoptée par l'administration de Georges W. Bush : une réponse militaire (et non judiciaire) au terrorisme. C'est bien sûr l'attaque de l'Afghanistan et la guerre en Irak, mais aussi la réactivation d'un certain nombre de doctrines d'engagement, comme la guerre « contre-subversive », c'est-à-dire de savoir-faire développés dans les guerres coloniales (Malaisie pour les Britanniques, Indochine et Algérie pour les Français). Parallèlement, nous avons assisté à une extension de la sphère de surveillance. Le sociologue Peter Gill¹⁴ a montré parfaitement qu'il existe une extension internationale à la fois technologique et législative de la surveillance. En France par exemple, la [loi de 2006](#) sur le terrorisme autorise un développement accru de la vidéosurveillance. Un troisième mouvement renvoie à

ce que nous avons qualifié de « pratiques illibérales » des régimes libéraux. Parmi celles-ci, figurent les enlèvements de suspects par les services de renseignements américains, parfois avec la complicité ou la connaissance de services occidentaux, ainsi que leur transfert vers un certain nombre d'États non démocratiques ou vers des « trous noirs » carcéraux. Parmi eux, on peut mentionner le camp de Guantánamo qui est précisément la figure type d'un lieu de non-droit judiciaire dans lequel on peut retenir sans charges et sans limites de durée les détenus. Si Guantánamo est particulièrement caricatural, il faut penser que les Anglais, dans le *Anti-terrorism, Crime and Security Act*¹⁵ de 2001, ont mis en place une procédure similaire qui leur a permis d'incarcérer dans la prison de haute sécurité de Belmarsh, des étrangers qui refusaient l'expulsion, sans jugement et sans limite de durée, jusqu'en 2004, où la Chambre des Lords a invalidé cette loi. Une autre pratique illibérale se développe à partir de 2001 : l'usage de la torture. Celle-ci n'est plus l'apanage des dictatures latino-américaines ou africaines : elle est utilisée par des démocraties occidentales. Certaines d'entre-elles l'avaient déjà pratiqué – la France en Algérie par exemple –, mais ce n'est désormais plus quelque chose de caché et d'inavouable. Elle est au contraire publiquement et officiellement justifiée. Des juristes du département de la justice américaine vont même déployer des trésors d'imagination procédurale pour distinguer le traitement des détenus de Guantánamo de la torture, telle qu'elle est définie dans les textes internationaux...

Mais, parallèlement, nous nous sommes intéressés, avec des spécialistes de chaque pays, à la situation

britannique, espagnole, italienne, allemande, française, etc. Et là, la continuité l'emporte sur le changement. Ainsi, en France, peu de choses se sont modifiées dans l'architecture de lutte contre le terrorisme jusqu'à la récente réforme du 1^{er} juillet 2008¹⁶, qui fusionne les renseignements généraux et la Direction de la surveillance du territoire (DST) dans la DCRI. L'Espagne qui a pourtant souffert, le 11 mars 2004, de l'attentat le plus meurtrier de son histoire, n'a pas connu de bouleversement du fonctionnement de ses services de renseignement. L'enquête a également mis à jour une tension récurrente entre une logique judiciaire et une logique de renseignement. Non pas qu'il n'existe pas de logique de renseignement dans le travail judiciaire mais, comme le dit M. Aghroum, on distingue deux types de renseignement. Le premier consiste en la collecte d'informations pour produire des preuves qui permettent d'amener quelqu'un devant un tribunal. Ce qui est traditionnellement le travail de la police judiciaire ou de la police criminelle, comme elle s'appelle dans d'autres pays. Et vous avez une seconde logique, plus proche de la surveillance politique, qui recherche l'accumulation d'informations sur un certain nombre d'individus et de groupes. Il est intéressant de regarder en série les mémoires des lieutenants de police ou des ministres de l'Intérieur successifs, qui racontent qu'à peine nommés, ils ont demandé leur fiche : tous convergent pour pointer les inexactitudes et les lacunes, comme Louis Andrieux, préfet de police de Paris (1879-1881). Mais ces informations souvent erronées empêchèrent-elles les ministres et les préfets d'avoir recours à ses fiches ? La réponse est non, car c'est le cumul des renseignements issus de sources

différentes (qui par la suite pourront être plus ou moins recoupées) qui forme la rationalité même de cette pratique de surveillance. Et l'une des grandes tensions existante en matière de lutte antiterroriste relève du fait qu'elle est au carrefour entre logique judiciaire et de renseignement. En matière criminelle, il est assez facile – dans les limites des difficultés de l'enquête, bien sûr – d'arrêter un individu qui a commis un méfait et de le punir. Dans l'antiterrorisme, la question n'est pas le plus souvent de trouver les coupables après la commission de leurs actes, mais bien de les appréhender avant. Or, comment arrête-t-on des gens pour un acte qu'ils n'ont pas encore commis ? Cette question traverse les différentes forces de sécurité occidentales, avec une acuité accrue après les attentats de 2001 aux États-Unis, de 2004 en Espagne, et de 2005 au Royaume-Uni, en raison de leur caractère particulièrement meurtrier. Les États occidentaux vont essayer, chacun à leur manière et en fonction de leur histoire, de résoudre cette tension. On observe ainsi un continuum, de l'Espagne, où les attentats du 11 mars 2004 ont fait l'objet d'un traitement très judiciaire, aux États-Unis, où la logique de renseignement l'a largement emporté. De ce point de vue, Guantánamo constitue une sorte de modèle type, puisqu'on peut y retenir un individu sans limite de durée, lui extraire de l'information même par la torture, le tout sans se soucier d'une quelconque dimension judiciaire. On oublie que si cette dernière est coercitive, elle demeure néanmoins protectrice. Or, des individus ou des groupes sont aujourd'hui pris dans les filets du contre-terrorisme global, et sont suspectés d'un certain nombre de choses sans très souvent avoir accès aux éléments qui leur sont reprochés,

pourtant nécessaires pour préparer leur défense. Les répercussions sont préoccupantes en matière de respect des Droits de l'homme et des libertés individuelles, mais aussi en termes de radicalisation. Ainsi, les exemples de l'Irlande du nord ou d'Israël ont montré clairement que la répression d'État précipite des individus dans la clandestinité et dans l'action violente.

Michel Alberganti : Christian Aghroum, existe-t-il une véritable politique de surveillance et sécurité en France ? Ressentez-vous une vision, un projet dans ce qu'il vous est demandé de faire ou bien n'est-ce pas vous qui, dans un certain nombre de cas, êtes force de proposition pour essayer de faire au mieux votre travail ?

Christian Aghroum : Je pense que les deux mouvements sont présents. Nous avons la chance d'avoir en France, et j'en suis intimement convaincue, un socle véritable de libertés publiques et individuelles. De notre côté, nous sommes soumis au contrôle du Parlement, du juge, du juge constitutionnel, qui limiteraient les éventuelles tentations liberticides. Nous n'avons pas besoin d'aller aussi loin. Nous détenons suffisamment d'informations à l'extérieur des fichiers de police. L'existence des fichiers de police était tout à l'heure évoquée, et il a été demandé les raisons de leur démultiplication. Il est heureux de constater une telle démultiplication des fichiers de police ; cela prouve qu'il n'y a pas d'interconnexions entre eux.

Michel Alberganti : Ils sont si nombreux maintenant que l'on commence à les fusionner.

Christian Aghroum : Ce n'est pas exact.

Michel Alberganti : Le fichier *ARIANE*¹⁷ est bien en phase de fusion...

Christian Aghroum : En effet, il s'agit du même fichier détenu par la police et la gendarmerie. Dans les faits, la fusion de JUDEX et du STIC est due au rapprochement des deux forces. En 2009, la gendarmerie intègre le ministère de l'Intérieur, et il est du devoir d'une administration moderne d'État d'éviter les redondances dans la mise en place de ses dispositifs. En outre, une police ne peut pas travailler sans fichiers. Il faut en être intimement convaincu. Une enquête de police se constitue à la fois à travers une enquête archéologique sur le terrain, et une enquête d'historien pour pouvoir remonter dans le passé. Concernant la multiplication des fichiers, elle s'explique par l'impossibilité d'interconnexions entre eux. L'idéal serait d'avoir un seul et même fichier dans lequel nous piocherions tous les renseignements nécessaires. Il est possible de le faire à travers un moteur de recherche, mais cela ne peut être réalisé avec les fichiers de police. Si j'ai besoin d'un renseignement, je dois interroger quinze fichiers différents. L'information ne se trouve pas centralisée. Ensuite, nous assistons à une démultiplication des fichiers : chaque fois qu'est pris en compte un nouveau paramètre, un nouveau fichier est créé. Pour exemple, la CNIL a évoqué l'existence d'un nouveau fichier de police ayant trait au signalement des contenus illicites sur Internet. Or, à partir du moment où l'on détient des éléments d'identification, nous sommes obligés de le déclarer et ainsi de créer un nouveau fichier.

Michel Alberganti : Pourquoi avoir étendu le FNAEG ?

Christian Aghroum : La raison est simple : pour pouvoir remonter à l'identification de l'auteur d'un délit, les éléments biométriques laissés sur les lieux peuvent être de précieux indicateurs. À partir du moment où sur une montre présente près d'un cadavre se trouvent contenues des informations biométriques, pourquoi devrions-nous nous priver des informations qui permettraient peut-être d'identifier l'auteur des faits ?

Michel Alberganti : Faites-vous alors des analyses biométriques des autres empreintes laissées sur les lieux ?

Christian Aghroum : Oui, s'il a laissé des traces sur le mur, etc. Il faut bien comprendre que le fait que vous ayez laissé une trace biologique quelque part ne veut pas dire pour autant que vous êtes l'auteur des faits. Il revient à l'enquête d'établir si vous l'êtes, oui ou non. Par contre, les traces biologiques laissées sur les lieux sont des éléments qui permettent, recoupement par recoupement, d'aboutir à une identification du criminel. Pourquoi se priverait-on de tels moyens ? Nous recherchons les auteurs d'infractions. Il faut utiliser les moyens modernes dont dispose la science pour pouvoir évoluer.

Jean-Claude Vitran : Je voudrais citer le cas d'un village alpin où une jeune femme a été violée. L'ADN des 150 personnes masculines présentes dans le village a été prélevé. Le coupable a été retrouvé. Pourquoi l'ADN des 149 autres personnes a-t-il été conservé ?

Christian Aghroum : Il n'est pas conservé, il est confronté. Dans ce cas, nous procédons par élimination.

Nous prélevons de l'ADN, nous le comparons et l'écartons. Il n'intègre pas le FNAEG.

Jean-Claude Vitran : Vous n'avez pas un million de personnes qui se trouvent concernées...

Christian Aghroum : Mais si, bien sûr. Vous avez un certain nombre de personnes qui ont été interpellées par les services de gendarmerie et qui ont commis une infraction, tout simplement.

Jean-Claude Vitran : Ce fichier ne contient-il pas uniquement les personnes ayant commis une infraction ?

Christian Aghroum : Le fichier conserve les suspects qui ont été interpellés.

Jean-Claude Vitran : Pourquoi les suspects restent-ils présents dans le fichier ?

Christian Aghroum : La loi nous autorise à les conserver dans le fichier.

Michel Alberganti : Pourquoi avez-vous conservé les 149 analyses ADN de personnes résidant dans le village dont a parlé M. Vitran ?

Christian Aghroum : Ce ne sont pas des personnes qui ont fait l'objet d'infraction. Ils n'ont pas été en garde à vue, etc. Il ne s'agit pas du même cas. Ce serait comme si l'on prenait votre verre, qu'on y prélevait vos empreintes et que l'on prenait autour de cette table les empreintes digitales de chacun. Ensuite, les fiches ADN collectées se verraient détruites.

Laurent Bonelli : Je crois que notre débat tourne en réalité autour de la constitution de fichiers policiers

portant non pas sur la base de la culpabilité mais de la suspicion. Le STIC, qui est un fichier très large, comportant un certain nombre d'erreurs, est composé d'individus qui ont été mis en cause...

Michel Alberganti : La grande majorité des gens qui composent le STIC n'ont pas été condamnés.

Laurent Bonelli : Tout à fait. Mais le point central de notre sujet se rapporte à la loi. Effectivement, M. Aghroum, vous êtes fonctionnaire de police, vous bénéficiez de dispositions légales et législatives pour utiliser un fichier. Il n'y a aucune raison de vous en priver... Par contre, l'absence quasiment totale de débat sur ces questions, avant leur vote constitue un véritable problème. Nous avons évoqué tout à l'heure le fichier EDVIGE. Un petit débat public a débuté sur ce dernier. Les hommes politiques ont ici une véritable responsabilité. Ils étaient invités à cette table ronde, mais ils ne sont pas venus, pour un ensemble de raisons sûrement tout à fait légitimes j'imagine, mais c'est regrettable. Nous devons être capables de poser politiquement la question : dans quelle société voulons-nous vivre ? On peut reconnaître la légitimité du fichage des individus. Mais, à quelles conditions, de quelle manière ? Or, les débats en matière de loi pénale, que ce soit pour la petite délinquance, le terrorisme, la délinquance sexuelle, sont généralement amorcés dans l'urgence, dans l'émotion provoquée soit par un crime particulièrement odieux, soit par une campagne d'attentats. Aucun débat contradictoire n'est organisé, aucune véritable audition des professionnels concernés n'a lieu. Par exemple, l'immense majorité des magistrats est parfaitement opposée à

l'empilement, à la multiplication des mesures judiciaires observables dans la lutte contre la petite délinquance. Ce serait sans doute une revendication forte des citoyens que ces débats soient de nature politique.

Michel Alberganti : Entamons ce débat, si rare et si absent de l'espace public. Comme le dit Christian Aghroum : « Il revient à la Loi de fixer le cadre de l'action de la police. » Or, la loi devrait être l'émanation du débat public dans une démocratie auquel participeraient les politiques. Malheureusement, ils ne sont pas là aujourd'hui malgré les invitations. C'est au public maintenant de poser les questions auxquelles nos invités vont essayer de répondre.

Public : Jusqu'à présent, la biométrie comme technique privilégiait la surveillance, mais il me semble que le débat n'est plus là. Le débat concerne l'introduction de toutes les techniques au sein de plates-formes, de systèmes, générateurs de systèmes, de normes, y compris de normes juridiques et qui s'installent au niveau européen. Il y a une compétition en particulier entre cette plate-forme, qui intègre la totalité des fonctionnements d'un cycle d'intelligence, et des techniques d'intelligence. C'est le cas en Angleterre et en Allemagne. L'intérêt n'est pas de se focaliser sur une technique ou une technologie particulière de la surveillance, mais il est bien de voir comment s'intègre la totalité des technologies dites d'intelligence au sein de systèmes normés. Ceci permet de se rendre compte de la pluralité des acteurs qui tournent autour de ces systèmes. Nous avons bien sûr les agences classiques, le milieu industriel, dont on a relativement peu parlé ici, mais aussi la société. Nous participons tous, d'une certaine

manière, à l'œuvre de surveillance au travers de la technologie que nous emportons. Un deuxième point concerne la question de la distinction entre l'information judiciaire et le renseignement. Sommes-nous dans la suspicion, ou plutôt dans une politique délibérée de la prévention, c'est-à-dire une politique destinée à préempter les actes ou les comportements délictuels – ce qui va bien au-delà de la suspicion ?

Michel Alberganti : Laurent Bonelli a un peu abordé ce sujet, en disant : « Il faut arrêter les terroristes avant qu'ils aient commis quelque chose et non pas le plus rapidement possible après » ; ce qui fait écho au fameux film *Minority Report*¹⁸ qui le met en perspective d'une certaine façon. Christian Aghroum, ressentez-vous cette évolution vers une forme de prévention du crime ?

Christian Aghroum : J'espère bien que nous n'arriverons jamais à la situation décrite dans *Minority Report*. La répression et la prévention font l'objet de vieux débats. Je rejoins ce que disait Laurent Bonelli lorsqu'il faisait la distinction entre la logique de renseignements, la logique judiciaire et la logique guerrière. Le vrai risque est là. Dès lors que nous travaillons sur les agissements d'une organisation terroriste, nous avons toujours la crainte de savoir à quel moment nous allons pouvoir interpellier quand de véritables enjeux sont présents. Nous n'avons donc pas le droit à l'erreur. Nous devons interpellier les individus au moment précis où nous allons pouvoir disposer des éléments constitutifs de l'infraction. Nous restons ainsi dans la perspective d'une logique judiciaire. Nous cherchons l'accumulation des preuves grâce à des outils de surveillance

(filatures, écoutes, etc.). Le travail de renseignement est identique. Il se trouve réalisé pour le bien de la société dans laquelle on vit et il faut en être convaincu. Par contre, le risque est de passer de ce type de phase de renseignement à une phase dite de « commission de l'infraction », digne des situations décrites dans *Minority Report*. Ainsi, à partir du fait qu'un individu se trouve appartenir à telle communauté, sera-t-il suspecté de pouvoir un jour participer à une entreprise criminelle ?

Michel Alberganti : Les interpellations ayant eu cours au sein du groupe de Tarnac (groupe de personnes suspectées aujourd'hui d'être les auteurs des attentats, ou plutôt des tentatives d'attentat contre des lignes de TGV) ne relèvent-elles pas un peu de ce dernier type de phase ?

Christian Aghroum : Il s'agit d'une affaire judiciaire qui fait l'objet d'une instruction. Ce n'est pas à moi de parler d'une affaire qui est sous le couvert d'une instruction.

Public : Je voulais revenir sur cette notion de socle démocratique, stable, solide qui serait présente en France et dont a parlé M. Aghroum. Cette notion de démocratie telle que nous la connaissons aujourd'hui dans son acception moderne, à savoir une démocratie où se trouve respecté le principe de l'État de droit et celui du droit des minorités. Cette notion n'est vieille que d'un demi-siècle, en France. Pour un historien, ce laps de temps est infime. Qu'est-ce qui permet de considérer ce socle comme immuable, tellement solide qu'il nous protégerait, nous mettrait à l'abri de nos dérives éventuelles ? La démocratie est-elle un état de choses stable, qui une fois établie ne craint

plus rien ? Est-elle plutôt un processus dynamique, vivant, alimenté ou mis en jeu, jour après jour, par des êtres en chair et en os et qui mérite notre vigilance de tous les instants parce qu'il est toujours potentiellement en péril ?

Jean-Claude Vitran : Tel est l'un de nos soucis majeurs. Rien n'existe réellement ; tout peut changer. Pour ses raisons, la Ligue des droits de l'homme se bat contre des problèmes que nous rencontrons sur le contrôle social et la surveillance du citoyen. Aujourd'hui, il semble que nous sommes dans un univers démocratique ; mais dans quel type de régime vivrons-nous demain ? C'est pourquoi nous voulons que des barrières très précises soient érigées, que des débats soient tenus et que la CNIL ait des moyens complémentaires qu'elle n'a pas aujourd'hui afin de lutter contre les éventuelles dérives. Rien n'est jamais acquis.

Laurent Bonelli : Pour répondre sur la double question du judiciaire et du renseignement, la logique adoptée n'est pas forcément celle de la suspicion *a priori*. Pour un certain nombre de services, il s'agit d'une accumulation compulsive d'informations (récupérer le plus de renseignements possible sur le plus de gens possible dans des secteurs déterminés). La question du traitement de cette information se pose alors. Il ne faut pas confondre la collecte de ces informations, qui est colossale dès lors que l'on mobilise des moyens technologiques (comme le système Echelon, qui intercepte la plupart des communications téléphoniques, e-mail, etc.), et la manière dont elles peuvent être exploitées. Ce n'est pas parce que l'on peut techniquement repérer tous les gens qui sont dans

cette salle grâce à leur téléphone portable qu'un service de renseignement saura qu'ils sont là. Le travail serait colossal ! Par contre, si l'on cherche Monsieur x, sa traçabilité peut être établie relativement facilement. D'autre part, les services de renseignements politiques, très souvent, ne savent pas la demande qui va leur être adressée. Je vais vous donner quelques exemples que l'on trouve de manière récurrente dans les entretiens. Ce peut être le cas caricatural du préfet qui appelle le directeur départemental des renseignements généraux pour connaître le « pedigree » du nouveau petit ami de sa fille. Plus banalement, le même préfet recevant des interlocuteurs agricoles ou syndicaux voudra savoir qui ils sont. Pour un service de renseignements interne, cela implique la capacité d'avoir des éléments d'information sur ces personnes ou d'être en mesure de les obtenir très rapidement. Aux côtés de cette collecte d'informations générales réalisée, vous avez bien entendu une focalisation sur un certain nombre de groupes et d'individus. Je parlais tout à l'heure de l'attention particulière portée à l'action violente. Que faire pour les contenir ? Et nous retombons sur la tension renseignement / judiciaire. En France, il semblerait que nous ayons dans une certaine mesure résolu cette tension par la création d'une figure judiciaire, qui consacre les logiques de renseignement. Il s'agit de l'association de malfaiteurs en relation avec une entreprise terroriste (AMT), figure souple dans notre code pénal, qui permet d'incriminer, au moins en enquête préliminaire, des individus, de manière très large, du moment qu'ils sont liés à un dossier. Un certain nombre de professionnels appellent cela la « stratégie du coup de filet » ou du « coup de pied dans la fourmilière ». Il s'agit

d'arrêter un grand nombre de gens grâce à une commission rogatoire pour AMT contre x. La plupart des personnes incriminées ne seront pas condamnées. Nombre d'entre elles n'arriveront même pas au procès. Il existe une large disproportion entre le nombre de personnes mises en examen sur ce chef d'accusation et le nombre de personnes condamnées ensuite au cours d'un procès. En France, cette figure judiciaire a été élaborée dans le cadre de la justice antiterroriste française par des magistrats spécialisés, à partir de 1986. À cette époque, des débats ont eu lieu, de plus violents encore en 1992, mais cette figure-là nous permet de tenir cette contradiction.

Christian Aghroum : Sur la question de l'association de malfaiteurs en relation avec une entreprise terroriste, je veux préciser que l'on est sous le contrôle du juge. Nous ne sommes pas dans un dispositif à l'anglo-saxonne. On est donc sous le contrôle du juge au quotidien. Il s'agit là d'une garantie largement supérieure à celle rencontrée dans les États anglo-saxons.

Michel Alberganti : Je voudrais ajouter un mot sur l'état de notre démocratie. Le simple fait d'organiser cette journée (les questionnements, les interventions) ne se justifie que parce que nous pensons que la démocratie n'est pas éternelle et n'est pas installée pour toujours de façon inamovible au sein de notre paysage politique.

Public : Vous parliez de garanties. Je fais partie de l'association Souriez, vous êtes filmés, qui se bat contre l'implantation de la vidéosurveillance. L'installation des caméras de vidéosurveillance se fait en général pour

tel ou tel motif (faits divers). Même si le problème est résolu, les caméras restent en place et continuent même à se développer de manière exponentielle. Ma question est la suivante : à quel moment est-il possible de revenir en arrière et de retirer ces dispositifs de surveillance et de fichage mis en place ? Une deuxième question concerne le FNAEG et le fichage des criminels sexuels. Quelles garanties le citoyen peut-il avoir sur la limitation de son usage à son seul terrain d'application prévue par la loi ? Une dernière question concerne l'antiterrorisme. À partir de quel moment la lutte antiterroriste glisse-t-elle vers le délit d'opinion ?

Michel Alberganti : Concernant la première question, les systèmes de vidéosurveillance pourraient, dans certains cas, ne viser qu'un objectif très temporel. Par exemple, nous constatons qu'actuellement ces systèmes restent de façon définitive une fois l'objectif temporel acquis ou atteint.

Christian Aghroum : À partir du moment où la loi et le règlement instaurent un dispositif, ces mêmes loi et règlement peuvent faire en sorte que le dispositif soit retiré du lieu où il a été installé. À titre purement personnel, je pense que l'on vit en France dans un système qui avance par réactions : le « syndrome du passage clouté ». Vous signalez depuis des années l'existence d'un endroit dangereux ; il est attendu qu'un enfant se fasse écraser pour décider de l'installation d'un passage clouté. Ensuite, on recherchera les responsabilités du maire, du préfet... Nous avançons donc par réaction et dans ces états de crise ou de rupture que nous pouvons connaître depuis le 11 septembre 2001 par exemple, nous avons tendance à accumuler les moyens.

Pour autant, nous ne devons pas aller trop loin dans l'utilisation des moyens de surveillance. Nous devons également être très attentifs au respect du bien-fondé de leur installation. Néanmoins, doit être également pris en compte l'aspect pragmatique lié à l'emploi de ces technologies et l'augmentation de notre capacité à accepter tel ou tel nouveau dispositif. À Londres, les Anglais sont autant attachés à leur liberté qu'en France. Pour autant, la capitale anglaise est traversée de caméras de vidéosurveillance. Pour expliquer cet état de fait, nous pouvons dire que les Anglais ont une conception des rapports entre sphère publique et sphère privée totalement différente de la nôtre. Je ne sais si cela est bien ou mal ; quoi qu'il en soit, il semblerait que nous ne vivrions pas plus mal à Londres qu'à Paris. Il nous revient donc de définir dans notre société si cette étape constitue un progrès. Dans quel cas elle peut être acceptable ou non ; et si elle constitue un risque. Pour ma part, je n'ai pas réponses toutes faites sur ces différentes interrogations. Cependant, pour exercer mon métier de policier au quotidien, la vidéosurveillance est un outil qui m'est utile. Tant que ce dispositif se trouve encadré et qu'aucune déviance n'est à déplorer, il n'y aura aucun problème quant à son utilisation.

Michel Alberganti : De votre point de vue, a-t-on une idée du nombre de caméras nécessaires ? Nous avons l'impression qu'il s'agit d'une question de moyens ou de budgets. Avez-vous estimé les besoins nécessaires pour atteindre un certain degré de sécurité ?

Christian Aghroum : Je ne saurais répondre à cette question. Les termes du débat se posaient de manière

identique à la fin du Moyen Âge, lorsqu'il s'agissait de savoir si les rues devaient être éclairées. Cet éclairage a été mis en place pour éviter que les rues ne deviennent des coupe-gorge. C'est l'une des raisons principales de l'acquisition du bec de gaz. Les guetteurs et les veilleurs allumaient et éteignaient la lumière dans les rues. Pour revenir à l'usage des dispositifs de vidéosurveillance, si nous voulions être dans un monde absolument sous contrôle, nous devrions pratiquement en placer à tous les coins de rue. Pour autant, des limites doivent être posées à ce qu'il est respectable de concevoir. À Londres, des caméras de vidéosurveillance sont postées à chaque coin de rue. Pour les Français, ceci est surprenant. Pour ma part, la première fois que j'ai vu ce phénomène, j'ai été très surpris. Puis, au bout de deux jours, l'habitude s'installe et l'attention ne se trouve plus mobilisée par elles. Pour autant, cela ne signifie pas que l'utilisation des caméras soit sans risques.

Laurent Bonelli : Je pense, effectivement, que des caméras de vidéosurveillance peuvent avoir une grande utilité dans des enquêtes judiciaires précises. Londres est un exemple très intéressant. Les caméras de vidéosurveillance y sont installées depuis longtemps ; plus de quatre millions de caméras se trouvent globalement installées en Grande-Bretagne. Ce pays possède la plus grande densité de caméras de vidéosurveillance. Par ailleurs, c'est également sur son territoire que nous allons retrouver des études sérieuses menées sur le sujet. Le *Home Office* (ministère de l'Intérieur britannique) possède un département de recherche très développé, qui a beaucoup travaillé sur

la question de la vidéosurveillance. C'est donc en connaissance de cause que le responsable de la police métropolitaine de Londres, en charge du thème des caméras, jugeait le dispositif comme « ayant entraîné une véritable gabegie et constitué un désastre ». Pour autant, ce constat n'épuise pas la pertinence d'un débat sur l'utilisation de la surveillance. Cette dernière semble avoir une utilité pratique au sein des espaces clos (supermarchés, parkings souterrains, etc.), notamment parce qu'il existe une intervention immédiate dès lors que vous êtes vus en train de commettre une infraction. Son utilisation sur la voie publique pose *a contrario* un certain nombre de difficultés. Ainsi, et au gré des études menées en la matière, les caméras sont incapables d'identifier les suspects, soit parce qu'elles sont aveuglées, soit mal placées, etc. De plus, pour que leur efficacité soit optimale, il devrait y avoir une intervention policière dès lors qu'une infraction est constatée – ce qui reste très improbable. Il faudrait une patrouille disponible et à proximité, et la plupart du temps, c'est une personne qui regarde un mur d'écrans et doit observer les images captées par une soixantaine de caméras. Il est donc rare qu'elle constate un délit en direct... Des anthropologues ont étudié ces lieux de surveillance. Ils ont établi que les groupes d'individus les plus ciblés par les agents en charge de l'observation des images étaient les jeunes à capuches et le second les jeunes femmes plutôt jolies...

Michel Alberganti : Vous décrivez des systèmes largement développés en Grande-Bretagne. Néanmoins, ils sont moins sophistiqués techniquement ; ils sont analogiques et imposent effectivement que quel-

qu'un regarde les images prises par les écrans. J'imagine qu'aujourd'hui, nous sommes à même de développer des systèmes numériques dans lesquels certaines alertes peuvent être données de manière automatisée ?

Christian Aghroum : Il faut arrêter de regarder *Les Experts*, s'il vous plaît ! C'est de la science-fiction. Ces séries faussent la réalité. Nous n'avons pas encore de logiciel de reconnaissance faciale digne de ce nom. Peut-être y arrivera-t-on un jour...

Michel Alberganti : Il est évoqué le cas de systèmes détectant des comportements suspects.

Christian Aghroum : En effet. Je peux prendre l'exemple d'un sac qui va être posé pendant x secondes quelque part. La caméra est alors calibrée sur ce type d'événements. Puis, vous avez une équipe qui donne l'alerte. On identifie le sac. Vous avez une alerte qui vous appelle ; une équipe sera envoyée sur place pour vérifier. Voilà un des moyens de protection, mais cela ne va guère plus loin pour l'instant.

Laurent Bonelli : Si *a priori* une large variété d'études montre que cela ne marche pas, pourquoi ne revient-on pas en arrière ? Il existe au moins deux séries de réponses. La première relève du fantasme technologique, de l'idée que la technologie va résoudre les problèmes de l'humanité. Elle trouve toutefois une résonance particulière dans un contexte de réduction de la forme et du format de l'État. Le développement de la vidéosurveillance urbaine, comme on peut le voir dans certaines villes, doit être pensé corrélativement à la réduction des forces de police présentes sur le terrain. Il doit aussi être pensé en rela-

tion avec ce qu'est le métier ordinaire d'un homme politique, qui consiste notamment à manier des catégories symboliques et dans lequel, parfois, dire c'est faire. La mise en place de caméras de surveillance, permet ainsi à un certain nombre d'entre eux de dire : « Regardez ! J'ai pris le problème en main et je fais quelque chose pour y répondre », quelque soit ensuite l'utilité réelle de ces caméras sur la baisse de la délinquance de rue.

Jean-Claude Vitran : Nous sommes en train d'installer pour une somme faramineuse (quarante millions d'euros) 1 660 caméras à Paris. Un fonctionnaire de police du XIX^e arrondissement de Paris a déclaré que l'installation des caméras de surveillance dans cet arrondissement, sans ajout de forces de police complémentaires, serait vaine. Ainsi, des caméras se trouvent installées pour éviter d'accroître les budgets dévolus au déploiement des forces de police. Je tiens à rappeler également qu'après les attentats perpétrés à Londres, un Brésilien qui portait un pardessus en plein été a quand même été « assassiné » de neuf balles dans la tête par les fonctionnaires de police anglais, au simple motif que son comportement avait été jugé anormal. Enfin, vous parliez tout à l'heure de caméras comportementalistes, avec des logiciels comportementalistes : elles existent en Hollande, où l'on repère le comportement des gens. Si vous n'accompagnez pas une vieille dame avec sa canne blanche pour traverser une rue, la caméra vous parle et vous accuse d'être incivil.

Christian Aghroum : Ce n'est pas la caméra qui vous parle mais la personne qui est à l'écran de contrôle et qui parle à travers un micro. Cela fait aussi partie du fantasme, mais la caméra ne vous parle pas.

Jean-Claude Vitran : Bien sûr que si...

Michel Alberganti : Je crois que nous n'avons pas tout à fait répondu à la question sur le FNAEG dont je ne me rappelle plus très bien l'intitulé.

Public : Comment faire confiance aux politiques qui prennent une loi destinée à ficher une population alors que cette population grandit énormément ?

Christian Aghroum : Je ne crois pas être le mieux placé pour répondre à cette question puisque j'ai confiance dans le système dans lequel je travaille, sinon je ne ferais pas ce métier. Un politologue serait plus à même de fournir des éléments de réponse sur ce sujet. Je peux seulement affirmer que la confiance des citoyens passe à travers le vote.

Laurent Bonelli : Pour ma part, je crois que l'absence de débat prime. Il est absolument incompréhensible de voter des lois sur des fichiers génétiques, et ceci est valable pour l'ensemble des pays occidentaux, à partir d'un fait divers ou d'un cas particulièrement crapuleux. Prenons l'exemple des lois sur la délinquance sexuelle adoptées aux États-Unis : certaines portent même le nom des victimes qui ont déclenché la campagne, comme la loi Megan¹⁹. Des lois sont rédigées dans un contexte d'alarme sociale particulière, de mobilisation des émotions, sans se soucier de ce qu'elles peuvent devenir à l'horizon de cinq ou dix ans. Nous sommes peut-être ici plus proches de la vengeance que de la justice.

Le retour en arrière est ensuite difficile ; d'autant plus difficile que peu de résistances se construisent. Les

mobilisations qui ont eu lieu contre le fichier EDVIGE ou plus récemment sur l'affaire de Tarnac, et contre la loi sur le fichage des enfants de moins de trois ans, portent le débat démocratique au cœur des dispositifs de surveillance. Elles ont permis de porter un coup d'arrêt au développement de certains d'entre eux. Mais nous devons avoir en tête que ces mobilisations n'ont prospéré qu'au moment où le contrôle s'est étendu au-delà des groupes traditionnellement ciblés et présentés de manière crédible comme menaçants. L'antiterrorisme français ne date ni de la mise en place du fichier EDVIGE ni de l'affaire de Tarnac. Il est très largement en place dès le milieu des années 1980 et du début des années 1990. Or, aussi longtemps qu'il n'affectait pas certains groupes spécifiques (basques, corses, islamistes), ses logiques n'étaient pas contestées. Pour salutaires qu'elles soient, il est dommage que ces mobilisations n'aient du succès que lorsque chacun se dit : « Cela pourrait être moi, ou mon enfant. » Être une démocratie signifie que même les individus aux comportements les plus répréhensibles bénéficient des mêmes droits que les autres...

Public : Jean-Claude Vitran, vous avez abordé tout à l'heure la relation entre le développement des technologies de surveillance et la montée du désir totalitaire. Pourriez-vous développer ce point ?

Jean-Claude Vitran : Ce sont des questions que nous nous posons et sur lesquelles nous sommes en train de réfléchir. Il se trouve, en effet, une concomitance entre le développement de la surveillance du citoyen et le développement technologique. En outre, nous sommes passés à un stade supérieur de développement à partir de

la miniaturisation de l'informatique. L'invention du microprocesseur, le 15 novembre 1971, a permis le développement exponentiel des capacités de stockage de données et un accroissement dans la rapidité de transmission de l'information. Tout à l'heure, vous évoquiez le cas de Londres : les technologies analogiques et numériques sont complètement différentes. Depuis le passage au numérique, le contrôle du citoyen est facilité. N'y a-t-il pas d'ailleurs une concomitance entre un désir de surveiller tout le monde et un désir totalitaire ou du moins autoritaire ? Nous pouvons alors nous poser des questions sur l'évolution de la république sous laquelle nous vivons. Pour autant, il ne s'agit pas d'un débat franco-français ; cette évolution est à constater au sein du monde occidental, dans un contexte de mondialisation.

Christian Aghroum : J'aurais une question à poser à la salle. J'ai abordé un sujet tout à l'heure, sans susciter véritablement de réactions : l'enjeu de la surveillance sur Internet. Le fait de livrer volontairement, dans des fichiers qu'on ne maîtrise pas, des données personnelles, ne fait-il pas craindre un risque pour la préservation de l'identité des personnes et, plus généralement, pour la démocratie ?

Public : La différence réside dans le fait suivant : j'ai seul le choix de donner ou pas, des informations sur Internet ou ailleurs. *A contrario*, la constitution de données de telle ou telle personne au sein de fichiers policiers préventifs contrecarre la liberté de choix des individus en la matière. Le choix de l'individu est quand même une dimension primordiale. Il est aussi possible de mentir sur Internet, de donner un faux nom

pour acheter un produit ou communiquer avec quelqu'un sans vouloir commettre un acte grave.

Christian Aghroum : Je ne pense pas que ces comportements sociaux (créer des avatars, etc.) soient partagés par tous. Nous nous rendons compte dans les enquêtes de la naïveté ou de la méconnaissance de l'usage des éléments de l'identité fournis par certaines personnes sur Internet. Cette absence de méfiance me surprend. Je comprends que l'on puisse être méfiant à l'égard des fichiers de police et autres, mais la méfiance est encore faible à l'égard des données personnelles circulant sur Internet. Il est à craindre que cette absence de méfiance ne conduise à la montée de comportements délinquants sur la Toile dans les années à venir.

Jean-Claude Vitran : C'est une de nos interrogations au sein de la commission en charge de l'observation des techniques de l'information et de la communication. Nous avons décidé d'y répondre de la façon suivante : nous nous sommes dit des militants des Droits de l'homme et que chaque personne disposait du droit de communiquer à travers la Toile. Nous n'avons aucune raison de nous prononcer sur les agissements de ces personnes. Seulement, il serait peut-être utile d'éclairer les individus sur les éventuels risques qu'ils encourent dans la divulgation sur Internet de certaines informations les concernant.

Public : Comment pouvons-nous accorder une quelconque confiance à des politiques qui, pour certains, se conduisent de manière anticonstitutionnelle ? J'envie le représentant de la LDH [Ligue des droits de l'homme],

qui a l'impression qu'il est encore en démocratie et que le pire est à venir. J'ai l'impression que nous avons déjà un pied dedans...

Jean-Claude Vitran : Je n'ai pas affirmé que nous n'étions plus en démocratie. Nous sommes toujours en démocratie sinon nous ne serions pas là. Néanmoins, il me semble que la démocratie est malade.

Public : Il est vrai que lorsque vous mettez en parallèle toutes les évolutions allemandes, espagnoles, françaises, il est à constater un « grignotage » des libertés d'opinion publique. Ce phénomène doit être pris en compte politiquement. Maintenant, il nous faut éviter de tomber dans l'interprétation inverse et considérer que nous sommes dans un État de surveillance généralisée, ne pas confondre ce qu'il devient possible techniquement de réaliser et ce qu'il est probable de voir advenir socialement. Il ne faut pas inverser le raisonnement. En effet, aujourd'hui, tout est quasiment possible au niveau technologique ; cependant, une dimension humaine appose ses limites. Pour obtenir un débat – urgent politiquement et serein – sur ces questions, je crois qu'il ne faut pas oublier ces deux dimensions.

Notes

* Ancien journaliste au *Monde* et producteur à *France Culture*. ↑

1. Animateur du groupe de travail « Libertés et technologie de l'information » à la Ligue des droits de l'homme, association fondée en 1898 au moment de l'affaire Dreyfus [voir [site ldh](#)]. ↑

2. Fichier national automatisé des empreintes génétiques. C'est un fichier commun à la police et à la gendarmerie françaises, créé en 1998. Il gère les traces d'ADN prélevées au cours d'investigations. ↑

3. Criminologue français, spécialiste des questions de sécurité qui a établi un rapport en 2006 sur les fichiers de police et de gendarmerie en France. ↑

4. Fichier d'Exploitation documentaire et valorisation de l'information générale. ↑

5. Système de traitement des infractions contestées (fichier de police informatisé du ministère de l'Intérieur). ↑

6. Art. 8 DDHC : La loi ne doit établir que des peines strictement et évidemment nécessaires, et nul ne peut être puni qu'en vertu d'une loi établie et promulguée antérieurement au délit, et légalement appliquée. ↑

7. Art. 10 DDHC : Nul ne doit être inquiété pour ses opinions, mêmes religieuses, pourvu que leur manifestation ne trouble pas l'ordre public établi par la loi. ↑

8. Art. 11 DDHC : La libre communication des pensées et des opinions est un des droits les plus précieux de l'homme ; tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi. ↑

9. Commission nationale consultative des droits de l'homme : institution nationale de promotion et de protection des droits de l'homme. [[plus d'informations](#)] ↑

10. Le Comité d'éthique au CNRS est une instance consultative indépendante, placée auprès du conseil d'administration du CNRS. Ses missions consistent au développement de la réflexion sur les aspects éthiques de la recherche, de formuler des recommandations et de sensibiliser les personnels à l'importance de l'éthique. [[www.cnrs.fr](#)] ↑

11. Maître de conférences à l'université Paris-X-Nanterre, membre du comité de rédaction de la revue *Culture & Conflits* et *International Political Sociology*. Il est notamment l'auteur de *La France a peur* (Éditions La Découverte, Paris, 2008). Il a également dirigé, avec Didier Bigo et Thomas Deltombe, *Au nom du 11 septembre... Les démocraties à l'épreuve de l'antiterrorisme*, aux Éditions La Découverte, en 2008. ↑

12. Voir les parties de Vincent DENIS (« L'histoire de l'identité en France »), de Pierre PIAZZA (« Du papier à la biométrie : identifier les individus »), et Sébastien LAURENT (« L'histoire de la surveillance »). ↑

13. Ces activités sont désormais réparties entre la Sous direction de l'information générale (SDIG) des directions départementales de la sécurité publique et la Direction centrale du renseignement intérieur (DCRI). ↑

14. Contributeur dans le collectif *Au nom du 11 septembre*, « Les nouveaux développements des réseaux de sécurité et de renseignements ». ↑

15. Loi entrée en vigueur le 14 décembre 2001. Le 16 décembre 2004, la *Law Lords* a statué sur l'incompatibilité de la loi par rapport à la Convention européenne des droits de l'homme. Elle a depuis été remplacée par le [Prevention of Terrorism Act](#) en 2005. ↑

16. Voir détails sur la [réforme de 2008](#). ↑

17. Système d'Application de rapprochement, d'identification et d'analyse pour les enquêteurs. Fichier né en 2006 d'une fusion du JUDEX (système Judiciaire de documentation et d'exploitation) et du STIC (Système de traitement des infractions constatées) ; deux fichiers conçus sans autorisation de la CNIL. ↑

18. Voir informations sur le film. (source allociné) ↑

19. Aux États-Unis, la *Megan's Law* est connue, en 1994, sous le nom de *Sexual Offender* (Jacob Wetterling) *Act*. Elle exige notamment des personnes condamnées pour des crimes sexuels contre des enfants de notifier à la police locale tout changement d'adresse ou d'emploi après la sortie de détention (prison ou hôpital psychiatrique). ↑

Technologies d'identification, de surveillance et libertés individuelles

- 62 Technologies de sécurité et respect des droits
et libertés individuelle : quelles protections ?**
Sylvia Preuss-Laussinote
- 70 Victimes et complices : les individus face aux technologies d'identification
et de surveillance**
Thierry Rousselin
- 76 Table ronde**
Animée par Michel Alberganti

Technologies de sécurité et respect des droits et libertés individuelles : quelle protection ?

Sylvia Preuss-Laussinotte *

Il m'est demandé d'intervenir sur la protection des droits et libertés. Je vais essayer de simplifier un ensemble complexe et très technique, pour voir ce qu'il implique pour nos libertés, et tenter de déterminer si et comment nous pouvons, vous et moi, nous protéger. La situation générale vous a déjà été exposée. Nous sommes dans ce que j'appelle le « grand cirque sécuritaire » : obsession sécuritaire des États, largement soutenue par les industries ; multiplication des discours – y compris médiatiques – autour de la prévention d'un risque permanent, futur, incertain et multiforme ; marché commercial très rentable, visant à créer une véritable addiction sécuritaire chez les individus.

Une enquête de la CNIL a, par exemple, déterminé que la plupart des personnes sont prêtes, sans hésitation à géolocaliser et tracer leurs enfants par tout moyen technologique performant. Notons quand même que le bracelet électronique a déjà été testé sur les bébés. Pour l'instant, cela ne passe pas très bien ; attendons la suite. Face à cette situation où les individus sont parfois à l'origine de leur propre aliénation sécuritaire, quelle protection le droit peut-il apporter pour défendre les libertés ? Je voudrais d'abord apporter une précision juridique généralement méconnue. De nombreux textes – comme la [loi du 21 janvier 1995](#) sur la vidéosurveillance, celle sur la [sécurité intérieure de mars 2003](#) – affirment, comme le martèlent de nombreux discours politiques, que la sécurité est un droit fondamental. Ce faisant, une véritable confusion est introduite entre sécurité et droit à la sûreté. Or, le droit à la sûreté¹ symbolise la protection de l'individu contre l'arbitraire. Jadis, il fut créé pour lutter contre les arrestations et les détentions laissées au bon vouloir des rois – donc contre l'arbitraire de l'époque. Je reviendrai sur ce droit à la sûreté, qui me paraît essentiel aujourd'hui, et sur son développement, qui me semble très utile.

62

Technologies de sécurité et respect des droits et libertés individuelles : quelle protection ?

Dans tous les textes internationaux, qui énoncent et garantissent les Droits de l'homme, la sécurité est entendue comme une fonction de l'État l'autorisant à restreindre les droits et libertés, mais de manière limitée dans le temps et l'espace, pour des motifs précis et sous réserve du contrôle d'un juge. D'ailleurs, les nombreuses théories sur la sécurité n'ont jamais fait mystère de cette réduction des libertés inhérentes à l'application des politiques de sécurité. Si nous considérons la jurisprudence de la Cour européenne des droits de l'homme, elle reprend systématiquement des termes qu'elle a employés, dès 1978. Dans un arrêt *Klass*² contre Allemagne, les affaires concernent tout type de surveillance au nom de la sécurité : « Les États ne disposent pas d'une latitude illimitée pour assujettir à des mesures de surveillance les personnes soumises à leur juridiction. » La Cour souligne fermement qu'elle est consciente du danger inhérent à pareil texte de détruire la démocratie, au motif de la défendre. Elle affirme, en conséquence, que les États ne sauraient prendre, au nom de la lutte contre l'espionnage – ou contre le terrorisme, qui a été évoqué – n'importe quelle mesure jugée par eux appropriée. Elle exige clairement, dans ces cas, quel que soit le système de surveillance retenu, qu'il existe des garanties adéquates et suffisantes contre les abus. Elle détermine ces abus comme étant l'arbitraire élément central. Dès qu'existe un soupçon d'arbitraire, elle condamne l'État pour

violation de l'article 8 de la Convention européenne³, c'est-à-dire le droit à la vie privée des personnes, conçu de manière extrêmement large par la Cour. Au vu de cette approche, notamment de cette question de lutte contre l'arbitraire, je reviens sur le droit à la sûreté. Il représente la lutte contre l'arbitraire, et sur son application, qui me semble essentielle aujourd'hui face aux technologies de sécurité. Juridiquement, dans un État démocratique, la notion de sécurité ne se conçoit que par rapport à l'obligation de respecter les droits fondamentaux. Il s'agit de notre point de départ et il s'agira aussi de ma conclusion.

Je vais, d'abord, tenter une présentation rapide du paysage juridique autour de la protection des droits, sachant que, au milieu de ce « grand spectacle sécuritaire », il va d'abord s'agir de resituer la personne (vous, moi) et de comprendre comment elle va pouvoir défendre ses libertés. Si je prends mon cas personnel, je suis, comme chacun d'entre vous, perplexe. J'ai mon portable, qui permet de me géolocaliser sans difficulté et d'écouter mes conversations, même quand il est éteint. J'ai une carte bancaire. J'utilise Internet. Sur mon lieu de travail, à l'université, je suis vidéosurveillée. Peu de personnes le savent d'ailleurs, car le panneau qui l'indique ne se voit pas. Je pense que je suis vidéosurveillée à Beaubourg aussi. Depuis fin décembre, j'ai accepté de guerre lasse un passe Navigo individualisé, qui me trace durant 48 heures, n'ayant nulle part réussi à trouver le passe Navigo découverte. Ce dernier a fait l'objet de la colère récente, et très justifiée, du président de la CNIL. Je figure dans un nombre de fichiers publics et privés dont j'ignore le chiffre exact, mais il est certainement important. Enfin, j'ai un passeport électronique aux normes, qui m'a permis de passer, voici un mois, la frontière américaine. Grâce à l'accord de l'Union européenne avec les États-Unis, toutes mes « données passager » (les « données PNR »), y compris mes préférences alimentaires, ont été transmises par ma compagnie aérienne au fichier des agences de sécurité américaines (FBI, CIA, etc.), accompagnées du scanner de mon iris – pris à la frontière – et de mes empreintes digitales. J'ignore ce que ces données vont devenir et leur durée de conservation. Néanmoins, je sais que les fichiers américains, y compris ceux du terrorisme, contiennent des milliers de personnes fichées par erreur. La France n'est donc pas le seul pays qui enferme de malheureux innocents dans le dédale de ces fichiers de sécurité. Rappelez-vous : « 25 % d'erreur », a dit la CNIL, dans le [STIC](#) et JUDEX. Comme vous tous, je suis donc au centre des technologies de sécurité.

Face à cette situation sécuritaire, dominée aujourd'hui par l'obsession biométrique, comment protéger nos libertés (liberté d'aller et venir, droit à la vie privée et surtout – élément souvent oublié – liberté individuelle à protéger contre l'arbitraire) ? Pour simplifier, je dirais que si les grands principes sont énoncés dans les conventions des Droits de l'homme, encore faut-il pouvoir les appliquer. En France, si les textes qui encadrent les technologies de sécurité ne manquent pas, leur accès est souvent difficile (manque de clarté, morcellement), puisqu'ils s'appliquent par secteur. Or, l'une des caractéristiques des technologies de sécurité est leur convergence, notamment à travers la création de bases de données aujourd'hui essentiellement biomé-

triques. Nous avons quelques lois françaises : loi sur la vidéosurveillance⁶, sur l'informatique et les libertés, sur l'interception des communications. Nous avons le Code pénal, avec une série d'articles créant des infractions liées à ces secteurs. Par exemple, en matière de fichiers, nous pouvons théoriquement porter plainte, puisque pas moins de quinze infractions sont prévues. Mais les sanctions sont très excessives – spécificité incompréhensible : 5 ans de prison, 75 000 € d'amende pour vol. En réalité, ces procédures ne sont pas appliquées, d'après une enquête menée par mes étudiants.

Nous constatons donc une profusion de textes, une incertitude quant à la réalité de la protection mise en place. D'autant que les lois sont complétées par des décrets et arrêtés innombrables, qui peuvent prévoir au cas par cas, des procédures spécifiques. Par exemple, le décret du 25 mai 2004⁴ prévoit une procédure très complexe pour tenter d'obtenir la suppression d'un nom du FNAEG, même en cas de mise hors de cause dans le cadre d'une procédure pénale. Lorsqu'une personne est soupçonnée et mise en cause, la durée de conservation dans le FNAEG est de 25 ans. Le nombre de textes de protection n'est pas important, mais leur effectivité l'est en revanche. L'effectivité est la possibilité d'exercer les droits qui sont prévus et de voir leur respect garanti par un juge ou un organe indépendant. Précisément dans le domaine des technologies de sécurité, nous avons, d'une certaine manière, privilégié le contrôle par des AAT⁵, notamment la Commission nationale de contrôle des interceptions de sécurité [CNCIS⁶] et la CNIL. Aujourd'hui, il s'agit essentiellement de la CNIL. La CNCIS a progressivement perdu son importance. D'ailleurs, la CNIL indique que si un dispositif d'écoute ou d'enregistrement téléphonique, par exemple sur un lieu de travail, repose sur des moyens numériques, il ne peut être installé que s'il a préalablement fait l'objet d'une déclaration auprès d'elle. De même, malgré la loi de 1995 sur la vidéosurveillance, qui prévoit un système d'autorisation préfectorale, la CNIL estime être l'autorité compétente en matière de vidéosurveillance numérique. Cette position vient d'être confirmée dans un [rapport](#) récent du Sénat du 10 décembre 2008. Progressivement, la CNIL revendique un rôle central pour l'ensemble du secteur des technologies de sécurité. Pourquoi pas ? Cependant, si elle ne manque pas de représentants d'honorables institutions – le collège de la CNIL est composé de 17 membres éminents – elle manque, en revanche, cruellement de moyens financiers et de personnels techniques pour mener à bien son rôle. Elle l'indique elle-même. Si son rôle, en matière de fichiers publics, notamment de biométrie, a été totalement réduit depuis une modification de 2004 (elle n'a plus qu'un avis à donner qui peut ne pas être respecté), elle a par contre acquis un pouvoir de contrôle. Celui-ci l'autorise à effectuer des enquêtes et à sanctionner les contrevenants. Encore faut-il qu'elle dispose de véritables moyens personnels. De plus, la CNIL est aussi l'autorité chargée d'examiner les plaintes des personnes (vous et moi). Un droit d'accès à un fichier, une rectification ou une suppression de données ne sont pas autorisés. Or, il apparaît que les procédures devant la CNIL sont très longues et inadaptées au contexte actuel des technologies de sécurité. Je vais encore exposer mon exemple personnel. Ayant contacté un organisme sur Internet lui demandant la suppression d'une donnée personnelle (inexacte et inappropriée), je me suis

64

Technologies de sécurité
et respect des droits et
libertés individuelles:
quelle protection ?

vu refuser cette suppression. Cet organisme n'a pas hésité à indiquer, sans complexe, au pied de sa réponse, tous les textes dont je demandais l'application. Il s'agit de l'illustration d'un travers bien français : nous inscrivons et proclamons des beaux principes, mais nous oublions de les appliquer. J'ai voulu saisir la CNIL, à l'heure d'internet et de la revendication officielle de l'« e-administration » ; il est impossible d'engager une procédure de saisine par courrier électronique. Il faut envoyer un courrier postal, avec une copie de sa pièce d'identité, et attendre. Le même problème se pose pour une personne qui veut exercer son droit d'accès indirect à un fichier de sécurité. Après son courrier, seul un magistrat de la CNIL peut se déplacer pour vérifier l'inscription et procéder éventuellement aux rectifications nécessaires. L'attente est extrêmement longue, puisque aucun délai n'est prévu pour répondre. Je voudrais comparer ces procédures, que je pense inadaptées, avec la possibilité de l'administration de se connecter instantanément aux fichiers de police et de gendarmerie (STIC et JUDEX), réunis pour le meilleur et le pire sous le nom d'ARIANE. L'administration a un droit de connexion pour ses enquêtes administratives, notamment pour vérifier si une personne qui veut entrer dans l'administration n'est pas fichée – je prendrai pour exemple l'article 1. I - 1° e) du décret n° 2005-1124 du 6 septembre 2005 qui prévoit la vérification, sur tous ses fichiers de police, des demandes d'emploi de futurs agents de la CNIL. Pour conclure cette partie, il peut sembler cohérent qu'une seule autorité de régulation existe pour les technologies de sécurité. La CNIL souhaite être cette autorité. Mais ce n'est possible que si une réelle modification de ses moyens financiers et de ses procédures est rapidement mise en place. Concernant le contrôle d'une autorité de régulation, le juge est normalement désigné pour faire respecter les lois et les libertés. Mais quel juge ? Au vu de l'accélération permanente des technologies de sécurité, le temps de réflexion nécessaire à la bonne justice peut paraître inadapté. Cela explique, en partie, pourquoi la question du contrôle a été envisagée sous l'angle de la régulation. Si le juge intervient, généralement, il arrive en fin de processus – sauf saisine de référé dans des cas particuliers – au point que son rôle est souvent peu connu.

65

Technologies de sécurité
et respect des droits et
libertés individuelles:
quelle protection ?

De manière plus générale, puisqu'il s'agit de droits fondamentaux, il existe le Conseil constitutionnel. Le Conseil constitutionnel est le garant national des droits fondamentaux. Il intervient uniquement avant la promulgation des lois. Cela va changer, heureusement. Lorsqu'il a été saisi de lois portant sur la sécurité, il a toujours repris la même doctrine. Je cite sa décision sur la loi sur la sécurité intérieure du 13 mars 2003 :

« L'ensemble des garanties prévues par la loi qui lui est soumise sont 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. »

Quant à définir ce qu'est l'ordre public au sens du Conseil constitutionnel, je cite un passage du rapport annuel présenté en 2003 devant la Commission de Venise dans le cadre des Rencontres des Cours constitutionnelles européennes :

« Le Conseil constitutionnel n'a jamais défini ce qu'il définissait par "ordre public". Mais, à la lecture de ses décisions, il est facile de comprendre à quoi il fait référence. Il s'agit en fait d'une notion que tout le monde comprend sans qu'il soit besoin de lui donner une définition précise. »

Jusqu'ici, les décisions du Conseil constitutionnel ne sont pas d'une audace excessive en matière de protection des libertés face aux technologies de sécurité.

Je voudrais m'arrêter plus particulièrement sur la Cour européenne des Droits de l'homme. Je l'ai citée tout à l'heure. Il me semble qu'aujourd'hui, les signes les plus prometteurs pour la protection de nos libertés, dans le domaine qui nous intéresse, viennent d'elles. L'inconvénient est de taille : il faut avoir épuisé toutes les voies de recours interne. Le terme « épuisé » est adapté puisqu'il faut attendre des années le résultat de la procédure effectuée devant tous les juges nationaux, avant de saisir la Cour. Mais la Cour européenne rend des décisions qui ont valeur de référence pour tous les pays européens, même si les États mettent parfois du temps à modifier leurs textes et leurs pratiques malgré une condamnation. Lorsqu'elle est saisie d'une procédure liée à la sécurité – par exemple, dans le cadre de fichiers ou de la vidéosurveillance – la Cour se fonde toujours sur l'article 8 de la Convention européenne des Droits de l'homme : le droit à la vie privée, auquel elle donne un sens extrêmement étendu. Pour illustrer sa position, je cite deux décisions qui me semblent intéressantes. La première nous rappellera le fichier EDVIGE, désormais mort-né. Ne soyons pas trop tristes : d'autres naissent, pour lesquels les parents choisissent souvent de jolis prénoms féminins (CRISTINA⁷, ARIANE, etc.). La Cour, dans un arrêt Segerstedt-Wiberg contre Suède du 6 juin 2006, avait été saisie du refus de l'État suédois de supprimer d'un fichier de surveillance (type ex-RG) la mention d'activités politiques de personnes appartenant à des partis politiques d'extrême gauche. Le fichage et le refus de retirer ces données étaient justifiés par le fait que ces partis prôneraient la destruction de l'État démocratique. Or, depuis la création de ces partis, aucune circonstance n'a pu démontrer que les dispositions litigieuses de leur programme constitueraient une menace réelle, ou simplement potentielle, pour la sécurité nationale. Le constatant, la Cour a jugé que la conservation de telles données constituait une violation de l'article 8 de la Convention européenne des Droits de l'homme, et par voie de conséquence, une violation de la liberté d'expression (article 10) et de la liberté d'association (article 11). Voilà une jurisprudence à faire connaître en France.

Plus récemment, le 4 décembre 2008, la Cour a statué à l'unanimité et en chambre de référence, pour souligner l'importance qu'elle accorde à cette décision. Il s'agissait d'un refus du Royaume-Uni d'effacer des grands fichiers anglais de données biométriques (le fichier anglais de données génétiques est le plus performant) deux personnes qui avaient été relaxées ou mises hors de cause lors de procédures judiciaires. La Cour a indiqué clairement que la

protection offerte par l'article 8 « serait affaiblie de manière inacceptable si l'usage des techniques scientifiques modernes dans le système de la justice pénale était autorisé à n'importe quel prix ». En lien avec ces décisions, je voudrais évoquer un moyen de résistance, dont la tradition n'est pas française, mais américaine : la désobéissance civile. En France, elle est plutôt conçue comme un mouvement de résistance de type politique – ce qu'elle est d'ailleurs. Mais la « désobéissance civile⁸ », imaginée par Henry David Thoreau⁹ est un mode de résistance non violent, qui s'insère dans le système juridique. Il s'agit de refuser d'appliquer un texte considéré comme contraire à un droit fondamental en assumant les conséquences de ce refus, jusqu'à ce qu'un juge reconnaisse la validité juridique de cette position au regard des droits fondamentaux. Ils sont protégés, aux États-Unis, par la Constitution et la Cour suprême. Actuellement, de plus en plus de procès ont lieu autour de personnes condamnées pour divers motifs – généralement liés à des actions militantes – qui ont refusé de se soumettre à des prélèvements d'empreintes génétiques. Il s'agit de squatteurs, de syndicalistes, de faucheurs d'OGM, etc. Ce type de refus entre bien dans ce processus de désobéissance civile. Certains ont obtenu une relaxe du juge. Je cite le cas de jeunes gens qui avaient été déclarés coupables de vol aggravé parce qu'ils avaient remplacé, à Grenoble, des plaques « rue Thiers » par « rue de la Commune de Paris ». Évidemment, Thiers et la Commune de Paris ne sont pas tout à fait la même chose ! Deux ans plus tard, il leur a été demandé de se soumettre à un prélèvement biologique. Ils ont refusé. La Cour d'appel de Grenoble a prononcé leur relaxe le 5 juillet 2007. D'autres jurisprudences existent, toutes ne relaxent pas. Il s'agit d'un débat central. Le débat porte sur la disproportion entre ce prélèvement obligatoire en fonction d'une condamnation liée à l'article du code de procédure pénale et ces infractions. Par exemple, celui qui tague un mur peut être condamné et devra donner ses empreintes génétiques. Cette disproportion pose question. Par les temps qui courent, pas de prélèvement génétique en cas de condamnation pour un délit financier ! Ils ne sont pas prévus. Rappelons quand même que l'empreinte génétique est aujourd'hui considérée comme l'identifiant parfait. L'objectif des États est bien d'avoir un maximum de données génétiques.

67

Technologies de sécurité
et respect des droits et
libertés individuelles:
quelle protection ?

Cet exposé est bref, car la matière est immense. Je termine donc en revenant au droit à la sûreté, à savoir la résistance à l'arbitraire. Le secteur des technologies de la sécurité est en évolution fulgurante et permanente (nous venons de vous le démontrer à l'instant) sans qu'ait eu lieu une réflexion générale qui pourrait être opposée. Or, un ensemble de liberté est menacé (droit à la liberté d'aller-venir, droit à la vie privée, libertés individuelles), mais les textes sont morcelés, peu connus, ponctuels, même si la Cour européenne concentre son contrôle en se fondant sur l'article 8. Elle vérifie, au surplus, qu'il n'existe pas d'arbitraire. Cela souligne l'importance que la Cour attache à cet élément. Il faudrait redonner tout son sens au droit à la sûreté, celui de lutte contre l'arbitraire, et l'adapter au contexte actuel en se référant à la définition qu'en donne le professeur Jean Rivero¹⁰. Pour mieux comprendre l'importance de cette approche, il faut se rappeler que le recours aux technologies de sécurité est discret, peu décelable. Il s'agit d'une insinuation dans la vie de tous les jours, d'une surveillance peu visible,

mais de plus en plus généralisée. Finalement, il s'agit d'une grande question, puisqu'elle aboutit à la perte de maîtrise de son identité, voire à la perte de la maîtrise même de son corps.

Je prends un exemple pour terminer : le scanner corporel, destiné à remplacer la fouille corporelle intégrale dans les aéroports. Pour ne pas être arbitraire au sens classique, une fouille corporelle physique ne peut être effectuée que dans des cas précis, sur des personnes déterminées et soupçonnées. Avec le scanner corporel, cette même intrusion intégrale dans le corps est effectuée sur nous tous, sans distinction, en fouillant le corps dans son intimité la plus totale. La violence n'est pas physique. Mais en quoi cette violence est-elle moins grave parce qu'elle n'est pas physique au sens classique ? Et ne s'agit-il pas de l'expression la plus aboutie de l'arbitraire avec cet acte qui consiste à dénuder et fouiller intégralement le corps d'une personne, sans garantie, sans procédure, sans contrôle d'un juge ? Cet arbitraire se dissimule sous l'utilisation d'instruments discrets et silencieux. Insonores et pratiques, ils sont destinés à remplacer sans bruit, dans les aéroports, les portiques qui sonnent. Ces portiques, nous les trouvons à l'entrée de nombreuses administrations : à l'entrée de Beaubourg notamment. Si nous suivons cette logique, de nombreuses intrusions liées à la vidéosurveillance se mettent en place également, scrutant nos iris, nos visages, nos attitudes, nous enregistrant dans des bases de données. Le Comité national d'éthique [COMETS] s'était inquiété, dans un avis du 31 mai 2007 à propos de la biométrie. On accepte finalement d'être fiché, observé, repéré, tracé, sans souvent en avoir conscience. Certes, nous pourrions dire que nous illustrons le *Discours de la servitude volontaire*¹¹, mais pas uniquement. Nous sommes en effet, pour le moment, sans grand moyen de défense de nos libertés. Il est donc urgent de réagir et d'analyser ces intrusions pour ce qu'elles sont : des actes arbitraires, analogues à ceux qui étaient jadis effectués, lorsqu'il n'était possible de disposer que de contraintes physiques. Il est urgent d'adapter le droit à la sûreté à la situation d'aujourd'hui.

68

Technologies de sécurité
et respect des droits et
libertés individuelles:
quelle protection ?

La grande question reste : « Jusqu'où la sécurité autorise-t-elle des atteintes aux droits fondamentaux, sans atteindre, voire détruire, l'essence de l'État démocratique ? »

Notes

* Docteur en droit, maître de conférences en droit public à l'université de Paris-X-Nanterre et rédactrice du site d'*Actualités juridiques* concernant le droit des libertés fondamentales. ↑

1. Droit de ne pas être détenu arbitrairement, qui porte nécessairement atteinte à la liberté individuelle. ↑

2. Gerhard KLASS, procureur général, Peter LUBBERGER, avocat, Jürgen NUSSBRUCH, juge, Hans-Jürgen POHL et Dieter SELB, avocats, tous ressortissants allemands, ont dénoncé le droit de recourir aux mesures de surveillance prévues par la législation. Ils l'ont attaqué car ces mesures n'obligent pas les autorités à en aviser, *a posteriori* et dans tous les cas, les intéressés. ↑

3. Droit au respect de la vie privée et familiale. ↑

4. Décret n° 2004-471 du 25 mai 2004 modifiant le décret du 6 février 1997 relatif aux conditions d'agrément des personnes habilitées à procéder à des identifications par empreintes génétiques dans le cadre d'une procédure judiciaire. [voir [texte de loi](#)] ↑

5. Autorités administratives indépendantes. ↑

6. Organisme chargé de l'organisation, du fonctionnement, du contrôle des autorisations d'interception, de l'exécution, du matériel, etc. ↑

7. Centralisation du renseignement intérieur pour la sécurité du territoire et des intérêts nationaux.

- Fichier français relatif au terrorisme et à l'espionnage, classé « secret-défense ». ↑
8. *Résistance au gouvernement civil* (1^{re} éd., 1849), *Désobéissance civile* (rééd. 1866), trad. de l'anglais par Guillaume Villeneuve, éd. Mille et Une Nuits, 1996. ↑
9. Essayiste, enseignant, philosophe, naturaliste amateur et poète américain (1817-1862). ↑
10. Jean Rivero (1910-2001), spécialiste de droit public et de la question des libertés publiques, un des premiers commentateurs des décisions du Conseil constitutionnel, professeur à l'université Panthéon-Assas, à la Faculté de droit de Poitiers, puis de Paris, et dans plusieurs universités étrangères. ↑
11. LA BOÉTIE (de), Étienne, *Discours de la servitude volontaire ou Contr'un* (1^{re} pub. 1576), Payot (coll. Petite bibliothèque), 2002. ↑

Victimes et complices: les individus face aux technologies d'identification et de surveillance

Thierry Rousselin*

Il me revient le difficile exercice d'être le dernier intervenant. Mes prédécesseurs ont traité de manière exhaustive des principaux sujets. Nous allons seulement revenir sur quelques points me paraissant primordiaux, à propos de nos comportements individuels devant les technologies en question et leurs politiques de mise en œuvre.

Nous avons beaucoup abordé les thèmes de l'État et des institutions, ainsi que nos relations avec ces dernières. Nous avons aussi entamé, à travers un certain nombre d'exposés, l'analyse de notre propre rôle dans le système. Il s'agit à présent de décrire la manière dont nous sommes à la fois victimes et extraordinairement complices de la mise en place du système. Notre dualité est à la fois individuelle et collective. Il s'agit ainsi de dénombrer les raisons pour lesquelles nous acceptons d'entrer dans un système de surveillance, dans un système automatisé d'identification, décliné en de multiples formes. La vidéosurveillance, les fichiers et la biométrie focalisent la majorité des débats, au détriment de bon nombre d'autres techniques de surveillance tout aussi importantes.

De prime abord, toutes les technologies mises en place se fondent sur de bonnes raisons. Il existe toujours, au démarrage, une raison annoncée, qu'il est impossible de remettre en cause. Nul, au sein du corps social, ne défendra Dutroux. Nul ne défendra Thierry Paulin. Le fichier des empreintes génétiques est donc mis en place dans l'atmosphère d'émotion liée aux grands crimes sexuels, jouant ici un rôle légitimant. Dans le même ordre d'idées, il est question aujourd'hui du RFID¹ dans le passe Navigo. D'où vient ce dispositif ? Il s'agit d'une technologie existant depuis soixante ans, utilisée pendant la Seconde Guerre mondiale dans l'identification ami/ennemi des avions. La première guerre du Golfe a été l'occasion de sa réactivation dans la plus importante opération logistique jamais menée par l'armée américaine : des camions et leurs pièces de rechange étaient embarqués dans des bâtiments séparés, avec aucun système fiable de recoupement des informations. L'utilisation de puces RFID sur les conteneurs a offert une solution efficace et adaptée à la situation, qui n'a pas soulevé de débats particuliers. Viennent ensuite les grandes crises sanitaires des années 1990 (vache folle, etc.) où des opérations de marquage des troupeaux bovins ont été massivement réalisées. Ces démarches sont également apparues légitimes, eu égard à la nécessaire traçabilité alimentaire à mettre en place. Par la suite, une directive européenne a instauré l'obligation de « taguer » nos animaux de compagnie. Nos vétérinaires se sont, accessoirement, transformés en auxiliaires de la mise en place d'un système de fichage. Là encore, peu de réactions se sont fait entendre au sein de l'opinion publique.

Bien entendu, à l'heure des premières expérimentations sur l'homme, la motivation mise en avant est celle, positive, du dossier médical. Des individus ayant oublié leur identité ou en état de choc présenteront toujours, avec une puce RFID sous-cutanée, un dossier médical fiable, accessible *via* un simple lecteur. L'exemple du RFID illustre cette séquence-type, non d'acceptation (puisque'il n'y a jamais eu de consultation), mais de passivité devant les motifs impérieux présentés, qui cependant perdent progressivement de leur

consistance, jusqu'au fait accompli de la mise en place d'un système. Car en parallèle, quand on passe de quelques centaines d'avions à des millions d'animaux, on assiste à la création d'un marché de masse de fabrication des puces avec les effets induits sur les prix. Et comme cela s'accompagne de la miniaturisation des composants, les applications possibles explosent. Les puces RFID destinées il y a quinze ans à des objets de très grand prix, sont aujourd'hui incluses dans un passe Navigo ou dans un billet de la coupe du monde de football (2006). Un tel résultat est d'abord l'aboutissement d'une séquence de non-décisions qui mènent à une situation de fait accompli.

Mais l'exemple des puces dans les passes de transports illustre aussi un autre aspect. Notre acceptation collective fut d'abord motivée par l'apport positif en matière de qualité de service. La totalité des enquêtes effectuées auprès des usagers – la RATP ayant essuyé bon nombre de critiques au sujet du passe Navigo – ont abouti à des pourcentages avoisinant les 95 % de satisfaction, par opposition aux aléas de l'ancien système de tickets. L'utilisateur perçoit donc avant tout les avantages du nouveau système en matière de confort et de performance. Mais l'engouement peut aussi reposer sur des motivations factices : les systèmes de cartes, déployés par les grands magasins (Fnac, Champion, Auchan, etc.), remplissent la même fonction que le système antérieur des bons de réduction. À une différence près, qui est l'opération de profilage progressif du comportement de consommateur. Il relèverait toutefois de la paranoïa de former une hypothèse d'interconnexion de tous les fichiers de magasins avec ceux des banques et autres. Toutefois, le profilage établi de manière plus ou moins fiable une identité de consommateur qui est d'un grand intérêt pour les commerçants.

71

Victimes et complices

Relevons aussi l'essor du GPS², passant en l'espace de trois ans seulement de la rareté absolue à la généralisation. Les Français se perdaient-ils davantage il y a cinq ans qu'aujourd'hui ? Certainement pas. Nous avons seulement valorisé, jusqu'à la nécessité absolue, le service rendu par le GPS. Or, aux États-Unis, des dysfonctionnements liés au GPS ont déjà eu lieu. Au printemps dernier, un accident de la circulation avait conduit au blocage d'un des plus importants ponts d'accès à San Francisco. La plupart des GPS des automobilistes, *via* les services de cartographie en ligne auxquels ils sont abonnés, ont immédiatement pris en compte l'incident, mais ont transmis à leurs usagers des directives tellement mal coordonnées qu'elles ont causé le lendemain matin le plus grand embouteillage qu'ait jamais enregistré la baie de San Francisco. Deux jours plus tard, l'État de Californie a été visé par les attaques prévisibles des citoyens. Comment pouvait-on disposer d'une vision totale d'un champ de bataille à Bagdad et ne rien pouvoir contrôler à San Francisco ? Il s'agit, on l'aura remarqué, d'une attente de réponse technologique, en termes d'exigence vis-à-vis des systèmes déployés (davantage de rapidité, d'efficacité, de technologie), et non la remise en cause de celle-ci. Une autre préoccupation récurrente est celle de l'accès aux avions, exigeant de plus en plus de temps, notamment depuis les attaques terroristes du 11 septembre 2001. Il constitue un véritable imbroglio pour les personnes empruntant régulièrement les compagnies aériennes, que propose désormais de résoudre un certain nombre de systèmes de « *fast tracks* » (voie réservée).

Quasiment généralisés aux États-Unis, déjà mis en place à l'aéroport de Nice, il s'agit de couloirs permettant d'accéder à l'avion en évitant l'essentiel des contrôles, du fait que l'utilisateur sera enregistré au préalable auprès d'une compagnie privée disposant d'accords avec les États. Les sociétés prenant en charge le dispositif exigent, en contrepartie d'un abonnement, un nombre optimal de données biométriques. Le passager est donc considéré d'une fiabilité absolue, le dispensant des lourds contrôles d'usage. Nous avons consulté nombre de blogs d'utilisateurs du dispositif durant l'été 2006 (période de sa mise en place). Le débat y était foisonnant. Une réaction d'internaute, fort révélatrice, consistait en ceci :

« J'espère que toutes les données transmises à l'entreprise sont bien protégées contre le piratage, vu la quantité d'informations que je leur fournis. Mais je n'y penserai plus quand je passerai en sifflant par la voie réservée en regardant la queue des cent couillons qui attendent. »

Le phénomène en présence ici est la différenciation ordinaire par le luxe technologique, ignorant le revers de la question : les technologies les moins luxueuses sont aussi les moins facilement traçables. Un téléphone de dernière génération est plus facile à localiser qu'un téléphone rustique.

Les citoyens accordent d'emblée une certaine confiance aux institutions en matière de technologies de surveillance. Le large impact récent des mouvements d'opposition à la mise en place du fichier EDVIGE provient, dans une large partie, de la diffusion massive du texte du projet de loi. Une lecture sommaire mettait en lumière les contradictions dans le contenu et la rédaction du texte : les articles 2 et 4 étaient contradictoires, ambigus, installant un flou propice aux applications les plus abusives. S'en est suivie une réaction de rejet identique à celle du référendum pour la Constitution européenne, où le citoyen s'est senti en quelque sorte lésé dans sa confiance accordée au législateur responsable d'établir des garde-fous. De telles réactions de masse restent toutefois rares. Le plus souvent, seules les personnes directement affectées entreront en contestation active, l'ambiance générale demeurant à la confiance. La mobilisation contre EDVIGE provient en large partie du fait que les populations visées étaient des leaders d'opinion (chefs d'entreprise, syndicalistes, journalistes, etc.), qui ont donc logiquement relayé le débat sur la place publique. L'ambiance de confiance générale est également facilitée, par la complexité technique des dispositifs, dont assez peu de citoyens comprennent les tenants et aboutissants. La vulgarisation du fonctionnement des technologies de pointe n'est qu'une question de méthode. Il y a partout des dispositifs de vidéosurveillance, mais fonctionnent-ils en réseau ? Quelles en sont les connexions ? On ne le sait pas. Il serait possible de localiser des armes de destruction massive en Irak par images satellitaires, pourtant il nous est impossible de dénombrer le nombre de réfugiés de guerre. Le décalage est abyssal entre le plausible et le non-plausible, la réalité et l'image que l'on s'en fait, jusqu'à générer une atmosphère d'incompréhension générale des conséquences sur la société du développement des systèmes de surveillance.

Mais que signifie donc cette notion de système ? Des laboratoires entiers,

au CNRS ou ailleurs, travaillent à la compréhension et à la maîtrise de systèmes complexes. La principale difficulté est la coordination des données et des procédés. Quelles sont les capacités techniques intrinsèques d'une caméra de vidéosurveillance fraîchement installée au sein d'une mairie ? Répondent-elles aux besoins ayant motivé la mise en place d'un tel dispositif ? A-t-il été déployé au bon endroit au bon moment ? Les agents manipulant le matériel sont-ils compétents ? Y a-t-il en permanence une personne physique derrière le dispositif afin d'en relayer les alertes ? Une chaîne de commandement est-elle fonctionnelle ? A-t-on prévu des palliatifs aux dysfonctionnements ou aux attaques visant les données privées stockées, tant contre le temps que contre les piratages ? Enfin, quelles sont les perspectives d'évolution prenant en charge les systèmes en place ? Souvent, les politiques se contentent de présenter un nombre *x* de caméras mélangeant celles des banques, des magasins, de circulation et autres, et faisant l'hypothèse implicite qu'un dispositif cohérent serait ainsi constitué. Il s'agit quelque peu de propagande, leurrant le public sur l'efficacité du système. On ne peut que douter de l'interconnexion concrète, de l'interopérabilité, de l'efficacité 24h/24 d'un réseau composé d'éléments aussi disparates. Une question se pose à nous : les politiques sont-ils eux-mêmes dans l'ignorance de ces réalités ?

Dans tout discours traitant de la surveillance, il est extrêmement rude de faire la part de la réalité et de la fiction. Le site internet, Rue 89³, ouvrait récemment un débat autour des écoutes téléphoniques. Un journaliste s'affirmant spécialisé dans les nouvelles technologies, indiquant qu'il tenait ses informations d'un ami travaillant au sein des services secrets, évoquait des écoutes visant les téléphones portables, même éteints. S'agissant d'affirmer qu'un téléphone éteint pouvait être (ou non) mis sur écoute, les frictions étaient vives. Un doctorant en prétendait la possibilité technologique ; un salarié d'Alcatel le niait au nom de la responsabilité des industriels, etc. Même au sein de spécialistes, il est difficile d'établir un consensus autour du sujet. À quoi se raccrochera le « citoyen ordinaire » dans une telle situation ? La confiance lui est, pour ainsi dire, imposée, alors qu'il reste empreint de méfiance. D'aucuns proposent de le rassurer *via* des chiffres magiques, dont politiques ou citoyens s'emparent en premier. Étant moi-même dans le monde de l'observation spatiale, la question qui m'est le plus fréquemment posée depuis vingt ans est : « Peut-on lire ou non une plaque d'immatriculation depuis l'espace ? » Cette fixation sur un chiffre n'a pas de réponse simple (la réponse optimale pourrait être « ça dépend ! ») mais surtout n'est pas en soi représentative de l'efficacité réelle du système (il y a des tas de résultats qu'on arrive à obtenir en jouant sur d'autres paramètres que la taille des objets). Un autre chiffre magique porte sur les trois millions de caméras (mis en avant aussi bien par les « propagandistes » du système comme cible d'efficacité que par les opposants à la surveillance comme chiffre qui fait peur). Qui maîtrise vraiment la réalité que voile l'aura du chiffre magique ?

Un autre instrument de conviction s'appuie sur les sondages. Les Français se prononcent à 70 % en faveur de la vidéosurveillance. Le ministre de l'Intérieur le réaffirme, bien entendu, en diverses occasions. Malgré la fluctuation des opinions, une donnée aussi stable ne peut être que pertinente.

D'où peut provenir un tel engouement de la part des Français : du discours des politiques ou de celui des médias ? Une tendance récurrente en France consiste à dénoncer l'influence des médias. Pourtant, une mise en revue de la presse française des deux dernières années, toutes tendances politiques confondues, du support papier aux reportages télévisés (y compris ceux de TFI), montre que sur les aspects de la surveillance, la tonalité générale du traitement est majoritairement négative. Les reportages de TFI sur la vidéo-surveillance à Londres en soulignent clairement les dysfonctionnements. Une proposition d'explication pourrait prendre en compte la confrontation de la vision critique des médias et l'illusion de performance véhiculée par des programmes de fiction, comme *Les Experts*. Depuis les années 1990 (avec la série *Urgences* dans le domaine médical), un changement profond dans l'écriture des séries dramatiques us de fiction, tend vers une abolition de l'effet de fantaisie (que l'on trouvait par exemple chez Jules Verne) ou de démesure (cycle James Bond, etc.), au profit d'une illusion de réalité. D'abord, l'effet feuilletonnant lié au côtoïement des personnages plusieurs heures par semaine durant de nombreuses années, tend à les transfigurer en personnes réelles de notre quotidien. Mais lorsque ce feuilleton installe le mythe du « scientifique parfait », à la méthodologie et à la morale irréprochables, intervenant avec un discours et des outils scientifiques et technologiques après le crime et avec un taux de réussite proche de 100 %, notre confiance est totalement gagnée. Pourtant Gil Grissom⁴ et ses confrères de fiction mènent des recherches dans lesquelles le point d'arrivée est connu (le crime a eu lieu), et où il s'agit de retourner vers les origines. Une sorte d'astrophysique du crime. La politique réelle d'application des technologies de surveillance procède à l'exact opposé. Il est question de prévention de la délinquance. Il n'est jamais question de prévention dans *Les Experts*. Les gestes, outils, technologies utilisés par les fictions télévisées tiennent intégralement de la réalité, du fait de l'intervention de professionnels comme conseillers techniques et d'une très bonne documentation des producteurs. En revanche, le parcours de l'enquête tient de l'insolite. L'observateur transite entre des caméras de banques, de circulation, de voie publique, de magasins. D'un simple clic, l'agent transite d'une caméra à une autre, synchronise des données éparées – chose qu'aucun agent français n'a la possibilité de faire. Dans la réalité, nous sommes aux antipodes de l'organisation idéale représentée. Les programmes exploitant cet « effet de réel » tiennent seize heures hebdomadaires de programmes sur CBS, chaîne leader aux États-Unis depuis 2001 (et guère moins sur TFI en France). D'où, de plus en plus, cette difficulté des spectateurs à faire la part des choses entre réalité et fiction.

En conclusion, nous pouvons nous demander si de simples citoyens, malgré la complexité et l'ambiguïté du système, ont la capacité de produire des parades de réponses, de s'approprier et de retourner le dispositif, de pratiquer, en quelque sorte, un retournement de surveillance. Au sein de mon domaine, qui est la surveillance géospatiale, des réactions appréciables ont eu lieu au moment de l'ouragan Katrina. Des citoyens américains, se basant sur la directive Clinton de 1994 ouvrant l'accès aux données publiques, ont recoupé à partir des observations de la Nasa et d'autres organismes, des preuves accusant le gouvernement Bush d'inaction. Recueillies sur le Web,

des cartographies démontraient la passivité des pouvoirs publics. Des universitaires et de simples citoyens pratiquaient ainsi, tout à fait légalement, la surveillance des surveillants. Un retournement de l'outil comme on en voit de plus en plus et qui pourrait devenir la nouvelle norme de comportement responsable.

Notes

* Consultant en observation spatiale. ↑

1. La radio-identification, plus souvent désignée par le sigle anglais *RFID*, *Radio Frequency IDentification*. ↑

2. *Global Positioning System*, que l'on peut traduire en français par Système de positionnement mondial. ↑

3. Site d'information et de débat participatif sur l'actualité (www.rue89.com). ↑

4. Personnage fictif incarné par l'acteur William Petersen dans la série télévisée américaine *Les Experts*. ↑

Table ronde : Identification et surveillance des libertés individuelles

Animée par Michel Alberganti*

Quelle est l'articulation, fatale et complexe, entre liberté et sécurité – sans confondre avec la sûreté ? Je voudrais citer un exemple pour illustrer cette frontière fragile entre liberté et sécurité. Il s'agit d'un système nommé OpTag, actuellement à l'étude, qui a fait l'objet d'investissements européens – 4 ou 5 millions d'euros. Le système OpTag¹ a pour objectif de réduire les retards au décollage des avions. Des puces RFID, intégrées au billet d'avion, permettent de localiser dans l'aéroport tous les flâneurs, en particulier ceux qui passeraient trop de temps au « *free shop* », au café ou ailleurs avant de se rendre à la salle d'embarquement. Cette technique permet de limiter les retards. Il n'y a pas de lien avec la sécurité à proprement parler. Il s'agit d'un autre enjeu : améliorer le fonctionnement des compagnies aériennes. Ce système pourrait s'intégrer aux aéroports. Les aéroports sont des espèces de microcosmes dans lesquels se concentrent quasiment toutes les technologies de surveillance existant aujourd'hui. Nous avons même évoqué ces systèmes qui permettent de détecter les comportements des gens en analysant les vidéos. La biométrie concerne le personnel, le « *body scanner* », les portiques, le passeport. Bientôt, s'ajoutera cette puce RFID dans les avions. À quel moment le citoyen peut-il intervenir, vis-à-vis de mesures qui ont comme alibi (ou motivation) la sécurité ? Nous voyons, de plus, que d'autres motivations viennent se greffer sur ces technologies. Le débat tourne autour de ces atteintes aux libertés individuelles.

Tout le débat tourne autour de ces atteintes aux libertés individuelles. Nous allons en débattre avec trois intervenants : Anastassia Tsoukala, maître de conférences HDR² à l'université Paris-XI et chercheuse à l'université Paris-V. Elle a travaillé sur ces questions de sécurité, politique et Droits de l'homme en Europe, ainsi que la « construction sociale de la menace » ; Vincent Dufief, avocat au barreau de Paris, spécialisé en droit pénal des nouvelles technologies et en droit de la vie privée ; il s'est beaucoup intéressé aux réseaux sociaux, entre autres ; Jérôme Thorel, membre de l'association *Privacy International*, qui organise un événement assez connu, les *Big Brother Awards*³, qui existent en France depuis l'an 2000.

Anastassia Tsoukala : Je suis juriste et criminologue de formation. Depuis vingt ans, je travaille sur les droits de l'homme. Au cours des années 2000, cela a été développé dans le cadre de six programmes européens. J'ai beaucoup publié sur ces questions, en anglais. Il existe trois sortes de surveillances. Il y a la surveillance imposée. Puis, une surveillance consentie : le passe Navigo, l'acceptation du transfert de ses données par le voyageur qui se rend aux États-Unis (PNR). Enfin, il existe une surveillance librement choisie : *Facebook*, les blogs, etc. D'habitude, nous pensons que la surveillance imposée est celle qui pose problème. Je n'insisterai pas davantage sur ces trois types de surveillance. Il faut garder à l'esprit que le terme « surveillance » ne renvoie pas toujours à la même réalité. Nous avons aussi une grande difficulté à définir une des valeurs menacées : la vie privée. Qu'est-ce que la vie privée ? Nous avons parlé du passe Navigo. Il en existe deux : l'un est nominatif, il trace nos déplacements ; l'autre est anonyme. Il a été dit qu'il est révoltant – et je partage cet avis – que le passe prétendument anonyme soit payant. Or, ce qui m'intéresse dans

ce système de passe n'est pas tant le fait que l'un des deux soit payant, mais le fait que la CNIL ne s'est pas prononcée sur la question. Soit le passe ordinaire (nominatif) est légal et ne pose aucun problème ; dans ce cas, la CNIL n'avait pas à recommander la création d'un autre passe. Soit... quoi ? Même le passe Navigo ordinaire a, en effet, été accompagné de précautions. Existerait-il alors un noyau dur non négociable de la valeur sociale à protéger ? Dès lors, le contour de la valeur ne serait-il pas librement délimité, par chacun de nous ? La CNIL nous renvoie la balle, en avançant avoir fait ce qu'elle pouvait et en nous invitant à réagir selon nos besoins, notre définition, notre conception, notre perception, nos valeurs. En somme, qui s'accommode d'être déjà localisable par le portable, par le GPS et autres technologies, prendra le passe Navigo ordinaire. Les plus sensibilisés, les plus frileux ou « délirants » (selon les termes de M. Aghroum), prendront le passe anonyme. La valeur n'est plus clairement définie sur le plan juridique. Le juridique se compose-t-il avec des réflexions sociales ? Je n'aurai pas le temps de développer ce point.

Je passe au deuxième volet de ma réflexion, qui n'est plus lié à la question de l'atteinte à la vie privée mais au fait que toutes ces techniques de surveillance imposent *de facto* un grand bouleversement dans notre système juridique. En effet, le soupçon est introduit en tant que base de justification de l'action de la police, et même de plus en plus de l'imposition de sanctions. C'est nouveau. Jusqu'ici, hormis la surveillance politique, donc lorsque la police « ordinaire » agissait, le but était de collecter des preuves afin de poursuivre un individu. Or aujourd'hui, la surveillance ne vise

plus à la collecte de preuves. Si des preuves sont trouvées, tant mieux. Mais lorsque des preuves ne sont pas trouvées, il est possible de contourner le judiciaire et d'imposer directement des sanctions. Nous avons déjà parlé du cas des suspects pour terrorisme au Royaume-Uni, qui ont été mis en prison pour une durée indéterminée dans un premier temps. Aujourd'hui, certes la loi a été modifiée, mais dans quel sens ? Il a été estimé que cela était discriminatoire. Elle est maintenant appliquée aussi aux citoyens britanniques. Mais comme il n'est pas possible de les mettre en prison, il s'agit d'autres mesures qui peuvent aller jusqu'à la détention à domicile, par exemple. Au nom de quoi ? D'un soupçon. Si vous considérez que, finalement, cela permet de repérer les « méchants », les « potentiellement méchants » ou ceux dont on pense qu'ils pourraient être « méchants », je vais vous parler de cas moins dangereux, plus près de nous. Il s'agit des *hooligans*. Êtes-vous au courant des interdictions administratives de stade ? Ces interdictions impliquent des sanctions vis-à-vis des personnes déviantes qui, explicitement, n'ont commis aucun acte répréhensible, mais dont le comportement, en général, présente un potentiel d'atteinte à l'ordre public.

Michel Alberganti : Vous avez, avec le juridique, ouvert la porte à Vincent Dufief⁴, pour qu'il prenne la suite.

Vincent Dufief : Conformément à mon métier, je vais essayer de me faire l'avocat des fichiers et de la sécurité. En effet, tout ce que j'ai entendu jusqu'à présent m'a paru très critique. J'aimerais rappeler qu'il existe des principes fondamentaux : les principes de finalité, de proportionnalité et de transparence, qui font que tout

fichage n'est pas forcément négatif. Toute surveillance, notamment étatique, n'est pas nécessairement un danger si la finalité pour laquelle ce fichage ou ce contrôle est réalisé est respectée. Si, par exemple, une vidéosurveillance sert à s'assurer de la présence ou de l'absence de *hooligans* dans un stade, je ne vois pas ce qu'il est possible d'y redire. Dès lors que les gens sont informés qu'ils sont filmés et que la finalité est la prévention d'actes de délinquance ou de malveillance dans ce stade, cette finalité est légitime et nous devons l'accepter. Le danger est dans le détournement de finalité. Un système mis en place pour une finalité précise ne risque pas d'être détourné. Nous pouvons l'observer dans le cas d'organismes gouvernementaux, mais pas seulement. Je m'inscris en faux avec une deuxième idée : une surveillance imposée serait forcément pire. Je ne suis pas convaincu qu'une surveillance, sitôt qu'elle est imposée, notamment par une autorité gouvernementale ou policière, soit pire. Dans l'affaire du fichier EDVIGE, j'ai été choqué de voir une opinion qui semblait terrifiée par la composition d'un fichage comportant des données éminemment sensibles : opinions politiques, croyances religieuses, préférences sexuelles. Ces données sont traitées par des sites comme *Facebook* et certaines personnes consentent au traitement de celles-ci. Certaines personnes vont donc accepter que ces données soient traitées par une entreprise privée, qui plus est américaine (non soumise à la législation française).

Le problème, pour moi, est qu'il existe une divulgation volontaire de données personnelles à des fichiers que nous ne maîtrisons pas forcément. Un fichier tel que celui de *Facebook* est parfois

extrêmement complet. Certaines personnes renseignent de nombreuses données. *Facebook* conserve ces données, parce qu'il les revend. Il existe donc une marchandisation de la donnée personnelle. Ce genre de site fonctionne parce que les gens donnent des données personnelles. Ils sont financièrement gratuits, mais se payent en données. Ces sites revendent ensuite des profils de consommateurs à des annonceurs et font leur *business* ainsi. Ce n'est pas anodin. J'ai l'impression que l'opinion ne le réalise pas. Elle considère le fichier EDVIGE très dangereux, mais pas *Facebook*. Dès lors, l'autorité politique constate que des données privées peuvent constituer un fichier de façon librement consentie par les personnes qui ne font plus attention. Je rejoins Alex Türk⁵ : les gens n'ont plus réellement conscience de la vie privée, puisqu'ils sont si habitués à communiquer leurs données personnelles qu'ils ne font plus vraiment attention. Le danger est là, et il rejoint, à un certain stade, le danger gouvernemental.

J'ai vu comment se constituaient certains fichiers de police. Il ne faut pas croire qu'ils soient basés sur des informations extrêmement secrètes. Des enquêteurs des RG ou de la DST⁶ m'ont dit que leur première source d'informations est Internet. Il s'agit des « sources ouvertes », dans le langage des renseignements : informations publiées sur Internet, où la plupart des gens les ont volontairement laissées. Je ne dis pas que le fichage gouvernemental n'est pas dangereux, mais je considère qu'il faut aussi faire attention à la divulgation volontaire d'informations personnelles par l'individu. Cette problématique ne peut se résoudre que par la sensibilisation des personnes et par l'éducation. J'observe les consé-

quences à des niveaux inférieurs. Je m'interroge sur le fichage policier. Il est difficile de mesurer le danger que représenterait, par exemple, l'intégration de mes empreintes génétiques à un fichier gouvernemental. J'ai du mal à visualiser le danger, concrètement. Je serais très intéressé par une explication. En revanche, je vois un autre danger concret. Certaines personnes viennent me voir parce que leur compagne ou leur employeur ont eu accès à des informations publiées sur des forums ou sur *Facebook*, qu'ils ne souhaitaient pas forcément voir publiées. Ils se retrouvent dans des situations problématiques et viennent me voir pour obtenir la suppression des données. Je leur demande alors s'ils ont été piratés ; ils reconnaissent alors avoir publié ces données. Ils disent qu'ils ignoraient la possibilité d'accès. Voilà les dangers du fichage auxquels je suis quotidiennement confronté.

Jérôme Thorel⁷ : Cela me fait bondir d'observer que soit pris au mot le ministre de l'Intérieur qui, juste après la révélation de l'affaire EDVIGE, avait rappelé l'existence de *Facebook*. La différence fondamentale c'est le consentement. Sur Internet, nous ne sommes pas contraints de laisser des informations ; contrairement à un fichier policier ou de renseignement. À propos du profilage, autrement dit l'intelligence de ces systèmes experts tels que *Facebook* ou *Google*, il n'appartient pas au ministère de l'Intérieur mais à *Facebook*, entreprise commerciale qui vend de la publicité. Il existe une grande différence entre laisser une trace sur un site internet et pouvoir exploiter toutes ces données à des fins mercantiles. Faire croire aux gens que les policiers ont accès à cette intelligence, cela n'est pas vrai. Il s'agit là d'une manière de nous faire

accepter tout cela, au prétexte que celui qui n'a rien à se reprocher n'a pas de raison de refuser d'être dans ces multiples fichiers. Selon cet argument, celui qui possède un téléphone mobile ou un GPS dans sa voiture n'aurait pas à refuser d'être dans un fichier « scélérat », un fichier de suspicion. La présomption d'innocence existe : il s'agit d'un principe fondamental. Comment pouvons-nous continuer à accepter que des principes fondamentaux soient violés quotidiennement ? Les lois antiterroristes sont des lois d'exception. Vous rappelez-vous comment cela s'est passé ? Évidemment, à chaque fois, il existe une frénésie à la suite d'un fait divers ou d'une grosse affaire qui fait pleurer dans les chaumières ou qui effraie tout le monde (le terrorisme). En France, plusieurs lois antiterroristes ont été votées. À chaque fois, dans le préambule de la loi, il est précisé que députés et sénateurs sont conscients qu'il s'agit d'un droit d'exception et que, pendant deux ans, ces lois seront « testées ». Tout le monde se souvient de la loi sur la sécurité quotidienne de novembre 2001. Son préambule précisait bien que le Parlement reconnaissait que la loi était en vigueur pendant deux ans, qu'elle était anticonstitutionnelle – donc illégale. Il faut tout de même arriver à l'accepter ! Pendant deux ans, il est donc demandé à la société dans son ensemble de l'accepter et d'évaluer l'impact de ces exceptions. Il me semble que les rapports parlementaires, qui étaient prévus dans le cadre de ces lois d'exception, pour faire le bilan et déterminer ce que cela a apporté de positif ou de négatif et si nous avons eu raison de céder, n'existent pas. En décembre 2008, nous avons à nouveau repoussé de deux ans les dispositions de la dernière loi antiterroriste de 2006. Cette extension s'est faite dans le cadre

d'un amendement, en pleine nuit. Il nous est demandé d'abandonner ces principes fondamentaux pour lesquels des générations entières se sont battues, en faisant confiance à l'État et à nos représentants. Mais, alors que cela se pérennise, nous observons qu'il existe encore moins de débat.

Je signale aussi la notion de « tolérance zéro », que nous entendons beaucoup dans la bouche des représentants politiques, à droite et à gauche. La « tolérance zéro » revient à l'idée d'une bataille constante, grâce aux technologies, pour réduire la partie de fraude possible pour le citoyen. Pour moi, c'est totalitaire. Ne pas accepter que, dans la société, il soit possible que des gens fraudent, volent quelque chose ou ne payent pas leurs impôts, est totalitaire. Il existe une différence d'interprétation sur la manière dont les lois sont votées pour sanctionner tout cela. Peut-être est-ce cela qui explique notre surprise, au sein des *Big Brother Awards*, de constater que, depuis dix ans, nous répétons les mêmes choses sans voir l'emprise de notre discours dans la société.

Il est question aujourd'hui d'identification. La biométrie est un système qui, malgré tout, risque d'accroître le risque de fraude. Le talon d'Achille des papiers d'identité biométriques n'est pas la technologie en tant que telle (puce RFID, code barre, données), mais les documents qui servent à fabriquer ce passeport. Quelles sont les personnes les plus à même de falsifier ces documents ? Ce ne sont pas des gens, tels que vous et moi, qui se rendent aux États-Unis en se faisant ficher pour 40 ans, acceptant de laisser une empreinte digitale, etc. Nous ne sommes pas capables de falsifier ces documents. Ceux qui en sont capables sont précisément les personnes qui sont réellement

les cibles de l'antiterrorisme. Les terroristes potentiels ont une plus grande facilité à falsifier des papiers, donc à avoir une fausse identité. Cela me révolte de voir à quel point nous continuons à faire croire aux citoyens que cela est pour leur bien. Le principe fondamental consiste à faire croire que la surveillance de tout le monde arrêtera les vrais délinquants. Or, prenons l'exemple de la caméra de surveillance dans le métro : ceux qui veulent vraiment rester cachés le restent. Qui est surveillé en permanence ? Les gens qui considèrent n'avoir rien à se reprocher.

Le commissaire [M. Aghroum] s'est exprimé, et il a dit que nous serions tous très satisfaits si le cambrioleur qui pénètre chez nous en notre absence se faisait alpagner grâce aux caméras installées devant chez nous. En revanche, il n'a pas rappelé que la dernière occasion où nous avons parlé de la vidéosurveillance, était après les attentats de Londres. La dernière loi importante a été votée dans l'urgence à la suite d'un attentat terroriste. Relisez les articles du *Monde*, du *Figaro*, de *Libération* : à l'époque, toute la presse, tous les chefs d'opinion de droite et de gauche ont pris cet attentat comme prétexte pour avancer que les caméras allaient prévenir le terrorisme. Nous savons très bien que, dans les faits, cela résout parfois des affaires criminelles ou délictuelles. Après le 11 septembre, il nous a été dit que les caméras avaient rendu possible l'identification des terroristes. Mais à ce stade, quelque 3 000 personnes étaient déjà mortes. Prévenir le terrorisme avec des caméras de surveillance est impossible. Pourtant, tout le monde le croit. La loi le présentait ainsi. Je m'étonne aussi qu'il soit encore possible d'avoir confiance dans la CNIL.

J'ignore si M. Lemoine est encore là pour répondre à mes propos. La Commission nationale de l'informatique et des libertés existe depuis trente ans. M. Lemoine nous a parlé du passe Navigo ; il a fait rire tout le monde en disant que la RATP avait des « arguments à la noix ». Il est commissaire à la CNIL ; il a donc entendu des gens s'exprimer pendant des heures sur la justification d'un passe électronique qui suit à la trace les personnes. Il a aussi dit tomber des nues, sept ans après que le projet de cette carte ait été connu, que la RATP ait conservé la possibilité d'identifier les personnes en les traçant selon les stations auxquelles elles entrent et sortent. À quoi sert la CNIL ? Ne vaudrait-il pas mieux la supprimer ? À mon avis, elle laisse une espèce d'illusion de la protection. Ce n'est pas un contre-pouvoir, mais un rouage du pouvoir. La CNIL participe à tout cela et elle existe parce qu'elle ne peut rien faire contre ce fichier. En 2004, de nombreux pouvoirs lui ont été retirés, avec l'aval des commissaires de la CNIL, avec aussi le sénateur Türk. Il a été rapporteur de la loi qui a modifié ses propres pouvoirs. Je me demande comment il est possible aujourd'hui de parler de la RATP en évoquant des « arguments à la noix » et de ne pas expliquer à tous à quoi sert cette institution, qui est toujours mise en avant.

La CNIL devrait être une institution permettant de faire avancer les choses. Cette instance ne peut pas dire non à un État, à une entreprise, et s'opposer à la mise en place de tels fichiers. Dans une société, que nous appelons encore « démocratique », il vaut mieux se débarrasser de la CNIL, à partir du moment où elle ne peut dire « non » à un État ou à un autre type de pouvoir qui fiche les

gens. Ainsi, ce serait plus clair pour tout le monde : cela ne donnerait pas au citoyen une « illusion » de contre-pouvoir.

Michel Alberganti : J'apporte une précision puisque, malheureusement, M. Lemoine n'est plus là et que la CNIL ne participe pas à cette table ronde et ne peut donc pas répondre. La CNIL a servi à l'existence du passe Navigo découverte.

Jérôme Thorel : Il ne s'agit pas de nous dresser des lauriers, mais les *Big Brother Awards* avaient déjà commencé à parler du passe Navigo en 2001. La CNIL n'en avait jamais parlé, à l'époque. Le passe « Découverte » (qui ne nécessite pas d'enregistrer son identité dans un fichier central) est un peu la conséquence de la dénonciation citoyenne, et non pas de l'intervention de messieurs Türk et Lemoine ! C'est pourquoi nous osons poser la question : « À quoi sert la CNIL ? »

Michel Alberganti : Il s'agit d'une bonne question, à laquelle la CNIL ne répondra pas, du moins, pas ce soir.

Jérôme Thorel : La CNIL a été plusieurs fois nominée (aux *Big Brother Awards*), mais n'a pas encore remporté de prix. Le jury est plus clément que les personnes comme moi qui ne fais partie que du comité de sélection.

Michel Alberganti : Je reviens sur les propos de Vincent Dufief à propos de *Facebook*. Il est assez important de trouver que *Facebook* puisse être un alibi. En effet, si les gens mettent volontairement des données personnelles – religieuses, sexuelles et politiques – sur *Facebook*, cela signifie qu'il n'existe aucune raison que l'État ne puisse pas faire de même dans ses

fichiers de police. Est-ce bien l'argumentaire que vous défendez ?

Vincent Dufief : Pas exactement. Je considère que la surveillance de l'individu à travers des sites privés est telle que les gens ne font plus attention. Il existe un manque de vigilance, ils baissent la garde.

Michel Alberganti : Cependant, tout le monde n'est pas sur *Facebook*. Commençons les questions tout de suite ; les mains se lèvent.

Public : Quand il s'agit d'un fichier de la DCRI⁸, autrement dit d'un fichier politique avec les moyens de la DST, il s'agit de moyens d'action. Les fichiers des RG, voici dix ou vingt ans, consistaient en une information policière et politique. Maintenant, les moyens de la DST sont appliqués à cette information. Il ne s'agit pas du tout de la même chose. Lorsque la DST vous demande le nom de votre grand-mère ou de votre arrière-grand-mère, vous devez le lui dire ; elle a les moyens de vous le faire dire. La DST est autre chose qu'un service d'information. Il s'agit d'un service de renseignement, qui a son propre système d'action. Il s'agit d'un service de renseignement, de défense et de surveillance du territoire. Quand vous êtes membre de *Facebook*, ce n'est pas la DST qui va venir vous chercher. Vous êtes là pour laisser une information. Vous savez que la fusion de la DCRI est celle de la DST et des fichiers RG. De quels moyens techniques dispose la DST – un service de renseignements agressif – en situation de défense du territoire ? Il ne s'agit pas des moyens des RG ni de la police normale, mais d'un service dépendant du ministère de l'Intérieur. C'est un service de renseignement. Ce n'est pas la même chose.

Michel Alberganti : La DST est un

service de police qui instruit sur une enquête préliminaire ou sur un juge d'instruction.

Public : La DST est la Direction de la surveillance du territoire. Il s'agit d'un service de renseignement interne, contrairement à la DGSE, service de renseignement externe.

Vincent Dufief : Le sujet de la DST n'est pas central. Ce qui est sur *Facebook* est déclaratoire. Je peux mentir et me déclarer musulman sur *Facebook*. L'objectif des fichiers de police n'est pas d'obtenir une information fausse.

Anastassia Tsoukala : Il existe une confusion importante. Que l'information soit vraie ou fausse sur *Facebook*, l'initiative vient de la personne. Qu'elle soit bien informée sur les conséquences de son acte ou pas, à la rigueur, peu importe. En effet, de quelle liberté d'action disposons-nous en réalité ? Il s'agit de l'illusion et des mythes fondateurs. Pouvons-nous toujours imaginer les conséquences de nos actes ? Selon notre jargon, il s'agit d'un « acte libre », venu de l'initiative d'un individu. Les informations, même si elles sont collectées par les RG (ou autres), conduisent à la question de la finalité. Si je veux vous montrer des photos de mon postérieur, tel est mon droit. Je pense à une utilité, à une finalité. Si ces photos sont collectées à mon insu, même si elles ne sont montrées à personne, il s'agit d'autre chose. Vouloir dire à tout prix que cela est la même chose, ou presque, au prétexte de la ressemblance, conduit à une confusion absolue. Hier soir, j'étais invitée à un dîner. J'ai surpris la discussion d'adolescents, à côté de moi. Soudain, l'un d'eux mentionne le fichier EDVIGE. L'autre demande ce dont il s'agit ; le premier répond

qu'il s'agit d'une sorte de « *Facebook* pour la police ». Que cela soit sorti de la bouche d'un adolescent en dit long sur la perception de la vie privée. Mais qu'un avocat tienne le même discours rend la situation un peu plus compliquée.

Vincent Dufief : C'est précisément parce que je suis un utilisateur que je connais.

Anastassia Tsoukala : Je voudrais évoquer une autre question qui me préoccupe : l'efficacité. Il est dit au citoyen, au nom de la protection et de la sécurité, que cela est pour leur bien et qu'il faut le faire. Quelle est l'efficacité ? Nous avons un retour de l'application du PNR. Ce transfert de données est fait pour lutter contre le terrorisme. Jusqu'à ce jour, une dizaine de personnes ont été arrêtées pour deux motifs. Dans la majorité des cas, ils avaient des démêlés avec le fisc dans leur pays d'origine, ou ils avaient du retard pour verser une pension alimentaire. Avons-nous mis en place ce système pour arrêter les fraudeurs du fisc et ceux qui ne versent pas d'argent à leur ex-épouse ou à leur enfant ?

Autre cas anecdotique : le système d'information Schengen, mis en place pour lutter contre la délinquance et le crime organisé. Dans les faits, il sert pour retrouver les véhicules volés et pour contrôler les immigrés clandestins. Cela coûte beaucoup d'argent, « notre argent », et sert à autre chose que la finalité initiale.

Les caméras de surveillance qui ne vous posent pas trop de problèmes m'en posent un. Toutes les études montrent qu'elles ne font pas

baisser la délinquance dans la rue. Lorsqu'elles le font, c'est parce qu'elles la déplacent.

Vincent Dufief : Il n'existe pas assez de caméras...

Anastassia Tsoukala : Donc, elles ne résolvent rien. Ni le comportement du public ni la délinquance n'ont changé à cause des caméras. Tout cela pose problème par rapport à la raison d'être de ce système qui nous est présenté. Alors que nous nous inscrivons par ailleurs dans une logique très « managériale », où tout est calculé, quantifié, tout doit être expliqué et justifié en termes chiffrables ; à ma connaissance, ni au niveau national ni au niveau européen, aucune analyse coûts/profits n'a été produite portant sur les dispositifs de sécurité. La question n'est jamais portée en de pareils termes. Il nous a récemment été dit, au sein de la Commission européenne, qu'il est envisagé de modifier radicalement tous les dispositifs de contrôle aux frontières externes de l'Union européenne. Cela coûte des sommes faramineuses. Est-ce parce que l'autre système était inefficace ? Je n'ai pas de réponse. Par rapport à quoi le nouveau système sera-t-il donc meilleur ? Il m'est répondu que l'on ne s'est pas posé la question. Je ne vais pas entrer dans la paranoïa, mais je ne peux m'abstenir de penser à des pressions exercées par les *lobbies* industriels.

Michel Alberganti : Une difficulté à l'évaluation de l'efficacité de certains systèmes de sécurité existe, quand ils ont pour objectif d'éviter que des événements se produisent. S'ils sont efficaces, il ne se passe rien, justement. Les gens qui défendent ces systèmes peuvent toujours arguer

du fait qu'ils sont très efficaces. Comment le prouver ? Cette évaluation est difficile.

Jérôme Thorel : Les politiques publiques, notamment de médiation et de prévention sociales, sont aujourd'hui sacrifiées parce que nous ne savons pas les évaluer. Nous ne savons pas comment un jeune éducateur de rue va à la rencontre de personnes en difficulté. En général, elles sont remplacées, le plus souvent, soit par des politiques sécuritaires soit par des politiques dites « technologisantes ». Mettre une caméra de sécurité évite d'envoyer un éducateur de rue, qui rencontre des personnes sans domicile fixe ; qu'il pourrait éventuellement aider. Il est assez drôle d'observer que, tout comme les politiques sociales, on ne sait pas évaluer le travail fait par une éventuelle solution technologique.

Michel Alberganti : Il est vrai que l'application n'est pas la même et que les conséquences sont radicalement différentes. Dans un cas, le poste d'éducateur est supprimé ; dans l'autre, la caméra est laissée. Cela coûte beaucoup moins cher.

Public : S'il n'y a personne derrière, à quoi sert la caméra ?

Jérôme Thorel : Je vous rassure : le travail social est tout à fait évaluable avec un logiciel. La loi⁹ de prévention de la délinquance de 2007 demande aux conseillers généraux de tout intégrer à une base de données. Évidemment, au gré d'amendements et d'arrêtés bien placés, sont créés des liens entre administrations. Les familles les plus précaires sont les premières à être fichées, à être victimes d'une erreur de traitement ou d'un policier zélé qui prendra note de per-

sonnes sans-papiers passibles d'expulsion. Le fichier « base-élèves¹⁰ », dans les écoles, est en phase expérimentale depuis 4 ans et est devenu obligatoire l'année dernière. Un identifiant est donné aux élèves dès leur entrée à l'école maternelle (à 3 ans !) ; et cet identifiant est lui-même stocké dans un fichier national (la BNIE), qui restera valide durant trent-cinq ans. Le droit à l'oubli pour les enfants est évacué. Concernant l'évaluation du lien social, il devient très facile pour les gouvernants de considérer qu'avec un outil informatique, nous allons rationaliser tout cela et mieux connaître l'impact que nous aurons. Le danger est que les gens se retrouvent encore une fois sous surveillance.

Public : Je souhaite revenir sur la CNIL. Lors d'une pause, tout à l'heure, j'ai discuté avec M. Lemoine. Il a parlé de Navigo. Lors des trois « occupations » de la CNIL, nous avons chaque fois parlé du passe Navigo. Je trouvais bon de rappeler qu'il existait une interaction. Le débat sur l'utilité de la CNIL a lieu à partir du moment où il n'existe pas de mouvement social sur les libertés, où nous pensons que la CNIL est le seul rempart pour ces questions. Il est bon de pointer les problèmes précis de cette commission. Pendant longtemps, nous avons fait des rassemblements à trois ou quatre personnes sur la question de la vidéosurveillance, tout comme la LDH (Ligue des droits de l'homme). Concernant le regroupement familial des populations immigrées sur la base de prélèvements ADN, une grosse mobilisation a eu lieu, tout comme pour EDVIGE. Pour le fichier « base-élèves », il existe une mobilisation importante dans les écoles. Peut-être avons-nous à présent les bases d'un débat de société sur les libertés ? J'aimerais connaître vos positions sur

le sujet. Nous avons tendance à croire que nous ne sommes pas nombreux, mais peut-être s'ouvre-t-il un débat sur les libertés ? Si un nouveau 11 septembre a lieu demain, peut-être ce débat s'ouvrira-t-il plus largement ?

Anastassia Tsoukala : Vous soulevez une question très pertinente : quelle est notre position de citoyens vis-à-vis des valeurs que nous souhaitons voir défendues ? Et par qui souhaitons-nous les voir défendues ? Les Droits de l'homme et les libertés publiques, telles que nous les entendons aujourd'hui, sont assez récents. Cela date du lendemain de la Seconde Guerre mondiale. Il s'agissait d'une réaction face à l'horreur de la guerre, juridique et politique. Celle-ci avait un sens tant que durait la Guerre Froide. Il s'agissait alors d'être crédible vis-à-vis de l'adversaire idéologique. Il fallait, coûte que coûte, que ces droits et libertés publiques fussent, de manière ostensible, respectés et promus au sein des pays occidentaux, puisqu'il fallait convaincre et appâter les autres.

Après 1989, le contexte change. Il ne s'agit plus de guerre idéologique mais de guerre économique. Les Droits de l'homme sont toujours utilisés, comme une carte parmi d'autres, pour mener cette guerre économique avec la Chine, avec la Russie : les puissants d'aujourd'hui. Leur utilité à l'intérieur des pays occidentaux est affaiblie. Elle l'est d'autant plus que nous, citoyens naïfs, nous y avons cru sincèrement. Nous avons créé nos associations de défense des Droits de l'homme, des groupes de juristes qui défendent cela. Mais à l'exécutif, ils veulent que sa part du pouvoir reste limitée. L'exécutif l'a accepté du temps de la guerre froide, mais n'a aucune raison de continuer à l'accepter. Un bras de

fer est aujourd'hui engagé au nom de la protection de la sécurité, de la lutte antiterroriste et de toutes les menaces vagues, multiples et variées qui planent. Ce bras de fer est engagé entre nous et l'exécutif, alors que, cyniquement parlant, l'utilité politique de ces libertés publiques n'est plus aussi évidente qu'elle l'était. Il faut le concevoir ainsi.

Il n'est plus possible d'attendre qu'une seule institution mène la guerre. Il revient à tous de se sensibiliser et de mener la guerre. En France, de manière très empirique, nous avons constaté que le gouvernement au pouvoir ne cherche pas vraiment le conflit. En effet, à chaque levée de boucliers, il recule. Il convient donc de tirer la leçon qu'il ne revient pas à telle ou telle organisation de mener la bataille pour nous, et de nous contenter qu'elle fasse le travail à notre place.

Michel Alberganti : Le fait de supprimer la CNIL ne résoudrait pas tout. Une véritable efficacité pourrait plutôt découler de l'association entre la CNIL et un véritable mouvement populaire.

Jérôme Thorel : Le constat que j'ai dressé tout à l'heure est évidemment radical. Tout à l'heure, a aussi été évoqué le fait qu'il faudrait davantage de débat démocratique, que la biométrie soit abordée au Parlement, que les sénateurs et députés s'imprègnent de ces technologies et fassent des cours de morale sur les risques éventuels. Par exemple, le débat sur la guerre en Afghanistan a-t-il eu lieu à l'Assemblée ? Pendant plusieurs semaines, nous avons entendu qu'il fallait un débat à l'Assemblée. François Fillon a approuvé un débat de trois heures. Il a duré une heure trente et la moitié de l'hémicycle était vide...

Le fichier « base-élèves » a été créé par simple arrêté ministériel du 20 octobre 2008. Il s'agit du premier texte officiel qui régit l'obligation des parents de confier des données personnelles sur leurs enfants dès qu'ils entrent en école maternelle. Pour rappel, l'école est obligatoire à partir de 6 ans. Cet arrêté oblige au fichage dès l'âge de 3 ans. Lorsque les parents refusent, il leur est répondu qu'il est impossible d'accueillir l'enfant. Il paraît complètement aberrant que les parents d'élèves et les quelque 170 directeurs d'école, qui refusent d'entrer dans le fichier, risquent le retrait de salaire et la perte de leur poste. Ils réclament la tenue d'un débat au Parlement. Je le réclame aussi mais je n'y crois pas. Les députés et sénateurs ne vont pas nous apprendre les dangers de la technologie et les mésusages qu'il est possible d'en faire. Je ne suis donc pas optimiste sur le rôle de la représentativité parlementaire dans le fait du respect des libertés. Je vous ai exposé tout à l'heure le cas des lois antiterroristes. Il était demandé de les laisser deux ans, en usage. Or, après deux ans, un amendement les prolonge encore de deux ans. Le rapport prévu pour faire le bilan n'existe pas. Je veux bien que nous continuions à croire en ce système : nous votons, nous élisons des gens.

Sylvia Preuss-Laussinotte nous a montré tout à l'heure un arrêt de la Cour européenne des Droits de l'homme très précis. Au Royaume-Uni, il existe deux Chambres. Deux recours ont donc eu lieu. Cinq ou six tribunaux se sont prononcées et ont refusé de retirer les gens relaxés de ces fichiers ADN. En juillet 2008, un Français a porté plainte à Strasbourg parce que la Cour de cassation lui a refusé, à deux reprises, le droit de refuser ce prélèvement. J'ai aussi du

mal à croire au judiciaire. Nous nous apercevons en effet qu'il faut attendre huit ou dix ans pour que de vieux messieurs-dames, à Strasbourg, protègent nos droits. Or, les juges et les tribunaux sont censés le faire avant. Difficile, donc, d'avoir confiance en tant que citoyen et de croire que nous pouvons être défendus par d'autres.

Michel Alberganti : Il se trouve que les hommes politiques ne sont pas très friands des occasions de s'exprimer sur le sujet, à l'évidence. Cela renforcerait plutôt votre crainte que la représentation parlementaire ne soit pas à la hauteur. Concernant le débat politique, nous pouvons constater qu'il a été absent : la sécurité et ces notions que nous abordons aujourd'hui ont été absentes des débats politiques, nationaux et locaux. Comme si c'était une chose acquise, ne faisant pas débat dans la population.

Anastassia Tsoukala : Au contraire, tous ont été présents, en alimentant explicitement ou implicitement la justification de ce qui se passe aujourd'hui. S'il n'existe pas suffisamment de réactions de la part de la société civile, cela est dû à la mise en place d'un discours dominant, hégémonique, dans la presse française – toutes tendances politiques confondues –, et je me réfère surtout à la presse dite « de qualité ». La liberté vis-à-vis de la sécurité a été mise dans une logique de fausse opposition, comme s'il s'agissait de valeurs sociales opposées, d'après la règle élémentaire du droit que, lorsque nous avons deux valeurs sociales opposées et égales, l'une des deux doit être sacrifiée au profit de l'autre. Or, la liberté n'est pas une valeur sociale. Il s'agit de la base même de l'existence d'un régime démocratique. Elle en est la quintessence. Il ne s'agit pas d'une

valeur comme « ma liberté d'expression », « ma liberté de manifester » : ce sont des émanations, non des droits absolus. Mais la liberté en tant que concept n'est pas négociable. Si nous la limitons, nous limitons la démocratie : une inversion de la définition même de la liberté. J'ai bien analysé les discours médiatiques dans les presses françaises, anglaises, italiennes. La liberté qui y est défendue et protégée n'est pas notre liberté d'agir librement dans un régime démocratique en tant que citoyen ; il s'agit de la libération d'une peur, d'une menace. Il nous est dit : « Nous allons vous protéger pour que vous soyez libérés de la menace. » En d'autres termes : « non pas pour que vous soyez capables d'agir librement ». Le discours sur la liberté est donc devenu un discours sur la sécurité. Ainsi, Daniel Vaillant¹¹ estimait que la sécurité est la condition première de l'exercice de la liberté. Il n'a pas été contredit, hormis quelques réactions timides de la part des Verts. Le reste de la classe politique n'a pas réagi. Toutes tendances confondues, les dirigeants défendent leur part du pouvoir. Ils cherchent à récupérer cette part du pouvoir qu'ils avaient cédée au nom des Droits de l'homme. Or, cyniquement parlant, tôt ou tard, socialistes ou élus de droite reviennent au pouvoir.

Jérôme Thorel : Même ceux qui n'auront aucune chance de se retrouver un jour au pouvoir n'ont pas beaucoup réagi, à l'extrême gauche, par exemple.

Anastassia Tsoukala : C'est très inquiétant. Voilà qui m'amène à m'interroger sur l'utilité des Droits de l'homme dans les sociétés occidentales, depuis qu'elles ont été créées à la sortie de la Seconde Guerre mondiale

et telles que nous les connaissons. Sommes-nous dans une logique de mythe fondateur ? Nous nous sommes accrochés à ces idées, après les horreurs que nous avons commises, par besoin de créer des mythes. Nous refusons de voir la réalité.

Vincent Dufief : Je persiste à penser qu'une liberté s'use quand on ne s'en sert pas. En matière de vie privée, les gens divulguent de plus en plus de données et sacrifient, eux-mêmes, cette liberté. Ils contribuent à l'affaiblissement de cette liberté. Si je divulgue quelque chose me concernant dans la presse, sitôt qu'elle est publique, je ne peux plus attaquer pour atteinte à la vie privée. Je ne suis pas un expert en sociologie, mais j'ai tendance à penser que nous assistons à l'émergence d'une tendance collective des citoyens à mettre de côté cette liberté. Si j'étais ministre de l'Intérieur, observant que les gens ne sont pas si attachés à leur liberté, peut-être en profiterais-je pour faire passer des réformes telles que le fichier EDVIGE. Je ne suis pas ici pour défendre ce fichier ; je le trouve très critiquable. Je pense simplement que ces fichiers sont à l'image de notre société. Et si quelque chose d'aussi considérable qu'EDVIGE a pu être proposé, c'est précisément parce que le gouvernement s'est dit que l'opinion publique était prête et qu'il était possible d'agir.

Anastassia Tsoukala : L'opinion publique l'a su parce que des syndicats de policiers homosexuels ont réagi. Sans cela, nous n'en aurions rien su du tout.

Vincent Dufief : Le fichier EDVIGE est sorti le 25 juin 2008. Les vraies réactions se sont fait sentir aux mois de septembre et octobre.

Jérôme Thorel : Non. Le 1^{er} juillet, un premier communiqué a été publié. La pétition était en ligne le 2 juillet.

Michel Alberganti : Nous allons recueillir quelques questions, car beaucoup de mains se lèvent.

Public : Je souhaite faire une remarque. Lors de la Seconde Guerre mondiale, la République française a, par le biais de ses préfectures, établi ses fichiers, son recensement des populations étrangères, sa livraison des populations. Il s'agit d'un État rationnel, sensiblement le même que celui d'aujourd'hui. Il existe deux générations d'écart. Permettez-moi un avis personnel : je suis surpris par la facilité d'un retour en arrière, d'un renversement culturel. Nos États européens ont rationnellement organisé l'élimination massive de certaines populations. Il est tout de même surprenant que nous en arrivions si vite à de tels renversements. Pour parler de l'aspect européen des choses, nous pouvons féliciter la Cour européenne des Droits de l'homme ou la Cour européenne de justice. M. Thorel, avez-vous songé organiser des *Big Brother Awards* à l'échelle européenne ? Avez-vous des contacts à l'échelle européenne, à Bruxelles ? Comment se passe la mise en place de la société civile européenne, la sensibilisation aux élites européennes des administrateurs ou de ceux qui négocient au niveau de chacun des États-nations ? Existe-t-il un espoir de ce côté ?

Jérôme Thorel : *Privacy International* est une organisation britannique qui a des antennes à Washington et des antennes informelles, telles que la nôtre, dans plusieurs pays d'Europe. Nous sommes une quinzaine de

pays dans le monde. Nous avons chacun nos critères de sélection, mais travaillons généralement de la même manière. Voici deux ans, a été organisé un *Big Brother Awards* global, avec des nominés de tous les pays. Cela n'a pas été très convaincant, car revenaient toujours Poutine, la Chine, etc. À noter malgré tout, l'attribution d'un prix à Tony Blair, avant qu'il ne quitte le pouvoir. Nous avons eu l'initiative, voici trois ou quatre ans, de créer une catégorie de sélection centrée sur l'Europe, le prix Orwell « Union européenne ». Il s'agit de la catégorie où nous avons eu le plus de travail, mais nous n'avons pas les moyens de traiter cela. Nous avons publié un livre¹² en octobre 2008, qui est promu sur notre [site](#). Nous sommes cinq auteurs¹³, qui avons travaillé sur les origines des lois liberticides en France. Nous nous rendons compte que cela fonctionne bien entre Bruxelles, Strasbourg et Paris. Généralement, en France, pour passer une loi liberticide, nous nous inspirons beaucoup de ce qui se fait à Bruxelles, et *vice versa*. Cet alibi, qui consiste à dire qu'il faut que nous légiférions parce que cela se fait ailleurs, fonctionne très bien. Tout cela est lié, puisque nous sommes obligés d'appliquer les directives européennes. Mais, parfois, dans un pays, cela peut aller plus loin.

Michel Alberganti : Dans le cas du nombre de doigts sur le passeport biométrique, la France est allée plus loin que la demande européenne. Une autre question ?

Public : Derrière toutes ces actions, qui ont pur but de mettre en fiche et de surveiller, nous nous apercevons que l'un des enjeux majeurs n'est pas d'ordre philosophique, mais économique. Dans le cas de

la vidéosurveillance, les budgets en jeu sont très importants. Nous ne pouvons évaluer ce que cela apporte, mais nous savons que cela coûte très cher. Et de nombreuses personnes s'enrichissent. Il en va de même pour toutes les technologies développées. Finalement, ne serait-il pas possible d'accepter l'idée que nous sommes face à un rouleau compresseur, qui ira au bout de sa course, parce que les enjeux économiques sont tels qu'il est impossible de s'y opposer ? Ne pouvons-nous pas opérer un glissement sémantique, et considérer que nous nous inscrivons, davantage que dans des problématiques philosophiques liées aux Droits de l'homme, dans un questionnement déontologique ? Cela induirait, après la mise en place des outils, d'appliquer une déontologie.

Je pose une question qui n'est pas innocente. J'avais saisi la CNIL au sujet des bornes biométriques. Dans ma fonction de correspondant informatique et libertés, j'ai pu approcher des personnels de la CNIL et leur poser la question directement. Je rebondis sur ce que disait Maître Dufief. Du point de vue du droit, la CNIL considère que la finalité de ce dispositif était économique. Distribuer des cartes, qu'il est possible de perdre et qui passent plus vite en caisse, est plus rentable. Il existe un enjeu soi-disant économique. La CNIL dit également que, de toute façon, la donnée biométrique est obsolète d'une année sur l'autre, puisque l'enfant grandit et que l'empreinte de la main n'est plus la même. Or, cela n'est pas si simple. En effet, au-delà de l'aspect économique, s'opère un conditionnement des jeunes à accepter ces mesures de surveillance et de contrôle. Cela est très grave. Sur ce point, la CNIL me donne raison et elle a convoqué un comité d'éthique et de

déontologie pour réfléchir au sujet. Mais elle estime que ce n'est pas son travail ; lequel consiste à évaluer un dispositif par rapport à la loi. J'ignore si la CNIL est utile ou pas, et s'il faut la faire disparaître ou pas. Toujours est-il qu'elle dit clairement que son travail ne porte pas sur la déontologie mais sur la loi. Ne sommes-nous pas confrontés à des enjeux sociétaux, presque philosophiques ? N'est-il pas possible d'évoluer vers une prise en considération de la déontologie. Car la déontologie nous ramène à la sphère marchande : l'artisan, etc.

Jérôme Thorel : Pour moi, la déontologie est comme l'autorégulation des marchés financiers. Cela est aussi peu crédible. Un chef d'entreprise sera déontologue quand cela l'arrangera seulement. C'est comme demander à *Lehman Brothers* de réguler ses produits toxiques.

Anastassia Tsoukala : Il ne faut pas dépolitiser pour autant. Il existe une articulation entre l'économie/financier et le politique. Il ne faut pas oublier le politique. Laurent Bonelli a souligné le fait qu'en l'absence de capacité d'intervention dans les domaines majeurs de la vie sociale, dans le contexte de la mondialisation et des transferts de compétences nationales vers le niveau communautaire, le politicien national ne peut que se replier sur tout ce qui se réfère à la sécurité. Qu'a-t-il d'autre à dire à son électorat ? Lorsqu'il invite à voter pour lui, que propose-t-il de faire ? Il ne lui reste plus grand-chose, hormis tout ce qui se réfère à la sécurité. Voilà tout ce qu'il peut promettre.

Je suis tout à fait d'accord avec vous sur les questions de déontologie, d'économie et de finance. Mais, politiquement, il s'agit aussi d'une

question de crédibilité de la classe politique et de souveraineté nationale. Il s'agit de questions majeures dans la manière dont délibère un homme politique.

Public : Il me semblait que la protection des Droits de l'homme, que vous sollicitez est, par nature, défensive face à « *Big Brother* ». Même l'aspect ironique des *Big Brother Awards* est relativement peu efficace, de même que la protection juridique, qui arrive avec parfois dix ans de retard. La démocratie a une origine. Des révolutions ont été faites pour que l'argent public ne soit plus dépensé n'importe comment. Je me demande si la suggestion de Mme Tsoukala n'est pas une voie possible : l'évaluation des politiques. N'existe-t-il pas une voie possible, presque de façon préventive ou du moins à très brève échéance, pour contrôler des politiques ? En effet, rapporté à l'objectif, l'inefficacité est avérée. Cela serait un moyen d'arrêter les politiques, sans attendre dix ans.

Jérôme Thorel : À qui reviendrait-il d'évaluer ces politiques ? À M. Besson ? J'approuve l'idée, mais il faudrait que les instances existant aujourd'hui, acceptent d'être évaluées. Si M. Besson évalue les politiques de M. Sarkozy, nous avons du mal à imaginer la conséquence pratique sur les citoyens. S'il est question d'auto-régulation ou d'auto-évaluation, il faudrait une instance supranationale pour, préventivement, statuer que telle loi créera des problèmes et inviter à ne pas la voter.

Public : Dans l'exemple que citait Mme Tsoukala du nouveau fichier européen, s'il n'existe aucune estimation d'un gain, cela ne devrait même pas exister.

Jérôme Thorel : Pourtant, cela existe.

Anastassia Tsoukala : Vous vous référez à une rationalité idéale des politiques publiques. Elles sont rationnelles, mais obéissent à des critères autres que la rationalité à laquelle vous faites allusion. Tout l'écart est là. Lesdits critères ne vont pas être proclamés, car ils ne sont pas toujours très nobles.

Cependant, il ne faut pas être alarmiste. Personnellement, j'assume pleinement mon retard en tant qu'universitaire, pour une raison simple. J'analyse beaucoup les discours médiatiques. Pour analyser, il faut qu'ils existent. Il existe donc un retard dans le temps. Par ailleurs, j'enseigne, je fais de la recherche, j'ai une maison que j'entretiens, j'ai une vie sociale que je maintiens, une vie personnelle, etc. En face, existent des groupes d'individus, de vrais professionnels de la communication et de trouvailles conceptuelles. J'ai du mal à l'admettre, mais ces personnes sont aussi intelligentes que moi, sinon plus. Il peut être long le temps que le fruit de leur pensée devienne visible, le temps que nous comprenions de quoi il s'agit, que nous prenions connaissance des enjeux qui, parfois, sont opaques. Lire des rapports, cela prend du temps. Il s'agit ensuite de comprendre de quoi il s'agit, d'analyser et produire le résultat de l'analyse. Nous avons du retard. Si nous considérons cela à court terme, c'est inquiétant. Je reprends une des expressions favorites du commissaire divisionnaire : le « balancier ». À moyen terme ou à long terme, si nous réagissons, nous finirons par rétablir un certain équilibre. Nous pouvons continuer en gardant à l'esprit qu'il faut toujours être vigilant. Sinon, il faut être très alarmé et inquiet.

Michel Alberganti : Un des espoirs peut venir de ce commissaire qui dit : « Les choses s'arrêteront lorsque les gens en auront marre. » Ce « balancier » sera alors bloqué par la résistance des gens. La balle est dans notre camp, puisque nous faisons partie des « gens ». Cela prouve que rien n'est gravé dans le marbre. Plusieurs signes laissent entendre qu'une réaction émerge. Le fichier EDVIGE en est un exemple. Lorsqu'une réaction se produit, les choses se passent différemment que lorsqu'il ne s'en produit pas.

Public : Normalement, nous devrions compter sur l'Assemblée nationale pour défendre cela. Mais où sont les élus du peuple ? Ne sont-ils pas devenus des élus des *lobbies* ?

Michel Alberganti : Comme je l'ai dit plusieurs fois, nous avons invité des hommes politiques, qui ne sont pas venus.

Public : Il faut alors dissoudre l'Assemblée nationale ! Quelque chose à la base fonctionne mal. Je considère qu'il ne faut plus voter lors des élections législatives.

Michel Alberganti : Si personne ne votait, plus personne ne siègerait à l'Assemblée nationale, donc le problème ne serait pas résolu.

Public : S'ils ne sont plus élus que par 5 % de la population, ils n'ont plus de justification.

Public : Il me semble que tout repose sur le mythe de l'efficacité. Comme les sociétés sont en bout de course, économiquement et politiquement, l'efficacité doit les justifier. Je voudrais faire remarquer également que l'État n'est pas le seul à recourir à la

surveillance. Citons la RATP, avec le passe Navigo. La région parisienne compte quelque 12 millions d'habitants ; 75 % acceptent ce passe qui suit leurs traces.

Michel Alberganti : La RATP n'est pas une entreprise privée.

Public : Oui, mais il ne s'agit pas du gouvernement.

Michel Alberganti : Elle dépend quand même de l'État. Il s'agit du STIF¹⁴.

Vincent Dufief : Je souscris totalement à ce que vous dites. Je pense qu'il ne faut pas se tromper d'ennemi. Il est vrai que les sociétés privées, les autorités et sociétés non gouvernementales, disposent d'une masse de données qui pourront se retrouver un jour dans l'escarcelle du gouvernement. J'ai assisté à diverses enquêtes policières. Il existe la réquisition judiciaire ou une commission rogatoire. En tant que juge, je vais voir n'importe quelle société et je saisis la totalité de ses fichiers. N'importe quel OPJ¹⁵ ou, dans le cadre d'une commission rogatoire : n'importe quel juge d'instruction, peut avoir accès à toutes les données qu'une entreprise stocke.

Jérôme Thorel : Voilà pourquoi il leur est demandé de ne stocker que sur 6 ou 12 mois.

Michel Alberganti : Aux États-Unis, depuis juillet 2008, les autorités américaines ont le droit de saisir n'importe quelle donnée numérique traversant leur frontière, sans aucune justification ni suspicion particulière. Par simple décision de la personne se trouvant à la douane, votre disque dur d'ordinateur peut être saisi, copié,

sans justification. Ce n'est pas une commission rogatoire. Il ne s'agit pas de quelque chose de spécial, encadré par la justice. Il s'agit d'une règle appliquée depuis le mois de juillet aux États-Unis. En général, l'Angleterre suit assez rapidement les États-Unis.

Anastassia Tsoukala : Puis nous suivons assez rapidement l'Angleterre.

Michel Alberganti : Cela pose énormément problème aux entreprises dont les cadres voyagent et qui vont se retrouver devant la possibilité de voir l'État américain au courant de tous les secrets de ces entreprises, parfois engagées dans des marchés et des offres internationales importantes.

Vincent Dufief : Il existe le *Blocking Statute*¹⁶, qui est une loi permettant de refuser de communiquer aux Américains des documents d'ordre stratégique français.

Michel Alberganti : Apparemment, ce n'est plus valable aux frontières.

Vincent Dufief : Je n'ai jamais connu le cas, mais, dans les procédures de « *discovery* »¹⁷, la filiale peut s'opposer au transfert de données. Nous atteignons une distinction, entre le renseignement et l'investigation. Dans le cadre d'une investigation policière, il existe un cadre légal, des limites, des frontières que je connais et arrive à apprécier. Quand il s'agit de renseignement, je suis incapable de vous répondre sur leurs limites. Il s'agit d'ailleurs de la question du fichier CRISTINA. EDVIGE est une chose et CRISTINA en est une autre, tout comme l'ancien fichier des RG.

Je veux bien défendre, jusqu'à une certaine limite, la surveillance. Mais quand nous arrivons à des zones de

non-droit, floues, où il n'existe aucun texte, je m'interroge. Et je n'ai aucune réponse car je les tire uniquement des textes. Or, je n'ai pas de texte, ou bien il s'agit de textes couverts par le « secret défense », auxquels je n'ai donc pas accès.

Anastassia Tsoukala : Que faites-vous en cas de texte très rassurant mais néanmoins flou ? Que faites-vous de la peine de rétention de sûreté ? Au nom d'un soupçon établi par des experts, nous pouvons maintenir en détention une personne après sa peine initiale effectuée. Il existe un texte. Sur le plan juridique, tout est parfait. Il en va de même pour les supporters de football. Il existe la loi du 23 janvier 2006¹⁸, qui autorise les préfets à interdire aux supporters l'entrée du stade, en contournant le juge. Ces personnes sont fichées pendant 5 ans, à leur insu le plus souvent, au nom d'un soupçon en général, pour un comportement vaguement interprété comme potentiellement dangereux. Pour ne rien vous cacher, ces lois m'effraient, moi qui suis juriste comme vous.

Vincent Dufief : Mais elles ont quand même le mérite d'exister. La rétention est une chose ; la détention provisoire en est une autre. Nous pouvons les contester. Je les conteste quotidiennement. Je n'ai jamais eu à apprécier le texte sur la rétention. Mais, concernant la détention provisoire, il existe des critères qui peuvent être contestés devant une juridiction.

Anastassia Tsoukala : Ne comparons pas l'incomparable. La détention provisoire est une chose prévue dans toutes les juridictions du monde. La rétention est une exception française, du moins en Europe.

Public : Je suis inquiet. Je comparerai ces données à un dossier médical, que je n'ai pas le droit de consulter. Beaucoup de choses sont écrites sur moi, auxquelles je ne peux accéder. Avons-nous des moyens pour consulter les données qu'ont les autres sur nous-mêmes ? Il serait quand même bon de savoir ce qu'il sera fait de ces données et si nous avons donné l'autorisation d'en disposer. Par un exemple, à mon travail, des photos ont été prises. Il a été demandé aux gens de signer une autorisation d'utiliser celles-ci. Existe-t-il des moyens d'agir ? Cela me fait peur qu'un fou puisse acheter à une entreprise des données sur moi et les utiliser à sa guise.

Vincent Dufief : La loi informatique et libertés a été récemment modifiée (en 2004). Vous avez le droit d'accéder à vos données. Vous avez un droit de rectification permettant de modifier ou retirer toute information contenue sur vous dans un fichier. Cependant, nous nous posons la question de l'effectivité de ces lois qui sont purement théoriques.

Vous travaillez pour une entreprise française. Je m'inquiète au sujet des réseaux sociaux comme *Facebook* où les données sont à la disposition d'un site américain. Je vous mets au défi de faire jouer vos droits d'accès ou de rectification sur *Facebook*, car la loi informatique et libertés française (du 6 janvier 1978) prévoit qu'elle s'applique uniquement aux fichiers dont un serveur ou une société a un représentant sur le territoire. *Facebook* n'a ni représentant ni serveur en France. La loi de 1978, contrairement à ce que dit mollement la CNIL, ne s'applique pas à *Facebook*.

Une question d'effectivité et de compétence de la CNIL se pose. Vous faites une réclamation auprès de la CNIL : au cas où votre employeur ne respecte pas ce droit d'accès, celle-ci va-t-elle donner suite ? Elle le peut ; elle a des pouvoirs de sanction financière. Elle peut également transmettre au parquet. Si la société ne respecte pas vos droits d'accès, elle peut transmettre au parquet, qui peut engager des poursuites judiciaires et sanctionner pénalement. Si la société vous dit avoir effacé votre fiche et vos photos et ne l'a pas fait, elle peut se faire contrôler. En effet, la CNIL, depuis 2004, a un pouvoir de contrôle sur place. Ces agents peuvent débarquer à n'importe quel moment dans votre société, contrôler les fichiers et vérifier si vos droits ont été respectés ou pas. Maintenant se pose la question des moyens financiers concrets dont dispose la CNIL.

Michel Alberganti : Le problème se pose pour le STIC, avec un droit d'accès indirect passant par la CNIL. Le délai d'attente est d'un an, voire plus, pour accéder à des données concernant chacun d'entre nous : données contenues dans le STIC dans lequel il existe 25 % d'erreur minimum. Cela représente un exemple typique de l'inaction du public. Si le public – même une fraction infime – faisait appel au droit d'accès indirect de la CNIL, elle serait incapable de répondre, submergée. Si la CNIL était submergée, elle pourrait demander des moyens supplémentaires. Le fait de ne pas l'être, alors qu'elle a des moyens ridicules pour répondre à cette demande, montre qu'il n'existe aucune attente du public. Dans ce cas, il n'existe aucune raison d'augmenter les moyens de la CNIL. Une action publique très simple existe : il suffit de demander

l'accès aux données personnelles nous concernant. Cependant, je dis cela, mais je ne l'ai pas fait moi-même !

Vincent Dufief : L'organisme concerné par le droit d'accès indirect ne sera pas obligé de s'y plier. L'organisme peut vous répondre que vous figurez dans le fichier, sans vous dire pourquoi en raison de sécurité nationale.

Michel Alberganti : Dans ce cas, il n'est pas possible de corriger les erreurs, si elles existent.

Vincent Dufief : Non, il s'agirait d'une fin de non-recevoir, voire « secret défense ». Dans ce cas, votre droit d'accès ne vous sert à rien.

Anastassia Tsoukala : S'il s'agit d'une enquête judiciaire en cours, il ne vous sera pas dit si vous êtes fichés parce que vous êtes suspectés d'avoir commis un crime ou un délit. Là également, il n'existe pas d'automatisme.

Michel Alberganti : C'est compliqué. Il peut exister jusqu'à 25 % d'erreurs dans ces fichiers. Celles-ci peuvent avoir un impact sur une enquête de police ou une situation délicate. Il est fâcheux de ne pouvoir accéder à ces données pour participer à la correction de ces erreurs.

Jérôme Thorel : Je suis persuadé que ceux qui font une demande d'accès à ce fichier figurent dans un autre fichier.

Public : J'ai lu qu'il existait un précédent en Allemagne en matière de rétention. Paraît-il, le gouvernement nazi, dans les années 1930, aurait institué, pour la première fois, ce genre de décret visant les opposants allemands. Au Rwanda, d'autre part, avant 1994,

la carte d'identité instaurée au temps du colonialisme belge, indiquait l'origine ethnique, ce qui aurait favorisé le génocide des Tutsis. Qu'en est-il ?

Anastassia Tsoukala : Je peux confirmer la deuxième information. Mais concernant la première, je ne sais pas.

Jérôme Thorel : Je ne peux pas répondre avec certitude, mais il me semble qu'il existe une directive similaire en Allemagne. Cela avait été un argument pour le gouvernement, pour dire que ce n'était pas grave. Il faudrait vérifier cela, mais le syndicat de la magistrature avait alors diffusé des documents.

Ces technologies nouvelles sont utilisées d'une façon dangereuse, car si un jour un dictateur est au pouvoir, cela peut se retourner contre nous. Pour le moment, cela sert l'économie, génère de l'argent mais, fondamentalement, à qui cela profite-t-il ? Nous avons l'impression que nous sommes face à une monstruosité bureaucratique qui dépasse le cadre des nations.

Jérôme Thorel : Cela a été évoqué tout à l'heure. Quand un homme politique veut se faire réélire, il jongle avec les notions de sécurité et de liberté. Nous avons du mal à trouver au sein des partis républicains un réel clivage. Sur ces questions de sécurité, la droite et la gauche s'équivalent. Tous ces gens ont trouvé dans ces thèmes un moyen d'asseoir leur domination.

Michel Alberganti : Dans ce cas, le crime profite au pouvoir.

Anastassia Tsoukala : Tout en partageant cet avis, je voudrais aborder un autre aspect, lié au fait que nous

nous sentons tous – politiciens inclus – dépassés par les événements. Nous sommes en pleine transition. Tous nos points de repère habituels, autour desquels nous nous étions construits depuis le XIX^e siècle, volent en éclats : qu'il s'agisse de l'État-providence ou de la stabilité de notre vie, etc. Nous sommes dans la postmodernité : tout est fluide, rien n'est stable. Tout devient source de menace, d'insécurité.

Avant d'être un politicien, il y a un homme, et un homme stressé. L'Europe a traversé, toutes proportions gardées, une période analogue à l'époque victorienne. Nous pensons que ce qui nous arrive est neuf – la communication par exemple –. À cette époque, les hommes ont découvert la poste, qui a permis de communiquer. Ils ont découvert le train, qui simplifia les déplacements. Ils commençaient à fréquenter les écoles, pouvaient écrire et lire. Ils ont découvert le téléphone, la presse, etc. Ces révolutions les ont effrayés, tout comme les révolutions technologiques auxquelles nous assistons nous effraient. Ils ont eu les mêmes réactions. Nous ne faisons que reproduire le même processus, plus d'un siècle plus tard. Et, finalement, lorsque la grande phase de transition et de bouleversement des repères a pris fin, nous avons rétabli un nouvel ordre et avons créé l'État-providence. Nous avons reconfiguré l'espace politique, social et économique pour créer un nouvel ordre. Tant que ce nouvel ordre n'est pas visible, nous sommes en pleine ébullition.

Intervenant hors micro : Anastassia, deux guerres mondiales ont eu lieu ; il existait des empires coloniaux. Ce n'étaient pas les mêmes conditions, tout de même.

Anastassia Tsoukala : Je parle simplement des grands bouleversements technologiques auxquels nous assistons et de l'idée de perte de contrôle sur les choses. Les guerres mondiales, nous les avons déclenchées nous-mêmes. Elles ne nous ont pas effrayés parce que nous en étions partie prenante. Cela n'est pas la même chose d'être citoyen et de subir la presse qui, tout d'un coup, apparaît, comme le téléphone, le train, etc. Une guerre commence puis cesse.

Michel Alberganti : Nous allons nous en tenir là, car nous sommes au bord du risque d'égarement. Merci à tous d'avoir tenu jusque-là !

Notes

* Ancien journaliste au *Monde*, producteur de l'émission « Science Publique » sur France Culture et écrivain français. ↑

1. Système qui consiste à insérer des puces électroniques dans les cartes d'embarquement des passagers, afin de les localiser. ↑

2. Maître de conférences habilitée à diriger des recherches. ↑

3. Moment où sont décernés des prix à ceux qui ont bien développé l'aspect « *Big Brother* » dans la société, à travers des applications ou des prises de position. ↑

4. Avocat au barreau de Paris, spécialisé en droit pénal des nouvelles technologies et en droit de la vie privée. Il s'est beaucoup intéressé aux réseaux sociaux, entre autres. ↑

5. Sénateur du Nord (Nord-Pas-de-Calais). [[informations supplémentaires](#)] ↑

6. Direction de la surveillance du territoire, chargée du contre-espionnage, de la lutte antiterroriste et de la protection du patrimoine économique et scientifique français. Depuis le 1^{er} juillet 2008, ce service de renseignements a fusionné avec la Direction des renseignements généraux, donnant naissance à la Direction centrale du renseignement intérieur. ↑

7. Membre de l'association *Privacy International*, qui organise un événement assez connu, les *Big Brother Awards*, où sont décernés des prix à ceux qui ont bien développé l'aspect « *Big Brother* » dans la société, à travers des applications ou des prises de position. ↑

8. Direction centrale du renseignement intérieur. ↑

9. Loi n° 2007-297 du 5 mars 2007. [voir [texte de loi](#)] ↑

10. Voir [article](#) sur le site *Big Brother Awards*. ↑

11. Homme politique français, député de Paris, ministre des Relations avec le Parlement de 1997 à 2000 et ministre de l'Intérieur de 2000 à 2002 (gouvernements de Lionel Jospin). ↑

12. *Big Brother Awards : les surveillants surveillés*, éditions Zones/La Découverte, 2008. ↑

13. Jean-Pierre GARNIER, Jean-Marc MANACH, Anne-Lise MARTENOT, Jérôme THOREL et Christine TREGUIER. ↑

14. Syndicat des transports d'Île-de-France, qui est l'émanation des collectivités locales (présidé par le président de la région Île-de-France notamment). ↑

15. Officiers de police judiciaire: fonctionnaires nommés dans l'article 16 du Code de procédure pénale. ↑

16. Texte qui interdit à toute personne, sous peine de 6 mois d'emprisonnement et/ou 18 000 euros d'amende « de communiquer par écrit, oralement ou sous toute autre forme, en quelque lieu que ce soit, à des autorités publiques étrangères, les documents ou renseignements d'ordre économique, commercial, industriel, financier ou technique tendant à la constitution de preuves, en vue de procédures judiciaires ou administratives étrangères ou dans le cadre de celles-ci » (article 1^{er} de la loi n°68-678 du 26 juillet 1968, modifiée par la loi n° 80-538 du 16 juillet 1980). [[informations supplémentaires](#)] ↑

17. Les Américains viennent faire des investigations en France sur des sociétés américaines. ↑

18. Loi n° 2006-64 relative à la lutte contre le terrorisme et portant des dispositions diverses sur la sécurité dont l'interdiction administrative de stade. [voir [Texte de loi](#)] ↑