AJ Pénal 2010 p. 266

Usages et mésusages des fichiers de police : la sécurité contre la sûreté ? (1)

Virginie Gautron, Maître de conférences à la Faculté de droit de Nantes, Laboratoire « Droit et Changement Social », UMR CNRS 3128

*
**

Les fichiers de police ne sont pas nés avec l'informatique. Dès la fin des années 1960, plus de quatre cents fichiers ont été recensés dans les seuls services parisiens de la police nationale, composés d'environ 130 millions de fiches. En facilitant la collecte et la consultation des données, les progrès de l'informatique ont toutefois révolutionné la matière, de sorte que l'on assiste depuis une trentaine d'années à une véritable prolifération des fichiers de police (2). Après une longue période d'indifférence, les risques d'une surveillance policière généralisée ont récemment cristallisé les inquiétudes de l'opinion. En parallèle des débats sur la vidéosurveillance, la biométrie et les nanotechnologies, pétitions, articles de presse et rapports publics se succèdent pour dénoncer ou questionner l'impact de cette collecte d'informations nominatives sur l'exercice des libertés qui fondent notre régime démocratique. Le signalement et l'acquisition d'informations ayant toujours occupé une place de choix parmi les activités policières, il n'est certes pas question de reprocher aux pouvoirs publics de placer les avancées technologiques au service de la prévention et de la répression des infractions. Cette évidence n'exclut pas toute réflexion sur les conditions, les formes, les limites et l'encadrement du processus d'enregistrement et de consultation de cette masse de données personnelles. Ces applications informatiques se doivent de respecter les principes fondamentaux qui garantissent un État de droit. Or, sous couvert de la consécration d'un « droit à la sécurité », la réglementation desdits fichiers, les pratiques policières et la faiblesse des contrôles institués portent indéniablement atteinte aux libertés fondamentales.

Une mémoire policière aux contours indéfinis

Outre la multiplication des fichiers de police ces dernières années (3), auxquels s'ajouteront prochainement des applications en phase de conception ou d'expérimentation, de récentes réformes consacrées aux traitements existants potentialisent le développement d'une véritable société de surveillance. Avant même la publication du décret mort-né du 27 juin 2008 instaurant EDVIGE (4), les fichiers de police ne visaient pas seulement les délinquants avérés. Le STIC et le JUDEX, qui devraient fusionner prochainement dans la nouvelle base commune ARIANE, contiennent des informations sur 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. Le fichier d'analyse sérielle SALVAC (5), comme le futur fichier AJDRCDS (6), permettent ou permettront d'enregistrer des données relatives aux personnes à l'encontre desquelles « il existe des raisons sérieuses de soupçonner » qu'elles ont commis ou tenté de commettre des infractions contre les biens punies de plus de sept ans ou des infractions contre les personnes punies de plus de cinq ans (7), ainsi qu'aux personnes « susceptibles de fournir des renseignements sur les faits » dont l'identité est citée dans une procédure. De sorte que le nombre de personnes fichées dans les banques de données policières semblait déjà impressionnant : 5,5 millions de mis en cause et 33 millions de victimes dans le STIC fin 2008, 2 millions de mis en cause dans le JUDEX.

Tel que réglementé initialement, le fichier EDVIGE aurait adjoint à cette longue liste les personnes, mineures ou majeures « ayant sollicité, exercé ou exerçant un mandat politique, syndical ou économique ou qui jouent un rôle institutionnel, économique, social ou religieux significatif», ainsi que les « individus, groupes, organisations et personnes morales qui, en raison de leur activité individuelle ou collective, sont susceptibles de porter atteinte à l'ordre public ». Le décret n° 91-1051 du 14 octobre 1991 officialisant l'existence du précédent fichier des renseignements généraux (FRG) ne visait que les individus majeurs, groupes ou organisations « qui peuvent, en raison de leur activité individuelle ou collective, porter atteinte à la sûreté de l'État ou à la sécurité publique, par le recours ou le soutien actif apporté à la violence ». Le décret n° 2009-1249 du 16 octobre 2009 (8), qui remplace EDVIGE par un traitement relatif à la prévention des atteintes à la sécurité publique, a certes supprimé le fichage des personnalités et adopté une formulation plus proche de celle du décret de 1991 en limitant les enregistrements aux seules personnes de plus de 13 ans dont « l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique », notamment les personnes « susceptibles d'être impliquées dans des actions de violences collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives ». Si la notion de sécurité publique est plus circonscrite que celle d'ordre public, les critères d'enregistrement demeurent relativement flous (« peuvent porter atteinte », « susceptibles d'être impliquées »). Ceux qui souhaitent ne pas figurer dans ce traitement devront prendre garde à leurs fréquentations, puisque des données pourront être conservées s'agissant des individus « entretenant ou ayant entretenu des relations directes et non fortuites avec les personnes visées par le fichier ».

Ces décrets s'accompagnent d'une extension de la gamme des données enregistrées. La plupart des fichiers recensent des informations sur l'identité de la personne, sa situation familiale, sa filiation, sa nationalité, son adresse et sa profession. Certains traitements, parmi lesquels le STIC et le JUDEX, peuvent, sous certaines conditions, indiquer son origine raciale ou ethnique, ses activités politiques, philosophiques, religieuses et syndicales ou encore renseigner sur sa vie sexuelle. Si le décret du 27 juin 2008 autorisait l'enregistrement de données sur les « opinions » politiques, philosophiques, religieuses ou syndicales, celui du 16 octobre 2009 s'approche de la rédaction du décret de 1991 en restreignant la collecte d'informations aux « activités », notion plus restrictive et plus objective car fondée sur des faits concrets. L'enregistrement des données relatives à la santé ou à l'orientation sexuelle a par ailleurs été prohibé. Dans le nouveau fichier relatif à la prévention des atteintes à la sécurité publique figureront toutefois des informations sur les « activités publiques » et les « comportements » des personnes, des notions floues dont la CNIL avait pourtant demandé qu'elles soient mieux définies (9), ainsi que sur leur « origine géographique », nouveau concept juridique qui, toujours selon la Commission, devrait être fondé sur des éléments « de nature factuelle et objective ». Seront également mentionnés les adresses électroniques, les déplacements, les signes physiques particuliers et objectifs des personnes, des photographies, des informations fiscales et patrimoniales. Le fichier d'analyse sérielle AJDRCDS devrait également référencer toutes les sources d'informations disponibles dans les bases d'autres administrations (fisc, douanes, sécurité sociale) ou d'opérateurs privés (FAI, opérateurs de téléphonie, banques), ainsi que des éléments contenus dans les sources dites « ouvertes » (données déposées sur Facebook, les blogs, etc.).

À l'identique, les délais de conservation des données ne cessent de s'allonger. Ceux prévus pour le STIC et le JUDEX (jusqu'à 40 ans pour les mis en cause, 15 ans pour les victimes), le FNAEG (10) (40 ans pour les condamnés, 25 ans pour les suspects) ou le FIJAIS (11) (jusqu'à 30 ans après la fin de l'exécution de la sanction) semblaient déjà bien longs. Si le décret instaurant EDVIGE était muet sur le sujet, autorisant de fait une conservation des données illimitée dans le temps, le décret du 16 octobre 2009 a réparé cet « oubli » en limitant les enregistrements à dix ans pour les majeurs, trois ans pour les mineurs après « l'intervention du dernier événement de nature à faire apparaître un risque d'atteinte à la sécurité publique ayant donné lieu à un enregistrement ». Cette précision s'apparente toutefois à une garantie en trompe-l'oeil dès lors qu'il suffira aux OPJ d'ajouter des éléments avant terme pour repousser l'effacement

des données.

Des mécanismes de contrôle fictifs

Lorsque l'on se réfère aux garanties prévues par les textes pour assurer la légalité des pratiques policières, ce constat peut sembler de prime abord excessif. La loi informatique et libertés contient de nombreux mécanismes de protection, au premier rang desquels les contrôles effectués par la CNIL. Les fichiers de police sont placés sous le contrôle du procureur de la République. Des dispositifs de traçabilité des consultations policières ont été introduits, sous la forme d'un enregistrement de l'identifiant du consultant, la date et la nature de l'interrogation. Malgré ces diverses précautions, les contrôles et garanties offerts s'avèrent plus que théoriques. Certains fichiers ne font l'objet d'aucun contrôle, notamment le fichier CRISTINA (12) couvert par le secret-défense. Outre la restriction des pouvoirs de la CNIL en 2004, dont l'avis n'a plus à être favorable pour créer un fichier de police par arrêté, les délais qui lui sont accordés pour se prononcer ont été réduits à deux mois. Alors que son avis est réputé favorable lorsqu'il n'est pas rendu dans les délais impartis, son manque de moyens l'empêche régulièrement de se prononcer dans les temps, comme ce fut le cas en 2006 pour le fichier d'éloignement des étrangers (ELOI). Désormais, elle sera par ailleurs privée de tout moyen de contrôle au sujet des modifications qui seraient apportées à l'avenir au fichier de renseignement se substituant à EDVIGE. Le décret du 16 octobre 2009 a soumis le fichier relatif à la prévention des atteintes à la sécurité publique à la procédure de déclaration simplifiée, applicable aux fichiers gérés par la DST, la DGSE ou encore la direction du renseignement militaire (13). À leur sujet, la CNIL n'est pas informée des critères d'enregistrement, de la gamme et de la durée de conservation des données collectées. Les actes réglementaires autorisant ces traitements n'étant pas publiés, aucun contrôle démocratique n'est possible. Au regard de la jurisprudence de la Cour européenne des droits de l'homme, la légalité de tels procédés semble plus que contestable. Dans un arrêt du 6 juin 2006, *Segerstedt-Wiberg et autres c/ Suède*, la Cour s'est fondée sur les articles 8, 10 et 11 de la Convention européenne des droits de l'homme, qui consacrent respectivement le droit à la vie privée, les libertés de réunion et d'expression, pour condamner l'État suédois du fait de l'enregistrement de données personnelles dans un « fichier de la sûreté ». Cette condamnation est d'autant plus instructive que le champ d'application et la finalité du fichier en question (faciliter les enquêtes concernant le terrorisme et les infractions à la sécurité nationale) étaient nettement plus circonscrits que notre fichier de renseignement. Si la Cour admet que l'existence de services de renseignement peut s'avérer légitime dans une société démocratique, elle a précisé que « le pouvoir de surveiller en secret les citoyens n'est tolérable d'après la Convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques. Pareille ingérence doit se fonder sur des motifs pertinents et suffisants et doit être proportionnée aux buts légitimes poursuivis ». Au regard de la finalité du fichier de renseignement français, des personnes visées et de la nature des données collectées, on peut raisonnablement douter de la réunion de tels critères (14).

Concernant les dispositifs de contrôle *a posteriori*, la CNIL se trouve dans l'incapacité de répondre dans des délais raisonnables aux demandes de droit d'accès indirect. Faute d'un personnel suffisant (15), les personnes doivent attendre entre douze et dix-huit mois pour connaître les données contenues à leur sujet dans le STIC, deux ans pour les fichiers de renseignement, alors même que les textes exigent une réponse dans les six mois. Les contrôles de l'institution judiciaire, s'ils devraient s'accentuer avec la mise en place progressive du logiciel Cassiopée, sont tout aussi problématiques. Les magistrats n'ont pas à valider les données collectées préalablement à leur enregistrement. Le contrôle n'a lieu qu'*a posteriori* et semble là encore plus théorique qu'effectif, les parquets ne disposant pas de terminaux d'accès au STIC et au JUDEX, accès pourtant expressément prévu par la loi du 18 mars 2003. Compte tenu de leur surcharge de travail, les suites judiciaires données aux affaires ne sont quasiment jamais transmises aux forces de police pour que les fiches soient modifiées ou supprimées (16). Même lorsque le parquet procède à des demandes d'effacement, il n'est pas rare que la police ne s'exécute pas (17). Il est toutefois possible d'espérer quelques améliorations à l'avenir. Le projet LOPPSI II prévoit la nomination d'un magistrat pour suivre la mise en oeuvre et la mise à jour des fichiers. Il pourrait agir d'office ou à la demande de particuliers, disposerait d'un accès direct à ces applications, d'un pouvoir de rectification et d'effacement des données. En l'état, ces différents éléments permettent de comprendre la piètre fiabilité des informations enregistrées. S'agissant du STIC, la CNIL a évalué le taux d'exactitude des fiches des mis en cause à 17 % seulement (18).

Ces inexactitudes sont d'autant plus inquiétantes que les pouvoirs publics n'ont cessé d'étendre les finalités assignées auxdits fichiers, au point de les transformer en casier judiciaire parallèle. Alors que les personnes figurant dans ces traitements n'ont pas nécessairement fait l'objet de condamnations pénales, et bénéficient dès lors de la présomption d'innocence, les informations collectées sont laissées à la disposition, directe ou indirecte, d'un nombre croissant d'agents publics (préfets, maires, présidents de conseils généraux et régionaux) pour qu'ils réalisent les enquêtes administratives préalables à certains recrutements, notamment des professionnels exerçant des missions de souveraineté (agents de sécurité privée, magistrats, policiers, personnels de l'administration pénitentiaire, etc.). Si le Conseil constitutionnel a considéré « qu'aucune norme constitutionnelle ne s'oppose par principe à l'utilisation à des fins administratives de données nominatives recueillies dans le cadre d'activités de police judiciaire » (19), ces consultations occasionnent parfois des licenciements ou des refus d'embauche injustifiés. Outre l'impact des erreurs contenues dans ces banques de données, certains préfets se contentent d'une inscription pour refuser un agrément. Autorisée en 2009 par décret, la consultation des fichiers de renseignement pour réaliser de telles enquêtes ne fera qu'accentuer les risques d'atteinte aux libertés fondamentales.

Des fichiers liberticides

Les fichiers de police n'emportent pas de restrictions immédiates aux libertés d'aller et de venir, de réunion, de pensée, etc. Toutefois, avec l'utilisation des fichiers de renseignement aux fins d'enquêtes de moralité, ces dernières ne s'effectueront plus sur la base de faits délinquants supposés, mais de comportements « susceptibles » de porter atteinte à la sécurité publique ou, pire encore, d'affiliations partisanes, religieuses ou syndicales. Si le décret n° 2009-1250 du 16 octobre 2009 portant création d'un traitement automatisé relatif aux enquêtes administratives interdit de collecter des données sensibles, son article 3 dispose pourtant que « l'enregistrement de données, contenues dans un rapport d'enquête, relatives à un comportement incompatible avec l'exercice des missions envisagées est autorisé alors même que ce comportement aurait une motivation politique, religieuse, philosophique ou syndicale ». Des militants syndicaux et politiques, voire même des personnes périodiquement présentes dans telle ou telle manifestation, ne risquent-ils pas, dès lors que leurs engagements ne correspondraient pas à la ligne politique du pouvoir en place, d'être privés d'accès à la magistrature ou aux autres missions de souveraineté ? On nous rétorquera que ces exclusions sont prohibées en vertu des libertés fondamentales que sont les libertés d'opinion, d'expression et de réunion. Cela étant, à défaut de contrôles effectifs, l'opacité entourant l'utilisation des fichiers de renseignement ne peut permettre d'exclure d'office de telles dérives. Le droit au respect de la vie privée se trouve également affecté par les risques de détournement des données. Si de telles pratiques s'avèrent relativement marginales, des consultations sont parfois effectuées en complète illégalité. Au mépris des articles 226-21 et 226-22 du code pénal, certains fonctionnaires de police utilisent les fichiers pour satisfaire une curiosité malsaine, rechercher des informations pour régler des litiges personnels ou obtenir une contrepartie, monétaire ou non, à la divulgation des données à des tiers (20).

Au regard de ces différents éléments, les propositions d'Alain Bauer, président du groupe de contrôle des fichiers policiers, paraissent plus que surprenantes. Dans son rapport de décembre 2008, celui-ci a proposé une campagne d'information pédagogique vantant les atouts des fichiers. Face aux inquiétudes de la population, qui n'auraient selon lui aucun fondement, il conviendrait de « renforcer l'acceptabilité des fichiers » en démontrant l'existence de « garanties offertes pour la protection des libertés » (21). Ces appréhensions étant partiellement fondées, ne devrait-on pas au

contraire s'en saisir pour engager un véritable débat sur les dangers d'un fichage généralisé ? Si la pédagogie n'est pas sans intérêt, peut-être est-il temps de la faire porter sur les principes fondamentaux qui régissent notre système démocratique et qui limitent, en droit et en fait, le champ des possibles en matière de réponse à la demande sociale de sécurité. D'autant qu'un recours accru aux fichiers de police, sans renforcement corrélatif des mécanismes de contrôle, est à craindre à l'avenir. À l'initiative de J.-A. Bénisti, qui réclamait pourtant en 2008 l'intervention systématique du législateur, la proposition de loi de simplification et d'amélioration de la qualité du droit adoptée en première lecture par l'Assemblée Nationale en décembre 2009 valide la création de la plupart des fichiers de police par simple arrêté. Le procureur de la République serait par ailleurs autorisé à faire état d'informations visées dans les fichiers d'antécédents à l'occasion d'une comparution immédiate. Si cette réforme aurait le mérite d'encadrer des pratiques officieuses constatées dans quelques juridictions, et de porter à la connaissance de la défense l'utilisation de telles informations dans le processus pénal, elle aurait pour effet de légitimer des pratiques attentatoires à la présomption d'innocence. Une nouvelle fois, la preuve serait faite que le droit à la sécurité, pourtant présenté comme une déclinaison du droit à la sûreté, se déploie au détriment de la protection des citoyens contre l'arbitraire de l'État.

Mots clés :
FICHIER * Fichier de police * Contrôles * Droits fondamentaux

(1) L'AJ Pénal, dans son numéro 6/2010, a consacré un dossier aux Nouvelles technologies, sécurité et vie privée : l'impossible équation. Il est constitué, outre la présente contribution, des articles suivants :
Usages et mésusages des fichiers de police : la sécurité contre la sûreté ? par Virginie Gautron, p. 266 ;
Le *whistleblowing* et la protection des données par Emilie Bailly et Emmanuel Daoud, p. 269 ;
Vidéosurveillance, risques d'atteintes aux libertés : une dualité de régime insatisfaisante, interview d'Alex Türk, p. 273 ;
La vidéosurveillance est-elle une réponse efficace à la délinquance ?, par Tanguy Le Goff, p. 275.

(2) V. Gautron, La prolifération incontrôlée des fichiers de police, AJ pénal 2007. 57.

(3) Trente-quatre fichiers étaient recensés en 2006, une cinquantaine en 2009 ; Groupe de contrôle des fichiers de police et de gendarmerie, Mieux contrôler la mise en oeuvre des dispositifs pour mieux protéger les libertés, Rapport remis au ministère de l'Intérieur, déc. 2008.

(4) Décret n° 2008-632 du 27 juin 2008 portant création d'un traitement automatisé de données à caractère personnel dénommé « EDVIGE » ; Décret n° 2008-1199 du 19 nov. 2008 portant retrait du décret n° 2008-632 du 27 juin 2008.

(5) Système d'analyse des liens de la violence associée au crime.

(6) Application judiciaire dédiée à la révélation des crimes et délits en série. Fichier d'analyse sérielle, sa finalité sera de faciliter le rapprochement judiciaire des affaires imputables à un même auteur.

(7) Le projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI II) prévoit d'abaisser ce seuil à cinq ans pour l'ensemble des infractions.

(8) Décret n° 2009-1249 du 16 oct. 2009 portant création d'un traitement de données à caractère personnel relatif à la prévention des atteintes à la sécurité publique, JO n° 0242 du 18 oct. 2009.

(9) Délibération n° 2009-355 du 11 juin 2009 portant avis sur un projet de décret en Conseil d'État portant création de l'application relative à la prévention des atteintes à la sécurité publique, JO n° 242 du 18 oct. 2009

(10) Fichier national automatisé des empreintes génétiques.

(11) Fichier judiciaire national des auteurs d'infractions sexuelles ou violentes.

(12) Centralisation du renseignement intérieur pour la sécurité du territoire et des intérêts nationaux.

(13) Décret n° 2007-914 du 15 mai 2007 pris pour l'application du I de l'article 30 de la loi n° 78-17 du 6 janv. 1978 relative à l'informatique, aux fichiers et aux libertés.

(14) V. également CEDH 4 déc. 2008, *S et Marper c/ Royaume-Uni*, req. n° 30562-04 et 30566-04, AJ pénal 2009. 81, obs. G. Roussel.

(15) D. Batho, J.-A. Bénisti, Rapport d'information sur les fichiers de police, Assemblée Nationale, 2009, p. 136.

(16) CNIL, Conclusions du contrôle du STIC, 2009, p. 17 s.

(17) D. Batho, J.-A. Bénisti, *op. cit.*, p. 127.

(18) CNIL, Conclusions du contrôle du STIC, *op. cit.*, p. 26.

(19) Décis. n° 2003-467 DC du 13 mars 2003.

(20) D. Batho, J.-A. Bénisti, *op. cit.*, p. 143 s.

(21) Groupe de contrôle des fichiers de police et de gendarmerie, *op. cit.*, p. 86-87.