
MEDIAPART

<http://www.mediapart.fr/journal/france/070209/pierre-piazza-le-mythe-de-l-infaillibilite-technique>

Pierre Piazza: «Le mythe de l'infaillibilité» technique

Mis en ligne 7 février 2009 Pierre Piazza est maître de conférence en science politique. Il est aussi l'auteur remarqué de plusieurs ouvrages sur l'identification des individus. Pour Mediapart, il revient sur le taux d'erreurs astronomique dans certains fichiers de police, sur l'histoire du fichage à la française et sur l'évolution de la police, de plus en plus technique et scientifique.

La CNIL vient de rendre un [rapport préoccupant](#) sur l'usage du Système de traitement des infractions constatées (STIC). Erreurs de saisie en nombre, approximations, effacements prévus par la loi qui ne sont pas effectués (en cas de non lieu, classements sans suite, acquittements, ou requalifications pénales), «utilisations anormales» de cet énorme fichier auquel 100.000 fonctionnaires peuvent accéder et qui donne lieu à 20 millions de consultations par an, et on en passe. Que vous inspire ce bilan?

Ce bilan n'a rien de surprenant. C'est une confirmation des précédents constats qui, dressés par la CNIL depuis 2001, l'avaient déjà amenée à réclamer, dans une proportion dépassant le plus souvent 30% des dossiers vérifiés, des mises à jour ou la suppression d'informations erronées et injustifiées concernant les personnes inscrites dans ce fichier. Ce phénomène est à la source de sérieux problèmes: atteinte à la vie privée, au droit à l'oubli, à la présomption d'innocence, etc. Ces dysfonctionnements résultent en grande partie de la spécificité de la procédure de recueil des données. Ce fichier est alimenté en amont du procès-verbal et sans aucune intervention de l'autorité judiciaire. De ce fait, peuvent subsister dans le STIC des informations inexactes ou n'ayant pas été suffisamment vérifiées, ce qui peut dans bien des cas porter préjudice aux personnes concernées.

On évalue à un million, [le nombre de personnes qui n'aurait pas pu accéder à un travail à cause du Stic](#). C'est dire l'ampleur du fichier. Or, les «révélations» de la Cnil n'ont pas soulevé un émoi au-delà des cercles habituels (chercheurs, associations). Pourquoi une telle indifférence selon vous?

En effet, ce nouveau rapport de la CNIL rappelle une fois de plus que les désagréments occasionnés aux individus victimes des erreurs du STIC ont été tout particulièrement amplifiés par la décision autorisant la consultation de ce fichier de police judiciaire dans le cadre d'enquêtes administratives de moralité. Prévue par la loi du 15 novembre 2001, cette disposition a été élargie par la loi du 18 mars 2003 (notamment aux instruction des demandes d'acquisition de la nationalité française) et par un décret du 6 septembre 2005 (pour les enquêtes administratives préalables aux recrutements, affectations, autorisation, agréments, habilitations qui concernent les emplois publics participant à l'exercice des missions de souveraineté de l'État). En raison du nouveau rôle qui lui a ainsi été conféré, le STIC s'est vite transformé en un instrument de discrimination à l'emploi. Une seule «mention» dans ce fichier (même occasionnée par des infractions mineures) a, la plupart du temps, motivé le classement d'une multitude d'enquêtes administratives dans la catégorie «défavorable» et engendré soit le licenciement des personnes concernées, soit un refus d'embauche.

En la matière, la CNIL avait déjà souhaité, il y a maintenant plusieurs années, que les individus soient mieux protégés face à ces risques sérieux d'exclusion et d'injustice sociale. Elle avait notamment demandé à ce que les services préfectoraux se déterminent, dans le cadre des enquêtes administratives qu'ils diligentent, aux vues du contenu du bulletin n° 2 du Casier judiciaire mentionnant les condamnations dont font l'objet les personnes. Cette réforme n'a toujours pas abouti. D'ailleurs, si on lit attentivement le deuxième rapport du Groupe de contrôle des fichiers de police et de gendarmerie nationales intitulé «Mieux contrôler la mise en œuvre des dispositifs pour mieux protéger les libertés» qui a été rendu public en décembre 2008, on s'aperçoit aussi que la plupart des recommandations formulées deux ans plus tôt par ce même groupe pour améliorer le fonctionnement des fichiers de police sont restées lettre morte.

Mais sur l'indifférence? Je pense qu'elle résulte surtout d'un déficit d'information des citoyens sur cette question et plus généralement sur les nombreux problèmes que pose actuellement l'essor considérable d'une multitude de dispositifs technologiques potentiellement liberticides qui permettent aux acteurs en charge des questions de sécurité d'identifier mais aussi de tracer et de profiler les personnes. L'opposition politique serait bien inspirée de demander à ce que soient organisés sur cet enjeu crucial de véritables débats démocratiques transparents car on constate en particulier que sont désormais de plus en plus institués et utilisés de tels dispositifs à l'échelon supranational sans que n'ait été mis en place un cadre commun, cohérent et adéquat permettant de garantir l'effectivité d'un niveau élevé de protection des données.

« Le nombre d'erreurs engendrées par ces techniques dépend d'une multitude de facteurs »

Précisément, l'actuelle ministre de l'intérieur a une formule, qu'elle répète à l'envi: elle veut une «police technique et scientifique pour tous». En un mot, que les méthodes de la PTS soient appliquées pour la moindre affaire. Est-ce raisonnable? Est ce raisonné selon vous?

La politique de Michèle Alliot-Marie s'inscrit dans la continuité d'un processus enclenché à partir de 1995: le déploiement à Paris de la police technique et scientifique de proximité qui était destiné à accroître significativement le volume, et par là même l'efficacité, du Fichier Automatisé des Empreintes Digitales (FAED). Que la police ait remplacé ses anciens fichiers manuels dactyloscopiques par une telle base nationale centralisée d'empreintes digitales ne semble pas illégitime au regard des missions qui lui sont dévolues. Cette base, qui enregistre les empreintes des personnes mises en cause dans une procédure pénale pour crime ou délit et les traces dactyloscopiques relevées sur des scènes d'infraction, permet aux forces de l'ordre de résoudre certaines affaires en détectant notamment plus aisément les cas de variation d'état civil (le recours à des identités multiples par des individus s'adonnant à de coupables activités). Toutefois, d'autres choix sont beaucoup plus discutables, comme par exemple celui consistant à étendre très significativement le champ d'application du Fichier National Automatisé des Empreintes Génétiques (FNAEG) en se calquant sur l'option prise notamment par les britanniques. Initialement destiné à la seule identification des auteurs d'infractions sexuelles, ce fichier peut être alimenté, depuis la loi sur la sécurité intérieure de mars 2003, par des génotypages réalisables sur pratiquement tous les individus ayant commis des crimes ou délits d'atteintes aux personnes et aux biens et sur ceux à l'encontre desquels il existe des raisons plausibles de soupçonner qu'ils ont commis un délit ou un crime. La logique n'est ici plus du tout la même. Désormais les empreintes génétiques de personnes (y compris lorsqu'elles sont mineures) ayant perpétré de petites infractions peuvent être relevées et enregistrées pendant une longue période. On s'oriente ainsi progressivement vers un fichage de masse, comme l'atteste la croissance vertigineuse de ce fichier (qui contient désormais près d'un million de profils génétiques d'individus), susceptible à terme de déboucher sur un fichage de l'ensemble de la population. D'ailleurs, au cours de la discussion du projet de loi sur la sécurité intérieure en 2003, certains députés s'étaient déclarés favorables à une telle évolution, même si elle leur semblait à court terme matériellement irréalisable pour des raisons de coût. Ainsi, Jean-Christophe Lagarde avait alors déclaré: «À l'origine, le groupe UDF souhaitait déposer un amendement visant à élargir le FNAEG à l'ensemble de la population et à en faire le fichier d'empreintes digitales du XXI^e siècle (...) Ce serait d'abord un formidable moyen de changer la culture de la police française qui se fonde davantage sur l'aveu que sur la recherche de la preuve pour confondre une personne soupçonnée d'un crime ou d'un délit; dans d'autres pays, les polices privilégient la recherche de la preuve. L'utilisation de cette méthode d'identification génétique permettrait du même coup de mettre fin à nombre de discussions sur les méthodes employées dans certaines enquêtes policières.»

Une chose frappe quand on s'intéresse à la police scientifique, c'est le nombre important d'anomalies, comme par exemple le problème des relevés des empreintes ADN. Parfois leur code barres est incomplet (il manque une partie de l'ADN), soit il est mal pris; soit, pire: il est mal codé. [Dans l'ouvrage collectif La Frénésie sécuritaire](#), vous écrivez que les taux d'erreurs lors de l'enregistrement des données biométriques peuvent atteindre entre «1% et 2% dans le cas de l'iris, qui constitue l'identifiant le plus sûr avec l'empreinte digitale». Ce qui, ramené à un fichier de 60 millions de personnes, concernerait 60.000 à 120.000 personnes. Dès lors, vous parlez de «mythe de l'infaillibilité»?

De nombreuses technologies sont officiellement présentées comme infaillibles. Quand on y regarde de plus près, on constate qu'elles sont loin de revêtir un tel caractère. C'est notamment le cas des identifiants biométriques. Le nombre d'erreurs engendrées par ces techniques dépend d'une multitude de facteurs : les conditions matérielles et humaines de leur mise en oeuvre, les caractéristiques physiques des populations auxquelles elles sont appliquées, l'importance quantitative des catégories de personnes qui y sont soumises (le futur système VIS développé par l'Union Européenne concernera près de 70 millions d'individus!), etc. Avec l'ADN, ce problème se pose aussi et revêt surtout un double aspect. Tout d'abord, la montée en puissance du FNAEG a engendré de sérieuses difficultés de personnel du fait de l'augmentation considérable des saisines de ce fichier. Ce phénomène a occasionné un nombre croissant de «dossiers non-conformes»: c'est-à-dire des formulaires de demande d'inscription ou de simple comparaison incomplets ou imparfaitement renseignés. Ensuite, l'absence de rigueur dans la réalisation des «signalisations» s'avère ici déterminante. C'est ce qu'avait par exemple souligné le député Jean-Patrick Courtois en 2006: «La démarche [...] suppose des agents sur le terrain, en pratique souvent des agents de sécurité publique, une grande maîtrise de la scène d'infraction que les moyens de la police scientifique de proximité ne permettent peut-être pas encore [...] Rien ne sert en effet d'encombrer le FNAEG de traces trouvées sur une scène d'infraction mais n'ayant pas de lien avec celle-ci.»

Désormais, sur certaines scènes de cambriolage classique (maisons, magasins), des fonctionnaires dits «de la police scientifique de proximité» sont dépêchés pour y prélever, non plus de simples empreintes digitales mais aussi génétiques (ADN). Il existe même des expériences d'empreintes liées aux odeurs, [comme on peut le voir dans notre reportage vidéo](#). Tous ces actes s'inscrivent dans une longue histoire de la police à la française (Bertillon, etc) qui rejoint celle que vous avez étudiée (la carte d'identité). Pouvez vous nous rappeler les logiques qui sous-tendent cette histoire?

Concernant spécifiquement l'Identité judiciaire et la police technique et scientifique, un phénomène intéressant mérite d'être souligné. À la fin du XIX^e siècle et au début du XX^e siècle, la France semble en pointe dans ces domaines, notamment grâce au rôle clef joué par des «figures» comme Alphonse Bertillon (à Paris) et Edmond Locard (à Lyon). Les savoirs, les méthodes et les procédures qu'ils développent font alors autorité dans le monde entier. À cette époque, beaucoup de policiers étrangers viennent d'ailleurs se former en France. Par la suite, Vichy apparaît également comme une période importante: une «Police technique» sera institué par ce régime le 27 novembre 1943. Elle comprendra des services régionaux d'Identité judiciaire et quatre laboratoires d'Identité judiciaire (à Toulouse, Lyon, Marseille et Lille). Pour autant, quelques dizaines d'années plus tard, le plan Joxe de modernisation de la police datant de 1985 fustigera l'énorme retard accumulé par notre pays en la matière. Un net basculement s'est donc opéré durant l'après-guerre. La culture policière alors prédominante,

accordant surtout la priorité à la lutte contre les réseaux de stupéfiants et le grand banditisme, explique certainement ce progressif déclin des services d'identité judiciaire. C'est là une piste mais il faudrait engager des recherches précises sur ce phénomène afin de mieux le comprendre.

« L'aveu demeure en réalité une finalité à la fois recherchée et valorisée »

Il semble qu'en matière de police, la tendance générale soit de passer du culte de l'aveu à celui de la preuve. À première vue, cela pourrait être une bonne nouvelle pour les citoyens. Mieux vaut une preuve matérielle qu'un aveu arraché. De votre côté, vous craignez que, derrière tout cela, ne se cache un «fantasme technologique». Pouvez vous le décrire?

Les propos tenus par Jean-Christophe Lagarde en 2003 sont symptomatiques d'une telle tendance que beaucoup appellent de leurs vœux. Cependant, on constate actuellement que certains discours politiques et policiers érigeant la technologie comme solution miracle pour répondre aux problèmes auxquels les forces de l'ordre doivent faire face sont loin de correspondre à la réalité du terrain. Le fantasme technologique se situe certainement ici: il existe un complet décalage entre le mythe développé et entretenu par ces discours sur la toute puissance de technologies de plus en plus sophistiquées et la grande importance que revêtent encore, malgré le déploiement de plus en plus affirmé de ces technologies, les «éléments humains» dans l'activité policière quotidienne. Ce phénomène a par exemple été mis en lumière en matière d'enquête de police judiciaire par un travail de recherche du sociologue Laurent Muchielli reposant sur une analyse détaillée du traitement d'affaires d'homicide élucidées ou non élucidées par certains services de la police et de la gendarmerie nationales (1). Cette étude a montré combien les témoignages, les enquêtes de voisinage ou parfois les dénonciations restaient des éléments prépondérants dans la résolution de ces affaires. De plus, elle expliquait pourquoi, alors que le poids de ce facteur est régulièrement dénié par les enquêteurs eux-mêmes, l'aveu demeure en réalité dans la grande majorité des cas une finalité à la fois recherchée et valorisée par l'enquête.

Des policiers nous ont avoué que, pour les déjouer, certains criminels n'hésitent pas à « importer » sur les scènes des crimes des empreintes ADN qui ne sont pas les leurs (mégots, etc.). Est-ce à dire que, là comme ailleurs, et comme toujours, on risque d'assister à une adaptation du crime ?

Ce phénomène n'est pas surprenant. De tout temps, les dispositifs techniques et technologiques déployés en matière de sécurité ont engendré des stratégies individuelles ou collectives d'adaptation ou de contournement... qui ont d'ailleurs constamment constitué un habile moyen pour les pouvoirs publics de légitimer la nécessité de renforcer ces mêmes dispositifs. L'exemple que vous évoquez montre significativement que la technologie ne pourra jamais se substituer à l'intelligence humaine. La technologie fournit des informations, des indices, des traces, etc. mais, dans la plupart des cas, ces éléments objectifs ne constituent pas des «preuves». Seule une interprétation humaine intelligente de ces éléments permet à la police de dégager des pistes de recherche dans lesquels les éléments humains demeurent le plus souvent décisifs. Faire croire que la technologie permettra, à elle seule, de tout résoudre est un leurre. En 2005, j'ai interviewé le chef des sections techniques de recherches et d'investigations de l'Identité judiciaire à la préfecture de police de Paris. Il avait alors tout particulièrement pointé l'importance de ce problème engendré par la systématisation du recours policier à l'ADN: *«L'Angleterre, technologiquement plus avancée que la France, recourt à des procédures de "suramplification" pour révéler la moindre trace génétique. Une grande part de ces traces est "de contact", à l'instar de la sueur. Sur ce type de traces, on peut mettre en évidence votre ADN mais aussi le mien: nous nous serrons par exemple la main, vous emportez des molécules de ma sueur pour commettre ensuite un homicide. C'est alors toute la problématique de la preuve matérielle qui se trouve posée: plus de traces signifie aussi davantage de risques d'erreurs [...] Même si ces traces sont identifiées, tout le travail reste à accomplir car il faut ensuite, surtout, comprendre le contexte dans lequel ces traces ont été laissées (2).»*

Comment avez vous perçu le débat qui a entouré le fichier Edvige, vous qui ne cessez de mettre en garde contre ce que vous appelez «la logique d'accumulation» à l'œuvre dans la police?

Le cas d'Edvige a eu pour mérite de porter momentanément dans l'arène publique l'enjeu de l'identification policière des individus qui ne doit pas être appréhendé à l'aune de ce seul fichier. Je le répète, c'est une problématique bien plus large qui concerne également d'autres fichiers de police nationaux et transnationaux (STIC, FNAEG, EURODAC, VIS, SIS II, mise en réseau des fichiers dactyloscopiques et ADN des États membres de l'UE depuis la signature du Traité de Prüm en mai 2005, etc.), l'encartement (avec la diffusion de plus en plus massive de documents biométrisés), mais aussi la vidéosurveillance, les puces RFID, la géolocalisation, etc. Le rapide développement de tous ces nouveaux dispositifs pose d'importants problèmes en matière d'atteinte aux libertés, à l'anonymat, au droit à l'oubli, etc. Il soulève aussi de cruciales interrogations relatives à l'effectivité des moyens (matériels, humains, juridiques, etc.) dont disposent les autorités chargées de la protection des données personnelles (la CNIL, mais aussi par exemple le Contrôleur européen de la protection des données). Il renvoie encore à des questions fondamentales concernant le droit d'accès à leurs informations dont jouissent les individus et l'exercice des modalités de contrôle sur ceux qui accumulent et exploitent ces mêmes informations. Edvige aurait pu constituer une formidable occasion pour le Parlement d'engager un débat démocratique d'envergure et de légiférer sur l'ensemble de ces points qui touchent à des aspects déterminants du fonctionnement de la démocratie. De ce point de vue, une fois de plus en France, la montagne a accouché d'une souris !

(1) *L'élucidation des homicides: de l'enchaînement technologique à l'analyse des compétences des enquêteurs. Contribution à l'analyse du travail de police judiciaire*, Études et données pénales, CESDIP, n° 98, 2005.

(2) «Le second souffle de la police technique et scientifique», entretien avec le commissaire divisionnaire Richard Marlet réalisé par Pierre Piazza, *Les Cahiers de la sécurité*, n° 56, premier trimestre 2005, p. 131.