

La prolifération incontrôlée des fichiers de police

Virginie Gautron, ATER à la faculté de droit de Nantes

L'accentuation de la visibilité policière se double de nouvelles méthodes d'action qui se caractérisent au contraire par leur discrétion, voire leur opacité. Au travers d'une stratégie proactive de gestion des risques criminels, policiers et gendarmes usent de procédés novateurs pour faciliter l'identification et la recherche des délinquants. Investis dans une oeuvre d'acquisition d'informations, ils disposent désormais de vastes fichiers contenant des données nominatives sur les délinquants avérés, potentiels, mais aussi leurs victimes. Sous l'effet du processus d'informatisation entamé dès les années soixante, les fichiers et systèmes d'analyse criminelle se sont multipliés, notamment ces dix dernières années. Les personnes concernées, la durée de conservation des données, les motifs de consultation et la faiblesse des contrôles institués suffisent pourtant à susciter quelques inquiétudes au vu des risques d'atteinte aux droits fondamentaux des citoyens.

Des fichiers en nombre croissant

La police et la gendarmerie utilisent de nombreux fichiers au quotidien : système informatisé d'identification des auteurs fondé sur le signalement par présentation de photographies aux victimes (CANONGE), fichier automatisé des empreintes digitales (FAED), fichier des personnes recherchées (FPR), fichier des véhicules volés (FVV), fichiers informatisés des Renseignements généraux (terrorisme, personnes physiques et morales), système de traitement des infractions constatées (STIC) de la police nationale et système judiciaire de documentation et d'exploitation (JUDEX) de la gendarmerie nationale, système d'analyse des liens de la violence associée au crime (SALVAC), fichier national des informations douanières, etc (1). La loi n° 2003-239 du 18 mars 2003 (art. 21) a en outre donné une autorisation de principe aux services de police et de gendarmerie pour mettre en oeuvre des applications automatisées d'informations nominatives recueillies à tous les stades de l'enquête.

Parmi les créations récentes, il faut ajouter le fichier national automatisé des empreintes génétiques (FNAEG) et le fichier judiciaire national automatisé des auteurs d'infractions sexuelles et violentes (FIJAIS). Introduit par la loi n° 98-468 du 17 juin 1998, le FNAEG visait initialement l'enregistrement des traces biologiques et des empreintes génétiques recueillies lors d'enquêtes concernant les infractions de nature sexuelle. Sous l'effet des lois n° 2001-1062 du 15 novembre 2001, n° 2003-239 du 18 mars 2003 et n° 2005-1550 du 12 décembre 2005, il couvre désormais une vaste gamme d'infractions : trafic de stupéfiants, proxénétisme, exploitation de la mendicité, terrorisme, meurtre ou assassinat commis en état de récidive légale, vol, escroquerie, extorsion, etc. (c. pr. pén., art. 706-55 et s.). Depuis la loi n° 2006-399 du 4 avril 2006, il recense sous certaines conditions les empreintes des personnes de nationalité française ou étrangère condamnées à l'étranger pour les mêmes types d'infractions (c. pr. pén., art. 706-56-1). Quant au FIJAIS, autorisé par la loi n° 2004-204 du 9 mars 2004 et le décret n° 2005-627 du 30 mai 2005, il avait pour finalité initiale de prévenir le renouvellement des infractions sexuelles commises sur des mineurs et de faciliter l'identification de leurs auteurs, majeurs ou mineurs. Depuis les lois n° 2005-1550 du 12 décembre 2005 et n° 2006-399 du 4 avril 2006, il vise également le proxénétisme et le recours à la prostitution d'un mineur, les homicides volontaires commis avec tortures ou actes de barbarie, les crimes de tortures, d'actes de barbarie, de meurtre ou assassinat commis en état de récidive légale (c. pr. pén., art. 706-47 et 706-53-1 et s.). En fonction de la gravité des faits, cette inscription est obligatoire ou, lorsqu'il s'agit d'un délit puni d'une peine inférieure ou égale à cinq ans d'emprisonnement, laissée à la discrétion des juridictions de jugement.

Bien d'autres fichiers devraient voir le jour prochainement. La loi n° 2006-64 du 23 janvier 2006 sur le terrorisme étend considérablement les pouvoirs des institutions régaliennes en matière de collecte d'informations : exploitation des fichiers d'enregistrement d'images grâce au développement de la vidéosurveillance de l'espace public, traitement de données à caractère personnel portant sur les déplacements hors de l'Union européenne, contrôle des déplacements sur le territoire à partir de dispositifs de contrôle automatisé des données signalétiques des véhicules et de la prise de photographies des passagers sur le réseau routier. Enfin, le projet de loi relatif à la prévention de la délinquance en cours de discussion prévoit la création d'un fichier national des personnes hospitalisées d'office.

Le développement des banques de données et des systèmes d'analyse criminelle est par ailleurs fortement promu par les instances européennes. Les acteurs de la coopération policière européenne disposent eux-mêmes d'un nombre important de fichiers : le Système d'information des douanes (SID), le système EURODAC recueillant les empreintes digitales des demandeurs d'asile et des immigrants illégaux, le Système d'information Schengen (SIS) et le Système national Schengen (N-SIS), le Système d'information Europol (SIE). Pour stimuler l'utilisation d'instruments sophistiqués, Europol supervise actuellement l'installation et la gestion d'un vaste système informatisé permettant l'alimentation, l'accès et l'analyse de données fournies par les services policiers nationaux des pays tiers et des Etats membres de l'Union européenne : le système TECH (2). Le Conseil européen a également demandé à la Commission de présenter des propositions permettant d'accroître l'interopérabilité des bases de données européennes. Le SIS stockait en janvier 2006 environ 15 millions de données dont 1,2 million relatives à des personnes (étrangers signalés aux fins de non-admission, personnes disparues ou recherchées aux fins d'extradition, etc.) (3).

Une collecte d'informations visant potentiellement l'ensemble de la population
Qui peut être fiché ?

Ces fichiers sont loin de s'adresser uniquement aux délinquants avérés. Les fichiers STIC et JUDEX, qui devraient être fondus d'ici 2008 dans un système d'application de rapprochement, d'identification et d'analyse pour les enquêteurs (ARIANE), contiennent des données nominatives concernant les victimes et les personnes, mineures ou majeures, à l'encontre desquelles sont réunis des indices graves ou concordants rendant « vraisemblable » qu'elles aient pu participer à la commission d'un crime, d'un délit ou de certaines contraventions de cinquième classe (violences volontaires avec ITT inférieure ou égale à huit jours, provocation à la discrimination, à la haine ou à la violence, dégradations légères, etc.) (4). Sous le contrôle de l'autorité judiciaire, cette simple condition de vraisemblance est laissée à l'appréciation des agents habilités à exercer des missions de police judiciaire.

Selon la CNIL, le STIC inventorait 28,9 millions de procédures, 4,5 millions de personnes mises en cause et 22,5 millions de victimes au 1er janvier 2006. Du côté de la gendarmerie nationale, le système JUDEX, réglementé par le décret n° 2006-1411 du 20 novembre 2006 après vingt ans d'existence officielle, renseignait en 2000 sur 2,5 millions d'affaires et sur 1,9 million de personnes mises en cause. Avec la multiplication des contraventions de cinquième classe concernées et l'ajout de données en provenance de l'étranger, le nombre de personnes fichées devrait considérablement augmenter.

Cette condition de vraisemblance vaut également pour le FNAEG. Selon le ministère de l'Intérieur, ce fichier contenait fin 2005 plus de 150 000 profils, contre 31 894 en 2004 et environ 5 000 en 2003 (5).

En outre, les officiers de police judiciaire sont autorisés à comparer d'office les empreintes génétiques d'une personne à l'encontre de laquelle existe « une ou plusieurs raisons plausibles » de soupçonner qu'elle a commis un crime ou un délit avec les empreintes contenues dans le fichier. Sans être enregistrés, ces prélèvements visent donc de simples suspects, quelle que soit la nature de l'infraction commise. Quant au FIJAIS, y sont inscrits les condamnations, même non encore définitives, les compositions pénales ainsi que les non-lieux, relaxes et acquittements au bénéfice des individus déclarés irresponsables pénalement en raison d'un trouble mental. L'inscription au fichier et les obligations qui en découlent étant considérées

comme des mesures de sûreté, le législateur leur a conféré un caractère rétroactif. De sorte que le FIJAIS comportait, dès son entrée en vigueur, l'identité de plus de 20 000 personnes (6).

Récemment, l'article 30 de la loi n° 2005-1549 du 12 décembre 2005 relative au traitement de la récidive des infractions pénales a régularisé les fichiers de crimes en série SALVAC et ANACRIM. Le législateur a autorisé la conservation des données relatives aux personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer à la commission d'une infraction portant atteinte aux personnes punie de plus de cinq ans ou portant atteinte aux biens et punie de plus de sept ans. Sont également visées les personnes à l'encontre desquelles « il existe des raisons sérieuses de soupçonner » qu'elles ont commis ou tenté de commettre de telles infractions, les personnes « susceptibles de fournir des renseignements sur les faits » dont l'identité est citée dans une procédure ainsi que les victimes (7).

Au travers de ces différents exemples, on remarque que chaque Français, qu'il soit auteur d'une infraction, suspect, victime ou simple témoin, figure potentiellement dans l'un des fichiers évoqués, et ce pour de longues années.

Conservation des données

S'agissant du STIC et du JUDEX, les données sont en principe conservées pendant cinq ans pour les mineurs mis en cause, vingt ans pour les majeurs et quinze ans pour les victimes. Pour certaines infractions commises par des mineurs, ce délai peut être allongé à dix ans (vols avec violence, exploitation de la mendicité en bande organisée, trafic de stupéfiants, etc.), voire à vingt ans (enlèvement et séquestration, homicide volontaire, tortures, etc.). Il peut atteindre quarante ans s'agissant des majeurs (agression sexuelle, atteinte sexuelle sur mineur, empoisonnement, escroquerie, etc.).

Concernant le FNAEG, les empreintes génétiques des personnes condamnées sont conservées durant quarante ans. Par dérogation, celles recueillies sur les personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable leur participation aux infractions mentionnées à l'article 706-55 du code de procédure pénale sont conservées vingt-cinq ans, sauf si elles ont bénéficié d'un classement sans suite, d'une relaxe, d'un non-lieu ou d'un acquittement exclusivement fondé sur l'existence d'un trouble mental (c. pr. pén., art. R.53-14).

Quant au FIJAIS, la durée de l'enregistrement est de trente ans à compter de la fin de l'exécution de la sanction en cas de crime ou de délit puni d'une peine de dix ans d'emprisonnement, de vingt ans dans les autres cas (c. pr. pén., art. 706-53-4). Les personnes inscrites au fichier doivent justifier annuellement de leur adresse, faire état d'un éventuel déménagement voire, dans les cas les plus graves, se présenter tous les six mois dans les services de police ou de gendarmerie (c. pr. pén., art. 706-53-5). Le manquement à ces obligations constitue un délit puni de deux ans d'emprisonnement et de 30 000€ d'amende.

Des garanties insuffisantes au regard des risques de dérive Constitution et consultation des fichiers : quels contrôles ?

De prime abord, les contrôles institués pour garantir la protection des libertés individuelles sont à la fois nombreux et croissants. Les fichiers policiers sont placés sous le contrôle de l'institution judiciaire. Pour les consulter, les personnels de l'Etat investis d'attributions de police judiciaire doivent être individuellement désignés et spécialement habilités par leurs supérieurs ou par le procureur de la République. Les consultations du STIC et du JUDEX font désormais l'objet d'un enregistrement comprenant l'identifiant du consultant, la date et la nature de l'interrogation. Le FIJAIS n'est pas placé sous la responsabilité du ministère de l'Intérieur mais tenu sous le contrôle du magistrat dirigeant le service du casier judiciaire.

Les dispositions de la loi informatique et libertés du 6 janvier 1978 sont applicables en la

matière. Elles interdisent notamment le fichage des origines raciales, des orientations politiques, syndicales ou religieuses. Pour se conformer à ces nouvelles dispositions législatives, certains fichiers ont dû être modifiés, ceux des Renseignements généraux principalement (8).

Ces contrôles et garanties s'avèrent pourtant plus que théoriques. Les parquets ne disposent pas de terminaux d'accès au STIC et au JUDEX, alors même que les forces de police judiciaire profitent périodiquement d'une extension de leurs droits d'enregistrement et de consultation d'office. Outre qu'une majeure partie de la population ignore la procédure à suivre pour exiger la communication des données enregistrées, les dérogations apportées au régime général de la loi informatique et libertés amenuisent amplement son effet protecteur. Les personnes fichées sont contraintes de passer par l'intermédiaire de la CNIL lorsqu'elles souhaitent connaître la nature des informations détenues à leur sujet. Cette communication peut être refusée s'agissant des données qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique. Si la loi n° 2004-801 du 6 août 2004 transposant la directive européenne 95/46 CE du 24 octobre 1995 sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel a renforcé un certain nombre de garanties, la plupart des dispositions introduites ne s'appliquent pas aux fichiers policiers. Les autorités ont par ailleurs jusqu'au 24 octobre 2010 pour mettre ces fichiers en conformité avec les nouvelles dispositions législatives. En ce domaine, la réforme s'est même traduite par une restriction des pouvoirs de la CNIL. Le nouvel article 26 de la loi informatique et libertés dispose que les traitements de données à caractère personnel qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique sont autorisés par arrêté pris après avis motivé de la CNIL. Précédemment, il fallait que cet avis soit favorable (9). Pourtant, la Commission ne s'est jamais véritablement opposée à la constitution de tels fichiers. En pratique, elle adopte une stratégie pragmatique et cherche un compromis sur les aspects les plus contestables des banques de données, « au point que l'on peut se demander aujourd'hui si le "réalisme" de la commission n'a pas contribué à banaliser l'existence de ces fichiers » (10).

Les administrations policières n'hésitent donc guère à reproduire des pratiques plus que douteuses. Le 22 août 2006, SOS Racisme a déposé une plainte reprochant aux Renseignements généraux l'alimentation d'un fichier de délinquants sur la base de leurs origines ethniques. Il en donne pour preuve le contenu d'un rapport daté du 6 janvier 2005 répertoriant l'origine ethnique de 436 meneurs recensés dans 24 quartiers sensibles, parmi lesquels « 87% ont la nationalité française, 67% sont d'origine maghrébine et 17% d'origine africaine. Les Français d'origine non immigrée représentent 9% des meneurs ».

La procédure d'effacement des données

L'insuffisance des garanties est aussi flagrante en matière d'effacement des données. En ce qui concerne le STIC, le JUDEX et le SALVAC, les personnes ayant bénéficié d'une décision de classement sans suite, de relaxe ou d'acquiescement peuvent demander la mise à jour ou l'effacement des données au responsable du traitement, par l'intermédiaire du procureur de la République ou de la CNIL. Toutefois, l'effacement est loin d'être automatique. En cas de relaxe ou d'acquiescement, le parquet peut s'y opposer discrétionnairement « pour des raisons liées à la finalité du fichier ». Les décisions de non-lieu et les classements sans suite motivés par une absence de charges font l'objet d'une simple mention, sauf si le procureur de la République ordonne la suppression des données.

De même, les personnes inscrites dans le FNAEG sur la base de simples indices peuvent demander au procureur de la République l'effacement des empreintes génétiques. Là encore, il ne s'agit que d'une faculté puisque le maintien de l'enregistrement est possible lorsqu'il apparaît nécessaire compte tenu de la finalité du fichier (c. pr. pén., art. 706-54). Les mécanismes de contrôle assurent néanmoins une protection plus effective des libertés individuelles. En cas de refus du parquet, l'intéressé peut saisir le juge des libertés et de la détention, dont la décision peut être contestée devant le président de la chambre de l'instruction. La même démarche vaut pour l'effacement des données inscrites au FIJAIS (c. pr. pén., art. 706-53-10).

Les dangers d'un casier judiciaire parallèle

Si la CNIL ne s'est pas opposée à la mise en oeuvre des fichiers policiers, elle dénonce régulièrement leur utilisation comme casier judiciaire parallèle, et ce au mépris des droits fondamentaux de la personne, notamment de la présomption d'innocence. A la différence du casier judiciaire, les fichiers recensent des informations sur des personnes qui ne sont pas nécessairement condamnées. Or, ces banques de données sont laissées à la disposition, directe ou indirecte, d'un nombre croissant d'agents publics. Lorsque la CNIL s'est prononcée sur l'entrée en vigueur du STIC, elle avait pourtant demandé que ce fichier ne soit pas utilisé pour effectuer des enquêtes de moralité (11). Malgré cette invitation, la loi n° 2001-1062 du 15 novembre 2001 et la loi n° 2003-239 du 18 mars 2003 ont étendu les droits d'accès aux fichiers STIC et JUDEX pour les enquêtes administratives préalables au recrutement ou à l'agrément de certaines professions. Depuis le décret d'application n° 2005-1124 du 6 septembre 2005, ces consultations concernent les agents de sécurité privée et des sociétés de transports parisiens, les médiateurs et délégués du procureur, les enquêteurs de personnalité et les contrôleurs judiciaires, les magistrats, les préfets, les ambassadeurs, les policiers, les personnels de l'administration pénitentiaire, les policiers municipaux, les agents des services publics urbains de transports en commun, les agents des concessionnaires d'autoroute, etc (12). En 2005, plus de 120 000 enquêtes administratives ont été effectuées.

La CNIL dénonce donc un détournement de la finalité première des fichiers policiers, qui était de faciliter l'investigation policière et non d'alimenter « une mémoire policière supplantant totalement la mémoire du casier judiciaire » (13). Plus encore, les consultations s'effectuent parfois en complète illégalité (14). Elles occasionnent régulièrement des licenciements ou des refus d'embauche injustifiés (15).

En 2002, la Commission a demandé la suppression de 37% des données contrôlées contenues dans le fichier STIC et de 42% des données du SIS, parce qu'« erronées ou manifestement non justifiées » (16). L'installation d'un programme d'épuration automatique du STIC en 2004, qui s'est traduite par la suppression des fiches de plus de un million de mis en cause, n'a pas mis un terme à ces dysfonctionnements. En 2005, sur les 467 contrôles effectués par la Commission à la demande de particuliers, 207 personnes étaient indûment fichées, soit parce que le délai de conservation des signalements avait expiré, soit parce que les informations étaient erronées ou injustifiées (17). Face au déferlement des saisines de la CNIL (18), le ministre de l'Intérieur a dû préciser aux préfets, par une circulaire datée du 15 avril 2005, qu'une simple mention au casier judiciaire ou sur un fichier de police ne saurait conduire à émettre un avis défavorable. Il a indiqué que les fonctionnaires devaient apprécier la pertinence des éléments mentionnés aux fichiers, « leur gravité, leur ancienneté, les suites judiciaires qui, le cas échéant, leur ont été données, et leur éventuelle répétition ». En juin 2006, il a constitué un groupe de travail réunissant, sous l'égide du président de l'Observatoire national de la délinquance, les hauts responsables de la police et de la gendarmerie, des magistrats et des représentants de la CNIL (19). Leurs propositions encourageront peut-être les pouvoirs publics à préserver davantage les libertés individuelles. A défaut, le déploiement d'une véritable société de surveillance serait à craindre. Si le nouveau droit à la sécurité et la moralisation de certaines professions, notamment du secteur de la sécurité privée, justifient des contrôles renforcés, il ne faudrait pas que ces ambitions légitimes supplantent totalement les exigences du droit à la sûreté. (20)

Mots clés :

FICHER * Fichier de police * Recensement

(1) M. Schwendener, Les principaux fichiers de la police, AJ Pénal 2003. 21 et s. ; E. Heilmann, Le désordre assisté par ordinateur. L'informatisation des fichiers de police en France (1968-1998), Les Cahiers de la sécurité, n° 56, 2005, p. 145-165.

(2) N. Gersparacher, F. Lemieux, Coopération policière, marché de l'information et expansion des acteurs internationaux : le cas d'Europol, RICPT 2005, n° 4, p. 461-477 ; G. De Kerchove,

Brèves réflexions sur la coopération policière au sein de l'Union européenne, RSC 2004. 553-569 .

(3) R. Yung, Rapport sur le système d'information Schengen de deuxième génération, Commission des Lois, Les rapports du Sénat, n° 174, janvier 2006, p. 10.

(4) Décret n° 2001-583 du 5 juillet 2001 modifié par le décret n° 2006-1258 du 14 octobre 2006 portant création du STIC ; décret n° 2006-1411 du 20 novembre 2006 portant création du JUDEX.

(5) M. Schwendener, Les principaux fichiers de la police, préc.

(6) *Ibid.*, p. 139.

(7) M. Herzog-Evans, Les dispositions relatives à la récidive dans la loi n° 2005-1549 du 12 décembre 2005, D. 2006. Chron. 182 .

(8) Décret n° 91-1051 du 14 octobre 1991.

(9) J. Boyer, Interconnexions et fichiers policiers. Deux débats de notre temps, Les Cahiers de la sécurité intérieure, n° 34, 1998, p. 135-147.

(10) E. Heilmann, Le désordre assisté par ordinateur, préc.

(11) J. Boyer, Interconnexions et fichiers policiers. Deux débats de notre temps, préc.

(12) Le préfet dispose également d'un accès direct au FIJAIS pour l'examen des demandes d'agrément concernant des activités ou des professions impliquant un contact avec des mineurs et, depuis la loi n° 2005-1150 du 12 décembre 2005, pour le contrôle de ces activités ou professions (c. pr. pén., art. 706-53-7 et 706-53-12). Il faudra néanmoins qu'un décret en Conseil d'Etat pris après avis de la CNIL définisse les modalités et les conditions d'application de cette nouvelle disposition.

(13) J. Danet, Le droit pénal et la procédure pénale sous le paradigme de l'insécurité, Arch. po. crim., n° 25, 2003, p. 37-69.

(14) Ainsi, en mai 2006, le parquet de Meaux a poursuivi deux gendarmes retraités accusés de revendre à Eurodisney des données fournies par un ancien collègue. La société aurait utilisé ces informations pour sélectionner son personnel.

(15) 26e Rapport d'activité 2005 de la CNIL, 2006, p. 93 et s.

(16) M. Gentot, La CNIL et les fichiers de sécurité publique, Conférence des commissaires à la protection des données, Séville, 3-4 avril 2003. Disponible sur www.cnil.fr

(17) "Ne souriez pas, vous êtes fichés", Libération, 7 avril 2006.

(18) Les saisines ont ainsi augmenté de 70% pour la seule année 2004. 25e Rapport d'activité 2004 de la CNIL, 2005, p. 44.

(19) Sur ce sujet, V. *infra*, p. 70 « Fichiers de police et de gendarmerie utilisées à des fins administratives. Un meilleur contrôle pour une plus grande efficacité », par A. Bauer et C. Soullez.

(20) L'AJ Pénal, dans son numéro 2/2007, a consacré un dossier aux fichiers de police : concilier sécurité et liberté composé, outre la présente contribution, des articles suivants :

Fonctions et mutations des fichiers de police (surveiller, enquêter et punir), par Pierre-Yves Marot, p. 61 .

Le rôle des fichiers dans l'action opérationnelle des services de sécurité intérieure, par Renaud Vedel, p. 64 .

La CNIL exerce-t-elle un contrôle des fichiers de police suffisant ?, interview de François Giquel, p. 69 .

Fichiers de police et de gendarmerie utilisés à des fins administratives : un meilleur contrôle pour une plus grande efficacité, par Alain Bauer et Christophe Soullez, p. 70 .