GROUPE DE CONTRÔLE DES FICHIERS DE POLICE ET DE GENDARMERIE

MIEUX CONTROLER LA MISE EN ŒUVRE DES DISPOSITIFS POUR MIEUX PROTEGER LES LIBERTES

RAPPORT REMIS AU MINISTRE DE L'INTERIEUR, DE L'OUTRE-MER ET DES COLLECTIVITES TERRITORIALES

Décembre 2008

FICHIERS DE POLICE ET DE GENDARMERIE NATIONALES

MIEUX CONTROLER LA MISE EN ŒUVRE DES DISPOSITIFS

POUR MIEUX PROTEGER LES LIBERTES

SOMMAIRE

LETTRE DE MISSION DU MINISTRE DE L'INTERIEUR, DE L'OUTRE-MER ET DES COLLECTIVITES TERRITORIALES

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTERE DE L'INTERIEUR,
DE L'OUTRE-MER
ET DES COLLECTIVITES TERRITORIALES

Le Ministre

Paris, le 30 SEP. 2008

Monsieur le Président,

La confiance des Français est une exigence pour le ministère de l'Intérieur chargé de leur protection. J'ai la volonté de renforcer cette confiance en garantissant la meilleure application de la loi, dans le respect vigilant des libertés individuelles.

Le groupe de travail que mon prédécesseur vous a demandé de mettre en place en 2006 sur l'amélioration du contrôle et de l'organisation des fichiers de police et de gendarmerie vous a permis de faire des recommandations visant notamment à éviter le maintien dans ces fichiers d'informations erronées ou dépassées.

Je vous demande de bien vouloir réunir à nouveau ce groupe de travail, dont vous pourrez adapter la composition, pour examiner les conditions de mise en œuvre et d'exploitation des fichiers de police judiciaire et de police administrative gérés par les services de mon ministère et par la gendarmerie nationale qui lui sera prochainement rattachée.

Le champ de votre mission s'étendant à l'ensemble de ces fichiers, vous examinerez en priorité les évolutions intervenues depuis la remise de votre rapport de décembre 2006 et les projets en cours, notamment le fichier d'exploitation documentaire et de valorisation de l'information relative à la sécurité publique.

Compte tenu des nouvelles formes de délinquance et de criminalité organisée, vos travaux devront permettre de mieux définir l'équilibre entre l'efficacité de la protection des personnes et l'attention de tous les instants que requiert la protection des libertés.

... / ...

Monsieur Alain BAUER
Président du conseil d'orientation
de l'observatoire national de la délinquance
Les Borromées,
3 avenue du Stade de France,
93218 SAINT DENIS LA PLAINE CEDEX

ADRESSE POSTALE : PLACE BEAUVAU 75800 PARIS CEDEX 08 - STANDARD 01.49.27.49.27 - 01.40.07.60.60
ADRESSE INTERNET : www.interieur.gouv.fr

Vous proposerez, en outre, les mesures à prendre pour renforcer l'acceptabilité des fichiers au sein de la population.

Votre rapport, qui sera rendu public, me parviendra avant le 15 décembre 2008. Vous pourrez m'adresser une note d'étape chaque fois que vous le jugerez utile.

Mes services se tiennent à votre disposition pour faciliter la conduite de votre mission.

Je vous prie de croire, Monsieur le Président, à l'assurance de ma considération distinguée.

Amitiés

Michèle ALLIOT-MARIE

COMPOSITION DU GROUPE DE CONTRÔLE

Président : Monsieur Alain BAUER, Criminologue, Président du conseil d'orientation de l'OND
Secrétaire général : Monsieur André-Michel VENTRE, Inspecteur général de la Police Nationale
Rapporteur : Monsieur Christophe SOULLEZ, Criminologue, Chef du département OND, INHES

- Monsieur le Directeur Général de la Police Nationale (Frédéric PECHENARD)
- Monsieur le Directeur Général de la Gendarmerie Nationale (Général Roland GILLES)
- Monsieur le Préfet de Police (Michel GAUDIN)
- Monsieur le Directeur des Libertés Publiques et des Affaires Juridiques (Laurent TOUVET)

- Monsieur le Directeur des Affaires Criminelles et des Grâces (Jean-Marie HUET)

- Monsieur le Président de la CNIL (Alex TÜRK) représenté par Jean-Marie COTTERET
- Monsieur le Président de la HALDE (Louis SCHWEITZER)
- Monsieur le Président de la CNCDH (Joël THORAVAL)
- Monsieur le Médiateur de la République (Jean-Paul DELEVOYE) représenté par Luc CHARRIÉ

- Monsieur le Secrétaire Général de Synergie Police (Bruno BESCHIZZA)
- Monsieur le Secrétaire Général de l'UNSA Police (Henri MARTINI)
- Madame le Secrétaire Général du SCPN (Sylvie FEUCHER)

- Monsieur le Président de l'Union Syndicale des Magistrats (Christophe REGNARD)
- Madame la Présidente du Syndicat de la magistrature (Emmanuelle PERREUX)[1]

- Monsieur le Président du Conseil National des Barreaux (Paul-Albert IWEINS)
- Monsieur le Président de la Conférence des Bâtonniers (Pascal EYDOUX)
- Monsieur le Bâtonnier de Paris (Christian CHARRIERE-BOURNAZEL)

- Monsieur le Président de la LICRA (Patrick GAUBERT)
- Monsieur le Président de SOS Racisme (Dominique SOPO)
- Monsieur le Président de SOS Homophobie (Jacques LIZE)

- Monsieur Jean-Marc LECLERC, Journaliste, Le Figaro

[1] Le Syndicat de la Magistrature a souhaité quitter le groupe de travail le 17 novembre 2008. Voir annexe n°4.

A LA RECHERCHE DE L'EQUILIBRE

Si le mot fichier inquiète, souvent à juste titre, lorsqu'il est placé sous la responsabilité d'une administration ou d'une entreprise, l'outil semble beaucoup plus utile et attractif dès lors qu'il nous sert au quotidien (annuaire téléphonique, téléphone mobile, PDA, etc.). Et que dire de la multiplicité des informations intimes données volontairement sur les serveurs dits sociaux du web 2.0 ?

Les critiques les plus virulents des premiers pouvant, par la magie d'internet, se transformer en militants affirmés des seconds.

En France, fichiers de police et libertés individuelles sont usuellement opposés. La création, la modernisation ou encore l'extension des bases de données au sein de l'administration alimentent régulièrement le débat sur la protection du droit à la vie privée. Ceci est d'autant plus vrai que les fichiers, qui ont souvent été cachés par les services de l'Etat durant des siècles, font aujourd'hui l'objet d'une visibilité accrue du fait, tant de la législation en vigueur obligeant à leur déclaration, que de la veille médiatique et associative.

Pour agir efficacement en matière policière, il est pourtant essentiel de conserver, retraiter et rapprocher des informations. La mobilité des personnes et des flux, marque de notre société de liberté, et l'exigence du rapport de la preuve qui fonde l'Etat de droit, rendent plus que nécessaire le recours à des informations nominatives.

Bien entendu, aucun traitement automatisé ne peut à lui seul se substituer aux compétences des forces de sécurité sans lesquelles des affaires résolues en flagrant délit ne pourraient être constatées. Le raisonnement hypothético-déductif qui structure toute enquête, le recueil et la synthèse du renseignement opérationnel relatif à un risque ou une menace ou encore l'analyse de proportionnalité qui sous-tend la police administrative, sont également des activités capitales qui renvoient à l'exercice des facultés de jugement et de la capacité de discernement des agents de la force publique.

Les systèmes informatiques des services de sécurité doivent évoluer avec les structures sociales, les mutations technologiques mais également les évolutions criminelles et terroristes.

L'action policière ne peut être pleinement efficace que si elle s'accompagne d'un travail d'analyse et d'étude visant à mieux cerner les organisations criminelles, leurs évolutions mais également les modes opératoires ou encore le profil des victimes, le tout dans le respect des libertés de chacun.

Le groupe de travail mis en place en 2006 par Nicolas Sarkozy, alors ministre d'Etat, ministre de l'Intérieur et de l'aménagement du territoire, avait permis de recenser une grande partie des fichiers existants et d'émettre un certain nombres de recommandations sur l'amélioration du contrôle des fichiers utilisés dans le cadre des enquêtes administratives. Ces recommandations, rappelées dans ce rapport, et pour lesquelles sont mentionnées les suites réservées par l'administration, avaient, à l'époque, été acceptées par le ministère de l'Intérieur, tout autant soucieux de garantir les libertés, que de doter les services de l'Etat de moyens lui permettant d'assurer ses missions de protection des personnes, des biens et de la sûreté de l'Etat.

Réactivé par décision de la Ministre de l'Intérieur, de l'Outre-mer et des collectivités territoriales après l'émotion créée dans l'opinion publique par la présentation du fichier Exploitation documentaire et valorisation de l'information générale (EDVIGE), le Groupe de Contrôle des Fichiers de Police et de Gendarmerie s'est notamment attaché à compléter ce recensement en y ajoutant diverses applications et en étudiant les nouveaux développements prévus.

En effet, la loi n°2004-801 du 6 Août 2004, modifiant la loi Informatique et Libertés de 1978, prévoit dans son article 21 que : « Les responsables de traitements non automatisés de données à caractère personnel intéressant la sûreté de l'Etat, la défense et la sécurité publique, dont la mise en œuvre est régulièrement intervenue avant la date de publication de la présente loi disposent, pour mettre leurs traitements en conformité avec les articles 6 à 9 de la loi n° 78-17 du 6 janvier 1978 précitée, dans leur rédaction issue de la présente loi, d'un délai allant jusqu'au 24 octobre 2010 »

Dès lors, de nombreux fichiers, applications ou projets de fichiers, devaient faire l'objet d'une mise en conformité avec les règles nationales de protection des libertés, suivant ainsi le processus vertueux initié par le Premier Ministre Michel Rocard en 1990 lors de la sortie de la clandestinité des fichiers des renseignements généraux et de la direction de la surveillance du territoire.

Faisant suite aux fichiers mécanographiques et aux bases de données informatisées, les exigences de la société de l'information appuyées par le progrès technique impliquent une mutation du travail des policiers et des gendarmes. L'interactivité des traitements dans le cadre de systèmes d'information permettant aux forces de l'ordre de gérer l'abondance du renseignement et d'en évaluer la pertinence devient un enjeu majeur.

Les traitements récents tels qu'ANACRIM ou SALVAC, et plus encore les projets de nouvelle génération dédiés à la révélation de faits sériels ou à la gestion de données multiples ne constituent plus, à proprement parler, des bases de données, mais représentent parfois des traitements induisant la création de fichier temporaires de travail dédiés à une procédure judiciaire spécifique.

La protection des données ne doit pas être opposée au progrès technique mais au contraire en bénéficier. A des systèmes opérationnels performants doivent répondre des modalités de contrôle nouvelles profitant des avancées technologiques.

De nombreux points ont fait l'objet d'un consensus dans le Groupe de Contrôle. D'autres sujets ont révélé des divergences profondes. Le principe a été retenu, dès le départ, de publier toutes les positions et leurs éclairages et de donner des éléments pratiques de compréhension de la dynamique du groupe sur certaines options, notamment en matière de signalement des personnes recherchées, dans le cadre de la caractérisation physique de ces dernières.

Depuis les années 50, sur l'idée d'un policier Marseillais, un outil (portant son patronyme "Canonge") permet de rechercher des auteurs dont l'identité n'est pas toujours établie de façon certaine. Ce fichier, créé en prenant notamment en compte l'apparence physique, mentionnait la couleur de la peau, puis à évoluer vers des caractéristiques ethno-raciales composites du fait du développement des technologies et du politiquement correct de l'époque.

En 2006, le groupe de travail avait notamment constaté la parfaite inadaptation du dispositif au principe de « critères physiques objectifs » en mettant notamment en exergue la catégorie « gitan » qui ne correspondait à aucun type physique particulier .... Il avait alors recommandé, outre la suppression immédiate de ce critère et la requalification du stock de fiches correspondantes, la mise en place d'un nouveau dispositif, loin d'être encore parfait, mais plus conforme, en 2006, à l'idée que l'on pouvait se faire de la manière dont on peut éventuellement caractériser les habitants de notre pays.

L'impossibilité pratique des services de police à mettre en place cette recommandation, en grande partie du fait du retard de fourniture du nouveau système informatique, a permis au groupe de contrôle de reprendre la discussion sur cette question. Une majorité de membres du groupe de contrôle a souhaité une évolution progressive issue des recommandations du groupe de 2006 légèrement modifiées en conservant les critères "d'apparence". D'autres membres de la commission (milieu associatif et Conférence des Bâtonniers) ont proposé le principe d'un nouveau système permettant de sortir de la classification ethno-raciale, et, qui pourrait par exemple, être basé sur une grille chromatique (à l'exemple du dispositif utilisé pour l'établissement des portraits-robots). Les échanges ont ainsi montré la difficulté de mettre en place un outil utile pour les victimes, efficace pour les policiers, et qui ne heurte pas frontalement l'opinion publique dans l'idée qu'elle se fait de lutte contre les discriminations. Par conséquent, et bien que le groupe de contrôle ait décidé de maintenir les critères liés à l'apparence, il préconise, dans le cadre de son éventuelle institutionnalisation, de réfléchir à l'évolution du système pour tous les fichiers de personnes recherchées construits sur le modèle du Canonge.

De la même manière, si certains s'opposent à toute prise en compte des mineurs dans les fichiers de renseignement (alors qu'ils s'y trouvent, notamment comme personnes disparues, comme auteurs supposés non condamnés, etc.) confondant souvent ces outils avec les fichiers judiciaires basés sur des procédures, d'autres considèrent que la question de l'âge est centrale tout en constatant certains effets du rajeunissement en quantité (mais plus en proportion) des mis en cause. Le groupe de contrôle a surtout souhaité mettre en place un outil de protection des mineurs quel que soit leur âge afin de garantir le droit à l'oubli et l'effacement des informations sous le contrôle d'un magistrat selon des règles calendaires très précises.

Pour ce qui relève des nouvelles applications permettant de découvrir la criminalité sérielle, le groupe a recommandé que leur mise en place soit strictement réduite aux faits graves de violences physiques, de trafic de stupéfiants ou de criminalité informatique d'une particulière gravité.

De plus, si l'accès direct aux fichiers de renseignements couverts par le secret-défense apparaît comme impossible, la possibilité de mettre en place un outil de contrôle indépendant, sur le modèle de la commission du secret de la défense nationale, a fait l'objet d'une proposition.

La plupart des autres propositions ont fait l'objet d'un consensus général ou quasi général.

Par ailleurs, dans le cadre du rapprochement de la police et de la gendarmerie nationales, il conviendra de mettre en place un système visant à empêcher les doublonnements inutiles de fichiers.

Le groupe de contrôle souhaite donc que ces recommandations puissent être entendues et mises en œuvre par le Gouvernement comme par le Parlement.

A titre personnel, je tiens à remercier la ministre de l'Intérieur, les directions générales de la police et de la gendarmerie nationales, la direction des libertés publiques et des affaires juridiques, la Préfecture de Police, la direction des affaires criminelles et des grâces et l'ensemble des membres du groupe de contrôle pour leur participation, leur contribution et leur ouverture au dialogue dans un délai très court.

Je tiens également à remercier le secrétaire général, André-Michel VENTRE et le rapporteur général, Christophe SOULLEZ, pour leur dévouement dans la gestion au quotidien de cette mission et pour la synthèse de ce rapport.

Alain BAUER

Criminologue

Président du Groupe de travail sur le contrôle des fichiers de police et de gendarmerie

CHAPITRE 1 - ETAT DES LIEUX

La France compte de nombreux traitements automatisés de données à caractère personnel tenus par l'administration ou des organismes publics et parapublics. Ils visent notamment à faciliter le travail des agents et des services de l'Etat et couvrent de très nombreux secteurs d'activité de l'administration française : sécurité intérieure, défense nationale, recensement des personnes de nationalité française et étrangère ou des contribuables, gestion des assurés sociaux, des personnes sans emploi, des allocataires du RMI ou de prestations familiales, comptabilisation du nombre de véhicules en circulation ou de titulaires de permis de conduire, enregistrement des décisions de justice ou encore gestion des détenus et des prévenus, etc.

La création de traitements automatisés a été l'une des conséquences du développement de l'utilisation des nouvelles technologies. Ainsi, au fur et à mesure que l'ordinateur devenait un outil incontournable de travail, les fichiers mécanographiques et les registres ont peu à peu disparu ou ont été remplacés par des traitements automatisés. Cette évolution a d'ailleurs rendu nécessaire l'entrée en vigueur d'une réglementation spécifique visant à garantir les libertés individuelles et collectives : la loi du 6 janvier 1978 dite « loi informatique et libertés ».

C'est ainsi que les traitements automatisés visant spécifiquement à aider les services de police ou les unités de gendarmerie à prévenir et à lutter contre la criminalité se sont développés au même titre que les bases de données gérées par d'autres administrations pour répondre à d'autres finalités. Ces traitements s'adaptent quotidiennement à l'évolution des phénomènes criminels ou terroristes pour tenter couvrir aujourd'hui l'ensemble du spectre de la criminalité.

Ce sont principalement des fichiers à vocation opérationnelle, c'est-à-dire des systèmes automatisés de données regroupant des informations sur des procédures en cours, des personnes mises en cause, des victimes, des individus faisant l'objet d'une surveillance particulière ou encore des personnes devant faire l'objet d'un enregistrement au regard de leur statut (passagers aériens, personnes sans domicile fixe, etc.). Il peut aussi s'agir de fichiers contenant des traces et indices (empreintes digitales, par exemple) ou des objets.

Ainsi, les services du ministère de l'Intérieur gèrent plusieurs dizaines de traitements différents aux finalités variées mais devant tous faire l'objet d'une déclaration à la commission nationale informatique et libertés. Ils ne peuvent être utilisés que dans les cas strictement prévus par la loi ou la réglementation et par les fonctionnaires spécifiquement visés dans les textes.

Les traitements automatisés de données à caractère personnel mis en œuvre peuvent être divisés en deux catégories distinctes :

- les fichiers de renseignement, administratifs ou judiciaires regroupant des informations sur des personnes physiques ou morales, des objets, ou moyens de transport, des traces laissées par des auteurs d'infractions.
- les systèmes d'information qui permettent d'exploiter des données réparties dans plusieurs fichiers

Au sein des premiers, les fichiers peuvent être distingués selon leurs finalités. Il existe tout d'abord des **fichiers purement administratifs** qui regroupent des informations objectives et « techniquement neutres » sur des personnes ou des objets. Ces fichiers se contentent d'enregistrer des données administratives sur des personnes, objets ou moyens de transport.

Le deuxième type de fichiers de police et de gendarmerie concerne les bases de données liées aux **missions de renseignement**. Les éléments « qualitatifs » prédominent dans ces fichiers qui ont pour principale finalité d'aider les forces de l'ordre à prévenir la criminalité et les actes de terrorisme. Ainsi, l'ouverture d'une enquête judiciaire, tant dans le cadre préliminaire que dans celui d'une instruction, suppose un minimum d'éléments convergents susceptibles d'emporter, si ce n'est la conviction, au minimum le doute, sur l'éventuelle préparation de la commission d'un crime. Certaines informations justifient des repérages ou recoupements complémentaires avant de pouvoir être exploitées dans le cadre d'une procédure judiciaire. D'une sensibilité encore plus grande au regard des missions de protection de la souveraineté nationale et de la sûreté de l'Etat qu'exerce la direction centrale du renseignement intérieur, le fichier de ce service bénéficie du régime dérogatoire ouvert par les articles 30 I et 44 IV de la loi de 1978 (non publication de l'acte de création et absence de droit de contrôle sur place de la CNIL).

Les **fichiers d'antécédents judiciaires** constituent une troisième catégorie de fichiers. Il s'agit principalement du système de traitement des infractions constatées (STIC) et du système judiciaire de documentation et d'exploitation (JUDEX) qui sont respectivement mis en œuvre par les services de police et par les unités de gendarmerie et qui font actuellement l'objet d'une modernisation dans le cadre du projet ARI@NE. Ces fichiers collectent certaines informations extraites des procédures de police judiciaire

réalisées par les enquêteurs. Leur finalité première est de faciliter la constatation des infractions pénales, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs. Ils permettent notamment mais de façon très limitative d'effectuer des rapprochements entre différentes affaires présentant des similitudes mais surtout de matérialiser, dès la phase d'enquête, l'état de récidive de certains auteurs de crimes ou délits. STIC et JUDEX, s'ils sont également utilisés dans des conditions et dans le cadre d'enquêtes administratives strictement autorisées par la loi[2], demeurent à ce jour les principaux outils d'orientation des enquêtes, alors que les fichiers d'empreintes digitales et génétiques sont aujourd'hui les principaux outils permettant l'identification formelle des auteurs. .

Les **fichiers d'identification judiciaires** sont sûrement les fichiers les plus connus et ceux qui ont récemment fait l'objet d'une modernisation et d'un développement accéléré au regard de l'évolution de la science et des techniques. Depuis la fin du XIX^{ème} siècle, qui a vu l'adoption des empreintes digitales comme outil de l'enquête criminelle, la biométrie a fait d'énormes progrès, qui se traduisent par de nouveaux outils d'aide à l'identification des personnes et à l'élucidation. La police technique et scientifique est un outil d'une puissance importante indispensable à l'analyse des traces laissées sur les scènes de crime, surtout lorsqu'il n'existe aucun témoin. La faible part laissée à la subjectivité permet d'ailleurs aussi bien de confondre un criminel que de disculper un innocent. Aussi les fichiers d'identification sont tout autant des outils à charge qu'à décharge. En raison de leur mode d'alimentation et de fonctionnement, ces fichiers sont exclusivement utilisés en police judiciaire, jamais dans un cadre de police administrative.

Les **fichiers d'analyse criminelle** sont des systèmes de traitement du renseignement judiciaire. Ils permettent de détecter la sérialité de certaines infractions grâce au traitement des informations contenues dans les procédures.

Enfin, les **fichiers d'identification administrative**, tout comme les fichiers administratifs, sont des systèmes techniquement neutres permettant notamment le recensement de la population.

Comme lors de ses travaux en 2006, le groupe de contrôle a donc principalement porté son attention sur les fichiers de police et de gendarmerie ainsi que sur ceux gérés par la Direction des Libertés Publiques et des Affaires Juridiques du ministère de l'Intérieur et a exclu de son champ de réflexion l'ensemble des fichiers administrés par d'autres administrations, à l'exception du Fichier judiciaire national automatisé des auteurs d'infractions sexuelles et violentes (FIJAIS).

Ne seront pas recensés dans ce rapport :

- Les fichiers de la Défense nationale

- Le fichier Réseau Mondial Visas 2[3] (RMV 2)

- L'application de gestion des dossiers des ressortissants étrangers en France (AGDREF)[4]

- Le fichier ELOI[5]

- Le fichier national des personnes incarcérées[6]

- Le casier judiciaire national[7]

- Le fichier des naturalisations[8]

- Fichiers de l'office français de protection des réfugiés et apatrides[9]

- Le répertoire national d'identification des personnes physiques[10]

- Le fichier du recensement

- Les fichiers d'état civil

---

2 Voir « Fichiers de police et de gendarmerie. Comment améliorer leur contrôle et leur gestion ? », Collection des rapports officiels, La documentation française, mars 2006. Voir également l'annexe n°1

[3] Arrêté du 22 août 2001

[4] Décret du 29 mars 1993

[5] Arrêté du 30 juillet 2006 relatif à l'informatisation de la procédure d'éloignement

[6] Arrêté du 28 octobre 1996 portant création d'un fichier national automatisé de personnes incarcérées.

[7] Loi du 4 janvier 1980 relative à l'automatisation du casier judiciaire. Décret du 6 novembre 1981

[8] Arrêté du 27 avril 1998 régissant l'accès télématique aux fichiers d'acquisition et de perte de la nationalité française de la sous-direction des naturalisations

[9] Arrêté du ministère des affaires étrangères du 5 novembre 1990. Arrêté du ministère des affaires étrangères du 6 novembre 1995. Arrêté du ministère des affaires étrangères du 9 décembre 1999

[10] Décret n°82-103 du 22 janvier 1982. Géré par l'Insee.

- Le fichier national des comptes bancaires (FICOBA)[11]

- Le fichier national des chèques irréguliers[12] (FNCI)

- Le fichier central des chèques[13] (FCC)

- Le Fichier national des incidents de remboursement des crédits aux particuliers[14]

Par ailleurs, il est à noter que le Fichier des Avis des Condamnations Pénales (FACP), qui était une sous-rubrique du FAR, ne figure plus dans celui-ci depuis la parution de la loi n°2004-801 du 6 août 2004. Il en est de même du Fichier Informatisé du Terrorisme (FIT), anciennement géré par la Direction générale de la Police Nationale, qui a été supprimé par décret n° 2008-631 du 27 juin 2008 portant modification du décret n° 91-1051 du 14 octobre 1991 relatif aux fichiers gérés par les services des renseignements généraux et du décret n° 2007-914du 15 mai 2007 pris pour l'application du I de l'article 30 de la loi n°78-17 du 6 janvier 1978.

1. LES FICHIERS EXISTANTS

1.1. Les applications bureautiques

a) ARAMIS

L'application Aramis, utilisée par la Gendarmerie Nationale, est un système de traitement des informations présentant un caractère opérationnel. Elle se compose de trois modules :

- COG : gestion des interventions.
- EVT : messagerie interne de suivi de situation.
- RENS : réception de la messagerie opérationnelle et de la messagerie organique.

Cette application a pour objet d'informer les autorités hiérarchiques, des évènements en cours, de leur évolution et de leurs développements.

Nature des informations contenues

Essentiellement orientée vers la gestion et le suivi de l'évènement, dans sa partie COG, Aramis contient certaines données nominatives (nom, prénom, domiciliation, téléphone). Lorsqu'une personne signale un fait à l'opérateur du Centre opérationnel et de renseignement de la gendarmerie (CORG), ce dernier renseigne un masque informatique sur lequel sont mentionnées des données personnelles. Ces informations sont recueillies dans un but d'authentification de l'appelant et conservées temporairement.

Les deux autres modules Aramis sont des outils de transmission hiérarchique de points de situation quantitatifs (EVT) et de partage et de diffusion de message de renseignement formatés (32600) pouvant contenir des données nominative (RENS) pour le suivi des événements d'ordre public.

Destinataires des informations

Lors de la gestion d'une intervention, les informations recueillies par le CORG sont destinées à informer la patrouille sur la situation en cours. Les autorités hiérarchiques immédiatement supérieures aux intervenants (brigade et compagnie) sont également destinataires du message d'intervention.

Modes d'alimentation, de consultation et d'apurement

L'application Aramis est une application locale en service dans les centres opérationnels de la Gendarmerie dans les départements (CORG) et les régions, et à la DGGN (CRO Gend). L'alimentation directe n'est possible que par les militaires affectés dans ces centres opérationnels. Toute unité élémentaire disposant d'un terminal Rubis, peut contribuer à l'alimentation d'Aramis par l'envoi d'un message que les opérateurs du CORG ont seuls la possibilité d'intégrer dans l'application.

La consultation des données, dans la gestion immédiate d'une intervention, est réalisée par l'opérateur du

[11] Géré par la Direction générale des impôts. 1er alinéa de l'article 1649 A du code général des impôts créant l'obligation fiscale de déclarer à la direction générale des impôts (DGI) l'ouverture et la clôture des comptes de toute nature ; arrêté du 14 juin 1982 modifié, pour partie codifié à l'annexe IV du code général des impôts (articles 164 FB et suivants).
[12] Loi du 30 décembre 1991 relative à la sécurité des chèques et des cartes de paiement. Géré par la Banque de France
[13] Créé en 1955 et géré par la Banque de France.
[14] Loi du 30/12/1989 intégrée au code de la consommation (art. L.333-4 et L. 333-5)

CORG. Les cellules RENS, au niveau des groupements et des régions, peuvent consulter la base « évènements » (EVT). Enfin, l'échelon régional et l'administration centrale ont un accès au module RENS.

La possibilité de la consultation répond rigoureusement au principe du droit d'en connaître. A chaque niveau hiérarchique, ou pour chaque type de module, des droits sont ouverts pour une catégorie d'unité.

L'apurement des données personnelles relatives aux appelants est automatisé au terme d'un délai de trois mois.

La totalité du contenu d'une fiche d'appel téléphonique et des interventions qui lui sont associées est supprimée au bout de deux ans.

Les messages du module RENS et EVT sont effacés au bout de deux ans et demi (120 semaines) La partie des EVT relative aux VTU (violences de type urbaines) n'est pas épurée. Elle ne contient toutefois que des données chiffrées.

Evolution fonctionnelle ou juridique

Le système de gestion de l'intervention et de suivi des évènements sera géré à partir d'octobre 2009 par le système d'information ATHEN@ qui conduira progressivement à la disparition d'Aramis.

b) Bureautique Brigade 2000 (BB2000)

Réf. : Arrêtés ministériels du 28/10/1992 et du 28/05/1993 modifiés par l'arrêté du 13/05/1998

Présentation et finalité

La Bureautique Brigade 2000 est une application locale installée dans les unités territoriales de la gendarmerie nationale en vue de gérer sur le plan administratif le service et les registres (courrier et procès-verbaux) et de permettre un partage de l'information sur la connaissance de la circonscription de l'unité (lieux et personnes particuliers).

Nature des informations contenues

Elle contient certaines données à caractère personnel au sein des modules suivants :

- le registre : il comporte les données relatives au courrier reçu et envoyé par l'unité ainsi que celles concernant les procédures rédigées. On retrouve les références de la personne « cliente » de l'unité: le nom, le prénom, la date de naissance, le lieu de naissance et la qualité de la personne (victime, auteur entendu).
- les amendes forfaitaires : données relatives au nom, prénom, date de naissance, lieu de naissance de la personne à qui a été délivrée l'amende forfaitaire et le type d'infraction relevée.
- le message d'information statistique : données concernant le nom, le prénom, la date de naissance, le pays de naissance et la qualité (victime ou mis en cause) jusqu'au moment de la transmission de la procédure vers l'autorité destinatrice (parquet ou instruction). Sur le plan statistique, seules les informations concernant le sexe, l'âge et la nationalité sont prises en compte. Le nom et le prénom ne sont mentionnés que pour permettre à l'enquêteur de remonter les bonnes informations dans le cas de pluralité de victimes ou de mis en cause.
- le BAAC (bulletin d'analyse d'accident corporel) : données concernant le nom, le prénom, la date et le pays de naissance, la qualité (indemne, blessé, mort), la responsabilité au regard de l'accident et les infractions éventuellement relevées jusqu'au moment de la génération du bulletin (30 jours après l'accident) en vue d'alimenter l'ONISR (Observatoire National Interministériel de la Sécurité Routière), la CUB (Communauté Urbaine de Bordeaux – ne concerne que les accidents constatés sur cette emprise) et le CEESAR (Centre Européen d'Etudes de Sécurité et d'Analyse des Risques). Seules les informations statistiques sont envoyées à ces organismes (sexe, date de naissance, département ou pays de naissance, qualité, position dans le véhicule, la responsabilité au regard de l'accident, infractions éventuellement relevées (au nombre de deux).
- le dossier de circonscription : données concernant l'identité, le domicile, l'activité (hors toute indication à caractère politique ou syndical) des personnes travaillant ou résidant sur la circonscription de l'unité et devant être connues du fait de leurs responsabilités (députés, sénateurs, conseillers généraux, maires, chefs d'entreprise, commerçants, ...), de leur attachement au milieu militaire (parents proches d'un gendarme décédé, officier de réserve, ...) ou de décisions de justice (interdiction de séjour, permission pénitentiaire, assignation à résidence, ...).

Destinataires des informations

Seuls les personnels de la gendarmerie sont destinataires des informations contenues dans l'application en dehors du BAAC.

Modes d'alimentation, de consultation et d'apurement

L'alimentation des données se fait par saisie manuelle sur les postes de travail de l'unité. La consultation ne peut se faire qu'au travers de l'application en local à l'unité.

Les règles d'apurement varient en fonction des modules :

- le registre : apurement au terme de 2 ans échus.
- les amendes forfaitaires : apurement au terme de 2 ans échus.
- le message d'information statistique : apurement automatique de la partie nominative dès transmission du message.
- le BAAC (bulletin d'analyse d'accident corporel) : apurement automatique de la partie nominative dès transmission du message.
- le dossier de circonscription : toute mise à jour entraîne la suppression des données précédentes (pas d'historique).

Evolution fonctionnelle ou juridique

Cette application sera remplacée par l'application PULS@R en 2009

c) Logiciel de rédaction de procédures (LRP)

Réf. : Déclaration à la CNIL simultanée à la déclaration du STIC.

Le LRP permet de rédiger les procès-verbaux, notamment de plainte, et les rapports administratifs ou judiciaires, sur un poste informatique relié à une imprimante. Il permet de mémoriser au plan local les informations que ces documents contiennent pour automatiser les aspects répétitifs de la rédaction et améliorer la qualité des données recueillies.

Il correspond à la fonction bureautique du STIC et permet :

- la rédaction et l'édition des documents de procédure normalisés en utilisant la « bibliothèque » des modèles de documents les plus couramment utilisés, mise à leur disposition dans le logiciel ;
- l'automatisation de la rédaction de formules littérales ;
- une aide dynamique à la rédaction par l'utilisation de tables de contrôle normalisant le vocabulaire employé ;
- la constitution d'une base de modèles personnels pour chaque utilisateur ;
- la gestion des procédures avec la possibilité de créer des dossiers informatiques regroupant tous les documents concernant une même affaire.

Le logiciel permet de rappeler les identités déjà mémorisées et de les intégrer au document en cours, sans avoir à effectuer une nouvelle saisie.

Le LRP fait l'objet de mises à jour régulières, en fonction des évolutions législatives de la procédure pénale.

La dernière version, généralisée en 2004, a pris en compte les dispositions relatives à la garde à vue de la loi « Perben II ».

d) Main courante informatisée (MCI)

Réf. : Arrêté du 24/02/1995

Cadre juridique et finalités

La MCI est un traitement local conçu en 1990 par la direction centrale de la sécurité publique (DCSP) et autorisé par un arrêté du 24 février 1995. Son emploi est généralisé, depuis le 1er janvier 2005, dans l'ensemble des circonscriptions de sécurité publique (CSP).

La MCI poursuit plusieurs finalités :

- la gestion de l'emploi des effectifs en fonction des règles d'emploi en vigueur ;
- la gestion des événements de manière chronologique, de façon à faciliter les recherches opérationnelles et la production de statistiques ;
- la gestion des déclarations des usagers.

La MCI actuelle sera prochainement remplacée par un nouveau logiciel, dont le dossier de déclaration est en cours d'instruction. A cette occasion, la MCI sera élargie à d'autres services de police (notamment pour sa fonction de gestion du personnel).

Données enregistrées et durées de conservation

Les données concernant les personnes (requérants, témoins, victimes, personnes mises en cause) sont peu nombreuses (notamment état civil et adresse).

Sont collectés, en ce qui concerne les fonctionnaires de police : l'identité et l'état civil, les coordonnées téléphoniques et postales, le numéro de carte professionnelle, le type et le numéro de l'arme, la personne à prévenir en cas d'accident.

Aucune durée de conservation des données n'a été déterminée par l'arrêté portant création de la MCI. La règle applicable, comme d'ailleurs à tout traitement, est celle définie par l'article 6 de la loi du 6 janvier 1978 : une donnée ne peut être conservée que pour autant qu'elle est toujours nécessaire eu égard aux finalités du fichier. Le projet d'arrêté relatif à la nouvelle main courante informatisée (application qui remplacera la MCI en 2009) définit les durées de conservation.

Modalités d'alimentation et de consultation

Seuls les agents habilités et détenteurs d'un mot de passe peuvent accéder à la MCI.

Les différents profils d'habilitation sont définis dans chaque CSP : certains agents peuvent alimenter la MCI sans pour autant avoir la capacité de la consulter et inversement.

La consultation ne peut porter que sur des données enregistrées localement (les utilisateurs n'ont pas accès à une base départementale ou nationale).

Utilisation opérationnelle

La MCI permet de suivre en permanence l'activité d'un service. Les statistiques établies à partir des données de la MCI permettent de mesurer avec précision les contraintes et les marges de manœuvre, ainsi que l'adéquation entre la répartition temporelle des phénomènes d'insécurité et la distribution horaire des effectifs.

Enfin, les comptes rendus d'intervention et les déclarations du public constituent une source d'informations pour les enquêteurs. En effet, ces données peuvent aider à caractériser des situations délictuelles (occupation de hall d'immeuble, trafic de stupéfiants, etc.) ou à élucider des affaires judiciaires (recherche de domiciles, de fréquentations ou de véhicules).

e) Fichier de gestion du service central de préservation des prélèvements biologiques (SCPPB)

Réf. : Arrêté ministériel du 13/09/2002

Présentation et finalité

Le traitement automatisé du SCPPB a pour finalité d'assurer la gestion des prélèvements biologiques recueillis :

- sur une scène de crime ou de délit pour l'une des infractions mentionnées à l'article 706-55 du Code de procédure pénale ;
- à l'occasion des procédures de recherche des causes de la mort (cadavres non identifiés) ;
- à l'occasion des procédures de recherche des causes d'une disparition (personnes disparues).

Nature des informations contenues

Les catégories d'informations enregistrées sont celles relatives à l'autorité judiciaire et aux services ou unités requérants, aux scellés, aux éléments d'identité de la personne disparue, au service ou unité ayant effectué le prélèvement, à la restitution et à la destruction, à l'agent de saisie ou de stockage des scellés et au code-barres d'identification.

Destinataires des informations

Les destinataires des informations enregistrées sont, en fonction de leurs attributions respectives et du besoin d'en connaître :

- le service central de préservation des prélèvements biologiques ;
- les autorités judiciaires (procureur de la république – juge d'instruction) ;
- le magistrat du parquet et les membres du comité de contrôle désignés en vertu des articles R. 53-16 et R. 53-20 du code de procédure pénale.

Modes d'alimentation, de consultation et d'apurement

Les réquisitions et les scellés sont transmis par voie postale. Dès réception, un personnel du SCPPB procède à la saisie des informations citées supra dans la base locale.

La consultation du fichier se fait sur place par un personnel du SCPPB.

La durée de conservation des informations enregistrées est de quarante ans.

Au 31 juillet 2008, 18.129 scellés sont conservés au SCPPB.

Situation juridique actuelle

Le fichier de gestion du SCPPB a fait l'objet d'une déclaration auprès de la CNIL et d'un arrêté ministériel en date du 13 septembre 2002 (NOR: DEFG0202133A)

f) Logiciel Ic@re

Présentation et finalités

Le logiciel Ic@re est destiné à assister les militaires de la gendarmerie dans la rédaction de leurs procès-verbaux. Cet outil participe, par ailleurs, à la remontée d'informations en alimentant les bases de données opérationnelles des renseignements pertinents.

La finalité de ce traitement est :

- de rédiger des procès-verbaux et des rapports dressés par les officiers ou agents de police judiciaire ;
- de faciliter et d'optimiser les tâches des personnels de la gendarmerie nationale habilités à traiter les procédures dont ils sont saisis ;
- d'éviter la redondance de la saisie des informations procédurales ;
- de permettre aux destinataires mentionnés de disposer d'une copie papier de tout ou partie de la procédure ;
- de permettre la remontée d'informations vers les bases de données judiciaires. Les formulaires ICARE contiennent, à cet effet, des balises informatiques (format XML) permettant la sélection des éléments éligibles. Sont ainsi alimentés le fichier des véhicules volés (FVV) et le fichier JUDEX, puis, à leur remplacement, le fichier des objets et véhicules signalés (FOVeS), la base ARIANE et la future application CASSIOPEE du ministère de la justice en cours de développement.

Le système Ic@re n'est pas une base de données mais un vecteur d'information.

Nature des informations contenues

Les données sont enregistrées dans des documents au format Open Office. Elles ne sont pas stockées dans une base structurée. Elles sont conservées au niveau des unités élémentaires le temps de l'enquête et effacées suite à la transmission de la procédure aux autorités judiciaires en charge du dossier. Ces données sont enregistrées au niveau d'un registre de procédure et ne sont pas liées entre elles.

La nature des données contenues varie en fonction des besoins de l'enquête. Les pièces de procédure (audition de témoin, procès-verbal de garde à vue, ...) peuvent contenir des données considérées comme sensibles au sens de la législation sur la protection des données à caractère personnel. Ces informations sont inhérentes aux investigations judiciaires. Toutefois, elles ne sont pas accessibles par un index ou autre système automatisé de recherche. Par ailleurs, ces données ne sont pas éligibles pour l'alimentation des fichiers judiciaires.

Les catégories de données à caractère personnel soumises à déclaration sont celles relatives :

- à l'identité de l'officier ou agent de police judiciaire : nom, prénom, grade et qualité ;
- aux destinataires institutionnels habituels de l'unité de gendarmerie : nom, prénom, qualité, tribunal de rattachement, adresse, téléphone professionnel des magistrats, des services préfectoraux et des personnes requises dans le cadre de la procédure ;
- à l'identité de la victime ou du témoin : nom, prénom, adresse, date et lieu de naissance, profession, numéros de téléphone ;
- à l'identité du mis en cause : nom, prénom, adresse, date et lieu de naissance, filiation, profession, numéros de téléphone ;
- à la personne morale : forme juridique, secteur d'activité, raison sociale, numéro SIRET, adresse ;
- à la procédure judiciaire : cadre juridique, code et nature de l'infraction, date et lieu de l'infraction, caractéristiques des éventuels objets dérobés ou découverts ;

Destinataires des informations contenues

Peuvent accéder aux informations dans le respect des règles du code de procédure pénale et par utilisation directe de l'application, les enquêteurs de la gendarmerie nationale au sein d'une même unité territoriale.

Peuvent être destinataires de tout ou partie des données enregistrées, par copie papier de la procédure et en fonction de leurs attributions respectives et du besoin d'en connaître :

- les magistrats pour les affaires dont ils sont saisis ;
- les avocats en cas de mise en examen ou de comparution immédiate d'une personne mise en cause ;

Peuvent prendre connaissance par lecture et signature des actes relatant leurs propos et opérations réalisées en leur présence, les personnes victimes, témoins ou mises en cause dans le cadre d'une procédure.

Mode d'alimentation, de consultation et d'apurement

Issues des procès-verbaux rédigés par les enquêteurs, les données à caractère personnel sont conservées jusqu'à clôture de la procédure et transmission aux autorités judiciaires compétentes. Elles ne sont accessibles qu'au niveau de l'unité de rattachement de la procédure. Elles sont attachées à un numéro unique de procès verbal délivré par le système d'information de la gendarmerie nationale. Aucun transfert de données n'est possible entre deux procédures différentes.

Situation juridique actuelle

L'application a été présentée au commissaire du gouvernement auprès de la CNIL en févier 2008. Après des échanges techniques, le dossier de déclaration a été adressé en juillet 2008 à la direction des affaires juridiques (DAJ) du ministère de la défense conformément à la procédure en vigueur.

1.2. Les fichiers administratifs

a) Fichier de la batellerie

Réf. : Ce fichier n'a fait l'objet d'aucune déclaration. Sa destruction est prévue avant l'échéance du 24 octobre 2010 au titre de l'article 21 de la loi du 6 août 2004.

Présentation et finalité

Le fichier de la batellerie a été créé en 1942 afin d'assurer le suivi des mariniers ainsi que celui des bateaux affectés au transport fluvial de marchandises et des compagnies fluviales. Fichier mécanographique géré historiquement par la brigade de Conflans-Sainte-Honorine (78), il est aujourd'hui, stocké en l'état au service technique de recherches judiciaires et de documentation (STRJD) à Rosny-sous-Bois (93).

Nature des informations contenues

Riche de 52000 fiches, ce fichier recense des informations concernant les mariniers, leur famille, leurs ouvriers, leur bateau et leur employeur. Il regroupe également des informations concernant les compagnies fluviales et entreprises de transport fluvial.

Destinataires des informations

Les unités de la gendarmerie, et très exceptionnellement des services de la police ou des administrations, étaient les seuls destinataires des informations de ce fichier. En raison de la désuétude des données qu'il

contient, ce fichier n'est plus opérationnel aujourd'hui.

Modes d'alimentation, de consultation et d'apurement

Ce fichier n’est plus utilisé.

Les diverses informations recueillies sur les voies navigables par les unités de gendarmerie étaient transmises à la brigade de Conflans-Sainte-Honorine chargée de l'alimentation.

Le fichier de la batellerie est devenu obsolète en raison de son mode d'alimentation et de fonctionnement.

Depuis 1974, une procédure d'apurement a été mise en place et consiste en la destruction des fiches concernant les mariniers décédés ou ayant atteint l'âge de 80 ans, ainsi que celles des bateaux détruits.

Evolution fonctionnelle ou juridique

Une informatisation des données recueillies a été étudiée mais n'a pas été retenue. En conséquence de quoi ce fichier sera détruit avant l’échéance du 24 octobre 2010.Compte-tenu du développement de la navigation fluviale et de la problématique transfrontalière induite, le réseau Aquapol (réseau européen de polices fluviales développé depuis 2004) propose à ses membres l'élaboration d'un outil informatique visant à conserver une « mémoire » des contrôles effectués sur les voies d'eau européennes. La gendarmerie nationale suivra les développements de ce projet sur lequel elle n'a pas pris position et envisagera à temps sa contribution à ce nouvel outil.

b) Fichier des personnes nées à l'étranger de la Gendarmerie Nationale (FPNE)

Réf. : Aucune. Sa destruction est prévue avant l’échéance du 24 octobre 2010 au titre de l'article 21 de la loi du 6 août 2004.

Présentation et finalité

Créé en 1975, le fichier des personnes nées à l'étranger est un fichier mécanographique. A l'instar du fichier alphabétique de renseignements (FAR), il est constitué de fiches cartonnées individuelles. A ce jour, le FPNE comporte environ 7 millions de fiches.

Ce fichier a pour objet de collationner les renseignements relatifs aux personnes nées hors de France. Il ne concerne pas les personnes de passage pour une courte durée (tourisme, visite familiale...).

Nature des informations contenues

Ses modalités de tenue et d'exploitation sont relativement similaires à celles fixées pour le FAR (particularité par rapport au FAR : une fiche est établie à la suite d'un contrôle ou d'une identification par les unités de gendarmerie).

Destinataires des informations

Toute unité de gendarmerie établissant une procédure ou constatant un fait méritant d'être gardé en mémoire établit une fiche individuelle. Elle est destinée au STRJD implanté à Rosny Sous Bois (93).

Modes d'alimentation, de consultation et d'apurement

Ce fichier est aujourd’hui neutralisé

Situation juridique actuelle

Le FPNE est actuellement stocké à l’état d’archive et ne fait plus l'objet de consultations ni d'une administration fonctionnelle. Sa destruction (avec PV d'incinération) est prévue avant l’échéance fixée par l'article 21 de la loi n°2004-801 du 6 aout 2004 (24 octobre 2010).

Evolution fonctionnelle ou juridique

Aucune reprise des données n’est envisagée.

La mise à jour et la consultation du FPNE ont été abandonnées en septembre 2007 (message 126319 DEF/GEND/OE/SDPJ/PJ du 14 septembre 2007)

Droit d'accès aux informations

Le droit d'accès au FPNE s'effectuait indirectement et simultanément, à l'instar du FAR et JUDEX par l'intermédiaire de la commission nationale de l'informatique et des libertés.

c) Fichier de suivi des personnes faisant l'objet d'une rétention administrative

Réf. : Arrêté interministériel du 19/12/1994 modifié par l'arrêté du 30/07/2002.

Présentation et finalité

Les groupements de gendarmerie départementale de Seine-et-Marne, du Bas-Rhin et des Pyrénées-Orientales auxquels sont rattachés respectivement les centres de rétention administrative (CRA) du Mesnil-Amelot, de Geispolsheim et de Rivesaltes, mettaient chacun en œuvre un fichier nominatif informatisé dont la finalité est d'assurer le suivi des personnes faisant l'objet d'une décision de rétention.

Nature des informations contenues

Les catégories d'informations nominatives enregistrées dans ce traitement automatisé sont celles relatives à l'identité, à la nationalité et au domicile en France des personnes concernées. Depuis 2002, la photographie numérisée des personnes retenues est annexée au fichier automatisé.

Destinataires des informations

Les destinataires de tout ou partie des informations enregistrées sont, en fonction de leur besoin d'en connaître, les personnels de la brigade territoriale du lieu d'implantation du centre ainsi que les membres du CIMADE (service d'entraide).

Modes d'alimentation, de consultation et d'apurement

Les informations sont saisies directement par les militaires du détachement gestionnaire à l'occasion de la prise en compte du retenu lors de son arrivée au centre et mises à jour au fil de l'eau (libération du retenu, départ vers le pays de son choix, présentation à son consulat...).

Le droit d'accès prévu par l'article 34 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'exerce soit par écrit auprès du commandant de groupement de gendarmerie départementale du lieu d'implantation du centre, soit auprès du responsable du détachement de gendarmerie chargé de sa gestion.

Si la personne ne fait pas l'objet d'une nouvelle mesure de rétention pendant une durée de 2 ans, les informations sont effacées.

Evolution fonctionnelle ou juridique

Le MIOMCT (DCPAF) a développé le système « ELOI », qui permet une gestion commune inter services (police, gendarmerie, administration pénitentiaire et préfecture) des étrangers. La mise en œuvre du système « ELOI », en 2008 a entraîné l'abandon par la gendarmerie de l'application SUICRA

d) Fichier des passagers aériens (FPA)

Réf. : Loi du 23/01/2006, décret n°1630-2006 du 19/12/2006, arrêté du 19/12/2006

Cadre juridique et finalités

La directive du 29 avril 2004 du Conseil de l'Union européenne institue l'obligation, pour les transporteurs, de communiquer des données personnelles relatives à leurs passagers. Cette obligation a été introduite dans le droit interne par l'article 7 de la loi du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers, qui crée un dispositif expérimental.

Le FPA a pour but d'améliorer le contrôle aux frontières, de lutter contre l'immigration clandestine et de contribuer à la prévention et à la répression des actes de terrorisme.

Données enregistrées et durées de conservation

Actuellement, seules les compagnies aériennes assurant des liaisons directes avec cinq pays (désignés par une décision non publiée du ministre de l'intérieur mais communiquée à la CNIL) ont obligation de transmettre la liste de leurs passagers à l'arrivée et au départ de la France.

Les informations devant être transmises par les compagnies aériennes, dès la clôture du vol, sont des données d'enregistrement (données dites APIS) :

- nom complet, date de naissance, sexe, nationalité ;
- numéro et type du document de voyage utilisé ;
- pays de résidence ;
- point de passage frontalier utilisé pour entrer sur le territoire français ou en sortir ;
- code de transport (identifiant de la compagnie et numéro de vol) ;
- heures de départ et d'arrivée ;
- nombre total de personnes transportées ;
- point d'embarquement et de débarquement.

Le traitement est interconnecté avec le fichier des personnes recherchées (FPR) et le sera dans les prochains mois avec le système d'information Schengen (SIS).

La durée de conservation des données est de 5 ans pour la lutte contre le terrorisme et 24 heures pour la lutte contre l'immigration clandestine. Une procédure automatique de suppression des données est mise en œuvre.

Toute intervention sur la base de données fait l'objet d'un enregistrement qui permet une traçabilité totale.

Modalités d'alimentation et de consultation

Seuls ont accès au traitement les agents individuellement habilités appartenant aux services de police aux frontières et à certains services spécialisés.

Utilisation opérationnelle

Au 3 octobre 2008, 213 814 passagers ont été enregistrés dans la base de données (depuis le 1er mai 2007).

Evolution fonctionnelle ou juridique

Ce traitement a été créé par l'arrêté du 19 décembre 2006 pour une durée de deux ans. Il fait actuellement l'objet d'une nouvelle déclaration à la CNIL pour reprise de l'expérimentation.

e) Application de gestion du répertoire informatisé des propriétaires et possesseurs d'armes (AGRIPPA)

Réf. : Arrêté du 15 novembre 2007 portant création de l'application de gestion du répertoire informatisé des propriétaires et possesseurs d'armes.

Présentation et finalité du fichier

AGRIPPA est un traitement automatisé de données à caractère personnel concernant la gestion et le suivi des détentions d'armes et de munitions.

Ce traitement a pour finalité l'enregistrement et le suivi des autorisations et des récépissés de déclarations délivrés par l'autorité administrative relatifs au régime des matériels de guerre, armes et munitions des 1ère et 4ème catégories et des armes et éléments d'armes soumis à déclaration des 5ème et 7ème catégories.

Nature des informations enregistrées

Les catégories de données enregistrées dans AGRIPPA sont les suivantes :

1° En ce qui concerne les personnes physiques :

- état civil ;
- domicile ;
- profession ;

2° En ce qui concerne les personnes morales :

- raison sociale ;
- n° SIREN, SIRET ;
- adresse ;

3° En ce qui concerne les autorisations et déclarations d'acquisition et de détention :

- caractéristiques de l'arme ;
- date de la délivrance de l'autorisation ou du récépissé de déclaration ;
- date d'expiration de l'autorisation ;

4° En ce qui concerne la décision de refus de délivrance d'une autorisation d'acquisition et de détention d'arme ou d'un récépissé de déclaration de détention d'arme :

- le cas échéant, caractéristiques de l'arme ;
- date de refus et date de notification de refus ;
- le cas échéant, date des recours déposés à l'encontre de la décision.

Présence de mineurs et si, oui, existe-t-il une limite d'âge ?

Les mineurs sont présents dans AGRIPPA pour :

- les armes soumises à autorisation à partir de 12 ans (décret n° 95-589 du 6 mai 1995 modifié relatif à l'application du décret du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions, article 28 I b 2°),
- les armes soumises à déclaration à partir de 16 ans (décret n° 95-589, article 46-1 3°).

Destinataires des informations

Peuvent seuls être destinataires des données à caractère personnel enregistrées dans AGRIPPA :

- les agents des services centraux du ministère de l'intérieur (direction des libertés publiques et des affaires juridiques et direction des systèmes d'information et de communication) individuellement désignés et spécialement habilités respectivement par le directeur des libertés publiques et des affaires juridiques et par le directeur des systèmes d'information et de communication ;
- les agents des services préfectoraux, compétents pour l'application de la réglementation relative aux armes, éléments d'armes et munitions, individuellement désignés et spécialement habilités par le préfet.

Modes d'alimentation du fichier

AGRIPPA est alimenté par les agents des services préfectoraux.

Modes de consultation et traçabilité

Peuvent consulter les données à caractère personnel enregistrées dans AGRIPPA :

- les agents des services de la police nationale, dans le cadre de leurs attributions légales, individuellement désignés et spécialement habilités, soit par les chefs des services déconcentrés de la police nationale, soit par les chefs des services actifs à la préfecture de police ou, le cas échéant, le préfet de police, soit par les chefs des services centraux de la police nationale ou, le cas échéant, le directeur général de la police nationale ;
- les militaires des unités de la gendarmerie nationale, dans le cadre de leurs attributions légales, individuellement désignés et spécialement habilités par le commandant du groupement de gendarmerie départementale ou, le cas échéant, par le directeur général de la gendarmerie nationale ;
- les agents des services des douanes, dans le cadre de leurs attributions légales, individuellement désignés et spécialement habilités par le directeur régional ou, le cas échéant, par le directeur général des douanes et droits indirects ;
- les agents du service national de la douane judiciaire, dans le cadre de leurs attributions légales, individuellement désignés et spécialement habilités par le magistrat délégué aux missions judiciaires de la douane ou, le cas échéant, par le directeur général des douanes et droits indirects.

L'accès par tous moyens techniques mobiles aux données du fichier est ouvert à ces seuls personnels.

En ce qui concerne la protection de l'intégrité de l'information (traçabilité), il est opéré un contrôle des accès réalisés dans le réseau. Tout accès à un système est mémorisé avec l'identifiant de l'utilisateur. Les opérations de création, mise à jour et tout autre évènement de fonctionnement sont collectés dans des journaux.

Les logiciels sont compilés. L'identifiant et le mot de passe sont cryptés. Ainsi, ils ne peuvent être ni lus, ni déchiffrés, ni altérés frauduleusement.

AGRIPPA journalise les accès et enregistre quotidiennement l'annuaire LDAP. Les journaux d'évènements et l'annuaire d'authentification sont également sauvegardés quotidiennement.

Durée de conservation

Les informations relatives au détenteur d'armes, d'éléments d'armes et de munitions sont conservées durant vingt ans soit à compter de la date où l'intéressé(e) a cessé d'être en possession de ces matériels pour des motifs autres que la perte ou le vol, soit à compter de la date de leur déclaration de perte ou de vol.

En cas de décision de rejet d'une demande d'autorisation d'acquisition et de détention d'armes, d'éléments d'armes et de munitions, les informations relatives au demandeur sont conservées durant cinq ans.

Droit d'accès aux informations

Les droits d'accès et de rectification sont exercés auprès des préfets de départements et, à Paris, du préfet de police dans les conditions fixées aux articles 39 et 40 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Modalités d'apurement

La création, la modification et la suppression des comptes d'utilisateurs et des dossiers sont réalisés au niveau national par l'administrateur central de la DLPAJ.

Évolution fonctionnelle ou juridique

L'adaptation d'AGRIPPA à la réglementation introduite par le décret n° 2005-1463 du 23 novembre 2005 relatif au régime des matériels de guerre, armes et munitions, pris pour l'application du code de la défense et modifiant le décret n° 95-589 du 6 mai 1995, est en cours de réalisation avec la direction des systèmes d'information et de communication.

L'arrêté sera prochainement modifié pour tenir compte de la répartition des compétences entre les directions du ministère de l'intérieur, de l'outre-mer et des collectivités territoriales, issues du décret n° 2008-1241 du 28 novembre 2008 (changement du service gestionnaire du traitement).

Utilisation opérationnelle

Le traitement comporte 2 060 344 dossiers de personnes physiques détentrices et 8 966 dossiers de personnes morales détentrices.

f) Le fichier national des interdictions de stade (FNIS)

Réf. : Arrêté du 28 août 2007 portant création d'un traitement automatisé de données à caractère personnel relatif aux personnes interdites de stade.

Présentation et finalité du fichier :

Le FNIS est un traitement automatisé de données à caractère personnel concernant la lutte contre les violences lors de manifestations sportives et plus spécialement le contrôle des supporters violents ou « hooligans ».

Ce traitement a pour finalité de prévenir et de lutter contre les violences lors de manifestations sportives, notamment en garantissant la pleine exécution des mesures d'interdictions administratives et judiciaires de stade, en facilitant les contrôles aux abords et dans les enceintes sportives, en facilitant le suivi et la surveillance des supporteurs à risque ayant déjà fait l'objet d'une mesure d'interdiction, en permettant à l'autorité préfectorale, le cas échéant, de mieux apprécier le comportement d'ensemble adopté par les intéressés à l'occasion de différentes manifestations sportives et en réalisant des statistiques.

Nature des informations enregistrées :

Les catégories de données à caractère personnel enregistrées dans le FNIS sont les suivantes :

1° Données relatives à la personne :

- identité (nom, prénom, alias et sexe) ;
- date et lieu de naissance ;
- nationalité ;
- adresse ;
- le club de football, le championnat ou l'association de supporters fréquentés par la personne, en prenant notamment en compte les déclarations de l'intéressé ou les informations recueillies lors de la procédure ;
- la photographie.

2° Données relatives à la mesure d'interdiction :

- la nature administrative ou judiciaire de la décision ;
- la date de la décision ;
- la date de sa notification ;
- la durée de la validité de la décision ;
- le champ géographique ;
- le type de manifestations concernées ;
- l'obligation de pointage ou non ;
- le lieu de pointage ;
- l'autorité judiciaire ou administrative ayant pris la décision notifiée ;
- la décision de justice qui prononce la suspension ou l'annulation de l'interdiction de stade.

Dans le cadre des engagements internationaux, informations relatives aux sanctions pénales, aux mesures judiciaires ou administratives d'interdiction prononcées à l'encontre des ressortissants français ou non à l'occasion de manifestations sportives à l'étranger.

Présence de mineurs et si, oui, existe-t-il une limite d'âge

Sans objet, il n'y a pas de mineurs dans le traitement.

Destinataires des informations

Sont destinataires de la totalité ou, à raison de leurs attributions ou de leur droit à en connaître pour l'exercice de leur mission, d'une partie des données figurant dans le FNIS :

- les préfets de département et à Paris, le préfet de police ou les fonctionnaires de préfecture individuellement désignés et dûment habilités par l'autorité préfectorale ;
- les autorités judiciaires ;
- les militaires des unités de la gendarmerie nationale individuellement désignés et dûment habilités par le commandant du groupement départemental ;
- les fédérations sportives agréées ;
- les organismes de coopération internationale en matière de police judiciaire et les services de police étrangers, dans les conditions énoncées à l'article 24 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, sans préjudice des dispositions conventionnelles particulières.

Modes d'alimentation du fichier

Le FNIS est alimenté par extraction des données issues des fiches judiciaires ou administratives d'interdits de stade du fichier des personnes recherchées (FPR).

Dans le cadre des engagements internationaux, le traitement est, par ailleurs, constitué des données à caractère personnel équivalentes à l'interdiction de stade et provenant des traitements gérés par des organismes de coopération internationale en matière de police judiciaire ou des services de police étrangers qui présentent un niveau de protection suffisant de la vie privée, des libertés et des droits fondamentaux.

Modes de consultation et traçabilité

Peuvent accéder aux données figurant dans le FNIS dans chaque département :

- les personnels de la direction centrale de la sécurité publique individuellement désignés et dûment habilités respectivement par le directeur départemental de la sécurité publique dans chaque département ou, le cas échéant, le directeur central de la sécurité publique ;
- les personnels de la préfecture de police (direction de la police urbaine de proximité, direction de l'ordre public et de la circulation, renseignement généraux de la préfecture de police de Paris, individuellement désignés et dûment habilités par l'autorité préfectorale.

Chaque consultation de fiche fait l'objet d'un enregistrement de traçabilité :

- quel fonctionnaire habilité a consulté le fichier ;
- pour quelle fiche nominative ;
- quelle requête (question posée pour établir une liste nominative ;
- quel jour ;
- à quelle heure ;
- depuis quelle machine (adresse IP machine et MAC – adresse carte réseau).

Durée de conservation

Les données à caractère personnel sont conservées pendant cinq ans à compter de l'expiration de la dernière mesure prononcée.

Les données à caractère personnel issues des organismes de coopération internationale en matière de police judiciaire et des services de police étrangers sont conservées pendant une durée de cinq ans à compter de l'expiration du prononcé de la décision d'interdiction sous réserve des engagements internationaux.

Droit d'accès aux informations

Le droit d'accès et de rectification aux données s'exerce de manière indirecte auprès de la Commission nationale de l'informatique et des libertés dans les conditions prévues à l'article 41 de la loi du 6 janvier 1978.

Modalités d'apurement

Les données concernant les mesures sont récupérées automatiquement et exclusivement du fichier des personnes recherchées (fiche individuelle) ; elles ne sont pas enrichies de nouvelles données dans le FNIS. Elles concernent exclusivement des renseignements techniques (coordonnée de l'autorité, durée de l'interdiction, période d'exécution, portée territoriale) à l'exclusion des motifs de fond de la décision administrative ou judiciaire d'interdiction de stade.

Les mises à jour de ces données sont quotidiennes et systématiquement issues de la mise à jour des fiches individuelles du FPR. Elles peuvent concerner d'éventuelles rectifications d'adresse, les renseignements de notification ainsi que les dates de validité des mesures. Ces rectifications sont exclusivement réalisées par les services d'alimentation du FPR, jamais directement dans le FNIS.

Les anciennes adresses ne sont pas conservées.

Les données sont conservées le temps de la validité de la mesure pour faciliter leur exploitation opérationnelle ; elles sont également conservées au-delà de cette durée de validité pour des besoins d'aide à la décision des autorités en cas de nouvelle procédure d'interdiction de stade et des besoins statistiques.

Les données sont supprimées à l'expiration d'une durée de cinq ans après l'expiration de la dernière mesure prononcée.

Utilisation opérationnelle

Le traitement comporte à ce jour 633 fiches. Depuis la création du traitement en août 2007 on dénombre 636 connexions.

g) Le fichier national transfrontières (FNT)

Réf. : Arrêté du 29/8/1991 (modifié par arrêté du 3/11/2006)

Cadre juridique et finalités

L'article 7 de la loi du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles transfrontaliers donne une base législative au FNT, créé par l'arrêté du 29 août 1991 (modifié par celui du 3 novembre 2006).

Exploité par la direction centrale de la police aux frontières, le FNT a pour finalités d'assurer :

- l'amélioration du contrôle aux frontières et la lutte contre l'immigration clandestine ;
- la prévention et la répression des actes de terrorisme.

Données enregistrées et durée de conservation

Les catégories d'informations nominatives enregistrées sont les suivantes :

- état civil, sexe et nationalité ;
- pays de provenance et de destination ;
- durée du séjour ;
- nombre d'entrées ;
- informations relatives aux documents de voyage (type, date d'expiration, etc.) ;
- informations relatives à la bande MRZ ou à défaut à la date et au point de passage.

Les données enregistrées sont conservées trois ans.

Modalités d'alimentation et de consultation

Aux termes de l'article 7 de la loi 23 janvier 2006, le FNT est alimenté automatiquement à partir de la bande de lecture optique (MRZ) des documents de voyage, de la carte d'identité et des visas des passagers ou par la saisie manuelle de certaines données inscrites sur les cartes d'embarquement et de débarquement renseignées par les passagers en provenance ou à destination de certains pays sensibles dont la liste est établie par l'UCLAT (5 pays actuellement).

Seuls ont accès aux informations les agents habilités des services de la police nationale, de la gendarmerie nationale ou des douanes.

Techniquement, le FNT ne procède pas à une consultation automatique du fichier des personnes recherchées (FPR) ni du système d'information Schengen (SIS) : seul le logiciel de lecture optique de la bande MRZ procède à la consultation de ces deux traitements, sans qu'il y ait enregistrement de données. Aucune donnée en provenance de l'un ou l'autre de ces fichiers ne figure donc dans le FNT.

Utilisation opérationnelle

La collecte manuelle des informations, qui était la seule possible à l'origine, avait entraîné un retard tel que l'exploitation des données recueillies était devenue impossible.

C'est la raison pour laquelle la loi du 23 janvier 2006 a permis une automatisation du processus de collecte des informations par l'intermédiaire de la bande MRZ, améliorant fortement l'efficacité du traitement. Ce système trouve cependant une limite dans le fait que tous les Etats n'ont pas prévu une bande MRZ sur leurs documents officiels, ce qui oblige les services de police à saisir manuellement les informations dans le fichier.

1.3. Les fichiers à vocation judiciaire

a) Fichier des brigades spécialisées (FBS)

Réf. : Aucune

Cadre juridique et finalités

Le FBS est un fichier d'objectifs créé en 1991 pour les services de police spécialisés luttant contre la grande délinquance et le crime organisé (banditisme, terrorisme, stupéfiants, proxénétisme, trafics d'œuvres d'art, de fausse monnaie, blanchiment, grande délinquance financière, immigration clandestine).

L'objectif du FBS est de :

- collecter des informations sur l'environnement et les habitudes des délinquants spécialisés ;
- favoriser la coopération des services en assurant la confidentialité nécessaire grâce aux notions de visibilité, sensibilité et de « copropriété ».

Données enregistrées et durées de conservation

Informations collectées à l'occasion de la surveillance du milieu criminel.

Dans la mesure où ce traitement s'apparente à un fichier de renseignement, aucune durée de conservation uniforme n'a été fixée. La règle applicable, comme d'ailleurs à tout traitement, est celle définie par l'article 6 de la loi du 6 janvier 1978 : une donnée ne peut être conservée que pour autant qu'elle est toujours nécessaire eu égard aux finalités du fichier.

Modalités d'alimentation et de consultation

Le FBS est actuellement utilisé par les directions interrégionales de la police judiciaire, la plupart des offices centraux de police judiciaire et par les brigades centrales de la préfecture de police.

Le FBS n'est jamais utilisé dans le cadre d'enquêtes administratives. Il est alimenté et consulté exclusivement dans un cadre judiciaire pour la lutte contre la grande délinquance et la criminalité organisée.

Utilisation opérationnelle

Ce traitement comportait 191 647 fiches au 31 décembre 2007.

113 465 consultations ont été enregistrées en 2007.

Exemple d'affaire. - Le 26 février 2008, l'office central de lutte contre le crime organisé (OCLCO) était sollicité par la Belgique pour identifier une femme auteur d'un vol à main armée commis dans une agence bancaire. Une photographie extraite de la vidéosurveillance était jointe à la demande.

Le mode opératoire était le suivant : la femme se présentait une première fois sous prétexte de prendre rendez-vous afin d'ouvrir un compte, repérait les lieux et revenait le lendemain s'emparer de la caisse en exhibant une arme de poing.

Précédemment, en 1998, l'office central pour la répression du banditisme (OCRB) avait assisté la PJ de Bordeaux pour interpeller un couple de braqueurs qui utilisait le même mode opératoire du rendez-vous préalable. Cette affaire avait fait l'objet d'une synthèse nationale de l'OCRB.

Les recherches conduites pour faire suite à la demande des autorités belges entraînaient une consultation du FBS en utilisant comme critère les mots « téléphone » et « banque » dans la rubrique « banditisme ».

Le FBS a alors fait apparaître l'affaire de la synthèse de l'OCRB et a permis d'identifier la femme recherchée, interpellée le 18 juin 2008 alors qu'elle s'apprêtait à commettre un autre vol à main armée.

Evolution fonctionnelle ou juridique

Le maintien en condition opérationnelle du FBS est de plus en plus menacé (incompatibilité avec Internet Explorer 7, difficulté de faire évoluer les bases conformément à la réforme des structures de la DCPJ, absence de ressources à la DSIC capables d'intervenir sur des langages informatiques devenus obsolètes).

b) Fichier de travail de la police judiciaire (FTPJ)

Présentation

Le FTPJ a été conçu en 1987 en interne au bénéfice des services de police judiciaire.

Le contenu du fichier de travail est identique à celui du fichier des brigades spécialisées (FBS) mais, contrairement à ce dernier qui permet un échange d'informations entre services spécialisés, le FTPJ n'est constitué que de bases locales au sein des services régionaux de police judiciaire, non connectées entre elles. Ce fichier n'est plus actuellement utilisé que par quelques services territoriaux de police judiciaire.

Situation juridique

Le fichier de travail a été déclaré auprès de la commission nationale informatique et libertés (C.N.I.L.) en 1991, après un premier dépôt du dossier en 1989 et un retrait l'année suivante, pour des questions d'opportunité, en même temps que le fichier des renseignements généraux.

La délibération d'avis conforme sur le projet d'arrêté présenté par le ministère de l'intérieur et portant création du fichier de travail a été rendue par la CNIL, assortie néanmoins des mêmes réserves que celles présentées pour le FBS. Le dossier a été validé par la Chancellerie en 1994 après l'obtention de la modification des actes réglementaires au terme de nombreuses discussions.

L'année 1994, correspondant au démarrage opérationnel de l'application système de traitement des infractions constatées (STIC), le ministère de l'intérieur a privilégié la présentation du dossier STIC devant la CNIL, prioritaire. Celui n'ayant abouti qu'en 2001 qu'après plus de 15 ans de procédures, le dossier juridique FTPJ/FBS a été retardé d'autant.

Dans le même laps de temps, les besoins exprimés par les utilisateurs du FBS ont conduit à engager un projet de refonte de ce dernier, prenant en compte la dimension de « fichier de travail ».

c) Fichier national du faux monnayage (FNFM)

Historique

Le principe de la gestion centralisée des informations relatives aux faits de faux monnayage a été établi dans la Convention de Genève de 1929. Le FNFM a été créé pour satisfaire aux obligations européennes définies par le règlement européen 1338/2001 du 28 juin 2001 relatif à la protection de l'euro contre le faux monnayage : l'alimentation du système général d'information d'Europol et la création d'un outil opérationnel permettant l'identification des malfaiteurs récidivistes et les rapprochements entre les affaires. Il permet également la gestion des statistiques sur les saisies « police » et « gendarmerie » pour les contrefaçons de l'euro, les devises et les officines de fausse monnaie découvertes sur le territoire national.

Présentation

Le fichier national du faux monnayage (FNFM), recense l'ensemble des affaires de fausse monnaie commises sur le territoire national et sert de base de données de documentation et d'analyse opérationnelle. Ce fichier sert également à l'alimentation du système d'information d'Europol. Ce fichier a été mis en service au moment de la mise en circulation de la monnaie unique, l'Euro, le 1er janvier 2002.

Le cadre de saisie informatique

Le FNFM est alimenté à partir du double des procédures d'enquêtes relatives aux faits de faux monnayage diligentées par les services de police et de gendarmerie. Les informations sont saisies sur deux sites :à l'office central pour la répression du faux monnayage (OCRFM) de la direction centrale de la police judiciaire et au service technique de recherches et de documentation judiciaire (STRDJ) de la direction générale de la gendarmerie nationale. Sur ces sites, les gestionnaires du FNFM contrôlent la qualité des informations contenues dans la procédure (indicatifs des contrefaçons et leur comptabilité).

Sont saisies, les données relatives à l'identifiant de l'affaire, à l'infraction, aux coupures apocryphes saisies, à l'identité des personnes mises en cause, aux signalements et signes particuliers des mis en cause identifiés et non identifiés.

Les personnels habilités des services régionaux de police judiciaire et des sections de recherche de la gendarmerie peuvent consulter ce fichier. La consultation est réalisée à partir d'un poste de travail sécurisé et la réponse est en temps réel. Le FNFM est consultable à partir de la base CHEOPS sur l'intranet du ministère de l'Intérieur en fonction de ces habilitations.

L'alimentation du FNFM est journalière en fonction des informations transmises par les services ayant eu à connaître des affaires de faux monnayage. Les corrections éventuelles peuvent être directement effectuées depuis l'OCRFM ou le STRJD qui sont les deux seuls services habilités à saisir les informations dans le FNFM.

Le nombre de consultations réalisées entre le 1er janvier 2002 et octobre 2008 s'élève à 69 505. En 2008, 977 procédures ont alimenté le fichier.

d) Fichier des véhicules volés (FVV)

Réf. : Arrêté du 15/05/1996 modifié en 2005

Cadre juridique et finalités

Autorisé par un arrêté du 15 mai 1996 (modifié en 2005), le FVV répertorie au plan national les véhicules, bateaux et aéronefs signalés volés ou détournés par leur propriétaire ou mis sous surveillance à la demande d'un service de police ou de gendarmerie.

Comme le fichier des personnes recherchées *(v. la fiche sur le FPR)*, le FVV indique aux services de police, aux gendarmes et aux douanes la conduite à tenir en cas de découverte.

Données enregistrées et durées de conservation

Données enregistrées : état civil et coordonnées du plaignant, code et numéro de police de la compagnie d'assurance, caractéristiques permettant l'identification (numéro d'immatriculation, de série, de moteur ou de cadre, dénomination, marque, type, genre, couleur, signes distinctifs).

La radiation des véhicules volés ou surveillés est effectuée sans délai avant restitution du véhicule volé ou dès que la surveillance devient sans objet.

Modalités d'alimentation et de consultation

Le FVV est alimenté par les services de police et de gendarmerie au moyen de deux systèmes équivalents mais distincts, mis à jour en permanence.

L'accès à la base de données (tant en consultation qu'en alimentation) n'est autorisé qu'aux fonctionnaires et militaires habilités selon un profil correspondant à leur mission. Différents profils de services ont été définis et fixent les conditions pour l'inscription des véhicules. La consultation du FVV par les douanes judiciaires (autorisée par arrêté du 2 septembre 2005) s'effectue par le système de la gendarmerie nationale.

Une interconnexion a été établie en temps réel avec le FNA (fichier national des automobiles) :

- le FVV communique les déclarations de vol et de surveillance des véhicules, ainsi que les découvertes de vol et les fins de surveillance ;
- inversement, le FNA communique au FVV la liste des véhicules volés ou surveillés dont les numéros d'immatriculation, de série ou la marque sont erronés et la liste des véhicules surveillés ayant fait l'objet d'une transaction au FNA.

Il existe deux autres interconnexions :

- une liaison avec le système d'information Schengen (SIS) a été créée en 1995 pour permettre son alimentation par le FVV et, inversement, la consultation directe, à partir du FVV, des signalements effectués dans le SIS par les autres Etats parties à la convention de Schengen ;
- une transmission automatisée de données vers la base de données des véhicules volés ASF (*Automatic Search Facility*) d'Interpol a été mise en place en 2004.

Utilisation opérationnelle

Le FVV compte 131 949 fiches gendarmerie et 419 038 fiches au total.

Grâce au FVV, la gendarmerie a effectué 3 253 surveillances de véhicule.

Les unités de la gendarmerie nationale ont procédé à 7 664 389 consultations en 2006, 7 038 033 en 2007, et 5 727 862 *au 13/11/2008. En 2007, les* services de la police nationale ont procédé à 4 105 336 consultations.

Evolution fonctionnelle ou juridique

A partir du deuxième trimestre 2009, le FVV sera progressivement remplacé par un nouveau fichier, le fichier des objets et véhicules signalés (FOVES), qui comprendra non seulement les véhicules mais les objets

volés correspondant au STIC-objets (v. la fiche sur le STIC) et au FOS (fichiers des objets signalés) de la gendarmerie.

e) Fichier des Objets Signalés (FOS)

Réf. : Aucune

Présentation et finalité

L'application FOS constitue un fichier dit de contrôle en présence. Elle permet de connaître si un objet bien identifié (par un numéro de manufacture ou l'identité de son propriétaire) a été signalé par les unités de gendarmerie à l'occasion d'une enquête judiciaire ou par le système d'information Schengen (SIS) comme étant volé.

Nature des informations contenues

Le FOS comprend les éléments descriptifs textuels ou photographiques des neuf catégories d'objets suivantes : armes à feu, documents d'identité délivrés ou vierges, autres documents administratifs, billets de banque, matériels hi-fi, documents bancaires, objets d'art et objets divers. Il comporte également des éléments d'identité de la victime tels que le nom, le prénom et la date de naissance.

Destinataires des informations

Ont accès aux informations contenues dans la base les personnels habilités des unités opérationnelles de la gendarmerie, de certaines unités de la police nationale - offices centraux, directions interrégionales de police judiciaire (DIPJ), directions régionales de police judiciaire (DRPJ), Service central de documentation criminelle (SCDC) -, les groupes d'intervention régionaux (GIR), les centres de coopération policière et douanière (CCPD) et l'ensemble des services policiers et judiciaires européens connectés au SIS.

Modes d'alimentation, de consultation et d'apurement

L'alimentation se fait par l'intermédiaire de la messagerie opérationnelle de la gendarmerie RUBIS et la consultation peut se faire indifféremment par RUBIS ou par l'intranet de la gendarmerie. L'apurement des données est réalisé automatiquement par l'application en fonction des durées de conservation des objets[15].

Situation juridique actuelle

Créé comme une base de données sous-ensemble de JUDEX (c'est pourquoi ce fichier est encore appelé JUDEX-objets), ce traitement est techniquement réalisé à partir d'une extraction de ce fichier de documentation judiciaire. Le fichier des objets signalés, désormais autonome, n'a pas été déclaré en raison de la refonte du projet FOVES (fichier des objets et véhicules signalés). Ce projet mené conjointement par la police et la gendarmerie nationales doit fusionner le FOS et le STIC objets. Initialement, la conduite du projet permettait de compter sur une livraison de l'application à l'horizon 2007. Des retards liés aux difficultés de développement de cette application ont contraint à successivement reporter les dates de mise en production et de déploiement. La date de déploiement est aujourd'hui prévue pour le deuxième trimestre 2009.

Utilisation opérationnelle

Le FOS compte :

- Document d'Identité Délivré : 380 440

- Document d'Identité Vierge : 1 332

- Armes à feu : 23 184

- Billets de banque : 5 513

- Divers : 343 613

- Documents bancaires : 875 705

- Objets d'art : 83 447

- Document Administratif Délivré : 715 404

- Objets Hi-Fi : 787 408

Il a fait l'objet de 179 319 consultations en 2006, 153 787 en 2007 et 121 636 au 13/11/08

15 Ces durées tiennent compte des spécifications imposées par le SIS Schengen.

f) Le fichier d'information Schengen (SIS)

Réf. : Accord de Schengen du 14 juin 1985 ; Convention d'application du 19 juin 1990 ; Décret n° 95-577 du 6 mai 1995 relatif au système informatique national du SIS dénommé N-SIS

Présentation

Le système d'information Schengen (SIS), créé par la Convention d'application de l'Accord de Schengen du 19 juin 1990, est un fichier commun à l'ensemble des États membres de «l'espace Schengen», qui a pour objet de centraliser et de faciliter l'échange d'informations détenues par les services chargés de missions de police afin de préserver l'ordre et la sécurité publics. Ce fichier est présenté comme une mesure compensatoire à la suppression des contrôles aux frontières intérieures des États participants et à la libre circulation des personnes.

Le SIS, composé d'un système central installé à Strasbourg et de systèmes nationaux -«reflets» de la base centrale- implantés dans chaque pays, comporte deux grandes catégories d'informations : l'une concerne des personnes recherchées, placées sous surveillance ou jugées «indésirables» dans «l'espace Schengen» (articles 95 à 99 de la Convention), l'autre concerne des véhicules ou des objets recherchés (article 100 de la Convention).

En France, c'est la Direction générale de la police nationale, et en particulier le Direction centrale de la Police Judiciaire qui est chargée de gérer ce fichier.

Le cadre de saisie informatique

Pour être inscrite dans le fichier, il faut que l'information réponde aux finalités prévues par les articles 95 à 100 de la Convention Schengen : arrestations aux fins d'extradition, personnes recherchées (notamment en cas de disparition), arrestations pour comparution devant la justice dans le cadre d'une procédure pénale ou pour exécution d'une peine privative de liberté, surveillance discrète ou contrôles spécifiques, non admission dans « l'espace Schengen » résultant d'une décision administrative ou judiciaire.

Les agents des services de police et des unités de gendarmerie, les autorités judiciaires sont habilités à inscrire les informations au SIS.

Le SIS est alimenté, depuis 1995, par le Fichier des véhicules volés (FVV) et par certaines fiches du Fichier des personnes recherchées (F.P.R.- notamment celles relatives à des mandat d'arrêt et à des exécutions de jugement).

Depuis 1999, les armes, les documents d'identité et les billets de banque saisis dans la base nationale du STIC et auxquels est associé le qualifiant « VOLÉ », sont automatiquement enregistrés dans le SIS.

Le SIS II (nouvelle version informatique du fichier SIS 1+ actuel) devrait probablement être mis en œuvre en septembre 2009, et inclure pour les 25 Etats membres de l'espace Schengen[16] (9 nouveaux états membres entrés dans l'UE en 2004 ont rejoint « l'espace Schengen » en mars 2008, suivis de la suisse en décembre 2008) de nouvelles catégories d'objets (bateaux, aéronefs, équipements industriels, moteurs de bateaux, containers, moyens de paiement), des liens entre les signalements et introduire des données biométriques.

Pour l'instant il reste sous la configuration actuelle du SIS 1 +

Les personnes habilitées

- Les autorités compétentes pour exercer des contrôles frontaliers, des vérifications de police (services de police et des douanes, unités de gendarmerie),
- Les autorités compétentes pour l'examen des demandes de visas et la délivrance des titres de séjour et l'administration des ressortissants étrangers (agents du ministère des affaires étrangères et des consulats, agents du ministère de l'intérieur et des préfectures,
- Les autorités judiciaires

Un mode de recherche couplée STIC/SCHENGEN permet, dans une unique transaction, de consulter simultanément les informations (objets) contenues dans la base nationale du STIC et dans le SIS.

16 Le Royaume Uni, l'Irlande et Chypre attendent le démarrage effectif du SIS II pour se connecter au Système d'Information Schengen et devenir opérationnels. Le Lichtenstein devrait rejoindre le Système d'Information en décembre 2009.

De même, les signalements effectués dans le SIS par les autres pays signataires de la convention Schengen sont consultables directement à partir d'une interrogation effectuée sur le FPR et le FVV.

Par ailleurs, un règlement du Parlement Européen (n°1160/2005) et du Conseil de l'Europe du 6 juillet 2005 a autorisé l'accès des préfectures aux données relatives aux véhicules déclarés volés dans l'espace SCHENGEN, permettant ainsi d'éviter les ré-immatriculations de véhicules volés à l'étranger.

Au 9 décembre 2008, la base nationale comptait : 49 203 billets de banque ; 132 748 documents vierges ; 41 413 armes ; 1 535 336 documents d'identité délivrés ; 175 728 véhicules ; 154 582 personnes recherchées. Les opérateurs du Sirène France ont effectués près de 100 000 consultations en 2007.

1.4. Les fichiers de renseignement

a) Fichier alphabétique de renseignements de la Gendarmerie nationale (FAR)

Réf. : Arrêté du 17/09/1992. Déclaré à la CNIL le 13/10/1993

Se présentant sous forme de fiches manuscrites individuelles gérées localement, les fichiers alphabétiques de renseignements (FAR) avaient pour vocation de permettre aux militaires des unités opérationnelles d'acquérir une connaissance approfondie de leur population résidente, en particulier sur leur dangerosité. Ces renseignements sont essentiels pour la sécurité des interventions des personnels de la gendarmerie et de la population. De même, ils sont utiles pour certaines enquêtes de police administrative (enquête de moralité pour les candidats aux concours de la fonction publique, ouverture d'un débit de boissons, autorisation de détention d'arme...).

L'obsolescence du FAR liée principalement à sa gestion très lourde, ainsi que les contraintes légales relatives au respect des libertés individuelles, obligent la gendarmerie nationale à arrêter l'exploitation et l'administration de ce traitement.

Au terme de la période transitoire dont l'échéance est fixée au 24 octobre 2010, le FAR sera supprimé.

Destinataires des informations

Toute unité de gendarmerie établissant une procédure ou constatant un fait méritant d'être gardé en mémoire établit une fiche individuelle. De fait, plusieurs unités peuvent être destinataires des renseignements recueillis :

- la brigade territoriale du lieu de naissance ;
- la brigade territoriale de domicile principal ;
- la brigade territoriale de résidence secondaire ;
- les deux premières unités lorsque la personne, de passage sur la circonscription d'une autre unité, est concernée par la survenance d'un fait ;
- le fichier national des personnes nées à l'étranger (FPNE) implanté au STRJD à Rosny-sous-Bois.

Modes d'alimentation, de consultation et d'apurement

La gestion des fichiers alphabétiques de renseignements est entièrement manuelle. Il appartient à chaque militaire de tenir à jour le fichier de son unité à l'occasion de l'établissement des procédures ou des interventions. De même, la consultation reste libre par les militaires de l'unité.

Les conditions d'apurement des fiches sont définies par l'instruction initiale de 1971. Ainsi, les personnes décédées, ou ayant plus de 80 ans ne doivent plus faire l'objet d'une fiche. De même, les personnes ayant déménagé ne doivent plus figurer dans le fichier alphabétique de renseignements de l'unité de leur ancienne domiciliation.

En l'absence de procédure automatisée, l'alimentation, mais surtout l'apurement des fiches ne donnent plus satisfaction en raison des volumes à traiter, estimé à 60 millions sur l'ensemble du territoire national.

Evolution fonctionnelle ou juridique

La CNIL avait rendu un avis sur les conditions de collecte et de conservation d'informations nominatives par les brigades de gendarmerie, notamment le FAR, le 7 juillet 1992. Ce fichier a ensuite fait l'objet d'un dépôt de déclaration à la CNIL le 13 octobre 1993.

Dès 2010, les renseignements exclusivement administratifs seront intégrés dans le nouveau système Athén@

(voir fiche spécifique). Les fiches détenues dans les brigades seront détruites avant octobre 2010. Dans l'attente, des directives spécifiques visant à apurer le FAR seront données aux unités en vue de son intégration dans le système Athén@ (volumétrie limitée à 5 millions de fiches).

Droit d'accès aux informations.

Le droit d'accès au FAR s'effectue indirectement et simultanément, à l'instar du FPNE et JUDEX par l'intermédiaire de la commission nationale de l'informatique et des libertés.

En raison de l'implantation du FAR dans chaque communauté de brigades et brigade territoriale autonome, le nombre de demandes ne peut être précisé.

Le volume exact du FAR n'est pas connu car c'est un fichier mécanographique. On estime à 60 millions de fiches. Le nombre de consultations n'est pas comptabilisé.

b) Centralisation du renseignement intérieur pour la sécurité du territoire et les intérêts nationaux (CRISTINA)

Réf. : Décret non publié car couvert par le Secret Défense.

Cadre juridique et finalités

La réorganisation des services de renseignement du ministère de l'intérieur, intervenue le 1er juillet, a permis de constituer un service de renseignement intérieur unique, chargé des missions de l'ancienne DST et d'une partie de celles de l'ancienne DCRG. CRISTINA est le fichier de renseignement de cette nouvelle direction centrale du renseignement intérieur (DCRI).

Ce traitement, comme le fichier de la DST (qui datait de 1986), est soumis au régime juridique des fichiers « de souveraineté », défini par l'article 26 (III) de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et par le décret n° 2007-914 du 15 mai 2007 : CRISTINA ne peut faire l'objet d'un contrôle sur place de la CNIL et le décret en portant création n'est pas publié.

La CNIL a toutefois pu se prononcer sur ce projet (elle a émis un avis favorable avec réserves) et le fichier reste soumis au droit d'accès et de rectification garanti à chaque citoyen par les articles 39 à 41 de la loi de 1978. Ce droit s'exerce, comme pour presque tous les fichiers de police, par l'intermédiaire de la CNIL.

Données enregistrées et durées de conservation

CRISTINA étant un fichier de renseignement, aucune durée de conservation fixe n'est prévue : les données ne sont conservées qu'en fonction des finalités (très strictement délimitées) du fichier et donc, pour l'essentiel, de l'intérêt qu'elles présentent au regard de la sûreté de l'Etat et de la sécurité nationale. La règle applicable, comme d'ailleurs à tout traitement, est donc le principe général énoncé par l'article 6 de la loi du 6 janvier 1978 : une donnée ne peut être conservée que pour autant qu'elle est toujours nécessaire eu égard aux finalités du fichier.

Modalités d'alimentation et de consultation

CRISTINA n'est interconnecté avec aucun autre fichier et n'est consultable que par les fonctionnaires spécialement habilités par le directeur central du renseignement intérieur.

c) Exploitation documentaire et valorisation de l'information relative à la sécurité publique (EDVRISP)

Réf. : Le projet de décret portant création de l'application concernant l'exploitation documentaire et la valorisation de l'information relative à la sécurité publique (EDVIRSP) a été soumis à la Commission nationale de l'informatique et des libertés conformément à l'article 26 de la loi n° 78-17 du 6 janvier 1978 modifiée. La CNIL a délibéré le 20 novembre 2008, le projet de décret sera prochainement transmis au Conseil d'État.

La présente fiche décrit le projet dans son dernier état transmis à l'avis de la CNIL.

Présentation et finalité du fichier

L'application concernant l'exploitation documentaire et la valorisation de l'information relative à la sécurité publique (EDVIRSP) est destinée à collecter, conserver et traiter les données concernant :

- les personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique

- les personnes faisant l'objet d'enquêtes administratives afin de déterminer si leur comportement n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées compte tenu de leur nature.

Nature des informations enregistrées

Peuvent être enregistrées les catégories de données à caractère personnel relatives au motif de l'enregistrement des données, aux informations ayant trait à l'état civil et à la profession, adresses physiques, numéros de téléphone et adresses électroniques, aux signes physiques particuliers et objectifs, photographies, aux activités publiques, comportement et déplacements, aux titres d'identité, à l'immatriculation des véhicules, aux informations patrimoniales, aux antécédents judiciaires et à l'environnement de la personne, notamment aux personnes entretenant ou ayant entretenu des relations directes et non fortuites avec elle. Cependant, les signes physiques, les déplacements et l'immatriculation des véhicules ne peuvent être enregistrés lorsque les données concernent des personnes faisant l'objet d'enquêtes administratives. Par ailleurs, le traitement ne comporte pas de reconnaissance faciale à partir de la photographie.

La collecte, la conservation et le traitement par les services des données susceptibles de faire apparaître l'origine géographique, les signes particuliers et objectifs ainsi que les activités politiques, philosophiques, religieuses ou syndicales sont autorisés.

Présence de mineurs et, si oui, existe-t-il une limite d'âge ?

Les données collectées, conservées et traitées peuvent concerner les mineurs de treize ans et plus lorsque leur activité individuelle ou collective indique qu'ils peuvent porter atteinte à la sécurité publique. Ces données ne peuvent alors être conservées plus de trois ans après l'intervention du dernier évènement ayant justifié un enregistrement à ce titre.

Les données de l'application EDVIRSP peuvent également concerner des mineurs de seize ans et plus lorsque ceux-ci font l'objet d'une enquête administrative pour déterminer si leur comportement n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées compte tenu de leur nature ; ces données peuvent être conservées pour une durée maximale de cinq ans à compter de leur enregistrement ou de la cessation des fonctions ou des missions au titre desquelles l'enquête a été menée.

Destinataires des informations

Les fonctionnaires relevant de la sous-direction de l'information générale de la direction centrale de la sécurité publique individuellement désignés et spécialement habilités par le directeur central de la sécurité publique, les fonctionnaires affectés dans les services d'information générale des directions départementales de la sécurité publique individuellement désignés et spécialement habilités par le directeur départemental et les fonctionnaires affectés dans les services de la préfecture de police en charge du renseignement individuellement désignés et spécialement habilités par le préfet de police, sont autorisés, dans la limite du besoin d'en connaître, à accéder aux données de l'application EDVIRSP.

Tout autre agent d'un service de la police nationale ou de la gendarmerie nationale peut être destinataire des données de l'application EDVIRSP sur demande expresse visée de son chef de service précisant l'identité du consultant, l'objet et les motifs de la consultation.

Modes d'alimentation du fichier

Les services de la direction centrale de la sécurité publique et les services de l'information générale de la préfecture de police assurent l'alimentation du fichier.

Modes de consultation et traçabilité

Les consultations du traitement font l'objet d'un enregistrement comprenant l'identifiant du consultant, la date et l'heure de la consultation. Ces informations sont conservées pendant un délai de deux ans.

Durée de conservation

Lorsqu'elles concernent des personnes faisant l'objet d'enquêtes administratives, les données peuvent être conservées pour une durée maximale de cinq ans à compter de leur enregistrement ou de la cessation des fonctions ou des missions au titre desquelles l'enquête a été menée.

Les données concernant des mineurs de treize ans et plus ne peuvent être conservées plus de trois ans après l'intervention du dernier évènement ayant justifié un enregistrement à ce titre.

Droit d'accès aux informations

Le droit d'accès aux données s'exerce auprès de la Commission nationale de l'informatique et des libertés.

Le droit d'information et le droit d'opposition ne s'appliquent pas.

Modalités d'apurement

Le directeur général de la police nationale rend compte chaque année à la Commission nationale de l'informatique et des libertés de ses activités de vérification, de mise à jour et d'effacement des données enregistrées dans le traitement, notamment celles relatives aux mineurs. Ce rapport annuel présente les procédures suivies par les services gestionnaires pour que les données enregistrées soient en permanence exactes, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées.

d) Gestion du terrorisme et des extrémismes à potentialité violente (GESTEREX)

Réf. : Couvert par le Secret Défense.

Cadre juridique et finalités

La mise en œuvre de la réforme du renseignement intérieur au sein de la Préfecture de Police a conduit le ministère de l'intérieur, de l'outre-mer et des collectivités territoriales à créer, par un arrêté en date du 27 juin 2008 pris sur proposition du Préfet de Police publié au JORF du 1er juillet 2008, une Direction du renseignement de la Préfecture de Police (DR-PP), à compter du 1er juillet 2008.

A ce titre, et conformément à l'article 2 du décret n° 2008-609 du 27 juin 2008 relatif aux missions et à l'organisation de la direction centrale du renseignement intérieur (DCRI), la DR-PP concourt à l'activité de la DCRI pour la prévention des actes de terrorisme et pour la surveillance des individus, groupes, organisations et phénomènes de société susceptibles, par leur caractère radical, leur inspiration ou leurs modes d'action, de porter atteinte à la sécurité nationale.

GESTEREX constitue le fichier mis en œuvre par la sous-direction chargée de la lutte contre le terrorisme et les extrémismes à potentialité violente de la DR-PP pour exercer ces missions qui sont couvertes par le secret.

Ce traitement, comme le fichier CRISTINA de la DCRI, est soumis au régime juridique des fichiers « de souveraineté », défini par l'article 26 (III) de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Données enregistrées et durées de conservation

GESTEREX étant un fichier de renseignement, aucune durée de conservation fixe n'est prévue : les données ne sont conservées qu'en fonction des finalités (très strictement délimitées) du fichier et donc, pour l'essentiel, de l'intérêt qu'elles présentent au regard de la sûreté de l'Etat et de la sécurité nationale. La règle applicable, comme d'ailleurs à tout traitement, est donc le principe général énoncé par l'article 6 de la loi du 6 janvier 1978 : une donnée ne peut être conservée que pour autant qu'elle est toujours nécessaire eu égard aux finalités du fichier.

Modalités d'alimentation et de consultation

GESTEREX, qui n'est interconnecté avec aucun autre fichier, n'est alimenté et n'est consultable que par les fonctionnaires spécialement habilités par le Préfet de Police de la sous-direction chargée de la lutte contre le terrorisme et les extrémismes à potentialité violente de la DR-PP.

Le fichier est soumis au droit d'accès et de rectification garanti à chaque citoyen par ~~les articles 39 à 41~~ *l'article 41* de la loi de 1978. Ce droit s'exerce, comme pour presque tous les fichiers de police, par l'intermédiaire de la CNIL.

1.5. Les fichiers d'antécédents judiciaires

a) Système Judiciaire de Documentation et d'exploitation (JUDEX)

Réf. : Décret n°2006-1411 du 17/11/2006. Circulaire n° 51992 DEF/GEND/OE/SDPJ/PJ du 10/08/2007

Présentation et finalité

Le Système d'information judiciaire de la gendarmerie nationale JUDEX (acronyme pour système JUdiciaire de Documentation et d'EXploitation) met à la fois en œuvre des moyens centraux de traitement automatisé

qui recouvrent les applications JUDEX-Affaires et JUDEX-Personnes mises en cause, et des moyens déconcentrés au niveau de chaque département, qui concernent la seule application JUDEX-Groupement.

JUDEX a été développé en 1986 pour remplacer le système MIDOS (« microdossiers »), déclaré à la CNIL en 1980, qui rassemblait et stockait sur des microfiches les données relatives aux infractions constatées et nécessaires à la conduite des enquêtes judiciaires :

- les affaires relatives aux crimes et aux délits constatées et portées à la connaissance de la gendarmerie;
- les signalements de personnes mises en cause (personnes à l'encontre desquelles ont été rassemblés des indices ou des éléments graves et concordants attestant de leur participation à la commission d'un crime ou d'un délit) ;
- les victimes de ces infractions.

À compter de 1993, le système national a été complété par le déploiement de bases départementales afin de faciliter l'action prioritaire de la gendarmerie dans la lutte contre la petite et moyenne délinquance.

La finalité de JUDEX est de faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs. À ce titre, il fournit aux enquêteurs de la gendarmerie, de la police nationales et de la douane judiciaire, une aide à l'enquête judiciaire (recherche sur les personnes et les objets, rapprochements entre auteurs et manière(s) d'opérer, identification des délinquants et des personnes disparues, recherche des antécédents d'une personne ayant fait l'objet d'une procédure, etc.) et une information sur la délinquance en fournissant les éléments utiles à des analyses de phénomènes criminels.

Nature des informations contenues

Le fichier est constitué de données recueillies dans les procédures établies par les unités de la gendarmerie nationale ou par des services de la police nationale et des agents des douanes habilités à exercer des missions de police judiciaire, lorsqu'une unité de gendarmerie est appelée à en assurer la continuation ou la conduite commune.

Ces données concernent des personnes à l'encontre desquelles sont réunis, lors de l'enquête préliminaire de l'enquête de flagrance ou sur commission rogatoire, des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer, comme auteurs ou complices, à la commission d'un crime, d'un délit ou d'une contravention de 5e classe prévue aux articles R. 625-1 à R. 625-3, R. 625-7, R. 625-9, R. 635-1, R. 635-3 à R. 635-5, R. 645-1, R. 645-2 et R. 645-4 à R. 645-12 du Code pénal, ou les victimes de ces infractions.

En pratique, les informations relatives aux contraventions n'ont jusqu'à présent pas fait l'objet d'enregistrement. En outre, certaines affaires, pour lesquelles aucune information réellement utile au regard de la finalité du fichier n'est disponible, ne sont pas enregistrées. Le fichier n'est donc pas exhaustif et ne peut donc faire l'objet d'une utilisation statistique.

Le fichier peut traiter des données à caractère personnel de la nature de celles mentionnées au I de l'article 8 de la loi du 6 janvier 1978 (données dites sensibles), dans les seuls cas où ces données résultent de la nature ou des circonstances de l'infraction ou se rapportent à des signes physiques particuliers, objectifs et permanents, en tant qu'éléments de signalement des personnes, dès lors que ces éléments sont nécessaires à la recherche et à l'identification des auteurs des infractions inscrites dans le périmètre de l'application.

Enfin, en tant que de besoin, et dans le cadre des engagements internationaux en vigueur, le fichier est également constitué des données à caractère personnel issues des traitements gérés par des organismes de coopération internationale en matière de police judiciaire ou des services de police étrangers qui présentent un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font ou peuvent faire l'objet.

Destinataires des informations

Les destinataires pour les besoins des enquêtes judiciaires sont :

- les personnels de la gendarmerie nationale, de la police nationale et des services des douanes qui exercent des missions de police judiciaire, individuellement désignés et spécialement habilités (L'accès par tous moyens techniques mobiles aux données du fichier est ouvert à ces seuls personnels) ;
- les autres personnels de l'État investis par la loi de pouvoirs de police judiciaire, individuellement désignés et spécialement habilités par le procureur de la République territorialement compétent ;
- les magistrats du parquet ;

– les magistrats instructeurs pour les faits dont ils sont saisis ;

– les organismes de coopération internationale en matière de police judiciaire et les services de police étrangers (dans les conditions énoncées à l'article 24 de la loi du 18 mars 2003).

Les destinataires pour les besoins des consultations administratives dans le cadre des missions, enquêtes ou interventions prévues à l'article 17-1 de la loi du 21 janvier 1995 sont :

– les personnels de la gendarmerie et de la police nationales individuellement désignés et spécialement habilités ;

– des personnels investis de missions de police administrative individuellement désignés et spécialement habilités par le préfet. Dans ce cas, l'habilitation précise limitativement les motifs qui peuvent justifier pour chaque personne les consultations autorisées. Dans tous les cas, l'accès à l'information est alors limité à la seule connaissance de l'enregistrement de l'identité de la personne concernée dans le traitement en tant que mis en cause. (Nota : cette possibilité reste cependant encore théorique car elle n'est pas mise en œuvre aujourd'hui).

Ce deuxième cas, prévu par le décret en cours de publication, sera prochainement mis en œuvre.

Modes d'alimentation et de consultation

Alimentation

L'alimentation de la base JUDEX nationale est réalisée via les bases départementales. Ces dernières cèdent l'information à la base JUDEX-Affaires sous la forme d'un message de police judiciaire (MPJ) et à la base JUDEX-Personnes mises en cause sous la forme d'un message d'éléments d'identification (MEI). Les MPJ et MEI sont générés automatiquement par le système lorsque l'opérateur valide la transmission de l'information de la base départementale vers la base nationale.

Les bases départementales sont quant à elles alimentées, sous un formatage précis, par des messages d'information judiciaire (MIJ). Ces derniers constituent des synthèses des procédures judiciaires et comportent, lorsque des personnes ont été mises en cause, leur signalement détaillé. Les MIJ sont générés automatiquement par l'application de rédaction de procédure Ic@re au fur et à mesure de la rédaction des pièces de procédures par les enquêteurs. Ils sont adressés aux brigades départementales de renseignements et d'investigations judiciaires (BDRIJ) qui les fusionnent et assurent un contrôle de cohérence avant de les intégrer dans les bases départementales.

La « construction » de l'information se fait donc au fil de la procédure mais l'intégration dans la base départementale est réalisée de façon asynchrone après contrôle et validation.

La chronologie est la suivante :

– constatation d'une infraction par une unité de gendarmerie ;

– rédaction d'une pièce de procédure par un enquêteur ;

– génération automatique d'un MIJ vers la BDRIJ. Si les informations sont insuffisantes, le MIJ est mis en attente et n'est pas intégré dans la base départementale ;

– rédaction de nouvelles pièces de procédures et génération automatique des MIJ associés ;

– la BDRIJ collationne les MIJ et fusionne les informations en un message unique qu'elle intègre dans l'application JUDEX-Groupement. Elle contrôle sur le fond et sur la forme les informations ;

– récupération de clichés photographiques soit réalisés par les enquêteurs, soit remis par les victimes ou témoins et envoi à la BDRIJ ;

– intégration par la BDRIJ des photographies dans l'application JUDEX Groupement ;

– transmission de l'information vers l'application nationale (sous forme d'un MPJ et d'un MEI générés par le système). Réception de ces éléments par le service technique de recherches judiciaires et de documentation (STRJD) à Rosny-sous-Bois ;

– traitement et contrôle centralisés des messages et de leurs documents annexes (photographies) ;

– alimentation des applications JUDEX-Affaires et JUDEX-Personnes mises en cause.

Modes de consultation

Les consultations peuvent se pratiquer dans différents modes.

1) Consultation des applications centralisées :

Par réseau de transmission spécifique à la gendarmerie.

• Au niveau des unités élémentaires de la gendarmerie :

- interrogation en mode requête auteur (RA) et interrogation auteur (IA) : accès aux dossiers grâce à la connaissance de l'identité d'une personne ;
- interrogation en mode C1 : accès aux dossiers par rapport à une référence précise connue : soit la référence de l'affaire, soit le numéro de référence de signalement, soit, pour les objets, un numéro d'identification.

• Au niveau des BDRIJ et des sections de recherches de la gendarmerie :

- interrogation en mode C2 : accès aux dossiers grâce à une recherche effectuée sur un certain nombre de champs au choix parmi un nombre donné de champs.

Ces trois types de consultation représentent 35 000 interrogations par jour. L'ensemble des interrogations fait l'objet d'une journalisation qui permet de recueillir les informations suivantes : l'adresse du poste d'où émanent l'interrogation, la date et le libellé de l'interrogation.

Par réseau local spécifique à la gendarmerie.

• Au niveau du service technique de recherches judiciaires et de documentation (STRJD) :

- interrogation en mode C3 : interrogation multicritère sans limitation de champs et en recherche croisée.

Par réseau intranet gendarmerie.

Ce mode est disponible pour les seules unités reliées par le réseau intranet gendarmerie. Depuis septembre 2006, toutes les unités de gendarmerie sont reliées au réseau qui devient donc le mode d'accès privilégié pour l'ensemble des personnels de la gendarmerie. Il est également actuellement le seul mode d'accès ouverts aux personnels extérieurs à la gendarmerie (police, douane).

L'interrogation s'effectue, à l'instar du mode C2, à partir d'une sélection de critères. La consultation porte sur l'ensemble des applications centralisées après sélection de sept champs choisis parmi la totalité des champs disponibles.

Les consultations par intranet représentent 12 000 interrogations par jour. La procédure de journalisation permet de recueillir les informations suivantes : l'unité, la personne, la date, l'heure et le libellé de l'interrogation.

2) Consultation de l'application déconcentrée JUDEX-Groupement

La consultation n'est réalisée que par la BDRIJ en mode local direct. L'ensemble des informations et des documents concernant la criminalité ou la délinquance dans le département est disponible à partir d'interrogations croisées sur la totalité des champs de l'application.

Droit d'accès aux informations

La CNIL saisit par courrier le STRJD pour vérifier la nature des éléments détenus dans les fichiers judiciaires mis en œuvre par la gendarmerie nationale.

La cellule « droit d'accès indirect » du STRJD constitue un dossier après :

– exploitation du système JUDEX, du fichier des personnes recherchées et du fichier des personnes nées à l'étranger ;
– vérification par message auprès du fichier alphabétique de renseignement des brigades des lieux de domicile, de naissance, de commission d'infraction ;
– à la demande de la CNIL, la vérification peut être étendue à d'autres départements ;
– demandes auprès des procureurs de la République compétents des suites judiciaires de toutes les affaires indexées dans la base JUDEX (auteur ou victime).

Après collecte de tous les éléments de réponse, les dossiers sont présentés à la CNIL à Rosny-sous-Bois.

Les demandeurs sont essentiellement des agents de sécurité, convoyeurs de fonds, employés en centrale nucléaire et sites sensibles dont les demandes d'agrément ou de renouvellement d'agrément ont été refusées à la suite de la consultation des fichiers judiciaires mis en œuvre par la police ou la gendarmerie nationales,

dans le cadre des enquêtes administratives prévues par l'article 25 de la loi 2003-239 du 18 mars 2003 pour la sécurité intérieure.

Modalités d'apurement

Les règles d'apurement sont identiques à celles du STIC de la police nationale. Les durées de conservation des données à caractère personnel, décomptées à partir de la date de leur enregistrement dans le traitement, obéissent aux règles suivantes :

• Les données concernant les mis en cause majeurs sont conservées vingt ans. Par dérogation, elles sont conservées :

– cinq ans pour les infractions les moins graves (contraventions, délits prévus par le code de la route, délits prévus aux articles 227-3 à 227-11, 221-6, 222-19, 225-10-1, 311-3, 314-5, 314-6, 431-1 et 431-4 du Code pénal et L. 3421-1 du Code de la santé publique) ;

– quarante ans pour les infractions les plus graves dont la liste est arrêtée en annexe du décret de création du système.

• Les données concernant les mis en cause mineurs sont conservées cinq ans. Par dérogation, elles sont conservées :

– dix ans pour certaines infractions graves dont la liste est arrêtée en annexe du décret de création du système ;

– vingt ans pour les infractions les plus graves dont la liste est arrêtée en annexe du décret de création du système.

En cas de mise en cause dans une ou plusieurs nouvelles infractions avant l'expiration de l'un des délais de conservation des données initiales, le délai de conservation restant le plus long s'applique aux données concernant l'ensemble des infractions pour lesquelles la personne a été mise en cause.

Enfin, la durée de conservation des données à caractère personnel concernant les victimes est au maximum de quinze ans, sous réserve que la personne concernée ne demande pas à être retirée de droit du système après condamnation définitive de l'auteur des faits. La durée de quinze ans peut être prolongée jusqu'à la découverte des objets, lorsque l'infraction porte sur des œuvres d'art, des bijoux ou des armes.

L'apurement des données à caractère personnel est réalisé sur les bases départementales et sur la base nationale par un traitement automatisé.

Le système est automatisé et l'apurement s'effectue chaque nuit en fonction de la date de création de la fiche. Aucune statistique n'est réalisée. Les quantifications sont déduites de la variation de la quantité de fiches présentes dans le système entre deux dates. Ainsi, entre 2006 et 2008, 700.000 fiches ont été retirées.

Au 4 décembre 2008, JUDEX rassemble 9.811.933 fiches « affaires » et 2.145.329 personnes mises en cause.

Évolution fonctionnelle ou juridique

Cette application est en fin de vie opérationnelle et technique. Il doit être remplacé à l'horizon de la fin 2009 par l'application ARIANE commune à la police et à la gendarmerie nationales.

b) Système de traitement des infractions constatées (STIC)

Réf. : Décret n° 2001-583 du 5/07/2001 (modifié en 2006)

Cadre juridique et finalités

Autorisé par le décret n° 2001-583 du 5 juillet 2001 (modifié en 2006), le STIC est le fichier d'antécédents judiciaires de la police nationale. Il permet l'exploitation des informations provenant des comptes rendus d'enquêtes issus des procédures pénales, à des fins de recherches criminelles et statistiques. Il s'agit d'un outil d'aide à l'enquête qui offre une information sur la criminalité et facilite la gestion de la documentation en répertoriant les références d'archivage des procédures.

Le STIC peut également être consulté dans le cadre des enquêtes administratives.

Cadre législatif : article 21 de la loi du 18 mars 2003 pour la sécurité intérieure (police judiciaire), article 17-1 de la loi du 21 janvier 1995 d'orientation et de programmation relative à la sécurité (consultation pour les besoins d'enquêtes administratives).

Données enregistrées et durées de conservation

Les infractions concernées sont les crimes, les délits et certaines contraventions de 5e classe. Les informations contenues dans le STIC ne sont que des extraits du contenu des procédures judiciaires (lesquelles font l'objet d'un archivage séparé).

Personnes enregistrées :

- personnes à l'encontre desquelles sont réunis des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer à la commission de l'infraction, lors de l'enquête préliminaire, de flagrance ou sur commission rogatoire ;
- les victimes de ces infractions.

Autres informations collectées :

- informations non nominatives qui concernent les faits objets de l'enquête, les lieux, dates de l'infraction et modes opératoires ;
- informations relatives aux objets.

Durée de conservation des données :

- pour les majeurs, 20 ans en principe (mais 5 ans pour les infractions les moins graves, 40 ans pour certains délits graves énumérés dans le décret) ;
- pour les mineurs, 5 ans en principe (mais 10 ou 20 ans pour certaines infractions graves) ;
- pour les victimes, jusqu'à 15 ans (sauf opposition de la victime dans les cas prévus par la loi).

Un apurement automatique des données à l'expiration de leur délai de conservation a été mis en place en 2004. La mise en application de cet apurement a permis de supprimer 1 241 742 mis en cause et 49 483 victimes. Cet apurement automatique est dorénavant réalisé mensuellement (concerne environ 10 000 mis en cause et 200 à 400 victimes).

En 2007, l'apurement automatique a permis la suppression de 167 222 fiches de mis en cause et 4 165 fiches victimes. L'apurement manuel a permis la suppression de 7 743 fiches de mis en cause.

En 2008, l'apurement automatique des mis en cause concernera 143 565 fiches, et 4 371 pour les victimes. 6 983 fiches de mis en cause ont été supprimées manuellement.

Modalités d'alimentation et de consultation

Le STIC est une base nationale alimentée par une nouvelle saisie des informations contenues dans les procédures judiciaires et consignées dans le compte rendu d'infraction (CRI) ou le compte rendu d'enquête après identification (CREI). Les données sont dans un premier temps intégrées dans le STIC-FCE (pour « faits constatés et élucidés ») : il s'agit de la base locale du STIC, vecteur d'alimentation de la base nationale. Le cas échéant, elles sont ensuite retraitées et enrichies directement dans le STIC (objets, modes opératoires, affinement des qualifications d'infractions, de nature de lieu, etc.).

Seuls les fonctionnaires de police (et, dans certains cas, les militaires ou fonctionnaires de la gendarmerie et des douanes), individuellement désignés et spécialement habilités, peuvent consulter le fichier ; ils doivent disposer d'un mot de passe personnel.

Sont par ailleurs destinataires des données :

- les magistrats du parquet, et les magistrats instructeurs pour les recherches relatives aux faits dont ils sont saisis ;
- les personnes investies d'une mission de police administrative, selon un accès restreint, dans le cadre des enquêtes énumérées par le décret n° 2005-1124 du 6 septembre 2005 (pris pour l'application de l'article 17-1 de la loi du 21 janvier 1995) ;
- les organismes de coopération internationale en matière de police judiciaire.

Intégré dans l'architecture informatique CHEOPS (circulation hiérarchisée des enregistrements opérationnels de police sécurisés) du ministère de l'intérieur, le STIC bénéficie, de ce fait, des sécurités techniques qui sont associées à ce système (notamment la traçabilité des consultations).

Utilisation opérationnelle

La base nationale du STIC contenait au 1er octobre 2008 les antécédents de 5 486 297 individus mis en cause, plus de 36 millions de dossiers de procédures (représentant 40 millions d'infractions), 33 millions d'enregistrements de victimes et 10,4 millions d'objets inscrits dans la base « objets ».

Au 1er janvier 2008, 97 597 personnes sont habilitées à pouvoir consulter le STIC qui a fait l'objet de plus de 13,8 millions de consultations en 2007.

1119 services de police disposent de ce profil de police administrative, en plus de leur profil de police judiciaire, tandis que 220 services ne disposent que de la fonction de recherche de police administrative.

Ces services ont procédé à 1 001 051 consultations de police administrative durant l'année 2007 (+ 332 par rapport à 2006, soit + 0,03 %).

La LSI a également prévu la consultation des fichiers, en matière d'enquêtes administratives uniquement, pour une nouvelle catégorie de destinataires des données : «les personnels de l'Etat investis de missions de police administrative ».

Il s'agit en pratique des agents des préfectures qui, en vertu du décret du 5 juillet 2001 modifié par le décret du 14 octobre 2006, disposent d'un accès au STIC, lequel est toutefois limité à la seule connaissance de l'enregistrement de l'identité de la personne concernée dans le traitement en tant que mis en cause.

La mise en œuvre de cet accès se heurtait à des difficultés d'ordre technique, qui ont été levées depuis, puisque les premiers accès sont en effet opérants depuis le début du premier trimestre 2008.

De janvier à juin 2008, 534 841 consultations ont été effectuées à des fins administratives.

Evolution fonctionnelle ou juridique

ARIANE se substituera prochainement au STIC et au JUDEX de la gendarmerie.

Le STIC-Canonge

Créé en 1950 par l'inspecteur principal René CANONGE de la sûreté urbaine de Marseille (fichier signalétique manuel avec photographie). Informatisé en juin 1992, on compte au 1er janvier 2006, 1 079 postes installés dans l'ensemble des services de police.

Une nouvelle version, dite graphique, est opérationnelle depuis 2004. Elle s'est substituée à l'ancien système (Odyssée).

Développé dans le cadre du système de traitement des infractions constatées (STIC), le logiciel Canonge permet de rassembler dans un même fonds documentaire le signalement des auteurs d'infractions à l'échelon d'une circonscription, d'un département, du ressort territorial d'un SRPJ ou d'une DIPJ, du service central de documentation criminelle.

Il permet de rechercher des auteurs déjà connus des services de police à partir d'éléments de signalements fournis par le témoin ou la victime.

Les informations contenues dans le Canonge sont soumises aux mêmes règles juridiques que celles du STIC dont il continue à être une application préparatoire (décret n° 2001-583 du 5 juillet 2001 modifié par le décret n° 2006-1258 du 14 octobre 2006). Seules les personnes formellement mises en cause pour crime, pour délit ou pour certaines contraventions de 5e classe peuvent être enregistrées dans le Canonge. La signalisation des témoins ou autres personnes est proscrite.

Les informations concernant les individus ne peuvent être conservées que pendant la durée qui a été fixée par le législateur. Les suites judiciaires favorables doivent donner lieu à la mise à jour des fiches du Canonge et peuvent, le cas échéant, entraîner leur suppression.

La saisie des informations : 6 rubriques principales

- État civil (sexe ; âge ; taille)
- Surnom et alias
- Fait – historique
- Signalement
- Pilosité, yeux, cheveux
- Signes particuliers

- Photos anthropométriques

Dans la partie signalement, un filtre sur le « type » distingue actuellement 12 types différents : Blanc (caucasien) ; Méditerranéen ; Gitan ; Moyen-oriental ; Nord africain Maghrébin ; Asiatique Eurasien ; Amérindien ; Indien (Inde) ; Métis-Mulâtre ; Noir ; Polynésien, Mélanésien-canaque.

1.6. Les fichiers d'identification judiciaire

a) Fichier judiciaire national automatisé des auteurs d'infractions sexuelles (FIJAIS)

Réf. : Loi n°2004-204 du 9 mars 2004 créant le FIJAIS ; articles 706-53-1 à 706-53-12 et R53-8-1 à R53-8-39 du code de procédure pénale ; délibération de la CNIL n°2005-039 du 10 mars 2005 ; délibération de la CNIL n° 2005-153 du 21 juin 2005 ; Décret n°2005-627 du 30 mai 2005 ; circulaire d'application du 1er juillet 2005 ; loi n°2005-1549 du 12 décembre 2005, article 28 ; circulaire d'application du 27 février 2006 ; loi n°2006-399 du 4 avril 2006 ; circulaire d'application du 19 avril 2006 ; loi n°2007-297 du 5 mars 2007 relative à la prévention de la délinquance, article 42; décret n° 2008-1023 du 6 octobre 2008 ; circulaire d'application du 29 octobre 2008.

Historique

Ce dispositif, créé par la loi du 9 mars 2004 est entré en service le 30 juin 2005. Il a été modifié par la loi du 12 décembre 2005 relative au traitement de la récidive, la loi du 4 avril 2006 renforçant la prévention et la répression des violences au sein du couple ou commises contre les mineurs, la loi du 5 mars 2007 relative à la prévention de la délinquance et la loi du 25 février 2008 relative à la rétention de sûreté et à la déclaration d'irresponsabilité pénale pour trouble mental.

La mise en œuvre du FIJAIS a été assurée par un Comité interministériel (Justice, Intérieur, Défense) de pilotage présidé par le ministère de la Justice, converti en Comité interministériel de suivi.

Sept réunions interrégionales et interministérielles de lancement ont précédé l'entrée en service.

Chacun des trois ministères partenaires a créé un réseau de référents pour faciliter les échanges d'informations concernant le fonctionnement de l'application. Le gestionnaire du FIJAIS rencontre régulièrement les référents désignés par le procureur général de chaque cour d'appel, soit en se déplaçant, soit en organisant des visioconférences (une quinzaine en 2008).

Le ministère de la Justice est responsable et gestionnaire du FIJAIS. Il est tenu par le service du casier judiciaire national à Nantes ; il est placé sous le contrôle du magistrat qui dirige le CJN.

Finalités et fonctionnement

Le FIJAIS a pour objectif de :

- prévenir la récidive des auteurs d'infractions sexuelles ou violentes,
- faciliter l'identification des auteurs de ces infractions,

Sont inscrites au FIJAIS non seulement les personnes condamnées, même non définitivement, pour une des infractions suivantes : meurtre ou assassinat d'un mineur précédé ou accompagné d'un viol, de tortures ou d'actes de barbarie, agression ou atteinte sexuelle ou proxénétisme à l'égard d'un mineur, recours à la prostitution d'un mineur prévues par les articles 222-23 à 222-31, 225-7 (1o), 225-7-1, 225-12-1, 225-12-2 et 227-22 à 227-27 du code pénal, meurtre ou assassinat commis avec tortures ou actes de barbarie, tortures ou actes de barbarie, meurtres ou assassinats commis en état de récidive légale, mais également, concernant ces mêmes infractions, les personnes ayant exécuté une composition pénale, été mises en examen par une juridiction d'instruction, ayant fait l'objet d'un non-lieu, d'une relaxe ou d'un acquittement fondé sur des motifs tenant à l'abolition des facultés de discernement (article 122-1 du code pénal) ou encore, s'agissant de ressortissants français, ayant été condamnées à l'étranger pour une de ces infractions.

Selon la gravité de la peine encourue et le choix de procédure pénale applicable à la personne, son inscription est effectuée de plein droit ou sur décision expresse de l'autorité judiciaire (une telle décision est toujours nécessaire pour les mineurs jugés par le juge ou le tribunal pour enfants qui n'écartent pas l'excuse de minorité).

L'article 216 de la loi du 9 mars 2004 a prévu l'inscription de personnes ayant commis des faits antérieurement à l'entrée en vigueur de cette loi, voire ayant été condamnées avant cette date.

A titre de mesure de sûreté, les personnes inscrites au FIJAIS sont astreintes à l'obligation de justifier de leur adresse une fois par an et de déclarer leur changement d'adresse dans les quinze jours ; les auteurs d'infractions les plus graves, une fois la condamnation définitive, doivent, tous les six mois - voire tous les

mois si la juridiction l'a décidé, pour les faits commis à compter du 8 mars 2007 - se présenter en personne auprès de la police ou de la gendarmerie de leur domicile afin de justifier de leur adresse. Le séjour à l'étranger d'une personne inscrite ne fait pas cesser ses obligations, mais la justification se fait alors uniquement par envoi de courriers en LRAR.

Le non respect de ces obligations, à partir du moment où elles ont été notifiées personnellement, constitue une infraction pénale punie d'une peine d'emprisonnement de 2 ans et de 30 000 euros d'amende (une condamnation en 2005, dix neuf en 2006 et cent quatorze en 2007). Quand les personnes sont en prison au moment de l'inscription, la notification n'intervient qu'à leur libération.

Le système informatique du FIJAIS génère immédiatement une alerte à l'unité de police ou de gendarmerie du domicile de la personne qui n'a pas justifié dans les délais son adresse. Cette alerte provoque une enquête pénale, un compte rendu au procureur de la République et, en cas de vaine recherche, l'inscription immédiate de la personne au fichier des personnes recherchées (FPR).

Le FIJAIS rend accessible, permet ou génère 24 heures sur 24 et 365 jours par an :

- les données complètes : identité (nom, prénom, sexe, date et lieu de naissance, nationalité, alias éventuel, dans certains cas filiation), adresse, décision de justice fondant l'inscription au FIJAIS (nature de l'infraction, nature et date de la décision, peines ou mesures prononcées, juridiction les ayant prononcées, date et lieu des faits commis);
- la vérification de l'identité des personnes référencées au Répertoire national d'identité des personnes physiques ;
- l'émission des alertes;
- la gestion des justifications d'adresse ;
- la gestion des mises à jour :
- changement de régime de présentation, rectification ou effacement ordonné
- effacement suite à décision de non-lieu, relaxe, acquittement non fondé sur l'article 122-1 du code pénal ou expiration du délai
- la recherche multicritères : autorités judiciaires et officiers de police judiciaire habilités ;
- la consultation à partir de l'identité de la personne : préfectures (et par leur intermédiaire, maires, présidents de conseil généraux et régionaux), direction des ressources humaines de l'Education nationale, rectorats, inspections académiques, direction de la protection judiciaire de la jeunesse et ses directions régionales, direction de l'administration pénitentiaire et ses directions interrégionales, directions départementales des affaires sanitaires et sociales, direction de la jeunesse et de l'éducation populaire, direction des sports et ses directions régionales et départementales, directions départementales du travail.

Le procureur de la République ou le juge d'instruction procède à l'enregistrement des inscriptions. L'enregistrement des justifications et changements d'adresse sont effectués par les services de police et de gendarmerie, par l'intermédiaire de moyens de télécommunication sécurisés et après vérification de l'identité ainsi que par le gestionnaire.

Le gestionnaire du FIJAIS, avant de valider l'inscription d'une personne, vérifie son identité au vu du Répertoire national d'identification des personnes physiques. Il procède aux effacements ou refuse les enregistrements non conformes à la loi ou au règlement.

Les informations sont conservées pendant vingt ou trente ans selon la gravité de l'infraction commise.

Les informations sont effacées avant l'écoulement de cette durée maximale de conservation en cas de : non-lieu, relaxe ou acquittement non fondé sur l'article 122-1 du code pénal. ; cessation ou mainlevée d'une mesure de contrôle judiciaire ; mort de l'intéressé ; décision du procureur de la République (ou sur exercice d'une voie de recours, du juge des libertés et de la détention ou du président la chambre de l'instruction) compétent d'effacer des informations.

Tout accès au FIJAIS est tracé et archivé durant 3 ans.

Données statistiques

Nombre de personnes concernées par le FIJAIS :

30/06/05 20 222 à l'ouverture du fichier

30/06/06 31 198 (dont 15 418 notifiés)

30/06/07 37 191 (dont 24 089 notifiés)

30/06/08 42 127 (dont 32 526 notifiés)

30/10/08 43 408 (dont 34 768 notifiés)

Régime de justification :

31/01/07 17525 en régime annuel, 2480 en régime semestriel

31/01/08 23559 en régime annuel, 4309 en régime semestriel

30/10/08 26918 en régime annuel, 5958 en régime semestriel, 0 en régime mensuel

b) Fichier automatisé des empreintes digitales (FAED)

Réf. : Décret n°87-249 du 8 avril 1987 (modifié en 2005)

Cadre juridique et finalités

Créé par le décret n 87-249 du 8 avril 1987 (modifié en 2005), le FAED est un fichier commun à la police et la gendarmerie nationales, qui permet :

- d'identifier les traces digitales et palmaires relevées sur les scènes d'infraction afin de rechercher et d'identifier les auteurs de crimes ou de délits ;
- détecter les usurpations d'identité et les identités multiples.

Il est placé sous le contrôle d'un magistrat de l'ordre judiciaire.

Données enregistrées et durées de conservation

Le FAED contient :

- les traces relevées au cours des enquêtes judiciaires ou sur ordre de recherches délivré par une autorité judiciaire ;
- les traces relevées à l'occasion d'une enquête ou instruction pour recherche des causes d'une disparition inquiétante ou suspecte (articles 74-1 et 80-4 du CPP) ;
- les empreintes relevées, dans le cadre des enquêtes pour crimes ou délits, sur les personnes à l'encontre desquelles il existe des indices graves et concordants ;
- les empreintes relevées dans les établissements pénitentiaires afin de s'assurer de l'identité de la personne détenue et d'établir les cas de récidive.

Durée de conservation des données : 25 ans maximum pour les empreintes et selon le temps de prescription de l'action publique pour les traces (3 ans pour les délits, 10 ans pour les crimes).

Modalités d'alimentation et de consultation

Seuls peuvent accéder au fichier les fonctionnaires et militaires, individuellement habilités, des services d'identité judiciaire de la direction centrale de la police judiciaire (DCPJ) et des unités de recherche de la gendarmerie. 13 niveaux d'habilitation ont été définis en fonction des tâches susceptibles d'être accomplies par le fonctionnaire concerné.

Les relevés d'empreintes et les prélèvements de traces sont effectués par des agents formés au sein des services d'enquêtes. Ces relevés sont ensuite transmis à Ecully (DCPJ), Paris (préfecture de police) ou Rosny-sous-Bois (gendarmerie) pour l'alimentation du fichier.

Utilisation opérationnelle

Au 1er octobre 2008, le FAED comptait 2 998 523 individus enregistrés et 171 801 traces non identifiées.

Entre le 1er janvier et le 1er octobre 2008, il a permis d'identifier 11 697 traces et de détecter 61 273 usurpations d'identités ou identités multiples.

Exemples d'affaires

2005 : identification d'un individu dans le cadre d'une affaire de triple assassinat perpétré en Espagne. L'individu a été identifié suite à la découverte de ses empreintes digitales laissées par appui sur le capot d'un véhicule, confirmant ainsi sa présence sur les lieux.

2007 : identification d'un individu dans le cadre d'un attentat à la bombe perpétré contre la mairie de Bordeaux. La trace ayant permis d'identifier l'individu avait été découverte à l'intérieur de la cabine téléphonique localisant l'appel qui a revendiqué l'attentat.

Les relevés d'empreintes digitales et les prélèvements de traces sont effectués par des agents formés au sein des services d'enquêtes.

Pour la police nationale, les relevés d'empreintes sont adressés à Ecully ou à Paris (au moyen des terminaux de signalisation dans la plupart des cas). Pour la gendarmerie nationale, les relevés d'empreintes sont envoyés à Institut de recherche criminelle de la gendarmerie nationale à Rosny-sous-Bois (IRCGN), actuellement au moyen du courrier postal.

Les traces papillaires, quant à elles, sont adressées dans les 19 services régionaux d'identité judiciaire (SRIJ) ainsi qu'à Paris pour la police nationale. Pour la gendarmerie, elles sont envoyées à l'IRCGN à Rosny-Sous-Bois.

Les sites d'Ecully, de Paris, de Rosny-sous-Bois ainsi que les 19 SRIJ assurent l'alimentation du fichier à partir de ces flux de données.

c) Fichier national des empreintes génétiques (FNAEG)

Réf. : Lois du 17/06/1998 et du 18/03/2003. Décret du 18/05/2000 (modifié en 2004)

Cadre juridique et finalités

Créé par la loi du 17 juin 1998 relative à la répression des infractions sexuelles ainsi qu'à la protection des mineurs et mis en œuvre par un décret du 18 mai 2000, le FNAEG est un fichier commun à la police et à la gendarmerie nationales qui permet de faciliter la recherche :

- des auteurs d'infractions à l'aide de leur profil génétique ;
- des personnes disparues et des cadavres non identifiés à l'aide de leur profil génétique de leurs descendants ou de leurs ascendants.

Il s'agit un fichier d'identification qui n'a pas pour objectif de conserver les antécédents judiciaires.

Son champ d'application a été élargi en 2001 aux principaux crimes d'atteintes aux personnes et aux biens, puis en 2003 à plusieurs autres domaines de la criminalité.

Les dispositions relatives au FNAEG figurent aux articles 706-54 à 706-56-1 du code de procédure pénale.

L'enregistrement d'une empreinte génétique dans le FNAEG peut être effectué dans le cadre des infractions limitativement énumérées à l'article 706-55 du CPP, parmi lesquelles figurent notamment les infractions de nature sexuelle, les crimes contre l'humanité et les crimes et délits d'atteinte volontaire à la vie de la personne, de torture et actes de barbarie, de violences volontaires, de trafic de stupéfiants, d'atteintes aux libertés de la personne, de traite des êtres humains, de proxénétisme, d'exploitation de la mendicité et de mise en péril des mineurs.

Le FNAEG est placé sous le contrôle d'un magistrat du parquet hors hiérarchie, assisté par un comité de trois membres tous nommés par le ministre de la justice.

Données enregistrées et durées de conservation

Sont enregistrés :

- les traces biologiques non identifiées ;
- les empreintes génétiques des personnes condamnées pour une des infractions prévues ;
- les empreintes génétiques des personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient commis une des infractions prévues ;
- le profil génétique des personnes disparues ou décédées, ou issu de traces biologiques recueillies dans le cadre des procédures de recherche des causes de la mort ou de disparition (articles 74, 74-1 et 80-4 du CPP).

Durée de conservation des données :

- 40 ans pour les condamnés, les personnes décédées, les personnes disparues et les traces ;
- 25 ans pour les mis en cause et la parentèle des personnes disparues.

Le traitement ne conserve pas l'empreinte génétique des simples suspects (individus pour lesquels seules des raisons plausibles d'avoir commis une infraction existent) : il s'agit d'une simple comparaison avec les données de la base.

Modalités d'alimentation et de consultation

Les OPJ peuvent vérifier, à partir de l'état civil uniquement, si une personne figure déjà dans la base afin d'éviter plusieurs prélèvements biologiques sur un même individu.

Une fois cette vérification effectuée, les OPJ procèdent ou font procéder aux prélèvements sur les individus en cause avant de requérir un laboratoire pour analyse.

En revanche, seuls les fonctionnaires du service gestionnaire du FNAEG (rattaché au service central de l'identité judiciaire de la sous-direction de la police technique et scientifique, à Ecully), sont habilités à alimenter et consulter la base à la demande des magistrats et des services d'enquête.

Toute utilisation du fichier fait l'objet d'une traçabilité totale.

Utilisation opérationnelle

Au 1er octobre 2008, la base de données contenait les profils génétiques de 38 184 traces non identifiées et de 806 356 individus. Elle a permis de rapprocher 17 190 affaires depuis sa création.

Exemple d'affaire : Dans le cadre des constatations techniques effectuées sur la scène d'un nouveau fait de viol perpétré en 2007 à Grenoble, plusieurs traces papillaires latentes étaient mises en évidence dans l'appartement de la victime. Deux traces papillaires, exploitées au fichier automatisé des empreintes digitales (FAED), identifiaient un individu connu pour des actes d'exhibition sexuelle et violation de domicile en 1998. A la suite du prélèvement biologique effectué sur l'individu, le FNAEG rapprochait le profil extrait de ce prélèvement avec les profils extraits de dix traces différentes, relevées dans dix affaires de viol et agressions sexuelles aggravées, tous perpétrés à Grenoble.

Le traité de Prüm, du 27 mai 2005, relatif à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme, la criminalité transfrontalière et la migration illégale, a été ratifié par la France à la suite de la loi n° 2007-1160 du 1er août 2007 et publié par le décret n° 2008-33 du 10 janvier 2008.

Il comporte des stipulations en matière de partage d'informations transfrontalières ainsi qu'en matière de terrorisme concernant les fichiers des empreintes génétiques pour lesquels les Etats parties au traité disposeront désormais, et conformément à leurs législations nationales, d'un accès réciproque automatique.

En conséquence, le fichier national des empreintes génétiques et le fichier national des empreintes digitales sont en cours de modification afin de comporter de nouveaux destinataires et de faire l'objet d'un nouveau dispositif technique pour assurer la transmission de leurs données à caractère personnel vers les Etats parties au traité.

d) Fichier des personnes recherchées (FPR)

Réf. : Arrêté du 15/05/1996 (modifié en 2005)

Cadre juridique et finalités

Cadre législatif : articles 23 de la loi du 18 mars 2003 pour la sécurité intérieure qui détermine les motifs d'inscription judiciaire

Le FPR répertorie, au plan national, toutes les personnes faisant l'objet de recherches par l'autorité judiciaire, les services de police, des douanes, les administrations ou les autorités militaires dans le cadre de leurs compétences légales.

Chaque fiche comporte une conduite à tenir en cas de découverte de la personne recherchée, qui énonce des instructions précises aux services de police ou, dans le cadre de la délivrance de documents, aux services administratifs.

Données enregistrées et durées de conservation

L'inscription au FPR peut intervenir dans plusieurs cas de figure :

- en exécution d'une décision de justice ou dans le cadre d'une enquête de police judiciaire ;
- à la demande des autorités administratives (police des étrangers, recherches dans l'intérêt des familles, opposition à sortie du territoire des mineurs, application des mesures administratives relatives au permis de conduire, opposition à délivrance de documents d'identité ou de voyage, etc.) ;
- à la demande des autorités militaires (déserteurs, insoumis).

Données enregistrées sur les personnes : état civil, alias, sexe, nationalité, signalement (avec la photographie pour certaines catégories de fiches), motif de la recherche.

La radiation des personnes inscrites doit être effectuée sans délai en cas de découverte ou d'extinction du motif de la recherche.

Modalités d'alimentation et de consultation

Le fichier est alimenté par la police et la gendarmerie à travers deux systèmes parallèles. La mise à jour des données s'effectue en temps réel.

La consultation du FPR par les douanes judiciaires (prévue par un arrêté du 2 septembre 2005) s'effectue par le système de la gendarmerie nationale.

Les traitements portant sur les titres d'identité et de séjour consultent automatiquement le FPR avant délivrance du titre (CNI, passeport, visa, dossier des ressortissants étrangers).

Une liaison avec le système d'information Schengen (SIS) a également été mise en place en 1995 pour permettre son alimentation par le FPR. Inversement, les signalements effectués dans le SIS (par les autres pays signataires de la convention Schengen) sont consultables directement à partir d'une interrogation effectuée sur le FPR, depuis les mêmes postes de travail.

Utilisation opérationnelle

Au 30 novembre 2008, le FPR contenait 49 801 fiches Gendarmerie. Il a donné lieu à 6 028 047 consultations par la Gendarmerie Nationale en 2006, 6 281 274 en 2007 et 5 564 774 *en 2008.*

Ce traitement, doit aujourd'hui faire l'objet d'une mise en conformité aux termes de l'article 20 de la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Conformément à l'article 26 II de loi « informatique et libertés », le fichier des personnes recherchées doit être autorisé par décret en Conseil d'Etat pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés.

Cette mise en conformité s'accompagne de trois types de modifications :

Il s'agit, d'une part, de mettre le projet de décret en conformité avec de récentes évolutions législatives en permettant l'inscription des étrangers visés par une décision d'obligation de quitter le territoire français (OQTF) et des arrêtés préfectoraux de reconduite à la frontière pris depuis moins d'un an sur le fondement du 8° du II de l'article L. 511-1 du Code de l'entrée et du séjour des étrangers et du droit d'asile, dont les effets demeurent exécutoires une année après leur édiction quand bien même l'intéressé a quitté le territoire français.

Il s'agit, d'autre part, d'intégrer dans le FPR les ressortissants d'un Etat non membre de l'Union européenne faisant l'objet d'une mesure restrictive de voyage, interdisant l'entrée sur le territoire ou le transit par le territoire, adoptée par l'Union européenne ou tout autre organisation internationale. En effet, la France s'est engagée à procéder à ces inscriptions à compter du 1er juillet 2008, date à partir de laquelle elle exercera la Présidence de l'Union européenne.

Il s'agit enfin, dans un souci d'amélioration de la sécurité routière et de lutte contre la fraude et la conduite avec un permis invalidé, d'inscrire dans le FPR les personnes faisant l'objet de recherches en vue de la notification de mesures administratives concernant leur permis de conduire et celles faisant l'objet d'une mesure administrative visant au retrait d'un permis de conduire obtenu indûment.

La CNIL a rendu son avis le 13 novembre 2008 et le Conseil d'Etat sera prochainement saisi.

e) Outil de Centralisation et de Traitement Opérationnel des Procédures et des Utilisateurs de Signatures (OCTOPUS)

Textes réglementant le fichier

Article 26 (I) de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Articles 322-1 (2ème alinéa) et R. 635-1 du code pénal.

Service gestionnaire du fichier

Direction de la police urbaine de proximité de la Préfecture de Police (Service régional de police des transports - Brigade des réseaux ferrés d'Ile-de-France - Cellule tags).

Présentation et finalité du fichier

Le fichier constitue un outil utilisé par les OPJ et APJ de la cellule tags pour constater les infractions réprimées par les articles 322-1 (2ème alinéa) et R. 635-1 du code pénal, c'est-à-dire « le fait de tracer des inscriptions, des signes ou des dessins, sans autorisation préalable, sur les façades, les véhicules, les voies publiques ou le mobilier urbain », rassembler les preuves de ces infractions et rechercher leurs auteurs

A cette fin, le fichier permet :

- l'établissement de synthèses de faits et des recoupements (identiques ou/et dus à un même auteur) ;
- l'identification des auteurs de dégradation ;
- de répondre à des demandes de renseignements des services extérieurs.

Nature des informations enregistrées

Identité complète de l'auteur identifié, date, lieu d'infraction/constatation, nature du support, constatations effectuées, signatures ou/et *crew* (groupe d'appartenance de tagueurs).

Lorsque l'auteur est inconnu : date-lieu d'infraction/constatation, nature du support, constatations effectuées, signatures ou/et crew (groupe d'appartenance de tagueurs), interpellation d'une personne susceptible d'avoir commis ou participé aux dégradations (procédures extérieures).

Présence de mineurs et si, oui, existe-t-il une limite d'âge ?

Conformément à l'article 21 (II) de la loi du 18 mars 2003 pour la sécurité intérieure, le fichier contient des informations sur les mineurs, sans limitation d'âge, à l'encontre desquels il existe des indices graves ou concordants rendant vraisemblable qu'ils aient pu participer, comme auteurs ou complices, à la commission des infractions mentionnées aux articles 322-1 (2ème alinéa) et R. 635-1 du code pénal.

Destinataires des informations

OPJ et APJ spécialement habilités de la cellule tags et des services de police ou de gendarmerie sur demande pour éventuels rapprochements.

Modes d'alimentation du fichier

Informations collectées par la cellule tags (intégration des archives des procédures traitées), les transporteurs (RATP-SNCF), les services de police ou de gendarmerie extérieurs.

Modes de consultation et traçabilité

Moteur de recherches par mots clefs.

Traçabilité en cours de paramétrage.

Durée de conservation

La durée envisagée, qui sera déterminée par le texte autorisant sa mise en œuvre actuellement en cours d'élaboration, est de 10 ans à partir du dernier fait enregistré.

Droit d'accès aux informations

Le fichier est soumis au droit d'accès et de rectification garanti à chaque citoyen par les articles 39 à 41 de la loi de 1978. Ce droit s'exerce, comme pour presque tous les fichiers de police, par l'intermédiaire de la CNIL.

Modalités d'apurement

Seront déterminées par le texte autorisant sa mise en œuvre actuellement en cours d'élaboration.

Modes d'archivage ou de destruction

Enregistrement sur disque dur et copie de sauvegarde sur serveur indépendant à accès restreint.

Nombre de fiches : 237 fiches au 10/11/2008

1.7. Les systèmes de traitement du renseignement judiciaire

a) Système d'analyse et de liens de la violence associée au crime (SALVAC)

Réf. : Article 21-1 de la loi du 18/3/2003 modifié. Projet de décret et dossier de déclaration en cours d'examen à la CNIL.

Cadre juridique et finalités

SALVAC trouve son fondement dans l'article 30 de la loi du 12 décembre 2005 relative au traitement de la récidive des infractions pénales.

Le projet de décret et le dossier de déclaration sont en cours d'examen par la CNIL.

La finalité du traitement consiste à opérer des rapprochements entre les procédures judiciaires afin d'identifier et poursuivre les auteurs de crimes ou délits commis « en série », dans le domaine de la criminalité violente (meurtre, assassinat, actes de tortures et de barbarie, viol, agression sexuelle, atteinte sexuelle sur mineur, etc.).

Données enregistrées et durées de conservation

Concernant les suspects et les tiers (témoins et relation de l'agresseur) : état civil, adresse, photographie.

Concernant la victime et le mis en cause : état civil, adresse, lieux fréquentés, numéros de téléphone, apparence physique, photographie, mode de vie.

Certaines données sensibles concernant le mis en cause ou la victime peuvent également être mentionnées mais uniquement si cela a une importance pour l'enquête.

Durée de conservation des données : 40 ans.

Modalités d'alimentation et de consultation

L'alimentation et les consultations sont effectuées par 15 policiers et gendarmes de l'office central pour la répression des violences aux personnes (OCRVP), spécialement habilités et individuellement désignés.

Les données alimentant chaque dossier sont fournies par les services enquêteurs à partir d'un questionnaire détaillé.

Utilisation opérationnelle

Au 1er octobre 2008, SALVAC contenait 7891 dossiers.

Nombre d'affaires résolues : 12 séries, soit 95 victimes.

Exemple d'affaire : SALVAC a établi le rapprochement entre plusieurs affaires de viols, agressions sexuelles et tentative d'enlèvement de mineur à partir du signalement de l'auteur et des propos tenus avec ses différentes victimes. Le nom de Patrick M. a été proposé aux enquêteurs de la gendarmerie concernés (dans trois départements) au vu d'une série précédente datant des années 90, dans laquelle l'agresseur avait utilisé le même type de comportement criminel. Cette analyse a été confirmée ensuite par l'enquête.

b) ANACRIM

Réf. : Loi n°2005-1549 du 12/12/2005 et loi n°2003-239 du 18/03/2003

Présentation et finalité

L'analyse criminelle a pour objectif la recherche et la mise en évidence méthodique des relations entre des données issues des enquêtes afin d'améliorer la qualité des investigations par une meilleure compréhension des dossiers. Le logiciel d'analyse criminelle (ANACRIM) est un outil de travail qui fonctionne à partir de fichiers temporaires d'investigations criminelles élaborés exclusivement dans le cadre de procédures judiciaires. Certains services de la police nationale et d'autres administrations utilisent également ce logiciel.

Le système permet notamment de procéder aux analyses suivantes :

- analyse de cas (étude d'un crime ou d'un délit permettant de situer et de comparer dans le temps les actions des différents protagonistes d'une affaire) ;
- analyse comparative de cas (mise en évidence de relations entre les données disponibles concernant différents crimes et délits analogues) ;
- analyse de profil spécifique (recherche d'éléments permettant de déterminer la personnalité probable du ou des auteurs ayant commis un ou plusieurs crimes) ;
- analyse de groupe d'auteurs (étude de la structure d'un groupe d'individus connus et des relations entre les membres de ce groupe).

Il a pour finalité principale de mettre en évidence les liens objectifs entre différentes entités (personnes physiques ou morales, lieux, objets, moyens de transport, traces...) afin de relancer des investigations qui, sans cette mise en lumière, pourraient conduire à l'échec. Il s'agit :

- d'assister le directeur d'enquête dans le cadre d'affaires importantes présentant un très grand nombre de données à traiter, en permettant la gestion et l'exploitation de ces informations, afin d'orienter judicieusement la suite des investigations ;
- d'améliorer la présentation et la compréhension des informations fournies aux différents intervenants (enquêteurs et magistrats) ;
- de faciliter les rapprochements entre différentes enquêtes en cours (identité, numéros de téléphone, mouvements bancaires, etc.) dans le cadre d'une approche sérielle des faits constatés;
- de donner au commandement un outil permettant de suivre les enquêtes, de coordonner l'action des unités et d'organiser les opérations de police judiciaire les plus importantes.

Nature des informations contenues

Les fichiers temporaires sont constitués de l'ensemble des informations objectives issues des procédures établies par les unités de la gendarmerie nationale et les services de la police nationale dans le cadre de certaines enquêtes judiciaires portant sur des crimes ou des délits.

Le choix de faire appel à l'analyse criminelle repose sur la nature complexe[17] et/ou le potentiel sériel d'une affaire. Ainsi, seule l'exploitation complète des données recueillies permet, a posteriori, une discrimination entre des personnes (auteurs, complices, témoins ou personnes s'avérant finalement étrangères au dossier) ou entre des éléments matériels (lieux, véhicules, etc.).

Les éléments de toutes natures (noms, adresses, numéros de téléphone, immatriculations de véhicules, éléments matériels issus des constatations, etc.) et concernant l'ensemble des personnes mentionnées dans une procédure (personnes mises en cause, témoins, victimes) peuvent donc y figurer, dès lors qu'ils sont utiles à la compréhension d'un dossier.

La liste des types d'informations contenues n'est par conséquent pas limitative.

Destinataires des informations

Sont destinataires des analyses issues des traitements, pour les besoins des enquêtes judiciaires :

- les personnels des unités de la gendarmerie nationale exerçant des missions de police judiciaire, et notamment les directeurs d'enquête, chargés d'orienter les investigations ;
- les magistrats du parquet ;
- les magistrats instructeurs, pour les recherches relatives aux faits dont ils sont saisis ;
- les avocats des personnes mises en cause et des victimes constituées parties civiles, conformément à l'article 114 du Code de procédure pénale.

17 La notion de complexité trouve son illustration dans un nombre important de pièces de procédures, un volume important de données de nature différentes à traiter (données criminalistiques, traitement des données téléphoniques, images de vidéo surveillance, bandes sonores...), un nombre important de faits similaires portant sur un même type d'infractions, la multiplicité des reprises de procédures par des services différents.

Modes d'alimentation, de consultation et d'apurement

Alimentation

D'une manière générale, les données sont intégrées manuellement dans les fichiers temporaires d'investigations par des analystes criminels spécialement formés à partir du seul contenu des procédures. Certaines données obtenues par voie de réquisition judiciaire (ex. : facturation détaillée de téléphone) et transmises sous format électronique peuvent être indexées directement. Chaque information collectée comporte systématiquement les références de la pièce de procédure dont elle est extraite.

Consultation

Les fichiers temporaires d'investigations peuvent faire l'objet d'une interrogation directe du fichier pour confirmer la présence ou non d'une entité dans la base de données. Ce mode de consultation n'est utilisé que par la direction d'enquête au titre du contrôle qualité du traitement. De manière générale, les fichiers temporaires d'investigations font l'objet d'une analyse au travers du logiciel ANACRIM qui permet de réaliser des schématisations relationnelles (tableaux, graphiques) concernant les différentes entités connues dans la procédure. Cette « traduction » du fichier temporaire d'investigations permet à la direction d'enquête et au magistrat de comprendre instantanément les interactions possibles entre ces entités, de dégager des incohérences objectives et donc de relancer des investigations ciblées pertinentes et justifiées (perquisitions, auditions, garde à vue...).

Apurement

Les fichiers temporaires sont créés, conservés et utilisés le temps que les analyses nécessaires à l'enquête soient effectuées. Seuls les résultats obtenus sont intégrés au dossier, sous la forme d'un acte indiquant les conclusions de l'analyse et les références précises des pièces de procédure ayant permis d'y aboutir. Les fichiers de travail sont systématiquement détruits dès la fin des investigations.

Situation juridique actuelle

L'article 30 de la loi n° 2005-1549 du 12 décembre 2005 relative au traitement de la récidive des infractions pénales (rajoutant l'article 21-1 à la loi 2003-239 du 18 mars 2003 pour la sécurité intérieure) complètent les dispositions relatives aux traitements automatisés d'informations judiciaires.

Ces dernières s'appliquent aux fichiers temporaires d'analyse criminelle constitués et utilisés dans le cadre des :

- crimes ou délits portant atteinte aux personnes et punis de plus de cinq ans d'emprisonnement ;
- crimes ou délits portant atteinte aux biens et punis de plus de sept ans d'emprisonnement ;
- procédures de recherche de cause de la mort ;
- procédures de recherches de causes de disparitions inquiétantes.

Au regard du potentiel que représente l'analyse criminelle pour faciliter la résolution des affaires, le cadre légal proposé est très limitatif pour trois raisons :

- le périmètre infractionnel ne couvre pas le champ des infractions les plus sérielles (cambriolages, vols simples) et les moins bien élucidées ;
- la finalité visée à l'article 21-1 prévoit la mise en oeuvre de traitements informatiques destinés à faciliter la constatation des infractions alors même que l'analyse criminelle a pour objectif principal de faciliter l'élucidation de faits déjà constatés.
- l'obligation en pratique de déclarer le traitement pour chaque affaire.

Evolution fonctionnelle ou juridique

L'évolution législative envisagée au travers de l'article 6 du projet de LOPPSI doit permettre de distinguer enfin très clairement les fichiers d'antécédents judiciaires des fichiers temporaires d'investigations judiciaires.

Les premiers constituent la base de données des faits constatés, des auteurs et des victimes d'infractions.

Les seconds sont des outils de travail au service de la justice au travers de la démarche d'investigations policières indispensable pour instruire objectivement des dossiers qui peuvent se révéler très lourds, au regard de leur complexité (cf. définition supra) ou de la quantité des données aujourd'hui disponibles due essentiellement à la dématérialisation des échanges et donc à la multiplication des traces laissées par les personnes lors de leurs activités quotidiennes.

1.8. Les fichiers d'identification administrative

a) Fichier relatif à la carte nationale d'identité

Réf. : Décret n° 55-1397 du 22/10/1955 et notamment ses articles : 6-8-9-10- 11-12.

Service gestionnaire du fichier

La DLPAJ met en œuvre le traitement et est à ce titre la direction d'application.

La direction des systèmes d'information et de la communication (DSIC) assure le fonctionnement et la maintenance informatique du fichier.

Présentation et finalités du fichier

Les finalités du fichier ou traitement sont :

- limiter les risques de falsification ou de contrefaçon ;
- la mise en œuvre des procédures de délivrance et de renouvellement ;
- permettre au titulaire d'une carte d'identité de justifier de son identité ;
- faciliter pour les services de la police et de la gendarmerie nationales, leurs missions de recherche et de contrôle de l'identité des personnes notamment lors du franchissement des frontières.

Ce fichier ou traitement, est centralisé et mis à la disposition des services de l'Etat chargés de la délivrance de la carte nationale d'identité.

Nature des informations enregistrées

Les informations enregistrées dans le fichier sont :

- d'une part, les données personnelles du titulaire de la carte, son état civil (nom - prénom(s) - date et lieu de naissance – sexe - nationalité - adresse)
- d'autre part, les informations relatives à la gestion de la demande (dates d'enregistrement de la demande, de production du titre par le centre de production, numéro de la carte) et à l'état du titre (perte, vol, renouvellement, destruction).

Présence de mineurs et si, oui, existe-t-il une limite d'âge ?

La carte d'identité étant délivrée sans condition d'âge, les demandes formulées pour le compte d'un mineur sont enregistrées dans les mêmes conditions que celles qui existent pour les majeurs.

Destinataires des informations

Les destinataires des informations sont les fonctionnaires et agents :

- chargés de l'application de la réglementation relative à la carte d'identité au ministère de l'intérieur, en fonction à la Direction des libertés publiques et des affaires juridiques ;
- en fonction dans les préfectures et les sous-préfectures et chargés de l'établissement du titre (en métropole - dans les DOM et les COM) ;
- en fonction dans les consulats de France et en administration centrale du ministère des affaires étrangères, pour les titres délivrés à l'étranger.
- les agents en charge de la lutte contre le terrorisme à la DGPN, DGGN et à la DGSE dans le cadre de l'habilitation légale prévue par la loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme (article 9).

Les agents précités sont individuellement désignés et habilités.

Modes d'alimentation du fichier

Les données et informations sont saisies directement dans le fichier central dit fichier national de gestion par les agents en charge de l'établissement des titres.

Modes de consultation et traçabilité

Seuls les agents précités ont une possibilité de consultation directe.

A l'exception des services antiterroristes précités, les services de la police et de la gendarmerie ne bénéficient que d'un accès indirect au fichier via les préfectures ou la DLPAJ.

Durée de conservation

Les données et informations enregistrées dans le traitement sont conservées pendant 15 ans.

Droit d'accès aux informations

Le droit d'accès s'effectue auprès du représentant de l'Etat en charge de la délivrance des titres territorialement compétent au regard du domicile du demandeur (préfet, haut-commissaire de la République, consul).

Modalités d'apurement

A l'issue du délai de conservation qui comme indiqué ci-dessus est de 15 ans, les services de la DSIC procèdent à une purge des données sous le contrôle de la DLPAJ.

Évolution fonctionnelle ou juridique

Depuis sa création intervenue en 1987, le fichier n'a subi aucune évolution fonctionnelle ou juridique de fond. Le décret n° 2007-391 du 21 mars 2007 pris en application de l'article 9 de la loi du 23 janvier 2006 rend les services de lutte contre le terrorisme destinataires de données contenues dans ce traitement.

Nombre de fiches

Si la notion de « fiche » est assimilée à tout nouvel enregistrement opéré à l'occasion d'une demande de CNI, le volume annuel de fiches correspond au volume de CNI délivrée annuellement, soit 5 millions par an en moyenne depuis la mesure de gratuité intervenue le 1er septembre 1998 (4 millions / an avant cette date).

b) Fichier relatif aux passeports (Delphine et TES)

Réf. : Décret n°2005-1726 du 30/12/2005 modifié relatif aux passeports et notamment ses articles 18 et 19.

Service gestionnaire du fichier

La DLPAJ met en œuvre le traitement et est à ce titre la direction d'application.

La direction des systèmes d'information et de la communication (DSIC) assure le fonctionnement et la maintenance informatique du fichier.

Présentation et finalités du fichier

Les finalités du fichier ou traitement sont :

- en œuvre les procédures d'établissement, de délivrance, de renouvellement et de retrait des passeports ;
- prévenir et détecter leur falsification et leur contrefaçon.

Ce fichier ou traitement, est centralisé et mis à la disposition des services de l'Etat chargés de la délivrance du passeport.

Nature des informations enregistrées

Les informations enregistrées dans le fichier sont :

- d'une part, les données personnelles du titulaire du passeport, son état civil (nom - prénom(s) - date et lieu de naissance - sexe- nationalité - adresse- taille – couleur des yeux),
- d'autre part, les informations relatives à la gestion de la demande (numéro de demande, droit de timbre, identifiant de l'agent, indication du producteur, l'Imprimerie nationale) et à la création du titre (numéro du titre, date de délivrance, date d'expiration) ainsi que l'état du titre (perte, vol, renouvellement, destruction).

Présence de mineurs et si, oui, existe-t-il une limite d'âge ?

Le passeport étant délivré sans condition d'âge, les demandes formulées pour le compte d'un mineur sont enregistrées informatiquement dans les mêmes conditions que celles qui existent pour les majeurs, la seule différence résidant dans le dossier papier où figure l'accord parental pour délivrer le titre.

Destinataires des informations

Les destinataires des informations sont les agents et personnels :

- chargés de l'application de la réglementation relative aux passeports au ministère de l'intérieur, en fonction à la Direction des libertés publiques et des affaires juridiques ;
- en fonction dans les préfectures et les sous-préfectures et chargés de l'établissement du titre (en métropole - dans les DOM et les COM) ;
- en fonction dans les consulats de France et en administration centrale du ministère des affaires étrangères, pour les titres délivrés à l'étranger.
- les agents en charge de la lutte contre le terrorisme à la DGPN, DGGN et à la DGSE dans le cadre de l'habilitation légale prévue par la loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme (article 9).

Les agents précités sont individuellement désignés et habilités.

Modes d'alimentation du fichier

Les données et informations sont saisies directement dans le fichier central par les agents en charge de l'établissement des titres.

Modes de consultation et traçabilité

Seuls les agents précités ont une possibilité de consultation directe.

A l'exception des services antiterroristes précités, les services de la police et de la gendarmerie ne bénéficient que d'un accès indirect au fichier via les préfectures ou la DLPAJ.

Durée de conservation

Les données et informations enregistrées dans le traitement sont conservées pendant 15 ans pour les majeurs et 10 ans pour les mineurs.

Droit d'accès aux informations

Le droit d'accès s'effectue auprès du représentant de l'Etat compétent en matière de délivrance des titres (préfet, haut-commissaire de la République, consul).

Modalités d'apurement

A l'issue du délai de conservation ci-dessus indiqué, les services de la DSIC procèdent à une purge des données sous le contrôle de la DLPAJ.

Évolution fonctionnelle ou juridique

Depuis sa création intervenue en 1999, le fichier a été modifié en 2005 marginalement (décret n°2005-1726 du 30 décembre 2005 relatif aux passeports électroniques) pour prendre en charge les passeports électroniques et leur mode de fabrication depuis lors centralisé à l'Imprimerie nationale (envoi d'ordres de production à Douai via un réseau sécurisé).

En octobre 2008, une évolution a été apportée au fichier pour lui permettre de prendre en charge les nouveaux passeports d'urgence fabriqués désormais grâce à des imprimantes lasers (et non plus des imprimantes à aiguilles).

Nombre de fiches

Si la notion de « fiche » est assimilée à tout nouvel enregistrement opéré à l'occasion d'une demande de passeport, le volume annuel de fiches correspond au volume de passeports délivrés annuellement, soit 3 millions par an en moyenne depuis 5 ans.

Finalisant l'application du règlement (CE) n° 2252/2004 du 13 décembre 2004 du conseil, les passeports biométriques doivent être délivrés à du compter du 1er janvier 2009.

Conformément au décret n°2008-426 du 30 avril 2008 modifiant le décret 2005-1726 du 30 décembre 2005 précité, le traitement dénommé Titre électroniques sécurisés qui permet l'enregistrement de l'image numérisée du visage et des empreintes digitales et celui des pièces du dossier de demande sera mis en fonction de façon progressive, la généralisation étant prévue pour le 28 juin 2009. Le déploiement a commencé en novembre 2008 dans deux départements pilotes (Oise et Aube).

En conséquence, jusqu'à la mise à jour complète de l'application, les deux systèmes (Delphine et TES) coexisteront.

c) Fichier de suivi des titres de circulation délivrés aux personnes sans domicile ni résidence fixe (FSDRF)

Réf. : Arrêté interministériel du 22/03/1994 modifié par l'arrêté du 28/02/2005.

Présentation et finalité

Le SDRF a pour finalité le suivi des titres de circulation délivrés aux personnes circulant en France sans domicile ni résidence fixes, soumises aux dispositions de la loi n°69-3 du 3 janvier 1969.

Les personnes sans domicile ni résidence fixes depuis plus de six mois, âgées de plus de 16 ans, doivent, pour pouvoir circuler en France, être munies d'un titre de circulation délivré par les préfectures ou les sous-préfectures, qu'elles souhaitent ou non exercer une activité ambulante.

La gendarmerie nationale, rendue destinataire de l'un des deux exemplaires de la notice de délivrance du titre de circulation, le second étant conservé par la préfecture ou la sous-préfecture auprès de laquelle cette formalité a été accomplie, centralise les informations concernant ces personnes.

Mis en œuvre par le service technique de recherches judiciaires et de documentation (STRJD) à Rosny-sous-Bois, ce fichier a un caractère purement administratif et ne comporte aucune mention relative aux condamnations ; ainsi les informations recueillies et mises en mémoire font l'objet d'un traitement spécifique et sont isolées de tout système d'information judiciaire.

Nature des informations contenues

Placé sous la responsabilité du chef du service technique de recherches judiciaires et de documentation (STRJD) à Rosny-sous-Bois, ce fichier a un caractère exclusivement administratif. Les informations utilisées pour ce traitement sont conformes à celles mentionnées par les autorités préfectorales sur les notices de délivrance de titre de circulation.

Les informations mémorisées sont de deux ordres :

- Etat civil : nom patronymique, nom d'épouse, prénoms, date et lieu de naissance, surnom, alias, profession, nom du père, prénom du père, nom de la mère, prénom de la mère, sexe, nationalité, observations contenant le cas échéant :
  - les références des inscriptions au registre du commerce et au répertoire des métiers concernant les titulaires d'un livret spécial de circulation;
  - les signes particuliers (amputations, claudications...) du titulaire, à l'exclusion de tous éléments faisant apparaître directement ou indirectement les origines raciales de l'intéressé (rubrique "signalement" de la notice de délivrance de titre);
  - la mention « décédé » ou « sédentaire » permettent la mise à jour du fichier.
- Titre de circulation : numéro, catégorie, date de délivrance, commune de délivrance, département de délivrance, commune de rattachement.
- Photographie.

Destinataires des informations

Le fichier SDRF a vocation à être consulté par les diverses administrations ayant à connaître de la situation administrative d'une personne sans domicile ni résidence fixes Outre les personnels de la gendarmerie nationale, peuvent donc également accéder aux informations contenues dans le traitement, par l'intermédiaire du STRJD, les services de la police nationale, les services préfectoraux, les services du Trésor, les services du ministère de la santé et les autorités militaires exclusivement lors des procédures de recrutement.

La consultation du fichier des titres de circulation délivrés aux personnes sans domicile ni résidence fixes est faite exclusivement par le STRJD. Elle s'effectue au bénéfice des unités de la gendarmerie nationale, des services de la police nationale et des services préfectoraux.

En outre, peuvent accéder aux informations objet du traitement, les tiers autorisés énumérés ci-après : autorités judiciaires, services du Trésor, services de la Santé et autorités militaires.

Modes d'alimentation et de consultation

La saisie des informations relatives aux titres de circulation est effectuée à partir des notices de délivrance établies par les services préfectoraux et transmises immédiatement par les groupements de gendarmerie départementale. Après saisie, les notices de délivrance des titres de circulation sont détruites.

Une mise à jour des informations est réalisée lorsque :

- une rectification du titre initial est opérée par l'autorité préfectorale et portée à la connaissance de la gendarmerie ;
- une rectification doit être réalisée après exercice par la personne concernée de son droit d'accès ;
- un nouveau titre de circulation est établi au bénéfice d'une personne déjà connue du fichier (duplicata) ;
- le titulaire du titre de circulation se sédentarise, décède, ou atteint l'âge de 80 ans.

La consultation par les unités de gendarmerie est effectuée via le réseau intranet de la gendarmerie pour les consultations dites simples (identité, numéro de notice, surnom).

Les consultations complexes par les unités de gendarmerie et les services de police sont réalisées sur demande au STRJD pour procéder aux opérations suivantes :

- communiquer les informations du titre de circulation à partir d'une identité ou d'un numéro de titre ;
- préciser les identités associées à partir d'une commune de rattachement ou d'un département ;
- récapituler l'historique des titres de circulation détenus par une personne, etc...

Dans le cadre d'enquêtes judiciaires, ce fichier ne peut être consulté que par le biais de réquisitions adressées au STRJD, gestionnaire du fichier.

Toutes les demandes de renseignements relatives au fichier SDRF provenant d'organismes extérieurs à la gendarmerie sont traitées à l'échelon central (STRJD) afin d'assurer la sécurité des informations et le filtrage des accès. Leur satisfaction est subordonnée à une demande écrite et authentifiée, précisant l'identité du consultant, l'objet et le motif de la consultation.

En ce qui concerne les demandes provenant des unités de gendarmerie et des services de police, les réponses sont faites par message, par fax ou par la voie postale.

En ce qui concerne les demandes provenant des autres administrations, le STRJD ne communique par écrit (voie postale) que l'identité, les éléments relatifs au titre de circulation, la catégorie du titre et la commune de rattachement.

Mode d'apurement

Les informations nominatives enregistrées sont conservées six mois après sédentarisation dès lors que celle-ci est portée à la connaissance de la gendarmerie.

En l'absence de sédentarisation, elles sont conservées jusqu'à ce que l'intéressé atteigne l'âge de 80 ans.

Dans tous les cas, la connaissance par la gendarmerie du décès d'une personne SDRF entraîne la destruction des informations nominatives enregistrées.

Dès lors que l'une des conditions ci-dessus est remplie, la destruction des informations nominatives enregistrées concernant cette personne est effectuée d'office par le STRJD.

Droit d'accès aux informations

Le droit d'accès, prévu par la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, s'exerce directement auprès de la direction générale de la gendarmerie nationale.

A la réception de la demande d'accès et après vérification de l'identité du demandeur, les informations relatives à la personne exerçant son droit sont éditées par le STRJD et lui sont communiquées, en langage clair, dans un délai de 15 jours par la direction générale de la gendarmerie nationale.

A ce jour, aucune demande n'a été formulée.

Evolution fonctionnelle ou juridique

La circulaire relative au fichier des titres de circulation délivrés aux personnes sans domicile ni résidence fixes est en cours de refonte afin de prendre en compte les modifications de l'arrêté du 28 février 2005

autorisant l'insertion des photographies numérisées des personnes SDRF.

Le fichier comporte 170140 fiches. Le fichier est consulté environ 400 fois par jour.

d) Le fichier national des permis de conduire

Présentation du fichier - Historique

Au sein du ministère de l'Intérieur et de l'Aménagement du Territoire - Secrétariat général - Direction de la modernisation et de l'action territoriale (DMAT) / Sous-direction de la circulation et de la sécurité routières, le service du fichier national des permis de conduire (FNPC), créé par arrêté du ministre de l'Intérieur le 20 décembre 1972, gère l'application réglementaire Système national des permis de conduire (SNPC),

Le service du FNPC a donc pour vocation, en application de l'article L.225-1 du code de la route, d'enregistrer et gérer toutes les informations relatives aux permis de conduire, en particulier les droits de conduire de tout conducteur, ainsi que toutes les informations nécessaires à cette gestion.

Dans ce contexte, il assume essentiellement cinq missions :

- piloter la direction d'application du Système National des Permis de Conduire (SNPC) ;
- mener les opérations de fiabilisation de la base de données SNPC ;
- assurer la gestion du permis à points, et notamment l'exécution de son contentieux ;
- traiter des permis de conduire échangés à l'étranger ;
- diffuser toutes informations juridiques et techniques aux utilisateurs (services préfectoraux, officiers du ministère public).

Nature des informations contenues dans l'application SNPC

En application de l'arrêté ministériel du 29 juin 1992 modifié, le Système national des permis de conduire comprend des données centrales et des données locales.

a) Sont enregistrées comme données centrales les catégories d'informations ci-après :

Dans tous les cas :

- Etat civil : nom, nom d'usage, prénoms, date et lieu de naissance ;

- Adresse ;

- Numéro de dossier.

Selon les cas :

- Les conditions restrictives imposées au conducteur ou au demandeur ;
- Le numéro du dernier titre délivré; la délivrance de duplicata ;
- Les informations relatives aux catégories de permis de conduire demandées ou obtenues, le mode d'obtention, les dates limites de validité ;
- L'état de validité de chaque catégorie, la ou les causes d'invalidité ;
- L'état de validité du permis ; la ou les causes d'invalidité ;
- La déclaration de perte ou de vol du titre, la découverte du titre perdu ou volé ;
- L'échange du titre à l'étranger : la mention que le titre échangé est faux ou falsifié, la restitution de titre étranger ;
- Les décisions administratives, dûment notifiées, portant retrait de catégories et de titres obtenus irrégulièrement ou frauduleusement ;
- Les références du document présenté pour l'obtention d'un permis : permis étranger ou d'outre-mer, diplôme ou certificat professionnel, brevet militaire ;
- Les décisions administratives, dûment notifiées, prises sur avis de la commission médicale, et portant restriction, maintien, prorogation ou annulation, d'une ou plusieurs catégories du permis de conduire ;

- Les mesures dûment notifiées, en tant qu'elles portent avertissement, rétention, suspension ou interdiction de délivrance du permis de conduire, ainsi que les renseignements relatifs à la notification et à l'exécution de ces mesures ;
- Les mesures de retrait du droit de faire usage du permis de conduire qui seraient communiquées par les autorités compétentes des territoires et collectivités territoriales d'outre-mer ;
- Les mesures de retrait du droit de faire usage du permis de conduire prises par les autorités étrangères et communiquées aux autorités françaises conformément aux accords internationaux en vigueur ;
- Les procès-verbaux des infractions mentionnées ayant donné lieu au paiement d'une amende forfaitaire ou à l'émission d'un titre exécutoire de l'amende forfaitaire majorée ;
- Les décisions judiciaires à caractère définitif en tant qu'elles portent restriction de validité, suspension, annulation et interdiction de solliciter et de délivrance d'un permis de conduire, ou qu'elles emportent réduction du nombre de points du permis de conduire, ainsi que les renseignements relatifs à l'exécution de ces décisions ;
- Le décompte de points du permis de conduire ;
- Les références des documents constatant l'exécution d'une formation spécifique par les conducteurs entraînant attribution de points du permis de conduire;
- Les décisions rapportant, modifiant ou annulant les mesures précédentes.

b) Sont enregistrées comme données locales les catégories d'informations ci-après :

- Répartition des places d'examen du permis de conduire ;
- Organisation et fonctionnement des commissions médicales : nom, prénom, adresse des membres, organismes représentés ;
- Procès-verbaux d'infractions susceptibles d'entraîner la saisine de la commission spéciale, donnant son avis sur les mesures de restriction du droit de conduire ;
- Avis des commissions médicales sur l'aptitude des candidats et des conducteurs, à l'exclusion de tout renseignement de caractère médical confidentiel ;
- Projets de décisions préfectorales.

Les acteurs de l'application SNPC

Les Préfectures

Il s'agit de l'un des acteurs principaux du système.

Les différents services de la préfecture remplissent les rôles suivants :

- la délivrance des permis de conduire ;
- la répartition des places d'examen au permis de conduire ;
- la gestion du volet médical ;
- la gestion des procédures de suspension ;
- saisie des décisions judiciaires de 5ème classe et des délits dans SNPC.

Les préfectures sont également le relais des autorités judiciaires (Tribunal de Grande Instance) qui peuvent ainsi avoir communication des informations contenues dans le relevé intégral des mentions relatives au permis de conduire.

Les Sous-préfectures

Elles ont un rôle identique aux préfectures et agissent en délégation de ces dernières.

Les officiers des ministères publics près les tribunaux de police (DGPN)

Le rôle des OMP est centré sur les opérations de sanction et de suspension de permis, dans le cadre d'une procédure légale. Ils sont ainsi amenés à enregistrer dans SNPC les sanctions prononcées et à statuer sur la validité du titre que détient la personne.

A noter, que les OMP de Paris et de la petite couronne dépendent du ministère de la justice et remplissent le même rôle que les OMP de la DGPN.

Le Contrôle Sanction Automatisé (CSA)

Le CSA gère le flux des contrôles radar. Il accède à FNA pour obtenir l'état civil du titulaire de la carte grise correspondant à la plaque d'immatriculation photographiée.

Cet état civil est soumis à SNPC, ainsi que les informations relatives à la sanction prévue. SNPC traite le flux pour mettre à jour les informations relatives au conducteur et au permis.

La Police

Dans le cadre de leurs missions de contrôle, les services de police peuvent accéder au relevé **intégral** des dossiers contenus dans SNPC (article L.225-4 du code de la route).

Applications du ministère des transports

Deux applications du ministère des transports sont en interface directe SNPC.

D'une part AURIGE, qui permet la gestion des examens du permis de conduire, celle des inspecteurs et celle des auto-écoles. SNPC fournit les informations nécessaires à ces opérations de gestion.

D'autre part l'application CHRONOTACHYGRAPHE, qui assure le suivi des informations relatives aux conducteurs professionnels catégorie lourde. Cette application interroge par fichier SNPC qui en retour fournit les informations attendues, sous forme de fichiers également.

Les directions départementales de l'équipement (ministère des transports)

La DDE peut jouer un rôle semblable à celui d'une préfecture. Elle est raccordée à un CII et peut effectuer en temps réel les opérations suivantes :

- Mise à jour de SNPC pour les demandes et réussite à l'examen du permis de conduire ;
- Consultation des informations ;
- Gestion des examens.

Les DDE ne produisent pas de permis de conduire. Elles accèdent à SNPC par une liaison sécurisée, via le réseau ADER

La Gendarmerie

La gendarmerie est destinataire permanent des informations SNPC (dossier intégral, par consultation via un système propre DGGN).

L'Imprimerie Nationale

L'imprimerie nationale a en charge, à partir de SNPC, l'édition des lettres de type 46 (reconstitution de points ou réattribution) et 48 (retraits de points) et leur envoi aux personnes concernées.

La DMAT

La DMAT intervient au travers du service du Fichier National des permis de conduire (FNPC).

Les principales missions du FNPC, exercées dans le cadre de l'application, sont :

- de mener les opérations de fiabilisation de la base de données SNPC (détecter les anomalies existantes liées à un historique de 42 millions de titres, et mettre à jour les informations) ;

- d'assurer la gestion du permis à points, notamment l'exécution de son contentieux ;

- de traiter les permis de conduire échangés à l'étranger.

La DSIC

La DSIC joue le rôle d'administrateur technique de l'application.

L'accès à l'application SNPC

Toutes les informations traitées par SNPC sont, conformément aux dispositions de la loi informatique et liberté, strictement confidentielles.

Seuls peuvent y avoir accès : les agents du service du FNPC (liés à l'obligation de réserve), les juges, les préfets, les forces de l'ordre (policiers et gendarmes) dans le cadre de leur activité d'officier de police judiciaire et lors des contrôles routiers (en application de l'article L. 225-4 du Code de la route), l'intéressé lui-même, son avocat, son mandataire (en application de l'article L. 225-3 du Code de la route).

Prochaines évolutions envisagées

L'architecture fonctionnelle et technique de l'actuelle application réglementaire système national des permis de conduire (SNPC) ne permet plus de prendre en compte rapidement et efficacement des évolutions importantes impliquées par la mise en œuvre des directives européennes, des nouvelles mesures législatives et réglementaires et de la jurisprudence.

Elle a atteint la limite de ses capacités de traitement et est devenue fragile et rigide en raison de l'accumulation des modifications apportées au fur et à mesure des années. En conséquence, un projet de refonte globale de cette application informatique est en cours.

La nouvelle application devrait notamment permettre la fabrication centralisée du futur titre de conduire, sous la forme d'une carte plastique intégrant, à terme, une puce électronique. Elle permettra également une amélioration du fonctionnement général du système.

Cette nouvelle application, qui devrait a priori être opérationnelle en 2011/2012, offrira donc une meilleure qualité de service aux usagers, et permettra un renforcement de la lutte contre la violence routière, contre la fraude et le contournement des mesures restrictives prises au niveau national. Parallèlement, des économies importantes devraient être générées en maintenance évolutive.

2. LES FICHIERS EN COURS DE DEVELOPPEMENT

2.1. Les applications bureautiques

a) Traitement de données « pré-plainte en ligne » (PPL)

Réf. : Décret n° 2008-1109 du 29 octobre 2008.

Présentation et finalités

Il s'agit d'un téléservice susceptible de permettre à la victime ou son représentant d'effectuer une déclaration en ligne pour les seuls faits d'atteintes aux biens contre auteur inconnu, d'une part, et d'obtenir un rendez-vous auprès d'un service de police ou d'une unité de gendarmerie nationales de son choix pour signer sa plainte, d'autre part.

Le dispositif est d'abord destiné à améliorer les conditions d'accueil du public, dès lors qu'il devrait permettre de supprimer les délais d'attente auxquels sont actuellement confrontées les victimes lorsqu'elles se rendent au commissariat ou au sein d'une brigade de gendarmerie pour y déposer plainte. Il devrait également contribuer à réduire le temps nécessaire à l'enregistrement de la plainte par les personnels de police ou de gendarmerie.

Nature des informations contenues

Les catégories de données à caractère personnel enregistrées dans le traitement sont les suivantes :

- données relatives aux personnes physiques : identité (nom de naissance, nom d'épouse, prénom), date et lieu de naissance, nationalité, adresse, profession, numéro de téléphone, adresse de courrier électronique.
- données relatives aux personnes morales : raison sociale, numéros SIREN et SIRET, numéro d'inscription au registre du commerce et des sociétés, forme juridique, lieu du siège social, adresse.
- données relatives aux faits rapportés par la victime ou son représentant légal : date et lieu de l'infraction, circonstances de l'infraction, préjudice, éléments susceptibles d'orienter l'enquête.
- données relatives à la localisation du service de police ou de gendarmerie nationale choisi par la victime pour aller signer sa plainte.
- le numéro identifiant délivré à la victime par le traitement.

Destinataires des informations contenues

Les droits d'accès sont strictement limités, encadrés par le système d'habilitation défini ci-après.

1. Habilitation des agents

Pour la police nationale, les informations sont envoyées par le serveur DGME sur le serveur du commissariat concerné. Ce serveur donne accès aux informations sur la boîte à lettres fonctionnelle « aide aux victimes ».

Cette boîte n'est accessible qu'aux fonctionnaires habilités, titulaires d'un identifiant et d'un mot de passe. Les habilitations sont délivrées par le fonctionnaire réseau (correspondant départemental des systèmes informatiques et télécommunications) sur demande du directeur départemental de la sécurité publique. L'habilitation est systématiquement retirée lorsque le fonctionnaire « n'a plus à en connaître ».

Les courriels reçus sur la boîte «aide aux victimes » sont copiés sur le réseau local dans un répertoire principal « plainte Internet ». L'accès au réseau se fait selon la même procédure d'habilitation que pour la messagerie et les droits de chaque utilisateur sont gérés par l'administrateur réseau.

Le fonctionnaire « aide aux victimes » dispose d'un droit de création, de lecture et de suppression. Les fonctionnaires chargés de la prise de plaintes auront un droit d'accès en lecture et écriture.

Pour la gendarmerie nationale, les renseignements saisis par le déclarant seront traités par des gendarmes, agent ou officier de police judiciaire, de l'unité choisie comme lieu de signature de la plainte. Le militaire traitant sera identifié par un identifiant personnel et son mot de passe secret.

2. Traçabilité

Les procédures de surveillance du réseau sont sous la responsabilité de l'administrateur de réseau et du référent « aide aux victimes ».

Pour la gendarmerie nationale, chaque connexion au serveur central hébergeant les données saisies par les plaignants fait l'objet d'un marquage concrétisé dans un journal.

Mode d'alimentation, de consultation et d'apurement

Aucune mise à jour ni aucune modification des données saisies par le déclarant n'intervient jusqu'à la présentation de celui-ci au lieu de signature de la plainte. L'extraction et l'édition du procès-verbal entraînent l'effacement du dossier enregistré sur le serveur du commissariat ou sur la base de données de la gendarmerie.

Les données à caractère personnel sont effacées lorsque la victime vient signer sa plainte au service de police ou de gendarmerie choisi. Si la victime ne se rend pas au rendez-vous fixé par le service de police ou l'unité de gendarmerie, les données sont automatiquement effacées passé un délai de 30 jours après la réception de la déclaration.

Situation juridique

Le dispositif est actuellement en cours d'expérimentation dans les départements des Yvelines et de la Charente Maritime pour une durée de 12 mois maximum.

Il a été validé par la délibération CNIL n° 2008-102 du 29 avril 2008. Son décret de création du 29 octobre 2008 a été publié au *Journal officiel de la République française* du 31 octobre 2008.

b) PULS@R

Présentation et finalité

PULS@R est une évolution de l'application Bureautique Brigade 2000, déclarée à la CNIL.

Centralisée, cette future application permettra aux unités territoriales de la gendarmerie nationale de gérer sur le plan administratif le service et les registres (courrier et procès-verbaux), les amendes forfaitaires, ainsi que de générer les messages d'information statistique relatifs à la délinquance et les bulletins d'analyse des accidents relatifs à l'accidentalité. Un module « dossier de circonscription » complètera à terme l'application en vue du partage de l'information relative à la connaissance de la circonscription (lieux et personnes indispensables à connaître)

Ce nouvel outil bureautique constitue une adaptation nécessaire à la nouvelle organisation des unités de Gendarmerie dont une partie est regroupée depuis 2002 en communautés de brigades.

L'application PULS@R sera déployée au sein des unités en 2009

Nature des informations contenues

PULS@R contiendra certaines informations à caractère personnel au sein des modules suivants :

- **« gestion du service** » : les grades, nom, prénom des militaires composant l'effectif de l'unité, nécessaires pour planifier le service. Le commandant d'unité pourra également saisir les nom, prénom et adresse de tiers dans le cadre des ordres délivrés et que les gendarmes ont besoin de localiser sur la circonscription en vue de les rencontrer à l'occasion de leur service (poursuite d'enquête, remise de pièces).
- **« gestion du registre »** : il comporte les données relatives au courrier reçu et envoyé par l'unité ainsi que celles concernant les procédures rédigées. On retrouve les références de la personne « cliente » de l'unité: le nom, le prénom, la date de naissance, le lieu de naissance et la qualité de la personne (victime, auteur entendu).

  Ces informations sont nécessaires pour permettre de suivre les courriers et procédures et de renseigner les personnes sur l'état d'avancement des dossiers les concernant.
- **« gestion des amendes forfaitaires »** : données relatives aux noms, prénom, date de naissance, lieu de naissance de la personne à qui a été délivrée l'amende forfaitaire et le type d'infraction relevée.

  Ces informations sont indispensables pour permettre de suivre les amendes durant tout leur cycle de vie à la fois dans un souci de saine gestion à l'égard des comptables du trésor, et des éventuelles suites incombant aux officiers du ministère public.
- **« gestion des MIS et des BAA »** :

  Le Message d' Information Statistique (MIS) doit être créé à partir des éléments d'identité et de la qualité de la personne (victime ou mis en cause) appréciée au moment de la transmission de la procédure vers l'autorité destinataire. Généré à des fins statistique, le MIS est toutefois anonymisé avant sa saisie en base centrale. Seules les informations concernant le sexe, l'âge et la nationalité sont prises en compte. Le nom et le prénom ne saisis initialement que pour permettre à l'enquêteur de vérifier ces informations dans le cas de pluralité de victimes ou de mis en cause.

  Le Bulletin d'Analyse des Accidents (BAA) doit être créé à partir des : données concernant le nom, le prénom, la date et le pays de naissance, la qualité (indemne, blessé, tué), la responsabilité au regard de l'accident et les infractions éventuellement relevées jusqu'au moment de la génération du bulletin (30 jours après l'accident) en vue d'alimenter l'ONISR (Observatoire National Interministériel de la Sécurité Routière), la CUB (Communauté Urbaine de BORDEAUX – ne concerne que les accidents constatés sur cette emprise) et le CEESAR (Centre Européen d'Etudes de Sécurité et d'Analyse des Risques). Généré à des fins statistiques le BAA est toutefois anonymisé avant sa saisie en base centrale. Seules les informations statistiques anonymes sont envoyées à ces organismes (sexe, date de naissance, département ou pays de naissance, qualité, position dans le véhicule, la responsabilité au regard de l'accident, infractions éventuellement relevées (au nombre de deux).

Destinataires des informations

Seuls les personnels de la gendarmerie sont destinataires des informations contenues dans l'application en dehors du BAA et des amendes forfaitaires dans certaines conditions.

Modes d'alimentation, de consultation et d'apurement

L'alimentation et la consultation se font à partir de n'importe quel poste de travail connecté au réseau intranet. Les droits d'accès sont dérivés directement de l'authentification de l'utilisateur au réseau intranet. Les profils sont déterminés par l'unité d'appartenance et le niveau de responsabilité exercée.

Pour les registres, amendes forfaitaire, MIS, BAA et CR de service, les données sont créées au niveau de l'unité élémentaire (commandant d'unité ou exécutant) et consultables au niveau département, mais uniquement avec le profil de commandant de groupement.

Pour le dossier de circonscription (répertoire des personnes et des lieux) les données sont accessibles à tous les militaires d'un même département.

Toute action de consultation, création ou modification d'une données est enregistrée avec l'identifiant de connexion de l'utilisateur. Ce qui permet de tracer un éventuel usage irrégulier de l'application. Les règles d'apurement sont en cours de définition en fonction des objectifs liés à chacun des modules de l'application.

Les règles d'apurement varient en fonction des modules : Elles peuvent différer de celles adoptées pour BB 2000, afin de répondre au strict besoin correspondant à la finalité.

- le service : apurement prévu au terme de trois années
- le registre : apurement au terme de six mois après envoi du courrier ou d e la procédure à l'autorité destinataire. En pratique le traitement d'une grande majorité des procédures ne nécessite que quelques mois, à l'exception des affaires les plus importantes dont la durée de traitement ne peut être standardisée;
- les amendes forfaitaires : apurement au terme d'un délai de 100 jours.
- le message d'information statistique : apurement au terme de la transmission des procédures à l'autorité destinataire. C'est l'envoi de la procédure qui permet de générer la clôture du MIS.
- le BAA (bulletin d'analyse des Accidents) : apurement au terme de 31 jours consécutifs à l'accident. Ce délai procède de la prise en compte statistique des tués, arrêtée au 30ème jour après l'accident.

Fichiers de journalisation : la durée de conservation des données de connexion (autorisant la traçabilité des utilisateurs) préconisée par la CNIL de manière courante est de six mois.

Situation juridique actuelle

Le dossier de déclaration à la CNIL est en cours d'élaboration.

Il est à noter que PULS@R est une évolution de l'application BB2000, qui a déjà fait l'objet d'une déclaration.

Evolution fonctionnelle ou juridique

L'application doit être complétée par un module « dossier de circonscription » conçu comme un répertoire dédié regroupant les personnes et les lieux devant être connus du personnel de l'unité pour l'exécution de sa mission.

Le dossier de circonscription comportera les nom, prénom, adresse et numéro de téléphone à l'exclusion de toute donnée à caractère philosophique, politique, sexuel) des personnes ou autorités exerçant une responsabilité sur la circonscription et devant pouvoir être contactées à tout moment pour les besoins du service (élus, chefs d'entreprise ou de complexe sensible, garagistes fourriéristes, pharmaciens, médecins, magistrats), ou en raison de leurs liens avec la communauté professionnelle de la gendarmerie ou de la défense (retraités et veuves de la gendarmerie, officiers de réserve).

Il sera complété d'un répertoire ders lieux sensibles appelant à ce titre une surveillance particulière (établissements scolaires, sites industriels, zones d'activité) dans le cadre de la mission de sécurité publique générale des unités.

Ces données ont vocation à être conservées tant que les personnes référentes demeurent effectivement en exercice sur la circonscription. La mise à jour entraîne la suppression des données antérieurement saisies (pas d'historique).

c) Application de recueil de la documentation opérationnelle et d'informations statistiques sur les enquêtes (ARDOISE)

Réf. : Déclaration du traitement en cours. Avis de la CNIL rendu et Conseil d'Etat saisi.

Cadre juridique et finalités

Dans le cadre de la modernisation des moyens technologiques des forces de sécurité, l'actuel logiciel de rédaction de procédures (LRP) sera prochainement remplacé par un nouveau traitement dénommé ARDOISE destiné à uniformiser la rédaction de procédures et à alimenter notamment le futur fichier ARIANE, qui remplacera à la fois le STIC de la police nationale et le JUDEX de la gendarmerie nationale.

ARDOISE constituera donc, dans sa version définitive qui interviendra au terme des améliorations techniques successives :

- un support technique unique de l'activité procédurale de l'ensemble des services de la police nationale dans l'exercice de leurs missions de police judiciaire et administrative ;
- l'outil d'alimentation des traitements nationaux de documentation criminelle (ARIANE, fichiers d'objets volés).

Toutefois, la version actuelle d'ARDOISE (qui sera mise en service à la fin de l'année) n'est qu'une version modernisée du logiciel de rédaction de procédures. Elle n'alimente donc aucun autre traitement.

Données enregistrées et durées de conservation

ARDOISE permet la collecte et l'archivage des informations recueillies par les services chargés de l'établissement des procédures diligentées dans le cadre de leurs missions de police judiciaire ou administrative. Les données enregistrées sont donc issues des procès-verbaux, comptes rendus d'enquêtes et rapports administratifs ou judiciaires.

Dans la version « Rédaction de procédure », dont le dossier de déclaration est en cours d'examen à la CNIL, la durée de conservation des données a été fixée à 5 ans à compter de la transmission de la procédure à l'autorité judiciaire ou administrative compétente.

Modalités d'alimentation et de consultation

ARDOISE est accessible et alimentée par chaque service de police gestionnaire d'un registre de procédures judiciaires. Les bases locales ARDOISE propres à chaque service sont accessibles, par l'intermédiaire du réseau sécurisé CHEOPS du ministère de l'intérieur, aux seuls fonctionnaires habilités selon leur « profil » propre (enquêteur, gestionnaire de la base, chef de service, administrateur de la base).

Utilisation opérationnelle

Fin 2007 puis à nouveau au printemps 2008, plusieurs associations ont appelé l'attention du ministre de l'intérieur sur l'utilisation dans ARDOISE d'un thésaurus extrait de celui du STIC et permettant de collecter des données dites sensibles.

Afin de dissiper tout malentendu, le ministre a décidé en avril dernier de suspendre l'expérimentation du traitement et demandé que les termes les plus sensibles (notamment sur la vie sexuelle) s'appliquent à l'infraction et non plus à une personne.

2.2. Les fichiers d'identification judiciaire

a) Fichier des objets et véhicules signalés (FOVES)

Présentation et finalité

Projet de modernisation isofonctionnel conjointement mené par la gendarmerie et la police nationales, l'application FOVES doit fusionner les applications FOS (Fichier des Objets Signalés), FVV (Fichier des Véhicules Volés) ainsi que le STIC (Système de Traitement des Infractions Constatées) dans sa partie « objets ». Elle constitue un fichier dit de contrôle en présence des objets et véhicules afin de savoir si ceux-ci ont été signalés auprès de forces de police. Le déploiement est prévue en deux lots successifs, « objets » et « véhicules », et débutera au second semestre 2009.

Nature des informations contenues

Ce nouveau système inclura des éléments descriptifs textuels ou photographiques d'objets et véhicules déclarés volés, mis sous surveillance ou encore, pour certaines catégories, perdus. Il comportera également des éléments d'identité des propriétaires des objets ou véhicules tel que le nom, le prénom et la date de naissance.

L'ensemble des objets et véhicules gérés à travers l'application FOVES est classé en 12 catégories : arme, document, billet de banque, multimédia, moyen de paiement, objets d'art et horlogerie, objets divers, bijoux et montres, containers et équipements industriels non roulants, véhicules terrestres et plaques d'immatriculation, bateaux et moteurs de bateaux, aéronefs.

Destinataires des informations

Les applications seront déployées à l'identique dans les environnements de la gendarmerie et de la police. Dès leur mise en production, elles seront accessibles par les personnels habilités des unités opérationnelles de la gendarmerie nationale, de la police nationale et des douanes.

Modes d'alimentation, consultation et apurement

Un mode d'alimentation directe par une interface dédiée de manière à prendre en compte les inscriptions hors procédure (perte d'objets) et les inscriptions en urgence est envisagé, ainsi qu'un mode d'alimentation par le logiciel d'aide à la rédaction de procédure Icare de la gendarmerie nationale et par l'application Ardoise de la police nationale. La consultation pourra se faire indifféremment par RUBIS ou par l'Intranet de la gendarmerie. L'apurement des données sera automatiquement réalisé par l'application en fonction des durées de conservation des objets.

Situation juridique actuelle

Le projet de décret et la déclaration à la CNIL de l'application FOVES sont en cours d'élaboration.

b) Système de traitement des images des véhicules volés (STIVV)

Réf. : En phase préparatoire de déclaration auprès de la CNIL

Présentation et finalité

La création du « contrôle-sanction automatisé » a entraîné la mise en place de la Cellule de traitement des images des véhicules volés (CTIVV) au sein du Service technique de recherches judiciaires et de documentation (STRJD) implanté à Rosny-sous-Bois (93). Son outil est le Système de traitement des images des véhicules volés (STIVV). Cette cellule, à vocation interministérielle, a pour mission d'exploiter, à des fins d'enquêtes judiciaires, les photographies prises par des radars automatisés de véhicules volés, ou mis sous surveillance, ou circulant avec une immatriculation fausse ou altérée. Elle est également chargée de confirmer ou d'infirmer auprès du Centre automatisé de constatation des infractions routières (CACIR) à Rennes (35) la situation administrative ou judiciaire des véhicules au moment de la commission de l'infraction.

Nature des informations contenues

Les informations contenues dans le STIVV comprennent deux photographies de chaque véhicule concerné ainsi que la date, l'heure et le lieu de l'infraction, la vitesse relevée et la vitesse limite autorisée. La plaque d'immatriculation est toujours lisible. En fonction du réglage de l'angle de prise de vue des appareils de lecture, le visage du conducteur ou de passagers peut être apparent.

Destinataires des informations

Est destinataire, l'unité de gendarmerie ou de police qui a enregistré la plainte pour vol ou opéré la mise sous surveillance, ainsi que l'unité du lieu de commission de l'infraction à la vitesse.

Le CACIR est destinataire des renseignements concernant la position du véhicule (volé ou surveillé).

Modes d'alimentation, de consultation et d'apurement

Le CACIR génère quotidiennement un listing de photographies de véhicules volés ou surveillés qu'il adresse à la CTIVV. Tous les officiers et agents de police judiciaire disposant d'une liaison intranet peuvent consulter directement la base de données images du STIVV. Le STRJD répond directement aux demandes provenant des services de la police nationale et des unités de gendarmerie non connectées au réseau intranet de la gendarmerie nationale.

L'original des photographies ne peut être réclamé que par voie de réquisition au CACIR.

Aucune modalité d'apurement de données n'est encore prévue pour cette base nouvelle encore en cours de déploiement.

Situation juridique actuelle

Le STIVV, dans sa phase préparatoire de déclaration auprès de la CNIL rencontre des difficultés juridiques. En effet, le système de traitement de contrôle sanction automatisé ne prévoit pas dans son texte réglementaire la transmission de ses données à un service de police ou de gendarmerie sauf dans le cas d'une réquisition judiciaire. La transmission automatisée des données nécessiterait par conséquent la modification du texte encadrant le système contrôle sanction automatisé.

Ces informations n'ont donc actuellement valeur que de simple renseignement judiciaire.

Évolution fonctionnelle ou juridique

Le STIVV compte 12 373 dossiers et 24 746 photos.

Le futur système central de traitement du LAPI (SCTL) pose indiscutablement la question de la nécessité de conserver une application qui sera à terme redondante avec les fonctionnalités du SCTL. Un projet d'alimentation du SCTL avec les images des véhicules volés issues du CACIR est actuellement à l'étude.

Dans ces conditions, il est envisagé d'abandonner le traitement.

c) Lecture automatisée des plaques d'immatriculation (LAPI)

Texte réglementant le fichier

Le traitement automatisé de contrôle des données signalétiques des véhicules (Lecture automatisée des plaques d'immatriculation – LAPI) a été créé, à titre expérimental, par l'arrêté du 2 mars 2007. Il tire son fondement juridique de l'article 26 de la loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure, modifié par l'article 8 de la loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme.

Service gestionnaire du fichier

Le fichier est géré par la direction générale de la police nationale et la direction générale de la gendarmerie nationale.

Présentation et finalité du fichier

Il s'agit de traitements destinés à contrôler les données signalétiques des véhicules en prenant la photographie de leurs occupants.

Ils sont mis en œuvre par les services de police et de gendarmerie nationales afin de prévenir et de réprimer le terrorisme, de faciliter la constatation des infractions s'y rattachant, de faciliter la constatation des infractions criminelles ou liées à la criminalité organisée au sens de l'article 706-73 du code de procédure pénale, des infractions de vol et de recel de véhicule volés, des infractions de contrebande, d'importation ou d'exportation commises en bande organisée, prévues et réprimées par le deuxième alinéa de l'article 414 du code des douanes, ainsi que la constatation, lorsqu'elles portent sur des fonds provenant de ces mêmes infractions, de la réalisation ou de la tentative de réalisation des opérations financières définies à l'article 415 du même code et afin de permettre le rassemblement des preuves de ces infractions et la recherche de leurs auteurs.

Ils sont également mis en œuvre par les services de police et de gendarmerie nationales, à titre temporaire, pour la préservation de l'ordre public, à l'occasion d'évènements particuliers ou de grands rassemblements de personnes, par décision de l'autorité administrative.

Ces traitements comportent une consultation automatisée du fichier des véhicules volés ou signalés.

Nature des informations enregistrées : Les données enregistrées sont relatives à la photographie du numéro d'immatriculation du véhicule et son taux de lisibilité, au numéro d'immatriculation du véhicule, à la photographie du véhicule et de ses éventuels occupants, à la date et l'heure de chaque photographie et, pour chaque photographie, à l'identifiant et aux coordonnées de géolocalisation du dispositif de contrôle automatisé.

Dans les cas de rapprochement positif avec un des numéros d'immatriculation enregistrés dans le traitement automatisé des données relatives aux véhicules volés ou signalés, les informations relatives au motif du signalement et à la conduite à tenir pour les véhicules placés sous surveillance sont également enregistrées.

Destinataires des informations

Les agents des services de police et de gendarmerie nationales ainsi que des douanes, individuellement désignés et dûment habilités par leur chef de service, peuvent accéder à la totalité ou à une partie des données, selon leurs attributions.

Les agents, individuellement désignés et dûment habilités par leur chef de service, des services de police et de gendarmerie nationales ayant fait procéder à une inscription dans le fichier des véhicules volés ou signalés ainsi que des douanes sont également destinataires des données. Il en va de même des agents, individuellement désignés et dûment habilités, des services de la direction générale de la police nationale et de la direction générale de la gendarmerie nationale énumérés à l'arrêté du 31 mars 2006, modifié par l'arrêté du 17 août 2006.

Modes d'alimentation du fichier

Le fichier est alimenté par les agents des services de police et de gendarmerie nationales.

Modes de consultation et traçabilité : Les administrateurs peuvent exporter du système LAPI un tableau de statistiques qui permet de réaliser un retour d'expérience sur l'utilisation du système et un journal des évènements qui enregistre tous les évènements au sein du système LAPI (informations relatives aux connexions au dispositif, informations relatives aux actions d'import des extractions du fichier des véhicules volés, informations relatives aux actions d'export de fiches LAPI)

Durée de conservation

Lorsqu'elles n'ont pas donné lieu à un rapprochement positif avec le traitement automatisé des données relatives aux véhicules volés ou signalés, les informations sont conservées pendant un délai maximum de huit jours au-delà duquel elles sont effacées. Pendant cette période de huit jours, la consultation des données n'ayant pas fait l'objet d'un rapprochement avec ce même traitement est interdit, sans préjudice des nécessités de leur consultation pour les besoins d'une procédure pénale ou douanière.

Lorsqu'elles ont donné lieu à un rapprochement positif avec le traitement automatisé des données relatives aux véhicules volés ou signalés, les données sont conservées pour une durée d'un mois à compter de la réalisation de ce rapprochement, sans préjudice des nécessités de leur conservation pour les besoins d'une procédure pénale.

Droit d'accès aux informations

Le droit d'accès et de rectification s'exerce de manière indirecte auprès de la Commission nationale de l'informatique et des libertés.

Le droit d'opposition ne s'applique pas.

Modalités d'apurement

Lorsqu'elles n'ont pas donné lieu à un rapprochement positif avec le traitement automatisé des données relatives aux véhicules volés ou signalés, les informations sont effacées dans un délai de huit jours.

Lorsqu'elles ont donné lieu à un rapprochement positif avec le traitement automatisé des données relatives aux véhicules volés ou signalés, les données sont conservées pour une durée d'un mois.

A l'issue des délais légaux (8 ou 31 jours), les données sont définitivement détruites par le système par inscription de zéros sur le disque.

Évolution fonctionnelle ou juridique

Cette expérimentation a été autorisée pour une durée de deux ans à compter de la publication de l'arrêté du 2 mars 2007. L'arrêté pérennisant ce traitement et le dossier CNIL sont en préparation au ministère de l'intérieur.

Modes d'archivage ou de destruction

Les données sont définitivement détruites par le système par inscription de zéros sur le disque après 8 ou 31 jours.

Nombre de fiches (si possible avec évolution depuis 5 ans)

Depuis le début de l'expérimentation du fichier, 2,8 millions de plaques d'immatriculation ont été lues et les dispositifs LAPI ont permis de retrouver 296 véhicules volés, de détecter 150 véhicules mis sous surveillance et d'interpeler 205 individus.

2.3. Les systèmes de traitement du renseignement judiciaire

a) Application judiciaire dédiée à la révélation des crimes et délits en série (AJDRCDS)

Texte réglementant le fichier

A.J.D.R.C.D.S. est en phase de conception. Sa mise en œuvre suppose la modification préalable de l'article 21-1 de la loi du 18 décembre 2003 modifiée et l'élaboration consécutive d'un décret pris après avis de la CNIL. Les éléments décrits ci-dessous dépendent totalement de la réalisation de ces conditions.

Service gestionnaire du fichier

Le service technique de recherches judiciaires et de documentation implanté à Rosny-sous-Bois pourrait assurer la gestion centralisée du traitement.

Présentation et finalité du fichier

AJDRCDS est un traitement informatique qui s'adosse à la démarche de rapprochement judiciaire habituellement utilisée dans la pratique professionnelle de l'enquêteur. Outil de gestion de la complexité, elle appuie le praticien dans la gestion d'une masse sans cesse croissante d'informations mises à sa disposition dans le cadre de l'enquête. Levier d'efficacité, elle représente un enjeu majeur pour les forces de sécurité et les magistrats qui dirigent la police judiciaire. Consacrée à la délinquance de masse, elle fonde une

rénovation de la méthode d'enquête, de nature à répondre à la forte attente des victimes d'une plus grande efficacité dans la lutte contre la délinquance de proximité qui demeure impunie dans huit cas sur dix.

La finalité d'AJDRCDS est donc de faciliter :

- la détection de crimes et délits de même nature imputable à un même auteur ou groupe d'auteurs ;
- la détection des infractions ou des comportements délinquantiels polymorphes réitérés par un même auteur ou groupe d'auteurs ;

La recherche est réalisée à partir de la sélection des faits constatés par la police et la gendarmerie nationales à partir de la base ARIANE (fusion de STIC et JUDEX), par leur enrichissement au moyen d'autres données contenues dans les procédures judiciaires et par celles issues de toutes les sources d'informations disponibles pour les enquêteurs (messagerie opérationnelle, fichiers, sources ouvertes).

Nature des informations enregistrées

Outil d'investigations et d'analyse criminelle à la disposition des magistrats et des enquêteurs, AJDRCDS enregistrera tout type de données ayant un rapport direct et non fortuit avec une affaire judiciaire. A ce titre, les données sensibles visées à l'article 8 de la loi 78-17 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés pourront être enregistrées dans AJDRCDS.

Présence de mineurs et si, oui, existe-t-il une limite d'âge ?

Toutes les personnes pouvant être en rapport avec une affaire judiciaire peuvent faire l'objet d'un enregistrement dans AJDRCDS notamment les auteurs et les victimes. A ce titre des personnes mineures pourront être enregistrées dans AJDRCDS.

Destinataires des informations

- Les personnels de la gendarmerie et de la police nationales exerçant dans une unité de recherches, habilités judiciairement, spécialement formées à l'utilisation de l'application et désignés par l'autorité hiérarchique pourront accéder directement aux données du traitement.
- Les magistrats ainsi que les officiers et agents de police judiciaire chargés des investigations afin de mener à bien les enquêtes et procédures d'information dont ils sont saisis.

Modes d'alimentation du fichier

La principale fonction d'AJDRCDS est d'élucider des faits constatés qui, analysés isolément et par défaut de matériel probatoire conséquent, ne peuvent aboutir à une élucidation. Les éléments descriptifs pertinents (lieux, moyens de transport, objets, personnes, signalements) recueillis sur chaque fait constaté font l'objet d'une indexation dans ARIANE au travers des procédures judiciaires ouvertes par la police et la gendarmerie nationales. La sélection des faits se prêtant à une approche sérielle est réalisée à partir du système ARIANE. Les données relatives à tous les faits constitutifs d'une série potentielle sont enregistrées dans AJDRCDS.

La plus-value d'AJDRCDS repose sur la collecte de nouvelles informations à partir :

- des procédures judiciaires relatives aux faits considérés ;
- de systèmes d'informations dont les forces de sécurité sont légitimement destinataires (fichiers déjà mis en œuvre par la police et la gendarmerie nationale) ;
- de systèmes d'informations détenus par d'autres administrations ou opérateurs privés (ces informations sont obtenues nécessairement sur réquisition judiciaire) ;
- de sources ouvertes au public.

Modes de consultation et traçabilité

Consultation protégée à deux niveaux :

- gestion des accès à l'application protégée par login et mot de passe : concerne uniquement les opérateurs spécialement formés ;
- accès à un dossier d'enquête réservé aux seules personnes concernés par le dossier et autorisé par l'opérateur ayant créé le dossier considéré.

La consultation de tout document par un utilisateur répondant aux deux conditions précitées est journalisée.

Durée de conservation

La durée de conservation des données pourrait être fonction de trois critères : délai de prescription de l'action publique, statut des personnes inscrites dans le système, toute décision de justice devenue définitive connue d'Ariane.

Droit d'accès aux informations

Par dérogation aux dispositions de l'article 41 de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et afin de ne pas contrevenir à la finalité du traitement (article 11 du code de procédure pénale) le droit d'accès aux informations contenues est réalisé directement auprès du magistrat référent du fichier.

Sauf décision contraire de ce magistrat, la réponse à la demande, proposée par la cellule d'administration centrale, ne fait aucune mention relative au statut de la personne lorsque celle-ci est effectivement présente dans le traitement.

La CNIL est destinataire du rapport d'activité annuel du traitement lequel précise le nombre de demande et la qualité des réponses effectuées sur une annuité.

Modalités d'apurement

L'apurement des données tient compte des durées de conservation différenciées. Elle est réalisée automatiquement par une règle de gestion.

Modes d'archivage ou de destruction

Aucun archivage des dossiers d'analyse n'est prévu autrement que dans le cadre de la procédure judiciaire transmise au magistrat du parquet compétent. Cette procédure contient obligatoirement un procès-verbal d'investigations et de recherches effectuées à partir du traitement.

b) Cellule Opérationnelle de Rapprochement et d'Analyse des Infractions Liées (CORAIL)

Réf : Le dossier de déclaration à la CNIL est en cours d'élaboration. Les éléments décrits ci-dessous dépendent totalement de la réalisation de ces conditions et ne préfigurent en rien du dispositif final.

Texte réglementant le fichier

Article 26 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Article D. 3 du code de procédure pénale

Service gestionnaire du fichier

Etat-major de la direction de la police judiciaire de la Préfecture de Police (DPJ de Paris).

Présentation et finalité du fichier

Mis en place en 2006 à la direction de la police judiciaire de la préfecture de police, CORAIL a pour objet principal la mutualisation des diffusions d'informations opérationnelles auprès des enquêteurs (télégrammes via le réseau de commandement (RESCOM), circulaires d'information et de recherche diffusées par la police judiciaire.).

CORAIL permet également de suivre et de traiter les gardes à vues au sein d'un service.

Une cellule CORAIL située auprès de chaque État major au sein des structures concernées effectue des synthèses d'affaires qui peuvent être éventuellement enrichies par d'autres informations (photographies des auteurs...).

Exemple d'affaire – « Le Violeur de Rochechouart » : Entre décembre 2005 et mai 2006, le Groupe des Atteintes Sexuelles de la Première Division de Police Judiciaire a répertorié six faits de viols et agressions sexuelles au préjudice de jeunes femmes susceptibles d'avoir été commis par le même individu. La majorité des faits se sont déroulés vers minuit, dans un même lieu, à l'encontre de jeunes femmes ayant le même aspect physique et selon le même mode opératoire (demande d'un renseignement, utilisation d'une bombe lacrymogène..). L'auteur a pu être interpellé en septembre 2007 grâce à l'utilisation de CORAIL.

Nature des informations enregistrées

Les informations enregistrées et diffusées sont :

- les données issues des télégrammes d'information diffusés par le RESCOM (signalement des faits commis ou élucidés) ;
- les données issues des mains courantes d'informations ;
- les données d'affaires ou de synthèse correspondant à un résumé des faits ou de la procédure (dates, lieux, nombre d'auteurs, résumé de l'affaire, référence, service saisi, etc.) ;
- des données photographiques (photographie de suspect, portrait-robot, photographie d'objet) ;
- les données de garde à vue (identité de la personne, nature de l'infraction, nom de l'OPJ, etc.).

Ces données se présentent sous forme de fiches se rapportant à des faits, sous formes d'états opérationnels regroupant des faits de même nature ou commis dans la même zone géographique, ou encore sous forme de synthèses opérationnelles rassemblant des faits présentant des similitudes de mode opératoire.

Présence de mineurs et si, oui, existe-t-il une limite d'âge ?

Le fichier peut contenir des informations sur les mineurs.

Destinataires des informations

Les OPJ et APJ spécialement habilités des services de police judiciaire situés dans le ressort des DRPJ de Paris et de Versailles.

Modes d'alimentation du fichier

Le fichier est alimenté à partir des messages opérationnels de compte rendu à la Salle d'Information et de Commandement de l'état-major de la DPJ de PARIS tels que prévus au chapitre « INFORMATION » de la Charte des Diffusions et de l'Information (circulaire PN/CAB/n°4534 du 23/11/1984).

Modes de consultation et traçabilité

Les fonctionnaires habilités ouvrent une session avec mot de passe. Des profils d'habilitation définissent pour chaque utilisateur les fonctions autorisées ou les catégories d'informations accessibles. Les données de connexion sont enregistrées dans un historique. Toutes les actions sur l'application sont tracées à la seconde.

- Date et heure de connexion.
- Identifiant de l'utilisateur.
- Référence des données du fichier auquel il a été accédé. (document, fiche, état, synthèse)
- Type de l'action effectuée. (Création, modification, mise à jour, lecture)

Durée de conservation

- Les fiches et les états opérationnels sont conservés pour une durée maximum de trois ans à compter des faits. Pour les synthèses, les données sont conservées trois ans à compter de la date du fait le plus récent.
- Les synthèses élucidées concernant des faits, crimes ou délits « imputés aux personnes mises en cause dans des affaires similaires » (récidivistes) sont conservées jusqu'au terme de la période incluant la possibilité d'une « récidive légale » de l'auteur condamné.
- Les circulaires régionales de recherche pour identification sont conservées cinq ans.

Droit d'accès aux informations

Le droit d'accès est ouvert aux personnes physiques et morales par l'intermédiaire de la CNIL. Dès réception d'une demande de droit d'accès, l'application permet d'imprimer une copie de l'ensemble des données concernant le requérant et lui seul. Si la recherche nominative est négative, l'application permet l'impression immédiate d'une lettre type, référencée qui précisera les dates, heures, étendues et domaines de la recherche.

Évolution fonctionnelle ou juridique

CORAIL, actuellement en phase d'expérimentation au sein des DRPJ de Paris et de Versailles, sera généralisé en 2009 à l'ensemble de services territoriaux d'investigations de police judiciaire et de sécurité publique. Le dossier de déclaration du traitement à la CNIL est actuellement en cours d'élaboration.

Nombre de fiches

Le nombre annuel de fiches se limite à environ 4500 pour la DPJ de Paris (faits sériels graves), variable en fonction de l'évolution du volume des infractions. Le nombre de synthèses annuelles varie entre 50 et 60. Le nombre de circulaires régionales de recherche pour identification est estimé entre 150 et 300.

Nombre de consultations par an

Le nombre de connexions pour 3000 fonctionnaires habilités est estimé à 0,4 par jour travaillé, soit 240 000 pour 2008.

2.4. Les fichiers d'antécédents judiciaires

a) ARI@NE

Présentation et finalité

Début 2005, la gendarmerie et la police nationales, confrontées à la nécessité de moderniser leurs systèmes respectifs JUDEX et STIC, se sont associées pour réaliser un nouveau fichier commun de recherches et de rapprochements criminels : ARIANE (Application de rapprochements, d'identification et d'analyse pour les enquêteurs).

Cette coopération opérationnelle et technique s'inscrit dans le sens de la loi d'orientation et de programmation pour la sécurité intérieure d'août 2002 (LOPSI) qui prescrit en effet le rapprochement des grands fichiers informatisés des deux forces. Ce rapprochement, qui n'avait pas encore pu se concrétiser du fait des difficultés d'harmonisation des architectures techniques des systèmes d'information et de communication des deux forces, va donc connaître une première réalisation.

Outre les avantages attendus en termes de rationalisation des moyens techniques et financiers nécessaires à sa réalisation, le nouveau système permettra l'accès pour tout gendarme ou policier à l'ensemble des informations relatives aux enquêtes judiciaires quel que soit le service ou l'unité à l'origine de leur enregistrement. Cette avancée permettra une plus grande efficacité dans le cadre des enquêtes impliquant des malfaiteurs récidivistes d'autant plus que les fonctionnalités de rapprochements et d'analyse seront optimisées et largement ouvertes jusqu'à l'échelon de l'unité élémentaire.

La mise en œuvre opérationnelle devrait intervenir au second semestre 2009.

Nature des informations contenues

Les informations contenues dans ARIANE respecteront les mêmes règles que les applications STIC et JUDEX actuelles (cf. fiches JUDEX). Deux nouvelles catégories de données seront intégrées au système : les morts suspectes et les disparitions inquiétantes (articles 74 et 74-1 CPP).

Destinataires des informations

Les règles actuelles valables pour les applications STIC et JUDEX seront appliquées pour ARIANE et ouvertes, sous certaines conditions aux services de la Douane judiciaire. À noter notamment qu'il est prévu d'organiser l'accès direct effectif, déjà prévu par le législateur, au profit des parquets au titre du contrôle de la régularité du fichier. Sous certaines conditions extrêmement restrictives, certaines données pourront être communiquées aux services préfectoraux (enquêtes administratives en application du décret n° 2005-1124 du 6 septembre 2005).

Modes d'alimentation, de consultation et d'apurement

Alimentation

L'application sera alimentée par l'application ARDOISE en cours de réalisation pour la police nationale, et par l'application IC@RE pour la gendarmerie nationale. Les modalités précises sont en cours de spécifications détaillées.

Consultation

L'application sera consultée par un mode unique intranet pour l'ensemble des postes fixes de la police et de la gendarmerie. Les droits seront vérifiés et contrôlés individuellement par les gérants d'habilitation respectifs de la police et de la gendarmerie nationales. La consultation via les postes mobiles sera limitée en fonctionnalité aux anciennes interrogations de type IA-RA de JUDEX.

Modes d'apurement

Les règles d'apurement seront fixées par décret sur la base des règles actuelles valables pour les applications STIC et JUDEX. L'application comportera dès sa construction les modules techniques pour réaliser les apurements de façon automatique.

Situation juridique actuelle

L'intégration de données relatives aux morts suspectes et disparitions inquiétantes ne peut se faire à droit constant. Elles font actuellement l'objet de l'article 9 du projet de LOPPSI II.

La déclaration de l'application à la CNIL est en cours d'élaboration. L'application sera créée par décret en Conseil d'État après avis de la CNIL. Son champ intégrera ou non les deux thématiques susvisées en fonction de l'avancée des réformes portées par la LOPPSI II.

2.5. Les fichiers de renseignement

a) ATHEN@

Présentation et finalité

Le projet Athen@ permettra à partir de 2009 d'engager la rénovation des centres opérationnels, en dotant les groupements de gendarmerie de métropole et d'outre-mer, les régions de gendarmerie ainsi que la direction générale de la gendarmerie nationale d'une salle de commandement opérationnelle tout en améliorant la collaboration avec les salles de commandement des autres services de l'état. Elle permettra également la mise en place d'un outil performant de recueil et de traitement du renseignement d'ordre public et de défense.

Un projet de déclaration à la CNIL a été transmis à la DAJ pour étude préliminaire en avril 2008.

Nature des informations contenues

Le système Athen@ est principalement dédié aux unités opérationnelles de la gendarmerie, avec des fonctionnalités adaptées à leurs besoins. Des fonctionnalités plus avancées sont offertes aux personnels de la gendarmerie affectés dans les centres d'opérations et de renseignement aux niveaux départemental, régional et national.

La mise en œuvre de ce système poursuit trois finalités :

- améliorer l'accueil du public et la relation à l'usager ;
- aider et sécuriser les interventions dans le double intérêt des personnels de la Gendarmerie et des usagers ;
- optimiser le traitement du renseignement d'ordre public et de défense.

Organisation du système

Le système d'information Athén@ est composé de quatre modules : OPS, RENS, FAR et EVT qui sont en liaison avec une plate-forme cartographique permettant de géolocaliser les données et les moyens d'intervention.

Module RENS

Le système Athén@ comprendra tous les documents structurés, tels que les documents bureautiques (fiches de renseignement, synthèses, documents d'analyse, ...), des fichiers multimédias (images, séquences, vidéo,...) et des documents à partir de sites Internet externes ou de guichets spécialisés (AFP).

Il est également destiné à contenir des fiches descriptives alimentant le réseau de connaissances (événements, personnes, organisations, de moyens ou sites).

Module FAR

Il est destiné à contenir des fiches alphabétiques de renseignements sur les personnes inscrites d'autorité car présentant un risque pour la sécurité des interventions et de la population (personnes violentes, détenteurs d'armes, de chiens dangereux, etc.) et les personnes sollicitant ou nécessitant des mesures de sécurité particulières (personnes âgées, tranquillité vacances, victimes infractions pénales, résidences secondaires...) La volumétrie sera limitée à 5 millions de fiches.

Module EVT

Il permettra de stocker les données structurées traitant d'événements d'ordre public d'ampleurs nationale, régionale ou départementale (les formulaires EVT ne comportent pas de données nominatives).

Module OPS

Il permettra de stocker toutes les données structurées opérationnelles (données issues des fiches de prise en compte (FPC), journaux de conduite d'opération (JCO) produits par les centres opérationnels et les brigades, ainsi que les données nominatives à des fins d'annuaire.

Le principe d'une stricte séparation des renseignements judiciaires et administratifs sera observé. Ainsi, les informations de type judiciaire seront intégrées dans le système Ariane tandis que les renseignements administratifs et d'ordre public seront accessibles par le système d'information Athén@.

Les catégories de données à caractère personnel enregistrées dans le traitement concernant des personnes physiques sont les suivantes :

- informations ayant trait à l'état civil ;
- adresses physiques, numéros de téléphone et adresses électroniques ;
- informations ayant trait à la profession ;
- caractéristiques et immatriculation des véhicules ;
- données relatives à l'environnement de l'individu si elles sont nécessaires à la poursuite des finalités ;
- motif de l'enregistrement des données.

Le traitement peut enregistrer des données à caractère personnel dans la limite des dispositions de l'article 8 de la loi du 6 août 2004 concernant toutes personnes physiques. Il est toutefois interdit de sélectionner une catégorie particulière de personnes à partir de ces seules informations.

Modes d'alimentation, de consultation et d'apurement

Seuls les personnels habilités de la gendarmerie auront accès aux informations contenues dans les bases. La consultation pourra se faire par intranet.

L'alimentation des bases liées au traitement des appels téléphoniques, de l'accueil du public et de la gestion des interventions ainsi que celle relative aux procédures de collecte d'informations se fera par des interfaces de saisies spécifiques : la fiche renseignement, la fiche entité, le compte-rendu opérationnel, les sources externes formelles.

Toutes les données hébergées et manipulées au sein du système présentent un intérêt avéré pour la gendarmerie dans le cadre de l'ordre public et de la sécurité publique mais aussi pour mieux connaître son environnement de travail et la population dont elle a la charge.

Une partie des données collectées dans Athen@ sont des données à caractère personnel qui sont recueillies de différentes manières :

– par les appels téléphoniques reçus par les centres opérationnels et de renseignement des groupements de gendarmerie départementale (CORG) et les unités territoriales ; pour chaque appel reçu, l'opérateur remplit une « fiche de prise en compte » ;

– par les renseignements recueillis par les militaires de la gendarmerie à l'occasion de leur service transmis au CORG sous forme de fiche de renseignement ou de compte-rendu opérationnel en fin d'intervention (intégré au JCO). Ces documents sont exploités au besoin au niveau du CORG dans le réseau de connaissances sous forme de documents « fiches entité » ; il existe cinq catégories de « fiches entité » : les « fiches personnes », les « fiches sites », les « fiches organisations », les « fiches moyens » et les « fiches évènements » ;

– certaines données présentant un intérêt opérationnel du fichier alphabétique de renseignement (FAR)18 des brigades territoriales sont reprises dans Athén@ sous la forme de documents appelés « fiches FAR » ; les nouvelles données présentant un intérêt opérationnel seront directement saisies dans les « fiches FAR » du système Athén@.

– enfin, des documents provenant de sources externes (Internet, presse, AFP...) sont intégrés à la base.

Modalités d'apurement

L'apurement des données sera automatisé dans les conditions suivantes :

– Fiches FAR : 3 ans si pas d'indicateur LAT. 15 ans si indicateur LAT

– FPC : 2 ans

– JCO : 2 ans

– Fiches entités (personnes, sites, organisations, moyens, événements) : 15 ans

Droit d'accès

Toute personne ayant sollicité ou nécessitant des mesures particulières de sécurité et désirant accéder aux données à caractère personnel qui la concernent directement peut en faire la demande auprès de la brigade territoriale compétente sur son lieu de résidence (principale ou secondaire) qui communiquera sans délai à l'intéressée les données à caractère personnel la concernant.

Pour les personnes inscrites d'autorité, le droit d'accès aux données s'exercera, conformément à l'article 41 de la loi du 6 août 2004, auprès de la Commission nationale de l'informatique et des libertés (CNIL).

Cette application, en raison de sa configuration future, a vocation à remplacer le fichier alphabétique de renseignements (FAR) ainsi que la base de gestion des évènements ARAMIS.

18 Le Fichier Alphabétique de Renseignement (FAR) des brigades territoriales dans sa version manuelle sera détruit avant le 24 octobre 2010

CHAPITRE 2 - SUITES RESERVEES AUX RECOMMANDATIONS DU RAPPORT 2006

En 2006, sur demande du ministre d'Etat, ministre de l'Intérieur et de l'aménagement du territoire, et suite à la mise en place d'un groupe de travail sur l'amélioration du contrôle des fichiers de police et de gendarmerie utilisés dans le cadre des enquêtes administratives, un certain nombre de recommandations avaient été effectuées en vue de renforcer les garanties individuelles.

En effet, l'article 17-1 de la loi 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité (LOPS), introduit dans l'ordre juridique par l'article 28 de la loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, a autorisé la consultation des fichiers, dits d'antécédents judiciaires, dans le cadre d'enquêtes administratives (STIC et JUDEX).

L'article 25 de la loi n°2003-239 du 18 mars 2003 relative à la sécurité intérieure a modifié cet article en élargissant les cas dans lesquels il peut être procédé à la consultation de ces fichiers de police judiciaire à des fins d'enquêtes administratives. La liste des professions pour lesquelles la consultation de traitements automatisés de données à caractère personnel est autorisée a été fixée par le décret n°2005-1124 du 6 septembre 2005[19].

Ces traitements concernent les fichiers de police judiciaire dits d'antécédents (STIC pour la police nationale, JUDEX pour la gendarmerie nationale) par opposition aux fichiers de police judiciaire dits d'identification que sont, notamment, le FNAEG et le FAED qui ne peuvent en aucun cas être utilisés à des fins de police administrative.

Ainsi, aux termes de cet article, la consultation des fichiers de police judiciaire, dits d'antécédents, est possible, dans le cadre d'enquêtes préalables aux décisions administratives de recrutement, d'affectation, d'autorisation, d'agrément, ou d'habilitation concernant les emplois publics participant à l'exercice des missions de souveraineté de l'Etat, les emplois publics ou privés relevant du domaine de la sécurité et de la défense, ou les emplois privés ou activités privées réglementées relevant des domaines des jeux, paris et courses.

En 2006, malgré le contrôle de la CNIL, les diverses modifications législatives intervenues en vue d'améliorer l'encadrement de ces fichiers et les opérations d'apurement importantes réalisées par les services de police et de gendarmerie, il est apparu que l'utilisation de ces fichiers dans le cadre administratif pouvait entraîner certains dysfonctionnements susceptibles de porter atteinte aux libertés individuelles et collectives notamment sur les questions liées à la mise à jour des informations.

C'est en vue de remédier à ces risques que, par lettre de mission du 15 juin 2006, le ministre d'Etat, ministre de l'Intérieur et de l'Aménagement du territoire, a décidé la création d'un groupe de travail visant « *à l'amélioration du contrôle et de l'organisation des fichiers de police et de gendarmerie afin d'éviter le maintien d'informations erronées ou dépassées.* ».

Les différentes recommandations du groupe de travail de 2006 ont donc d'abord eu pour objet de renforcer les garanties individuelles en s'assurant que des informations non actualisées, inexactes ou dont la date de validité de conservation a expirée soient écartées des fichiers et ne risquent plus ainsi de nuire à l'employabilité des personnes.

Elles visaient également à rappeler que les décisions préfectorales, prises après consultation du STIC ou du fichier JUDEX, devaient faire l'objet d'une véritable instruction, prenant en compte la gravité, la répétition et l'ancienneté des faits.

Enfin, plusieurs recommandations concernaient l'amélioration du droit d'accès aux données et le développement des voies de recours et portaient sur des fichiers spécifiques.

Il est ici proposé de faire un état des lieux des suites réservées aux différentes recommandations du groupe de travail de 2006 qui avaient alors fait l'objet d'un consensus et d'une acceptation par le ministère de l'Intérieur.

1. Améliorer la communication publique

Le groupe de travail recommande que, dans le cadre de la communication publique sur les fichiers de police judiciaire, soient précisées non seulement les données détaillées relatives au droit d'accès indirect, qui résultent des contrôles de la CNIL, mais les statistiques qui concernent l'ensemble du fichier concerné,

[19] Voir annexe n°1.

faisant état notamment du nombre de personnes signalées en tant que mises en cause ou comme victimes, du nombre d'apurements et de mises à jour réalisés, du nombre de consultations à fin d'enquête administrative, etc., afin que le « taux de rectification suite à D.A.I. » ne soit pas transformé en « indicateur de qualité des fichiers ».

Concernant les statistiques relatives au droit d'accès indirect, un canevas commun a été établi en collaboration avec la CNIL. Ce canevas, rempli lors de la présentation des dossiers aux magistrats de cette commission, est en cours d'expérimentation depuis le 1er janvier 2008. Il reste à stabiliser définitivement ces statistiques, la méthode de calcul et l'unité de compte principale, et ce avant l'établissement du rapport annuel d'activité.

2. Rendre publique, chaque année, une information sur la consultation des fichiers de police et de gendarmerie à des fins administratives

Le groupe de travail recommande que le rapport du ministre de l'intérieur transmis chaque année à la CNIL aux termes de l'article 10 relatif au STIC porte à la fois sur son utilisation à des fins de police judiciaire et sur sa consultation à des fins administratives. Il recommande qu'il en soit de même pour le JUDEX et, dans un proche avenir, pour Ariane. Il recommande également qu'une information relative à ces consultations administratives soit rendue publique chaque année. Cette dernière ferait utilement l'objet d'une annexe au rapport précité adressé à la CNIL.

Conformément aux recommandations du groupe de travail, le rapport annuel 2007 relatif au fonctionnement du STIC destiné à la CNIL fait apparaître le nombre de personnes habilitées et le nombre de consultations en police administrative. Une information sur le site internet du ministère de l'intérieur est également à l'étude.

3. Créer un rendez-vous annuel technique

Le groupe de travail recommande qu'un rendez-vous judiciaire annuel permette à tous les parquets la transmission des informations qui ne l'auraient pas été « au fil de l'eau » et qu'un groupe commun se réunisse afin de contrôler l'application de ce dispositif et en rende compte aux ministres concernés. Ce groupe pourrait être composé soit du ministère de la justice, des directions générales de la police et de la gendarmerie nationales et de la CNIL, soit des mêmes acteurs que précédemment auxquels viendraient s'ajouter la HALDE, la CNDS et le Médiateur de la République.

Cette recommandation n'a pas encore fait l'objet de suite. La DGPN tient toutefois à rappeler que cette nécessité de mise à jour systématique des fichiers dits « d'antécédents » est une préoccupation prise en compte dans le cadre des travaux de modernisation des fichiers et notamment celui du chantier ARIANE, dont la compatibilité technique avec le fichier CASSIOPEE du ministère de la justice permettra des échanges automatisés de données. Des réunions de travail interministérielles ont régulièrement eu lieu entre les différents ministères concernés pour développer ces échanges interapplicatifs (cf. suites données à la recommandation n°4).

4. Mettre en place un groupe de travail police-justice-gendarmerie

Le groupe de travail recommande également que les étapes en cours de conception et de développement des systèmes d'information de police judiciaire (ARIANE) et du ministère de la justice (CASSIOPEE) soient mises à profit pour préparer la mise à jour automatisée des fichiers d'antécédents judiciaires. Un groupe technique justice-police-gendarmerie devrait étudier rapidement les conditions techniques et juridiques de l'interconnexion entre ces deux traitements afin de permettre l'envoi automatisé depuis l'application CASSIOPEE vers l'application ARIANE des suites judiciaires favorables, ce qui réglerait à terme une grande partie des dysfonctionnements constatés. En l'attente de la mise en œuvre de liens informatiques sécurisés entre l'application ARIANE et l'application CASSIOPEE, le groupe de travail recommande d'améliorer la transmission par les parquets des suites judiciaires, notamment les classements sans suite pour insuffisance de charges, donnant lieu à la mise à jour des fichiers STIC et JUDEX. Le groupe de travail propose, à titre transitoire dans l'attente de la mise en réseau de nouveaux dispositifs informatiques, que soit étudiée la possibilité que les officiers et agents de police judiciaire recevant, de la part des Parquets, dans le cadre du traitement en temps réel des instructions de classement sans suite pour insuffisance de charges, tirent effectivement et directement les conséquences de mise à jour des fichiers considérés, sans envoi par les parquets de la fiche navette afférant à la procédure. Il propose de limiter, pour ces mêmes décisions, l'envoi des fiches navettes par les bureaux d'ordre des parquets pour les seules procédures qui n'auraient pas été traitées dans le cadre du traitement en temps réel.

Un groupe de travail technique ARIANE-CASSIOPEE est effectivement constitué dans le cadre général des échanges de données contenues dans les procédures pénales entre les services d'enquêtes et les tribunaux (afin notamment d'assurer le continuum statistique) et dans le cadre plus particulier de la préparation de la mise à jour automatisée des fichiers de police judiciaire depuis CASSIOPEE vers ARIANE. Il se réunit régulièrement depuis juillet 2006, mais le calendrier des développements informatiques, de part et d'autre, ne permettra pas un début de réalisation concrète avant 2009-2010, du fait du calendrier de généralisation d'ARIANE d'une part, et de CASSIOPEE dans les juridictions de province d'autre part (selon les dernières informations communiquées dans le cadre du groupe de travail).

La proposition du ministère de la justice visant à ce que les officiers et agents de police judiciaire, qui peuvent recevoir directement dans le cadre du TJTR des instructions des parquets de nature à motiver une mise à jour des fichiers, fassent procéder à la mise à jour des fichiers sans envoi des fiches navettes correspondantes par les parquets, a suscité des réserves du ministère de l'Intérieur. C'est la raison pour laquelle elle n'a pas connu de suite. Aussi la circulaire du ministre de la justice du 26 décembre 2006 (faisant suite au décret du 14 octobre 2006 modifiant le décret du 5 juillet 2001 portant création du STIC) a-t-elle maintenu le dispositif de mise à jour par fiches-navettes : « Les suites judiciaires doivent être transmises au SRDC par le procureur de la République territorialement compétent au moyen de la fiche dite "navette" qu'il aura préalablement complétée. Généré tant par le logiciel de rédaction des procédures (LRP) que par ARDOISE-Rédaction de procédures lors de l'édition du compte-rendu d'enquête après identification (CREI), ce document est joint par les enquêteurs à la procédure judiciaire qui est transmise au magistrat, et concerne chacune des personnes mises en cause dans ladite procédure. »

Néanmoins, à Paris et en petite couronne, la mise en place de la nouvelle chaîne pénale (NCP), a permis d'automatiser la transmission des suites judiciaires vers le gestionnaire territorial.

La mise en œuvre concomitante de CASSIOPEE et d'ARIANE (2009-2010), qui instaurera une transmission informatique directe des données contenues dans les procédures pénales depuis le service d'enquête vers le bureau d'ordre du tribunal de grande instance, les suites judiciaires étant quant à elles transmises en retour par la même voie, assurera une réelle mise à jour systématique des fichiers d'antécédents judiciaires telle que préconisé par le groupe de travail dans ses recommandations.

Dans l'attente de cette automatisation, la direction des affaires criminelles et des grâces a réuni un groupe de travail pour permettre l'édition automatique par la «Nouvelle Chaîne Pénale », de la fiche-navette destinée aux services gestionnaires des fichiers d'antécédents. Cette solution technique, qui a permis une amélioration sensible de la mise à jour de ces traitements en région parisienne, zone où est traité 30% du contentieux pénal, n'a pas pu être mise en œuvre dans les juridictions de province en raison de l'insuffisante capacité des applications qui y sont utilisées.

Enfin, dans le souci d'améliorer plus encore le dispositif de mise à jour des fichiers d'antécédents judiciaires, et de pallier l'insuffisance des effectifs que les parquets peuvent y consacrer, le ministère de la Justice a obtenu du ministère de l'Intérieur, porteur de la LOPPSI (projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure) de confier cette tâche au futur magistrat dédié au contrôle des fichiers de police judiciaire, dont ce projet de loi porte création : L'instauration d'un magistrat dédié au contrôle des fichiers de police judiciaire de rapprochement était proposée par le ministère de l'Intérieur;

La chancellerie a demandé, et obtenu, que le dispositif prévu :

- soit étendu aux fichiers d'antécédents judiciaires: STIC, JUDEX et futur ARIANE ;
- comporte l'instauration effective d'un droit d'accès direct du magistrat aux fichiers dont il assure le contrôle, par l'installation d'un terminal dédié.

Le déploiement de CASSIOPEE en Ile-de-France et DOM-TOM (dernières juridictions à être pourvues) est prévu pour courant 2010. Le déploiement d'ARIANE est prévu sur le premier semestre 2010. Les échanges inter-applicatifs ne sont donc pas raisonnablement envisageables avant fin 2010.

5. Enrichir l'information à la disposition du préfet pour lui permettre de mieux fonder ses décisions et d'éviter des erreurs d'appréciation liées à un dossier parcellaire.

Le groupe de travail recommande qu'il soit étudié la possibilité pour le préfet de s'informer auprès du parquet à l'occasion d'une enquête administrative de certaines suites judiciaires. Il s'agirait de cas portant sur des faits établis, donc accessibles dans le module de consultation administrative des fichiers, dès lors que

la nature des faits apparaît incompatible aux exigences de moralité nécessaires à l'exercice des activités par la demande d'agrément, d'habilitation ou d'autorisation. Parmi ces cas pourraient figurer les décisions telles que le classement sans suite en opportunité, le rappel à la loi et la composition pénale, qui ne font pas l'objet, aujourd'hui, d'une mention au STIC ou au JUDEX. Une telle consultation ne pourrait revêtir de caractère systématique et devrait être appréciée in concreto.

Cette recommandation, qui relève de la compétence de la DGPN, de la DGGN, de la DLPAJ et du ministère de la justice, est toujours à l'étude.

Pour la DGGN, la mention de suites judiciaires dans les applications STIC et JUDEX, hors celles prévues aux décrets portant création de ces applications, ne peut être réalisée à droit constant. La question sera posée au moment de la présentation du projet de décret ARIANE devant le Conseil d'Etat.

Des procédures expérimentales ont été mises en place sur le ressort de la cour d'appel de Paris aux fins de renseigner l'autorité administrative au cas par cas, soit par courrier, soit par le biais d'un document standard d'information, soit au moyen d'un formulaire-navette reliant le parquet à la préfecture de police.

6. Réfléchir aux modalités de prise en compte des contraventions de 5ème classe

Le groupe de travail recommande qu'une réflexion de fond puisse être engagée sur les modalités de prise en compte des contraventions de 5ème classe dans le cadre des enquêtes administratives.

Cette réflexion n'a pas encore été entamée. La question pourra éventuellement être évoquée lors des discussions avec la CNIL et le Conseil d'Etat à l'occasion de la procédure de déclaration d'ARIANE. D'ici là, la DGPN se propose d'établir une liste des contraventions de 5^{e} classe susceptibles d'être occultées dans le STIC lors de la consultation en police administrative.

7. Diffuser une nouvelle circulaire du ministère de la Justice

Le groupe de travail recommande que les conditions de mise à jour du STIC et du JUDEX soient rappelées par circulaire du ministère de la Justice. Une telle circulaire, commune aux deux traitements, aura pour but de préciser leur régime et d'insister fermement sur la nécessaire transmission des suites judiciaires des parquets compétents vers les gestionnaires chargés du traitement et, partant, de la mise à jour de ces fichiers.

Dans une circulaire du 26 décembre 2006, puis dans une dépêche-circulaire du 31 mai 2007, la direction des affaires criminelles et des grâces a rappelé à l'ensemble des parquets généraux les règles relatives à la mise à jour des fichiers d'antécédents judiciaires et souligné la priorité qui devait y être accordée. La chancellerie demande systématiquement aux parquets généraux et aux parquets de rendre compte de leur action dans ce domaine dans leur rapport annuel de politique pénale. Le ministère de la Justice, comme les juridictions, exercent également un contrôle sur la mise à jour des fichiers d'antécédents par le traitement des requêtes de particuliers.

8. Mieux informer les victimes des garanties légales et réglementaires protectrices prévues à leur égard

Le groupe de travail recommande que l'information des victimes soit pleinement assurée sur l'usage qui peut être fait des données personnelles les concernant, et plus généralement sur leurs droits. Comme le prévoit la loi, ces données ne sont pas accessibles dans le cadre des enquêtes administratives et ne sont donc jamais prises en compte à l'occasion d'une décision administrative. En outre, bien que la loi informatique et libertés ne l'exige pas, le Gouvernement a récemment décidé de mettre en place une information des victimes sur la procédure de droit d'accès aux données les concernant lors du dépôt de plainte, comme la CNIL y est très attachée. Cette information rappellera également le droit d'opposition des victimes à voir les données les concernant supprimées dès lors que l'auteur des faits a été définitivement condamné.

Un droit à l'information des victimes qui font l'objet d'une inscription au STIC a été introduit par le décret de 2006. Cette information, claire et complète, doit permettre aux victimes d'être effectivement prévenues que des données à caractère personnel les concernant vont être collectées et enregistrées dans le cadre de la procédure judiciaire et qu'elles disposent d'un droit d'accès et de rectification à ces données ainsi que, sous certaines conditions, d'un droit d'opposition à leur maintien.

Ce droit à l'information a été mis en œuvre par affichage (modification de la charte d'accueil du public et d'assistance aux victimes, article 8), complété par une notice explicative et détaillée, document précisant l'étendue de ce droit et ses modalités d'exercice (mise à disposition de modèles de courrier à l'attention de la CNIL, du procureur de la République ou du service régional gestionnaire de la documentation).

9. Archiver et numériser les procédures judiciaires pour éviter le risque de décisions erronées ou insuffisamment argumentées

Le groupe de travail suggère que, dans le cadre de la mise en place du système ANADOC, les procédures judiciaires puissent être conservées de manière numérisée selon des règles de consultation et de durées fixées après avis de la CNIL.

Pour la Police Nationale, cette recommandation a été prise en compte dans le cadre du projet ANADOC, bien que celui-ci ne soit pas encore au stade des spécifications techniques.

Dans l'intervalle, une fonction dite "historique" sera disponible dans la version définitive d'ARDOISE (logiciel de rédaction de procédures doublé d'un vecteur d'alimentation des principaux fichiers de police du nouveau système d'information destiné à l'investigation) et permettra de conserver localement une image numérique des procédures transmises aux autorités judiciaires, notamment accessible à partir du niveau régional (SRDC).

Cette fonctionnalité constituera le socle des travaux de dématérialisation des procédures (échanges entre la police nationale et la justice ; archivage numérique des procédures en attendant ANADOC).

Pour la Gendarmerie Nationale, des réflexions sont actuellement en cours pour l'archivage des procédures rédigées via Ic@re et pour l'adoption d'un outil de gestion électronique de document (GED) permettant de faire face aux enjeux à venir en matière de dématérialisation des procédures.

10. Mieux informer les personnes sur les voies de recours existantes

Le groupe de travail propose que, lorsque les personnes se voient notifier une décision défavorable après une enquête administrative ayant donné lieu à la consultation des traitements automatisés de données personnelles, cette information soit assortie d'une mention sur les voies de recours administratives prévues pour l'effacement ou pour la rectification des mentions inscrites au sein des fichiers de police judiciaires (recours en rectification ou en effacement des données devant le procureur de la République territorialement compétent, recours indirect par l'intermédiaire de la CNIL 29). Il recommande d'élargir cette obligation d'information à l'ensemble des cas visés à l'article 17-1 de la loi du 21 janvier 1995 modifiée (instruction des demandes d'acquisition de la nationalité française, de délivrance et de renouvellement des titres de séjour, nomination et promotion dans les ordres nationaux). L'insertion d'une telle disposition risque cependant de multiplier des demandes de droit d'accès indirect, au risque d'alourdir encore la charge de travail de la CNIL et des services instructeurs, déjà considérable. Paradoxalement, il pourrait être préjudiciable au droit des personnes ayant bénéficié d'une suite judiciaire favorable justifiant une mise à jour des fichiers de voir l'examen de leur demande retardé par la multiplication de recours ayant peu de chances d'aboutir en raison du cadre légal. C'est pourquoi le groupe de travail suggère que la mention qui devrait être insérée dans ces courriers soit suffisamment précise quant au champ des suites judiciaires donnant lieu à effacement ou rectification. Les autorités administratives indépendantes pourraient également en tenir compte dans l'information dispensée aux requérants.

La DGPN rappelle systématiquement dans les courriers de réponse aux intéressés qui demandent un droit d'accès aux fichiers les voies de recours existantes dès lors que le courrier de la personne fait apparaître un problème lié à une enquête administrative.

11. Réfléchir à la création d'une voie de recours contre les décisions du parquet en matière de conservation ou d'effacement des décisions

Le refus d'effacement par le procureur de la République constituant une décision faisant grief à l'intéressé, le groupe de travail s'est interrogé sur la compatibilité de notre législation avec les exigences du droit européen et sur la nécessité d'instaurer une voie de recours à l'encontre des mesures de mise à jour des données, décidées par le procureur de la République. En l'état actuel de notre législation, le droit positif français pourrait être soumis à la censure de la Cour européenne des droits de l'homme car les contestations des décisions du procureur de la République sont actuellement dépourvues de recours.

Cette recommandation n'a pas fait l'objet de suite.

En effet, la chancellerie a estimé que le contrôle du procureur de la République, opéré à l'occasion de l'exercice du droit d'accès indirect, quelles qu'en soient ses modalités, a pour objet de déterminer si les mentions figurant dans les fichiers STIC et JUDEX, si elles existent, répondent lors de la demande aux conditions légales pouvant conduire à leur effacement ou à leur rectification.

Pour autant, en application de la loi du 6 janvier 1978, il appartient au seul responsable du traitement en application de la loi du 6 janvier 1978 précitée de prendre ou non la décision d'effacement ou de rectification dans le cadre du droit d'accès indirect.

Il s'ensuit que, si les conclusions du magistrat sur le mérite de certaines données à être rectifiées ou effacées sont adressées au responsable du traitement, celui-ci demeure la seule autorité compétente à l'exclusion de toute autre, pour prendre ou non la décision d'effacement ou de rectification et la notifier au requérant.

Certes, le procureur de la République peut porter ses conclusions à la connaissance du requérant à titre de simple mesure d'information, afin d'attester de l'effectivité de son contrôle sur les mentions enregistrées au STIC. Pour autant, cette information, matérialisée par le courrier du procureur de la République, ne faisant pas grief au demandeur, elle est insusceptible de recours quelle qu'en soit sa nature.

12. Permettre au tribunal de prononcer une dispense d'inscription dans la partie consultation administrative des fichiers STIC et JUDEX, des faits ayant donné lieu à condamnation

Le Médiateur de la République aurait souhaité, à l'instar de la possibilité offerte en matière de dispense d'inscription au bulletin n°2 du casier judiciaire (article 775-1 du code de procédure pénale), que soit introduit un droit d'omission dans la partie administrative des fichiers STIC et JUDEX pour les infractions les moins graves (notamment certaines contraventions de 5ème classe, cf. proposition n°6).

Cette proposition a fait l'objet de longues discussions et n'a pas été retenue par le groupe de travail. Le Médiateur de la République a pris acte de la position débattue au sein du groupe de travail.

13. Diffuser une nouvelle circulaire du ministère de l'Intérieur sur la nécessité de ne pas se fonder exclusivement sur la consultation des fichiers de police judiciaire pour les enquêtes administratives

Le groupe de travail recommande que le ministère de l'intérieur rappelle par voie de circulaire à ses agents qu'une décision défavorable ne peut être prise au vu de la seule mention d'une personne dans les fichiers STIC ou JUDEX, mais que l'enquête administrative doit être circonstanciée.

Il convient également que cette circulaire rappelle qu'en cas de consultation du fichier pour une finalité administrative, un affichage systématique sur écran apparaîtra pour rappeler ces dispositions.

Après la parution du décret du 14 octobre 2006 modifiant celui du 5 juillet 2001 portant création du STIC, une nouvelle circulaire d'application du STIC en date du 9 mai 2007 a été adressée par la Direction générale de la police nationale aux services de police.

Dans sa partie consacrée aux enquêtes administratives, cette circulaire revient avec précision sur les conditions d'utilisation du STIC en police administrative et sur les vérifications au dossier de procédure qui doivent être faites en cas de consultation positive, afin d'apporter à l'autorité administrative l'éclairage nécessaire au plein exercice de son pouvoir d'appréciation.

La circulaire INT/D/0800032C du 11 février 2008 relative au contentieux des autorisations et des agréments préfectoraux dans le domaine des activités privées de sécurité reprend les éléments préconisés par le groupe de travail en 2006.

Concernant la nécessité de mener des enquêtes circonstanciées, la circulaire prévoit la consultation du STIC mais rappelle qu'un acte pris sur le seul motif de cette consultation sera censuré par le juge. Aussi, il est recommandé de demander aux services de police un rapport de synthèse sur les activités de l'intéressé lorsque aucun autre élément ne figure au dossier.

Le texte rappelle également que les décisions individuelles prises en application de la loi du 12 juillet 1983 réglementant les activités privées de sécurité doivent être motivées. La motivation consiste à « *mentionner, par des termes non stéréotypés, les éléments de droit et de fait* » qui fondent la décision. La circulaire insiste sur la qualité de cette motivation qui permettra au juge, effectuant un contrôle de

proportionnalité, d'apprécier si les faits sur lesquels se fonde la décision la justifient juridiquement et d'en déterminer la légalité. Des éléments de jurisprudence ont été développés afin d'aider les préfectures à déterminer, au cas par cas, si les conditions de délivrance de l'autorisation ou de l'agrément sont remplies.

14. Mieux harmoniser les motivations des décisions préfectorales

Cette circulaire devra rappeler que les décisions préfectorales doivent être motivées de manière précise et que les autorités préfectorales disposent d'un large pouvoir d'appréciation quant à la prise en compte ou la non-prise en compte de certains faits mentionnés au regard de l'emploi requis. Le principe de proportionnalité doit être, en l'espèce, pleinement appliqué.

Pour tirer les conséquences de cette recommandation, la DGPN a transmis, par courrier du 27 février 2007, une proposition de modification de la circulaire du 15 février 2005 relative aux instructions en matière de traitement des dossiers présentés par les sociétés de sécurité privée lors de l'embauche des salariés. Il était notamment proposé d'ajouter un nouveau modèle type de courrier à l'attention des préfets encadrant la délivrance d'un agrément dans les cas où une inscription au STIC n'est pas incompatible avec l'activité exercée.

Une circulaire générale, relative à l'ensemble des enquêtes administratives menées par les préfectures, est actuellement en cours d'élaboration pour reprendre l'ensemble des dispositions afférentes et constituer une aide à la décision lorsque les enquêtes administratives menées par les services des préfectures supposent la consultation de traitements automatisés de données à caractère personnel mis en œuvre pour le compte de l'Etat et relevant de l'article 26 de la loi n° 78-17 du 6 janvier 1978 .

15. Améliorer la traçabilité des consultations

Le groupe de travail recommande que, dans le cadre de la mise en place du système ARIANE, les garanties de traçabilité déjà existantes soient renforcées notamment par la mise en place d'une traçabilité complète et accessible au responsable hiérarchique comme au titulaire du compte. Dans ce cadre, le groupe de travail invite à l'ouverture d'une réflexion sur le recours à l'usage de la biométrie par empreintes digitales pour protéger l'accès aux fichiers de police, afin de renforcer leur sécurisation et la traçabilité des utilisateurs.

Une traçabilité complète et exhaustive (déjà opérationnelle pour le STIC) est prévue dans le projet ARIANE, sur la base de l'accès CHEOPS fédérant l'accès aux traitements du ministère de l'intérieur.

Pour la gendarmerie nationale, le système PROXIMA garantit une traçabilité de l'ensemble des opérations réalisées sur les fichiers judiciaires et administratifs accessibles aux unités.

16. Poursuivre la formation des personnels

Le groupe de travail suggère que les directions générales de la police et de la gendarmerie nationales poursuivent leurs efforts importants relatifs à la formation des personnels au sein des écoles et au contrôle des consultations. Il préconise de développer la sensibilisation des personnels en termes de sécurité et de responsabilité et de renforcer le contrôle hiérarchique.

La circulaire du ministre de l'intérieur du 9 mai 2007 relative aux modalités de mise en œuvre du STIC consacre un chapitre entier à la procédure d'habilitation des agents, la traçabilité des consultations et le contrôle hiérarchique.

Pour les traitements dont elle a la charge, la DCPJ (sous-direction de la police technique et scientifique) rappelle également régulièrement à ses correspondants la nécessité d'une meilleure prise en compte de ces aspects, et plus généralement de tout ce qui concerne les modalités d'accès aux fichiers.

La DGPN n'est pas opposée à ce qu'une nouvelle circulaire plus générale soit adressée à l'ensemble des directions opérationnelles sur la bonne application des grands principes du droit des fichiers par les services de police ; cette circulaire pourrait être la même que celle évoquée dans leur proposition n° 1 par la DGPN et la préfecture de police.

Pour la DGGN, le strict encadrement de l'accès et de l'utilisation des fichiers opérationnels de police judiciaire de la gendarmerie fait l'objet de la note-express n°87 202 DEF/GEND/OE/SDPJ/PJ du 06 août 2007. De plus la circulaire d'application n° 51 992 DEF/GEND/OE/SDPJ/PJ du 10 août 2007 précise les conditions de fonctionnement de l'application JUDEX.

17. Poursuivre la démarche « qualité » de la gendarmerie et de la police nationales

Le groupe de travail encourage la poursuite et le développement de la démarche « qualité » entreprise au sein de la police et de la gendarmerie nationales.

Il souhaite, dans ce cadre, que tous les fichiers tenus par les directions générales de la gendarmerie et de la police nationales ou leurs unités ou services locaux soient recensés, identifiés et déclarés.

Cette démarche est en cours. Le cabinet du DGPN, avec l'ensemble des directions de la police nationale, a engagé une procédure d'inventaire de tous les fichiers mis en œuvre dans les services de police afin de les mettre en conformité avec les nouvelles dispositions de la loi « informatique et libertés ».

Pour la DGGN, cette politique qualité est clairement explicité dans la circulaire n° 85 171 DEF/GEND/OE/SDPJ/PJ du 10 août 2007 portant organisation du service technique de recherches judiciaires et de documentation (STRJD). Depuis le 1er mars 2007, le STRJD est le premier service central de traitement de l'information judiciaire à être entré dans cette démarche (création d'un bureau « qualité » et démarche visant à obtenir une certification par un tiers indépendant de type AFAQ-AFNOR sur la base d'un référentiel de type norme ISO). Le plan assurance qualité du fichier des personnes recherchées (FPR) a été transmis officiellement à la CNIL le 19 février 2008.

18. Ouvrir une réflexion sur l'évolution nécessaire des outils de travail des forces républicaines de sécurité

Eu égard aux différents dangers auxquels la population est confrontée, la collecte, l'enrichissement et le traitement de données objectives sont des actes indispensables dans l'exercice des missions de police et notamment en vue de prévenir les crimes de masse ou sériels. Assurer ces missions ne peut se concevoir sans la mise en œuvre de traitements automatisés adaptés et de dispositifs de contrôle et de protection des libertés individuelles adéquats.

C'est une évidence parfaitement prise en compte dans le cadre des travaux de mise en place du nouveau système d'information destiné à l'investigation (NS2I) qui comporte notamment les traitements ARDOISE et ARIANE.

En outre, le traitement SALVAC, dont le but est de détecter des phénomènes sériels en matière de criminalité violente, fait l'objet d'un dossier en cours d'examen à la CNIL.

L'adaptation du cadre juridique des fichiers de police judiciaire passe également par une refonte des articles 21 et 21-1 de la loi du 18 mars 2003 pour la sécurité intérieure, qui est prévue dans le projet de LOPPSI.

La DGGN porte l'article 6 du projet de LOPPSI relatif à la détection et la résolution des faits présentant un caractère sériel. Cet article permet également de consolider les bases juridiques de différents fichiers existant mais ne faisant pas encore l'objet de déclaration (SALVAC, FBS, CORAIL) et d'envisager la mise en œuvre de systèmes d'informations de nouvelle génération permettant de traiter la totalité du spectre de la criminalité, en particulier la délinquance de proximité, (AJDRCDS).

19. Prendre en compte la dimension européenne

La libre circulation des personnes, des travailleurs et des prestations de service au sein de l'espace européen change le contexte dans lequel interviennent les décisions administratives nécessitant des enquêtes administratives et la consultation des fichiers de police.

Des négociations européennes sont en cours pour adopter plusieurs projets de décisions-cadres du Conseil portant notamment sur l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre États membres ainsi que sur la protection des données personnelles. Le principe de disponibilité appliqué aux fichiers sera amené à connaître des développements européens au cours des prochaines années.

Le groupe de travail souhaite que soit étudiée au cours de ces négociations la possibilité de consulter, dans le cadre d'enquêtes administratives justifiant la consultation des antécédents judiciaires, les données issues des casiers judiciaires ou des traitements automatisés de données des autres États membres de l'Union européenne, conformément à l'article 7.2 de l'actuel projet, dans des conditions et avec des garanties équivalentes à celles offertes aujourd'hui par le droit français ou les autres États membres. Ces consultations

devraient porter sur les infractions pertinentes commises à l'étranger, aussi bien par des citoyens Français que par des candidats non-nationaux.

Le groupe de travail recommande la mise en place d'une réflexion ouverte sur cette question dans le cadre des travaux du groupe commun police-gendarmerie-justice-CNIL ou du groupe police-gendarmerie-justice-CNIL auxquels s'ajouteraient la HALDE, le Médiateur de la République et la CNDS (suivant la décision prise en application de la proposition 3)

La DLPAJ est chargée de la transposition du texte de la décision-cadre du Conseil du 18 décembre 2006, dite « initiative suédoise », relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des Etats membres de l'Union européenne. La DLPAJ a mené cette transposition en concertation avec les services de la DGPN, de la DGGN et des douanes et droits indirects. Les écritures ont été soumises pour validation au ministère de la justice.

Dans la continuité du principe de disponibilité de l'information défini en 2004 par le programme de La Haye, la décision-cadre « initiative suédoise » permet de simplifier l'accès aux informations, notamment en matière de lutte contre la criminalité organisée et le terrorisme, par la création d'un cadre juridique commun de l'échange des informations entre les Etats membres. La plus-value de cet instrument communautaire est de fixer des délais de réponse plus courts à une demande d'information, définis en fonction de l'urgence et de la nature de l'infraction (de 8 heures à 14 jours). Les informations échangeables doivent être déjà disponibles auprès des services répressifs, sans nécessité de recourir à des mesures coercitives, et peuvent contribuer à mener aussi bien des enquêtes de police administrative que des enquêtes de police judiciaire.

20. Le fichier national des immatriculations

Le Fichier national des immatriculations (FNI) et le Fichier national des automobiles (FNA), application du FNI sont régis par l'a*rrêté du 20 janvier 1994 (JO du 8 février 1994). Le FNI* est un traitement automatisé des informations, nominatives ou non, enregistrées en vu de l'établissement et de la gestion des autorisations et pièces administratives exigées pour la circulation des véhicules ou affectant la disponibilité de ceux-ci. Le FNI est constitué du FNA et de fichiers départementaux. Le nouveau système d'immatriculation SIV, qui entrera en vigueur le 1er janvier 2009, répond à la même finalité.

Par ailleurs, le ministère des transports gère, depuis 1983, un fichier national informatisé des véhicules immatriculés sur le territoire français intitulé Fichier central des automobiles (FCA) (a*rrêté du 11 octobre 1983 au JO du 25 novembre 1983).* Le FCA a deux finalités limitativement définies **:**

- suivi des immatriculations et du parc des véhicules en circulation ;
- fourniture d'informations statistiques et nominatives.

Le ministère de l'intérieur transmet au ministère des transports toutes les données relatives au véhicule et au titulaire du certificat d'immatriculation enregistrées dans le FNI.

Par une convention passée en 1983, le ministère des transports a confié à l'AAA (« association auxiliaire de l'automobile », émanation des constructeurs automobiles), l'exploitation des données du FCA pour le compte des administrations et des entreprises automobiles agréées par le ministère de l'industrie.

Cependant, les liens entre le FNI et l'AAA ne sont formalisés par aucun texte juridique.

A l'occasion de la mise en place du SIV, le ministère de l'intérieur a décidé de prendre le texte juridique qui fait actuellement défaut. Saisi par le Gouvernement au printemps 2008, le Conseil d'Etat a rendu un avis indiquant les textes législatifs et réglementaires à modifier. Un projet de modification des dispositions du code de la route a été rédigé :

- à l'article L. 330-2, il est ajouté un 9° pour prévoir la communication des données aux constructeurs (ou leurs mandataires) pour les besoins des rappels de sécurité ;
- à l'article L.330-5, il est ajouté un deuxième alinéa pour prévoir, dans le cadre des dispositions de la loi n°78-753 du 17 juillet 1978 modifiée, la communication des données du SIV à des tiers :
    - à des fins statistiques, historiques ou scientifiques sans qu'il soit nécessaire de recueillir l'accord préalable des personnes concernées mais sous réserve que les études réalisées ne fassent apparaître aucune information nominative ;
    - à des fins d'enquêtes et de prospection commerciales, sauf opposition des personnes concernées.

La CNIL a été saisie en octobre 2008 d'un dossier d'autorisation (5° du I de l'article 25 de la loi du 6 janvier 1978) de cette interconnexion entre le SIV et le fichier de l'AAA. Le dossier est en cours d'examen.

Le Parlement sera prochainement saisi de la modification législative du code de la route qui est nécessaire.

CHAPITRE 3 - RECOMMANDATIONS DU GROUPE DE TRAVAIL

AMELIORER LA PROCEDURE DE CREATION OU DE DEVELOPPEMENT DES FICHIERS DE POLICE ET DE GENDARMERIE

1. Institutionnaliser le groupe de contrôle sur les fichiers de police et de gendarmerie

Les récents débats suscités par la création du fichier EDVIGE ont montré à quel point la question des fichiers de police et de gendarmerie, de leur contrôle et de leur modernisation était particulièrement sensible, notamment au regard de leurs conséquences sur les libertés individuelles et collectives. En 2006, déjà, lors de la mise en place du premier groupe de travail sur l'amélioration du contrôle de l'utilisation des fichiers STIC et JUDEX dans le cadre des enquêtes administratives, les questions inhérentes au développement de ces fichiers avaient été soulevées et avaient fait l'objet de d'échanges passionnés.

La prévention et la répression des crimes et délits nécessitent des outils adaptés et modernes permettant à la police et à la gendarmerie de lutter plus efficacement contre la criminalité et le terrorisme. Toutefois, de tels systèmes ne peuvent être crées et utilisés que dans un cadre strictement défini par la loi et la réglementation et pour une finalité conforme aux principes de proportionnalité et de garantie des libertés individuelles et collectives. Par ailleurs, il est indispensable que la mise en œuvre de tels dispositifs soit comprise et acceptée par l'opinion publique et que tout fichier de police ou de gendarmerie nouvellement créé ou modernisé de façon substantielle fasse l'objet d'une présentation et d'une concertation préalable.

Le groupe de contrôle recommande l'institutionnalisation de ses réunions et propose qu'il puisse se réunir, une fois par trimestre, en vue d'analyser les suites réservées aux préconisations de son rapport et toute évolution substantielle liée à la création ou au développement des fichiers de police et de gendarmerie.

Il souhaite également que le CNIL puisse assurer l'ensemble des prérogatives qui lui sont dévolues par la loi et les textes réglementaires sachant que le groupe de contrôle n'a pas vocation à examiner, ni les conditions de mise en œuvre du droit d'accès, ni les fiches individuelles enregistrées dans les traitements automatisés de données nominatives. Il exerce de ce fait une mission technique différente et complémentaire.

Observations du représentant de la CNIL : La première des recommandations a pour objet l'institutionnalisation du groupe de contrôle sur les fichiers de police et de gendarmerie. A l'appui de cette proposition, il est fait état de la nécessité à ce que les fichiers considérés ne puissent être « *créés et utilisés que dans un cadre strictement défini par la loi et la réglementation et pour une finalité conforme aux principes de proportionnalité et de garantie des libertés individuelles et collectives* ». A cet égard, il convient de rappeler qu'il s'agit d'une prérogative de la CNIL. En effet, en application de l'article 26 de la loi du 6 janvier 1978, modifiée par la loi du 6 août 2004, elle doit notamment être saisie pour avis de tous les projets d'actes réglementaires portant création de ce type de traitements.

De même, conformément à l'article 44 de la même loi, elle procède au contrôle de la mise en œuvre de ces derniers et veille à l'effectivité du droit d'accès des personnes, en application des dispositions des articles 38 et suivants de la loi précitée. A titre indicatif, la Commission a réalisé près de 2 700 vérifications en 2008 et a reçu près de 5 444 demandes de droit d'accès aux fichiers de police cette même année. Dans ces conditions, la création d'un nouvel organisme de contrôle reprenant tout ou partie des missions de la CNIL n'apparaît pas pertinente. En effet, son activité parallèle pourrait à la fois obérer la lisibilité du contrôle des fichiers de police et de gendarmerie et, sans doute, son efficacité.

2. Fournir à la population une information pédagogique sur ces fichiers

En vue de lutter contre les idées fausses et de « renforcer l'acceptabilité de fichiers au sein de la population », une campagne d'information pédagogique visant le grand public, en particulier les jeunes, doit être envisagée. La création d'un site Internet dédié, à l'instar du site Cyberbudget réalisé par le ministère du budget sur un domaine pourtant plus austère, semble à cet égard intéressante.

Ce site pourrait mettre à disposition :

- des animations ou infographies illustrant l'utilité concrète des fichiers de police et/ou de renseignement et les garanties offertes pour la protection des libertés ;
- un jeu de simulation permettant de prendre virtuellement les commandes d'un fichier de police pour mener une enquête (tout en en subissant les contraintes juridiques) ;
- des éléments de comparaison internationale permettant de relativiser la situation française pour les principaux fichiers de police et/ou de renseignement.

Le groupe de contrôle recommande la réalisation d'une campagne d'information sur les fichiers de police et de gendarmerie et la création d'un site internet public visant à mieux expliquer l'utilité et les conditions d'utilisation de tels dispositifs. En accord avec la CNIL, il souhaite également qu'en cas de création d'un tel site une information sur le droit des personnes à l'égard de ces fichiers soit clairement mentionnée.

3. Définir les modalités de destruction, d'archivage et de transfert des fichiers

La création, le développement ou la modernisation de nouvelles bases de données ou applications bureautiques entraînent automatiquement l'abandon de fichiers plus anciens. C'est pourquoi, dans ce cadre, il est nécessaire de fixer les modalités de destruction, d'archivage ou de transfert des informations contenues dans les fichiers devant faire l'objet d'un abandon.

Le groupe de contrôle recommande la mise en place d'un groupe de travail, placé sous la responsabilité de la direction des archives nationales, et chargé de proposer le cadre légal et pérenne des modalités de destruction d'archivage et de transfert des données enregistrées dans des fichiers de police et de gendarmerie devenus obsolètes.

Le ministère de l'Intérieur a demandé au Ministère de la culture de lui désigner un expert chargé de cette mission. La chef de l'inspection générale des archives de France ayant été désignée pour conduire cette mission, le ministre de l'Intérieur lui a adressée le 4 décembre 2008 une lettre de mission en ce sens.

4. Intégrer la démarche qualité

Au cours des années, la CNIL a affiné ses pratiques et exigé le bénéfice d'une vision plus précise du fonctionnement des traitements soumis à sa validation au point d'accompagner ses avis de recommandations très précises quant à leur utilisation opérationnelle. Les textes réglementaires visant à garantir le respect de telles recommandations portant création des fichiers sont encore perfectibles.

Face a des exigences de plus en plus précises du fonctionnement des traitements soumis à la validation de la CNIL, il apparaît nécessaire d'instaurer une démarche qualité qui, assortie aux exigences juridiques, instaure un maillage plus fin de normes d'administration et d'utilisation des fichiers. Cette démarche bénéficierait également à la performance opérationnelle par l'élaboration d'un schéma directeur clarifiant l'architecture des flux d'informations propres à la police et à la gendarmerie nationales ainsi que les flux mutualisés entre ces institutions.

Le groupe de contrôle recommande l'instauration d'une démarche qualité visant à définir plus précisément les modalités d'usage des fichiers de police et de gendarmerie.

METTRE EN ŒUVRE LE DROIT DES FICHIERS DE MANIERE PLUS MODERNE ET PLUS EFFICACE

5. Désigner un expert « informatique & libertés » au sein des services de police et de gendarmerie

La nécessité de toujours veiller à l'équilibre entre protection des libertés, respect de la législation et nécessité de doter les services de la police nationale et les unités de la gendarmerie nationale de systèmes d'aide à l'enquête adaptés et modernes impliquent une meilleure prise en compte de l'environnement technologique et réglementaire.

Des personnels ressources, spécialisés sur les questions « informatique et libertés », pourraient être créés au sein des services opérationnels de la police et de la gendarmerie. Ces experts auraient d'abord pour mission de diffuser une « culture informatique et libertés » dans les services opérationnels, qui manquent souvent de

connaissances dans ce domaine alors même que le fichier est un des outils de travail fondamentaux des policiers et des gendarmes. Mieux au fait des contraintes juridiques mais aussi de leur raison d'être et de leur intérêt pour eux-mêmes, les services de police et les unités de gendarmerie seraient mieux à même de les prendre en compte dès l'expression d'un besoin opérationnel, alors qu'actuellement le droit des fichiers constitue davantage une contrainte exogène et assez abstraite, que le service a parfois tendance à ne prendre en compte qu'au dernier moment. Dès lors, le risque de voir se constituer des fichiers « sauvages » serait fortement réduit, de même que le risque de se rendre compte trop tard qu'un traitement ne répond pas aux contraintes liées au droit des fichiers (dossier de consultation, traçabilité, exercice du droit d'accès, etc.).

Au titre de cette mission, les experts, spécialement formés à la législation sur les fichiers, seront notamment chargés :

- de former les services opérationnels par des actions de formation ponctuelles ;
- de conseiller les services opérationnels quant à l'opportunité de déployer au niveau local des projets de fichier et quant au cadre juridique et à l'architecture les plus adaptés ;
- d'assister les services lors de l'élaboration du dossier de déclaration ;
- d'être les interlocuteurs, au sein de leur service, de l'administration centrale qui disposera ainsi de relais plus efficaces ;
- de permettre des échanges d'expériences entre services.

L'action de ces experts permettra de mieux identifier les petits fichiers mis en œuvre localement (comme ceux constitués par les DDSP sur les fourrières, les débits de boissons, les objets volés ou les procurations de vote) et ainsi de les déclarer de manière cohérente et ordonnée à la CNIL.

Ces experts devront avoir une position hiérarchique suffisamment élevée pour avoir l'autorité nécessaire au sein de leurs services (par exemple : un commissaire ou un commandant dans chaque DDSP et un officier dans chaque groupement de gendarmerie), le cabinet du DGPN et du DGGN restant bien entendu le seul interlocuteur de la DLPAJ et celui de la préfecture de police pour les fichiers qu'elle met en œuvre.

Le groupe de contrôle recommande au ministère de l'Intérieur de désigner au sein de chaque service opérationnel de police et de gendarmerie un expert « informatique et libertés ». Il recommande que les missions de ces experts soient précisées par une circulaire commune du DGPN et du DGGN. En accord avec les recommandations de la CNIL, il conviendra de clarifier le rôle de ces experts et contrôleurs par rapport à celui des correspondants à la protection des données à caractère personnel, tels que définis à l'article 22 de la loi du 6 janvier 1978, et dont le groupe propose la création au sein des directions générales de la police et de la gendarmerie.

6. Recourir systématiquement aux déclarations-cadres pour faciliter l'action des services de police et de gendarmerie et améliorer la cohérence des outils opérationnels

Dans le cadre du recensement des fichiers de police engagé par la DGPN au titre de leur mise en conformité avec les dispositions introduites en 2004 dans la loi du 6 janvier 1978, il a été constaté que de nombreux services de police locaux mettaient en œuvre les mêmes catégories de fichiers (fourrières, objets trouvés, etc.). Bien que poursuivant une finalité identique, ces traitements ne suivent pas toujours la même architecture technique ni par conséquent les mêmes règles de sécurité des données.

Ces initiatives dispersées ont trois autres inconvénients majeurs :

- elles multiplient le risque de voir se constituer des fichiers « sauvages » ;
- elles entraînent une forte déperdition de moyens, chaque service travaillant à mettre en place son propre système ;
- elles ne profitent pas aux autres services parce qu'elles ne peuvent pas être révélées pour être généralisées lorsqu'elles le méritent.

Le groupe de contrôle propose donc au ministère de l'intérieur de recourir systématiquement aux procédures de « déclarations-cadres » prévues par la loi « informatique et libertés » aux termes du IV de l'article 26 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés qui permet au gestionnaire du traitement de déclarer sur la base d'une déclaration unique des fichiers répondant aux mêmes finalités, portant sur les mêmes catégories de données et ayant les mêmes destinataires.

Cette modalité de déclaration unique des traitements à la CNIL permettra d'améliorer le respect des exigences légales et de réduire d'autant les pratiques clandestines. Elle favorisera également la mise en œuvre d'architecture technique uniformisée, offrant ainsi les mêmes

7. Définir des référentiels communs

Afin d'éviter les descriptions subjectives, les fichiers de police judiciaire susceptibles d'enregistrer des informations relatives au signalement des personnes pourraient être soumis à un thésaurus fermé, inspiré des recommandations faites à propos du STIC-Canonge par le précédent groupe de travail sur les fichiers. D'autres thésaurus pourraient être créés afin de mieux encadrer la saisie d'informations relatives à la nature des infractions commises.

Le groupe de contrôle recommande au ministère de l'Intérieur d'engager une réflexion sur la possibilité d'intégrer des référentiels communs dans chaque catégorie de fichiers. Ces référentiels permettraient ainsi, sur le plan technique, de normaliser des champs de données afin de les rendre plus conformes aux principes définis par la loi de 1978 en matière de collecte de données.

Cette réflexion devra notamment être à la charge des attributions du groupe de contrôle institutionnalisé (recommandation n° 1) afin de ne pas multiplier les instances de réflexion, de garantir la présence de tous les partenaires institutionnels concernés, et de préserver la cohérence du dispositif d'ensemble de contrôle.

MIEUX CONTROLER L'UTILISATION DES FICHIERS

8. Intégrer systématiquement un module de contrôle interne des données

Si chacun reconnaît l'utilité et la nécessité de disposer d'outils informatiques performants, il convient d'en contrôler l'usage de la manière la plus efficiente afin de limiter, de prévenir et éventuellement réprimer les utilisations contraires aux règles déontologiques et aux finalités.

Le groupe de contrôle recommande de développer les possibilités de contrôles au sein de chaque service.

Il conviendrait ainsi de renforcer le pouvoir de contrôle des chefs de service sur la volumétrie et la nature des consultations effectuées par chacun des fonctionnaires qu'il a habilité. Un tel dispositif aurait automatiquement un effet dissuasif en faisant apparaître les consultations « de curiosité » et permettrait de mettre en place des contrôles aléatoires sur les liens existants entre des recherches sur les fichiers de procédure et une enquête en cours.

Le groupe de contrôle demande qu'une réflexion soit engagée sur la possibilité de mettre en œuvre des traitements systématiquement dotés :

- **d'un dispositif de pilotage interne donnant des indications d'ordre quantitatif sur les consultations effectuées sur une période donnée par chacun des fonctionnaires du service habilité, avec un dispositif d'alerte sur des variations significatives du total moyen habituel ;**
- **d'une visualisation, à partir du nom des fonctionnaires habilités, du patronyme des individus mis en cause ayant fait l'objet d'une consultation de fichier par chacun d'eux.**

Ce module devrait obligatoirement être intégré dans les architectures techniques des fichiers dès leur phase de conception. Dès lors, l'ensemble des fichiers de police seraient constitués du même bloc de sécurisation des données (traçabilité des connexions, contrôle des habilitations, contrôle des accès aux traitements et ce nouveau module de visibilité interne).

9. Améliorer la gestion des habilitations

Le groupe de contrôle recommande que le contrôle des habilitations des fonctionnaires soit amélioré.

A cette fin, le système de gestion des habilitations mis en œuvre par la police nationale dans le cadre du portail d'accès CHEOPS devrait faire l'objet d'évolutions techniques destinées à mieux prendre en compte

les évolutions de carrière de chaque fonctionnaire. Ainsi, en cas de mutation, de changement d'affectation ou de départ à la retraite, les droits d'accès de la personne devront être automatiquement revus ou supprimés.

Cette recommandation permettra de lutter plus efficacement contre les consultations indues de fichiers mais aussi d'éliminer tout risque de consultation indue de fichiers à partir d'un matricule qui aurait été crée frauduleusement par un fonctionnaire mal intentionné. Sur ce second point, le groupe de travail propose qu'une réflexion soit engagée sur les possibilités techniques d'interrogation automatique du fichier de gestion du personnel de la police nationale de l'authenticité des matricules utilisés par le portail CHEOPS.

Observations du représentant de la CNIL sur les recommandations 8 et 9 : Elles participent d'une volonté d'amélioration des modalités techniques de contrôle des fichiers de police et de gendarmerie et rejoignent en cela les préoccupations de la Commission, laquelle a notamment obtenu ces dernières années que soient mises en œuvre de véritables politiques de traçabilité des accès auxdits fichiers. Leur mise en œuvre serait d'ailleurs de nature à faciliter l'accomplissement des missions de vérification et de contrôle sur site effectuées par la CNIL. A cet égard, il convient de noter que, au cours de l'année 2008, 1158 demandes de droit d'accès indirect au STIC ont fait l'objet de procédures de vérification sur place et que 19 missions de contrôle du STIC ont eu lieu[20].

10. Recourir à terme à la biométrie pour améliorer le contrôle de l'accès aux traitements

Le groupe de contrôle recommande l'utilisation, à terme, de systèmes de contrôle d'accès aux traitements par la voie biométrique (empreinte digitale du fonctionnaire, par exemple) afin de renforcer le dispositif de sécurisation et de traçabilité de l'accès aux fichiers.

Le recours à ces outils permettra en effet de mettre fin aux « prêts » de mot de passe entre fonctionnaires de police ainsi qu'aux consultations de fichiers par un agent non habilité qui aurait indûment disposé ou conservé le mot de passe.

En outre, l'identification par l'empreinte digitale devrait davantage responsabiliser le fonctionnaire dans la mesure où ce dernier serait personnellement impliqué dans le processus d'authentification.

Eu égard aux coûts induits par la mise en œuvre d'un tel dispositif, le recours à la biométrie doit être subordonné à une évaluation financière et serait sans doute réservé, au moins au début, aux traitements les plus sensibles.

11. Renforcer très nettement le rôle de contrôle et d'audit des services d'inspection

Le groupe de contrôle suggère le renforcement des missions de l'IGPN, de l'IGS et de l'ITGN en matière de contrôle des fichiers.

Ces services pourraient ainsi multiplier les contrôles ciblés sur l'utilisation des fichiers, notamment au regard de la déontologie et des règles fixées par la loi « informatique et libertés ». Les textes réglementaires concernant les missions respectives de ces services devront être modifiés en conséquence.

En outre, le groupe de travail recommande un suivi effectif des recommandations émises par l'Inspection générale de la police nationale (IGPN), l'Inspection générale des services (IGS) ou l'Inspection technique de la gendarmerie nationale (ITGN). Les services concernés devront se conformer aux éventuelles observations dans le délai qui aura été fixé par le rapport d'audit.

Un guide d'audit portant sur l'informatique et les libertés pourrait être élaboré à l'usage des inspections mais aussi, à titre pédagogique et pour favoriser l'« auto-contrôle », à l'usage des experts « informatique et liberté » (Cf. proposition n° 5). Une « cotation », un « label » ou une procédure interne de certification pourrait également être institué et faire l'objet d'une certaine publicité une fois l'audit effectué.

Il conviendra de préciser l'articulation entre ces missions d'inspection « institutionnalisées » et les possibilités de contrôle d'ores et déjà dévolues à la CNIL. Le périmètre d'action de ces missions d'inspection sera utilement limité aux services et unités dans lesquels des dysfonctionnements ont été effectivement constatés afin d'en déterminer les causes en termes d'organisation du service et d'agissements des personnels.

[20] Un rapport général de contrôle du STIC sera d'ailleurs prochainement rendu public.

12. Créer un contrôleur interne au sein de la DGPN, de la PP et de la DGGN spécialisé dans la protection des données

La désignation d'une personnalité qualifiée, chargée de la surveillance et du fonctionnement de chaque traitement, pourrait être proposée. Il s'agirait d'un interlocuteur spécialisé en matière de protection de données à caractère personnel, tant pour le responsable et les utilisateurs des traitements, que pour la CNIL. La désignation de ce type de correspondant garantirait ainsi la transparence de la consultation de ces données.

La mise en place d'un tel correspondant a déjà été entreprise au niveau européen. Au sein d'Europol, comme d'Eurojust, un membre du personnel est en effet spécialement désigné pour assurer la protection des données.

Le groupe de contrôle recommande que, la fonction de correspondant informatique et libertés introduite en août 2004 avec la réforme de la loi informatique et libertés (article 22 III de la loi informatique et libertés et titre III du décret du 20 octobre 2005) pour les traitements les plus courants soit étendue à la mise en place d'un correspondant à la protection des données au sein des directions générales de le police et de la gendarmerie nationales ainsi qu'au sein des services de la Préfecture de Police de Paris.

13. Désigner un magistrat en charge du contrôle des fichiers d'antécédents judiciaires

L'article 6 du projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure modifie l'article 21 de la loi n°2003-239 du 18 mars 2003 relatif aux fichiers d'antécédents judiciaires et introduit la désignation d'un magistrat chargé du contrôle de ces fichiers.

Un tel magistrat serait destiné à assurer, parallèlement aux parquets qui continueront à assumer la mise à jour quotidienne au fil de l'eau des fichiers, un contrôle en profondeur des traitements, notamment grâce à un accès direct aux données.

Le groupe de contrôle recommande donc la création de la fonction de magistrat chargé du contrôle des fichiers d'antécédents judiciaires.

En tout état de cause, il importerait de clarifier l'articulation de l'action dudit magistrat avec celle de la CNIL, même s'il est souhaitable que les magistrats soient plus étroitement associés au suivi des fichiers d'antécédents judiciaires, en particulier s'agissant de leur mise à jour.

14. Renforcer le contrôle des fichiers des polices municipales

Le groupe de travail a constaté que les textes qui encadrent la création et le fonctionnement des polices municipales restent très restrictifs en ce qui concerne le contrôle de ces services de police par une autorité extérieure. Ainsi, depuis la mise en application de ces dispositions, les services de contrôle de l'Etat (IGA et IGPN) n'ont été saisis qu'une seule fois. D'autre part, les services de police municipale sont susceptibles de créer des fichiers avec pour seule contrainte de respecter le droit commun en la matière.

Le groupe de contrôle recommande que les contrôles sur le fonctionnement des services de police municipale soient plus nombreux et ciblés notamment sur la recherche des fichiers qui pourraient avoir été créés, sur l'étude de leur conformité avec les prescriptions de la loi, sur leur alimentation, sur leur utilisation et sur leur éventuelle extension. Au besoin, le groupe de travail recommande une modification de la loi du 15 avril 1999 en vue de préciser les modalités des contrôles pouvant intervenir.

Observations du représentant de la CNIL : S'agissant du renforcement du contrôle des fichiers de police municipale, la publication prochaine de l'arrêté conjoint du ministre de l'Intérieur et du garde des Sceaux, cité plus haut, ainsi que d'une autorisation unique prise par la Commission devrait contribuer à fixer un cadre juridique à la mise en œuvre de ces traitements en voie de développement. Par ailleurs, la CNIL procède régulièrement à des missions de contrôle des traitements mis en œuvre par les services de police municipale, soit dans le cadre de son programme annuel de contrôle soit suite à des plaintes.

RENFORCER LA FORMATION DES PERSONNELS

15. Renforcer la formation des fonctionnaires de police et des militaires de la gendarmerie

Le groupe de contrôle suggère la mise en place d'un module d'enseignement spécifique relatif aux droits et à l'utilisation des fichiers dès la formation initiale.

A cette occasion, les élèves et les stagiaires devront bénéficier d'un enseignement particulier sur les règles relatives aux principaux fichiers ainsi qu'aux différentes sanctions encourues en cas de détournement de finalité. Le groupe de travail estime en effet essentiel que le fichier, avec toutes les contraintes que notre droit y associe, soit regardé comme un des outils de travail fondamentaux du policier et du gendarme et soit traité comme tel, au même titre que, par exemple, l'arme de service ; de même que celle-ci fait l'objet d'un enseignement détaillé (notion de légitime défense, etc.), il est indispensable que le droit des fichiers soit largement diffusé dans toute formation dispensée aux policiers et aux gendarmes.

Un module d'enseignement destiné aux fonctionnaires ou aux militaires de la gendarmerie déjà en activité pourrait faire partie du catalogue des formations prévues dans le cadre du droit individuel à la formation continue.

16. Renforcer la formation des agents administratifs chargés de l'alimentation des fichiers

L'alimentation de certains traitements (le STIC, par exemple) requiert un niveau de connaissance élevé en droit et en procédure pénale. Ces fichiers comportent en effet des informations relatives à la qualification judiciaire des infractions, qu'il est d'autant plus important de savoir exploiter sans commettre d'erreur que celles-ci peuvent avoir de lourdes conséquences du point de vue des libertés publiques.

Afin de remédier à cette difficulté, le groupe de contrôle recommande que ces agents bénéficient d'une formation juridique adaptée et régulièrement entretenue. Cet effort de formation permettra d'améliorer les conditions d'alimentation des fichiers et de réduire le risque de saisies erronées.

Le groupe de contrôle souhaite que les administrations centrales se rapprochent des autorités administratives indépendantes afin de garantir la pluralité et l'efficacité des formations dispensées.

ADAPTER LES PROCEDURES

17. Définir dans la loi du 6 janvier 1978 un régime d'expérimentation

Certains traitements complexes ou de grande ampleur nécessitent de longues procédures d'expérimentation et d'évaluation qui sont nécessaires à leur mise au point et à leur bon fonctionnement opérationnel. Dans ce cas, les services de police sont confrontés à une difficulté : au moment de passer de la procédure de « vérification d'aptitude » (VA), qui peut donner lieu jusqu'au dernier moment à de nombreux aménagements techniques, à celle de « vérification de service régulier » (VSR), ils sont juridiquement tenus de présenter un dossier de déclaration déjà totalement abouti puisque la VSR suppose un emploi dans des conditions réelles par des services opérationnels (généralement, dans un nombre réduit de services sélectionnés en fonction de critères donnés). Cette contrainte pose deux problèmes majeurs :

- l'élaboration du dossier de déclaration puis la procédure réglementaire (examen du projet par la CNIL puis, bien souvent, examen par le Conseil d'Etat) imposent en toute rigueur de suspendre le projet et par conséquent de surseoir à la phase de VSR pendant une période qui peut largement dépasser un an ;
- l'élaboration d'un dossier de déclaration alors que la VSR n'a pas eu lieu oblige le gestionnaire du traitement à fournir des informations susceptibles de ne pas correspondre à la version définitive du traitement, celle qui résulte précisément de l'expérience acquise pendant la phase de VSR.

Au plan opérationnel, surseoir à la VSR est d'autant plus difficile que cela peut entraîner une lourde charge financière, du fait par exemple des équipes d'ingénieurs qui ne peuvent plus travailler sur le projet ou des contrats passés avec les entreprises prestataires. La DGPN est d'ailleurs confrontée actuellement à ces difficultés avec ARDOISE et le FAED (dans le cadre de son adaptation aux dispositions du traité de Prüm).

Pour ces raisons, la procédure de déclaration ne peut bien souvent être entreprise qu'à l'issue de la VSR, celle-ci n'étant dès lors couverte par aucun cadre juridique.

Le groupe de contrôle recommande que, pour les fichiers relevant de l'article 26 de la loi (ceux intéressant la sûreté de l'Etat, la défense ou la sécurité publique et ceux ayant pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté), la loi du 6 janvier 1978 soit modifiée pour reconnaître une phase d'expérimentation permettant de ne produire dans un premier temps qu'une déclaration simplifiée.

Cette procédure d'expérimentation ne pourrait excéder une année et ne devait préjuger en rien de décision finale de la CNIL.

Le contenu de la déclaration simplifiée serait défini par décret en Conseil d'Etat, comme dans le cadre du dernier alinéa du I de l'article 30 de la loi (procédure utilisée récemment pour les fichiers CRISTINA et EDVIRSP) ; le même décret préciserait les critères permettant de bénéficier de ce régime d'expérimentation (par exemple les finalités du traitement ou sa complexité technique). Pendant les douze mois de cette période légale d'expérimentation, la CNIL disposerait naturellement de tous les pouvoirs de contrôle qui lui confie l'article 44 de la loi, notamment pour s'assurer que le champ de l'expérimentation est respecté.

La reconnaissance de cette procédure d'expérimentation, étroitement contrôlée par la CNIL, aurait le grand avantage de concilier les exigences du droit des fichiers et les contraintes techniques inséparables d'un projet informatique de grande ampleur. Elle mettrait également fin à une situation trop fréquente, mais parfois inévitable, de mise en place d'un traitement sans aucun cadre juridique (cas d'Ardoise).

Observations du représentant de la CNIL : Le groupe de travail recommande de modifier la loi « Informatique et Libertés » afin de permettre la reconnaissance d'une phase d'expérimentation pour les fichiers relevant de son article 26. Il convient de souligner que rien n'interdit actuellement la possibilité de recourir à une phase d'expérimentation. C'est un dispositif expérimental qui a, notamment, été retenu s'agissant du placement sous surveillance électronique mobile (PSEM), du système de pré-plainte en ligne, du fichier des passagers aériens (FPA) ou encore, dans un autre domaine, du dossier pharmaceutique.

En outre, si l'on comprend la nécessité de pouvoir adapter, dans certains cas, les modalités de présentation des dossiers techniques correspondant aux traitements déclarés, la généralisation du recours aux déclarations simplifiées serait de nature à obérer l'effectivité du contrôle *a priori* exercé par la CNIL puisqu'elle ne bénéficierait alors d'aucune information sur les caractéristiques techniques du fichier (son degré de sécurité etc.).

18. Renforcer la CNIL dans son rôle de conseil

Instance de contrôle, la CNIL s'est également vu reconnaître un rôle de conseil du gouvernement et, d'ailleurs, de tout gestionnaire de traitement afin que, par une relation de partenariat et un rôle pédagogique clairement assumé, les contraintes liées au droit des fichiers, trop souvent perçues comme exogènes et difficiles à mettre en œuvre, puissent être mieux intégrées et mieux comprises par les acteurs. Il paraît d'ailleurs évident que toute mission de contrôle est plus efficace lorsqu'elle s'accompagne d'une démarche active d'assistance, de pédagogie et d'incitation que lorsqu'elle se réduit à une censure.

Le groupe de contrôle propose que la Commission Nationale Informatique et Libertés voit renforcé son rôle de conseil des services et directions administratives chargées de mettre en œuvre des traitements automatisés de données à caractère personnel. Ce rôle ne pouvant, bien entendu, préjuger des délibérations ultérieures de la CNIL.

AMELIORER LES GARANTIES LIEES A L'USAGE DU STIC ET DE JUDEX DANS LE CADRE DES ENQUETES ADMINISTRATIVES

19. Simplifier la transmission des suites judiciaires dans le cadre du traitement en temps réel

Le groupe de contrôle suggère que soit examinée, en concertation avec la police et la gendarmerie nationales et le ministère de la Justice, la possibilité de simplifier la transmission des suites judiciaires dans le cadre du traitement en temps réel.

Il pourrait être ainsi étudié la possibilité de transmission des suites judiciaires, au niveau régional, par voie de courrier électronique (avec accusé de réception) sur une boite électronique fonctionnelle dédiée et dans le respect du code de procédure pénale.

L'instruction de classement sans suite des parquets pour insuffisances de charges pourrait, selon des modalités à définir, être immédiatement prise en compte par les services enquêteurs sans qu'il soit besoin de leur transmettre une fiche navette. Par ailleurs, une réflexion pourrait être menée sur le moment opportun de l'inscription de la personne mise en cause au STIC ou au JUDEX : différer l'inscription au moment où la responsabilité de la personne est véritablement bien établie peut être de nature à éviter le maintien de mentions erronées.

Observations du Syndicat des Commissaires de la Police Nationale : Il est indispensable de conserver un mode écrit et traçable de transmission des poursuites judiciaires (fiche navette) en direction des services enquêteurs, y compris pour les affaires bénéficiant du traitement en temps réel. Les services enquêteurs ne doivent pas supporter les effets du doute en cas d'absence de trace (présomption d'information par la Justice).

20. Étendre les cas de mise à jour des fichiers STIC et JUDEX

Le groupe de contrôle suggère d'élargir la liste des cas justifiant une mise à jour des fichiers STIC et JUDEX aux décisions alternatives aux poursuites, telles que les rappels à la loi et la composition pénale, qui ne font actuellement pas l'objet d'une mention au STIC ou au JUDEX.

Une ligne additionnelle devra apparaître sur l'écran indiquant « décision alternative aux poursuites » en cas de consultation pour une enquête administrative.

Ainsi que le groupe de travail l'avait déjà souligné en novembre 2006, l'autorité administrative n'est pleinement en mesure d'effectuer une prise en compte proportionnée des faits que pour autant qu'elle a connaissance des suites judiciaires qui leur ont été réservées.

21. Garantir dans certains cas une procédure contradictoire

Selon le premier alinéa de l'article 17-1 de la loi n°95-73 du 21 janvier 1995 modifiée d'orientation et de programmation relative à la sécurité, certaines décisions administratives de recrutement, d'affectation, d'autorisation, d'agrément ou d'habilitation peuvent faire l'objet d'enquêtes administratives donnant lieu à consultation des fichiers de police STIC et JUDEX.

Dans le cadre de cette procédure, il est souhaitable de garantir effectivement que la personne faisant l'objet d'une telle enquête soit, préalablement à une décision défavorable :

- informée qu'une décision défavorable est envisagée et de ses motifs ;
- invitée à formuler ses observations écrites ;
- entendue, si elle le demande.

En effet, le principe des droits de la défense implique qu'une « mesure individuelle d'une certaine gravité, reposant sur l'appréciation d'une situation personnelle, ne peut être prise par l'administration, sans entendre au préalable la personne qui est susceptible d'être lésée dans ses intérêts moraux et matériels par cette mesure ». [CE, sect., 9 mai 1980, Sté des établissements Cruse fils et frères : Rec. CE 1980, p. 217, concl. B. Genevois].

Le groupe de contrôle propose la mise en place d'un groupe de réflexion, composé de la CNIL, de la DGPN, de la DGGN, de la DLPAJ et du Médiateur de la République, visant à proposer de nouvelles garanties aux personnes faisant l'objet d'une enquête administrative au titre de la loi du 21 janvier 1995.

22. Créer une voie de recours contre certaines décisions du procureur de la République

Pour le Médiateur de la République, l'article 21-III de la loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure prévoit que « le traitement des informations nominatives est opéré sous le contrôle du procureur de la République compétent qui peut demander qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire ».

« La rectification pour requalification judiciaire est de droit lorsque la personne concernée la demande ». En revanche, en cas de « décision de relaxe ou d'acquittement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées sauf si le procureur de la République en prescrit le maintien pour des raisons liées à la finalité du fichier, auquel cas elle fait l'objet d'une mention ».

Le législateur a ainsi confié en cette matière au procureur de la République un pouvoir décisionnel, qu'il exerce selon son appréciation, qui s'impose au responsable du traitement et fait grief à la personne mise en cause.

Or, lorsque cette décision intervient, elle n'est pas notifiée à la personne mise en cause et n'est pas susceptible de recours. Pourtant, cette décision est susceptible d'avoir pour conséquence un refus d'embauche, d'agrément ou un licenciement, alors même que la personne a été relaxée ou acquittée.

En vue d'assurer « un meilleur équilibre entre l'efficacité de la protection des personnes et l'attention de tous les instants que requiert la protection des libertés [*] », la proposition suivante est par conséquent formulée :

En cas de décision de relaxe ou d'acquittement devenue définitive, la prescription du procureur de la République tendant au maintien des mentions relatives aux données personnelles concernant la personne mise en cause, devra désormais lui être notifiée et sera susceptible d'un recours devant le procureur général.

Le ministère de la Justice, observe pour sa part, que la demande de mise à jour des fichiers STIC ou JUDEX, selon les conditions précisées par le III de l'article 21 de la loi du 18 mars 2003 pour la sécurité intérieure, peut être adressée directement auprès du procureur de la République. Cette saisine peut alors être considérée comme une modalité d'exercice du droit d'accès indirect sui generis puisque la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés précise en son article 41 qu'une telle demande est adressée au gestionnaire du fichier via la Commission Nationale de l'Informatique et des Libertés.

C'est donc afin d'améliorer la procédure d'instruction de telles demandes qu'il a été prévu, par les actes réglementaires portant création de ces fichiers, qu'elles puissent être adressées directement au procureur de la République.

Son contrôle, opéré à l'occasion de l'exercice du droit d'accès indirect, quelles qu'en soient ses modalités, a pour objet de déterminer si les mentions figurant dans les fichiers STIC ou JUDEX, si elles existent, répondent lors de la demande aux conditions légales pouvant conduire à leur effacement ou à leur rectification.

Par ailleurs, la loi du 18 mars 2003 doit s'articuler avec la loi du 6 janvier 1978 ainsi que l'a rappelé le Conseil Constitutionnel dans sa décision n°2003-467 DC du 13 mars 2003. Ainsi, il appartient au seul responsable du traitement en application de la loi du 6 janvier 1978 précitée de prendre ou non la décision d'effacement ou de rectification dans le cadre du droit d'accès indirect, crée par la loi du 18 mars 2003 et ce même lorsqu'il est tenu de suivre la position prise par le procureur de la République.

Il s'ensuit que les conclusions du magistrat sur le mérite de certaines données à être rectifiées ou à être effacées ne sont adressées qu'au responsable du traitement, celui-ci demeurant la seule autorité compétente à l'exclusion de toute autre, pour prendre ou non la décision d'effacement ou de rectification et la notifier au requérant.

Elles peuvent être cependant portées à la connaissance du requérant à simple titre de mesure d'information attestant du contrôle opéré par le magistrat sur les mentions enregistrées au STIC ou au JUDEX. Il s'ensuit que cette information, ne faisant pas grief au demandeur, est insusceptible de recours quelle qu'en soit sa nature.

On relèvera qu'une analyse similaire a été retenue par le Conseil d'Etat, s'agissant du fichier des renseignements généraux. Ainsi la Haute assemblée à jugé que « la lettre réponse de la CNIL doit être regardée comme informant le demandeur qu'une décision de refus de communication lui est opposée et qu'à défaut dans le texte de la lettre de précisions faisant apparaître que la demande de l'intéressé aurait été soumise à la [CNIL], le refus de communication s'analyse, eu égard aux dispositions précitées[…]du décret, en une décision du ministre de l'intérieur et de la sécurité publique s'opposant à la communication au requérant des informations le concernant» (*CE, 23 juin 1993, M. Ruwayha*)

Ainsi, la circonstance que les prescriptions du magistrat ne puissent pas faire l'objet d'un recours ne prive en aucun cas l'intéressé de la possibilité de contester la décision finale prise par le responsable du traitement. L'accès au juge protégé par 6 de l'article de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales est donc garanti. Au surplus, l'instauration d'un recours contre les prescriptions du magistrat serait de nature à allonger le délai de traitement des demandes d'accès indirect et n'iraient donc pas dans le sens de l'intérêt des citoyens.

> *Cette recommandation, proposée par le Médiateur de la République, avait déjà été présentée lors des précédents travaux du groupe de travail de 2006. Elle n'avait pas fait l'objet d'un consensus et avait été rejetée par le ministère de la Justice.*

En tout état de cause, le groupe de contrôle recommande la mise en place d'une procédure de notification à l'intéressé par le service gestionnaire du fichier dès lors que la décision de maintien de son inscription dans les fichiers d'antécédents judiciaires serait prise sur prescription du parquet.

Observations de la conférence des Bâtonniers : La conférence des Bâtonniers est favorable à la suppression de toute décision d'opportunité du parquet, concernant le maintien d'une inscription dans les fichiers d'antécédent judiciaire, lorsqu'une décision de non lieu, d'acquittement ou de relaxe est prononcée par une juridiction.

Observations de Jean-Marc Leclerc : Jean-Marc Leclerc considère qu'il faudrait supprimer le droit accordé aux procureurs de maintenir dans le fichier STIC une personne ayant été blanchie par la justice pour les faits qui ont justifié son inscription initiale. Il s'agit, à ses yeux, d'un procédé déloyal, au même titre que celui consistant à faire passer par le dépôt une personne entendue dans une affaire de presse…

RECOMMANDATIONS PARTICULIERES

23. Sur la notion de signalement

A l'occasion de l'examen des suites réservées à la recommandation du groupe de travail de 2006 sur l'évolution de l'application « Canonge », et notamment des éléments sur les caractéristiques physiques des personnes recherchées, un débat a eu lieu sur les éléments les plus pertinents devant faciliter l'identification d'un individu suspecté d'avoir perpétré une infraction.

Les échanges ont notamment porté sur deux exigences, parfois contradictoires, et qui ont d'ailleurs fait l'objet de plusieurs contributions des membres du groupe de contrôle[21] :

- la nécessité, pour les services de police et de gendarmerie, de disposer d'un dispositif permettant d'orienter leurs recherches lorsqu'ils sont sur les traces d'un présumé délinquant, en enquête de flagrance, en enquête préliminaire ou lors d'une instruction ;
- la nécessité de ne pas stigmatiser telle ou telle catégorie de la population en fonction de son origine ;
- le refus de toute classification ethno-raciale suivant les recommandations des Autorités Administratives Indépendantes et de toute utilisation des données en vue de la constitution d'un outil statistique basé sur ces données ;
- la définition d'un outil de détermination de ce que sont les "critères physiques objectifs" retenus.

Ce dispositif doit permettre d'écarter tel ou tel individu du champ d'investigation en fonction de plusieurs critères dont les caractéristiques physiques de la personne. Il doit contribuer à limiter le champ de recherche des enquêteurs et leur faciliter l'identification des mis en cause.

La question qui a fait l'objet de débats concerne la manière de caractériser une personne : doit-on utiliser l'appartenance vraie ou supposée à une origine ethno-raciale ou doit-on plutôt se servir d'une gamme chromatique telle que proposée par le milieu associatif notamment ?

L'opposition entre les partisans de l'utilisation d'une typologie telle que définis dans le thésaurus du fichier « Canonge » issu des discussions du groupe de travail de 2006 et les tenants de l'utilisation d'une solution nouvelle tournant le dos à la précédente et prônant l'utilisation d'une gamme chromatique adaptée (milieu associatif et Conférence des bâtonniers) a révélé les difficultés à trouver un dispositif équilibré entre la nécessité de l'identification des personnes recherchées et le principe de non discrimination.

De plus, les partisans des deux solutions opposées n'ont pas considéré qu'une expérimentation concomitante des deux dispositifs fût possible en l'état.

C'est pourquoi la majorité du groupe de contrôle préconise, dans l'ensemble des fichiers sur les personnes recherchées de la police et de la gendarmerie nationales, et faisant référence à l'apparence :

- **L'usage du terme « apparence » qui devra se substituer au mot « signalement »**
- **L'utilisation corrigée de la classification adoptée par le groupe de travail de 2006**

[21] Voir le chapitre « Eclairages »

1/ Type CAUCASIEN

2/ Type MEDITERRANEEN

3/ Type MOYEN ORIENTAL

4/ Type MAGHREBIN

5/ Type ASIATIQUE/EURASIEN

6/ Type AMERINDIEN

7/ Type INDO-PAKISTANAIS

8/ Type METIS-MULATRE

9/ Type AFRICAIN/ANTILLAIS

10/ Type POLYNESIEN

11/ Type MELANESIEN (dont canaque)

- **En tout état de cause, la suppression du type gitan dans la typologie définie actuellement et le reclassement du stock sont recommandés**

Par ailleurs, et eu égard aux échanges sur cette problématique, le groupe de contrôle souhaite la poursuite de cette réflexion et la possibilité de poursuivre le débat dans le cadre de l'institutionnalisation éventuelle de son existence.

Observations du représentant de la CNIL : Dans ses recommandations du 16 mai 2007 sur la mesure de la diversité et la protection des données, la Commission avait émis de fortes réserves sur la création d'une nomenclature nationale de catégories « ethno-raciales » et estimé que la décision de principe de créer une telle nomenclature, si elle devait être utilisée de façon obligatoire, relèverait du Législateur, sous le contrôle du Conseil Constitutionnel.

Observations de Jean-Marc Leclerc : Concernant le fichage Canonge des personnes, et son équivalent dans le fichier Judex de la gendarmerie, il importe de constater que les forces de l'ordre ne sont pas demandeuses d'une réforme. Ces professionnels sont le mieux à même d'exprimer, dans un souci de pragmatisme, quelle typologie représente le moyen le plus efficace d'identifier un auteur d'infraction quand débute une enquête.

Observations de la HALDE : Dans un avis remis au groupe de contrôle le 1er décembre 2008, la haute autorité réitère ses recommandations issues de la délibération n°2006-31 du 26 février 2006 dans laquelle le Collège affirmait son opposition aux comptages ethniques et précisait que devaient « notamment être prohibés tous dispositifs basés sur des données anthropomorphiques ». En conséquence, elle donne un avis défavorable à la classification proposée[22].

24. Sur EDVRISP

Les recommandations du groupe de travail sur le projet de fichier EDVRISP portent sur la première version du projet EDVRISP (projet transmis à la CNIL le 19 septembre 2008). Depuis ce premier projet de décret, un deuxième projet a été transmis à la CNIL en novembre 2008 et a fait l'objet d'un avis rendu le 20 novembre 2008.

Article 2 du décret EDVIRSP

Sur les origines ethniques et raciales

Le groupe de contrôle des fichiers de police et de gendarmerie, après débat, relève que l'enregistrement d'informations relatives à l'origine raciale ou ethnique ne présente pas d'intérêt, et ce d'autant plus que l'article 4 du décret prévoit la possibilité d'enregistrer « les signes physiques particuliers et objectifs ».

Le groupe de contrôle propose la suppression de cette mention.

Sur les opinions politiques, philosophiques ou religieuses

[22] *Cf. l'avis de la HALDE reproduit dans la partie « Eclairages »*

Le groupe de contrôle relève que ce ne sont pas les opinions qui doivent être enregistrées mais les informations sur des comportements, qui sous couvert d'opinion politiques, philosophiques ou religieuses ou d'une appartenance syndicale, sont susceptibles de porter atteinte à la sécurité publique.

Il est donc proposé une nouvelle rédaction de l'article 2 :

Art. 2. - Par dérogation, sont autorisés, pour les seules fins et dans le strict respect des conditions définies aux articles 3 à 9 du présent décret, la collecte, la conservation et le traitement par les services mentionnés au précédent article de données à caractère personnel de la nature de celles visées à l'article 1er et qui sont relatives aux manifestations extrémistes sous couvert d'opinions ou d'appartenances politiques, syndicales, philosophiques ou religieuses. [Les données relatives aux origines raciales ou ethniques, aux opinions politiques, philosophiques ou religieuses, à la santé ou à la vie sexuelle des personnes sont strictement prohibées.].

Dans le projet de deuxième décret transmis à la CNIL (voir la fiche sur EDVRISP), le ministère de l'Intérieur a supprimé toute référence aux origines ethno-raciales pour les remplacer par les signes physiques particuliers et objectifs et l'origine géographique.

Article 3 du décret EDVIRSP

Cette rédaction exclue le recueil d'informations sur des groupes, organisations et personnes pouvant porter atteinte à la sécurité publique. Par ailleurs, tel que le décret est rédigé, l'enregistrement d'informations économiques et sociales nécessaires aux institutions et services publics dans le cadre de leurs missions institutionnelles est devenue impossible.

Afin d'éviter toute tentation de réintroduction de fichiers non déclarés, le groupe de contrôle propose une nouvelle rédaction de l'article 3 :

Art. 3. - Les données mentionnées à l'article 2 ne pourront être collectées, conservées et traitées que dans les cas suivants, à l'exclusion de toute autre finalité :

1° Lorsqu'elles concernent des personnes morales ou personnes physiques dont l'action individuelle ou collective indique qu'elles sont susceptibles de porter atteinte à l'ordre public.

2° Lorsqu'elles concernent des groupes, mouvements ou organisations dont l'activité peut faire l'objet de la mission de renseignement et d'information du gouvernement, et des représentants de l'Etat dans les collectivités territoriales, en ce qui concerne le domaine institutionnel, économique et social ainsi que dans tous les domaines susceptibles d'intéresser l'ordre public notamment les phénomènes de violence.

Le groupe de contrôle précise qu'il est favorable à la suppression du fichier des personnalités et qu'il s'agit ici de garantir l'information des services publics sur des manifestations ou événements ayant une influence sur la vie sociale ou économique du pays.

Observations de la HALDE : La haute autorité émet un avis défavorable à cette nouvelle proposition de rédaction considérant, au contraire, que le projet de décret actuel permet déjà de recueillir les informations sur les groupes et personnes susceptibles de porter atteinte à l'ordre public. Cette nouvelle rédaction pourrait conduire à réintroduire, de fait, la finalité des « personnalités » alors que la HALDE s'était félicitée de son retrait. En effet, des informations sur des groupes ou organisations pourront être collectées dans le fichier et ce, alors même qu'aucun risque de trouble à l'ordre public n'est établi.

Sur l'enregistrement des mineurs

Considérant que les données criminelles factuelles enregistrées dans les procédures comme dans les décisions de justice indiquent un nombre de mineurs mis en cause, considérant le nombre de mineurs déjà présents dans les fichiers criminels (STIC) ou de renseignements, il apparaît que les mineurs, pour des raisons légitimes et depuis plusieurs dizaines d'années, sont enregistrés.

Dés lors il apparaît au groupe de travail que la question qui doit se poser porte plus sur la protection renforcée dont doivent bénéficier les mineurs enregistrés que sur le principe même de leur enregistrement.

L'évolution de la personnalité durant la minorité justifie en effet une attention particulière, nécessitant que le bien-fondé de l'inscription des mineurs soit réexaminé périodiquement.

Quelque doit l'âge en définitive retenu pour l'enregistrement des mineurs dans les fichiers de renseignement, le groupe de contrôle recommande la mise en place d'un dispositif assurant une protection particulière et renforcée. Il consistera en un contrôle approfondi de l'inscription du

mineur sur un fichier de renseignement. La validité de cette inscription sera examinée tous les 12 mois. Il sera complété par l'obligation d'extraire automatiquement leur fiche au moment de la majorité.

Les fiches ainsi extraites seront soumises à l'examen d'un magistrat de l'ordre administratif, spécialement chargé cette mission au niveau national, pour décider du maintien dans le fichier ou de la radiation, selon la nature et l'ancienneté des faits ayant motivé l'inscription.

Observations du représentant de la CNIL : La Commission a rendu son avis sur le projet de décret en Conseil d'Etat portant création du traitement « EDVIRSP » le 20 novembre dernier. La délibération correspondante sera publiée en même temps que ledit décret. A ce jour et conformément à la loi, il n'est donc pas possible d'en révéler le contenu.

Observations de Jean-Marc Leclerc : S'agissant du fichier EDVIRSP, Jean-Marc Leclerc est hostile au fichage des mineurs de moins de 16 ans. Des propositions de nouvelles procédures de contrôle ont certes été émises au cours des débats du groupe fichier. Mais il ne faudrait pas marginaliser la CNIL. Au fil des projets exposés lors des discussions, il semble que l'administration soit mue par la volonté de contourner cet organisme essentiel au respect des libertés publiques et individuelles.

Observations de la HALDE : S'agissant du fichier EDVIRSP, la haute autorité recommande l'abandon du fichage des mineurs dont les activités indiquent qu'ils sont susceptibles de porter atteinte à la sécurité publique (Cf. avis de la HALDE reproduit dans la partie « Eclairages »).

25. Sur la révélation des infractions sérielles par des applications informatiques.

Le groupe de travail relève que les fichiers relatifs à la révélation d'infractions sérielles (AJDRCDS, CORAIL[23], etc.) peuvent avoir une capacité de traitement des informations très large due à la possibilité importante des croisements et rapprochements qu'ils peuvent opérer.

Si le groupe de travail reconnaît l'utilité de ces applications visant à révéler une criminalité qui n'a pas pu et qui n'aurait pas pu être découverte par les dispositifs traditionnels existants, il émet des réserves sur l'idée qu'une telle capacité puisse être mise en œuvre pour l'ensemble des crimes, délits et contraventions.

Le groupe de contrôle recommande que les applications visant à révéler une criminalité inconnue par l'analyse de la sérialité soient limitées aux infractions les plus graves :

- **Celles présentant un niveau de gravité qui les rendent particulièrement insupportables à la société telles que les atteintes aux personnes (homicides, agressions à caractère sexuel, coups et blessures délictuels ou criminels), les atteintes aux biens graves, le trafic de stupéfiants et la cyber-criminalité concernant les faits visés précédemment,**
- **Celles qui sont punies au moins de 5 années d'emprisonnement pour les atteintes aux personnes et de 7 années d'emprisonnement pour les atteintes aux biens.**

Il préconise également qu'un magistrat de l'ordre judiciaire, disposant d'une compétence nationale, soit nommé et dédié au contrôle des ces applications.

26. Sur les fichiers classés secret défense

Certains fichiers sont soumis au régime juridique des fichiers « de souveraineté », défini par l'article 26 (III) de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et par le décret n° 2007-914 du 15 mai 2007. Ces fichiers ne peuvent faire l'objet d'un contrôle sur place de la CNIL et le décret en portant création n'est pas publié.

Afin de garantir la légitimité des informations contenues dans ces fichiers, le groupe de contrôle recommande la création d'une Commission nationale du secret des fichiers de police et de renseignement afin de permettre, sur le modèle de la Commission du Secret de la Défense Nationale, une validation de la présence dans les fichiers de renseignements couverts par le secret de la défense nationale sur des personnes soupçonnées d'activités portant atteinte à la sûreté de l'Etat. Cette commission, composée de personnes habilitées et désignées par le gouvernement, serait au moins composée d'un magistrat.

[23] Il est à noter que le projet « CORAIL » comporte une durée de conservation des données très limitées (3 années maximum).

CHAPITRE 4 - ECLAIRAGES

Les textes qui suivent sont issus des réflexions des membres du groupe de travail et sont, soit des déclarations de principe, soit des appréciations portant sur des aspects particuliers de certains fichiers. Ils n'ont pas fait l'objet d'une adoption par l'ensemble des membres du groupe de travail.

1. BATONNIER DE PARIS

L'Ordre des Avocats de Paris représenté par son Bâtonnier, a été invité à participer aux travaux des membres du groupe de travail sur les fichiers de Police relatif à l'examen des mises en œuvre et d'exploitation des fichiers de Police Judiciaire et de Police Administrative, dirigé par monsieur Alain BAUER Criminologue, Président du Conseil et d'Orientation de l'observatoire National de la délinquance.

Le groupe de travail s'est réuni en l'état à trois reprises et a souhaité des représentants de différentes associations qui participent à ces travaux et de l'Ordre des Avocats, la communication d'une recommandation pour le 14 novembre 2008.

Aussi, l'Ordre des Avocats entend rappeler que le fichier EDVIGE n'a pas pour objectif de lutter contre des actes accomplis mais est fondé sur le soupçon de ce qui pourrait être fait et en tant que tel doit être condamné.

Il déplore qu'il ait fallu attendre une réaction citoyenne pour que soit envisagée la suppression du fichier dit des personnalités et du classement selon des critères inadmissibles tels que le type racial, l'orientation sexuelle, l'engagement syndical ou politique.

Il dénonce le critère de l'hypothétique atteinte à l'ordre public comme permettant de réintroduire de manière indirecte, le fichier des personnalités dont l'action individuelle ou collective indiquerait qu'elles sont susceptibles de porter atteinte à l'ordre public.

Il déplore que pèse sur l'ensemble des citoyens une présomption de soupçon d'atteinte à l'ordre public.

Il souhaite l'instauration d'un droit permanent à la consultation et à la rectification de tout ou partie des données enregistrées sur tel ou tel fichier qu'il s'agisse du fichier EDVIGE, du STIC ou encore du JUDEX (dont la confusion est prévue).

Il recommande la reconnaissance d'un droit à l'oubli.

S'agissant des mineurs, l'Ordre de Paris déplore qu'aient été fichés sur l'ancien fichier des renseignements généraux, des mineurs de moins de 13 ans et que l'actuelle Commission n'envisage aucune condition d'âge à leur fichage en l'état de ces réflexions sans même prévoir un droit permanent à la consultation, à la rectification et à la suppression.

Il préconise l'instauration d'un système de contrôle régulier par un collège de Magistrats de l'ordre administratif ou judiciaire ou par une autorité administrative indépendante créée à cet effet, qui en concertation avec les personnes intéressées, aura vocation à organiser la rectification et la suppression des données figurant sur les fichiers lesquels devront être supprimées en tout état de cause dès l'âge de 18 ans pour les mineurs.

Enfin, l'Ordre entend rappeler, que toute personne a droit à la protection des données personnelles le concernant comme à l'oubli de celles enregistrées sur des fichiers quels qu'ils soient, lesquels ne sauraient avoir d'autres finalités que la protection de la démocratie.

2. BUREAU DE LA CONFERENCE DES BATONNIERS

Examiner le fonctionnement pratique des fichiers de police et de gendarmerie ne doit pas interdire de s'interroger sur le principe même de leur existence.

Principe

« Identifier un individu, c'est déjà porter atteinte à sa vie privée » (D. GUTMAN – Le sentiment d'identité – LGDJ., t. 327, 2000, n°381, p. 317).

« La police, instrument de la puissance publique pour maintenir l'ordre, est généralement comprise sous son aspect préventif, si bien qu'elle deviendrait une police de gestion des risques » (PY. MAROT – Actualité juridique pénale 2007, p. 61).

Les citoyens peuvent être contrôlés, fiché, filmés, (et bientôt, sans doute, leurs ordinateurs secrètement piratés).

Alors même qu'aucune étude ne semble avoir été faîte sur les risques pour les libertés face aux avantages promis pour la sécurité, incontestablement les fichiers portent atteinte à la liberté de la vie privée et à celle d'aller et venir.

Ils sont donc en opposition avec les libertés individuelles piliers de la démocratie.

La CNCDH le disait en juin 1991 et l'a rappelé à Madame le Ministre de l'Intérieur par une lettre du 19 septembre 2008.

La création d'un fichier ne peut donc être qu'exceptionnelle et le fichage drastiquement contrôlé.

Il existe déjà un fichier « d'antécédents » : le casier judiciaire, et un autre pour les enquêtes en cours : les répertoires des bureaux d'ordre pénal.

D'autres étaient-ils nécessaires ? Ils existent et, à défaut d'être supprimés, peuvent être mieux contrôlés.

Pratique

Il est un fait indiscutable : l'augmentation très importante, depuis une quinzaine d'années des fichiers de police et de gendarmerie, liée sans doute, d'une part à l'évolution des technologies, et, d'autre part, à une demande croissante des services de sécurité, liée au développement de nouveaux types de criminalité et au terrorisme.

Cette multiplicité des fichiers rend plus difficile leur contrôle.

De même la multiplicité des sources peut conduire à s'interroger sur la véracité des informations stockées.

Ainsi, en 2002 la CNIL avait demandé la suppression de 37% des données qu'elle avait contrôlées dans le STIC et de 42% de celles contrôlées dans le SIS, *« erronées ou manifestement non justifiées »*.

Dans son rapport 2004, elle indiquait que 26% de ses vérifications avaient donné lieu à rectification d'une erreur au moins.

L'épurement automatique du STIC, installé en octobre de la même année, a entraîné la suppression d'un million deux cent quarante-et-un mille sept cent quarante-deux fiches « mis en cause ».

Pourtant en 2005 sur 467 contrôles effectués sur demandes de particuliers, 207 ont révélé des fichages indus ou erronés.

En outre, STIC et JUDEX sont alimentés par les enquêteurs et le contenu résulte donc de leur appréciation des faits et de la qualification qu'ils leur donnent. *« Mais cette qualification peut être complétée, réformée ou infirmée par l'autorité judiciaire… »* (A. BAUER/C. SOULLEZ – Actualité juridique pénale 2007, p. 70).

La notion *« d'atteinte à la sécurité publique »* retenue pour EDVIRSP est floue et bien entendu variable d'un enquêteur à l'autre.

Cette situation est d'autant plus préoccupante que le nombre de personnes habilitées à consulter ces informations ne cesse de croître (85 000 pour le STIC au 01/01/04 d'après la CNIL).

Les avocats n'ont aucun accès et aucun moyen de vérifier les éléments recueillis par les enquêteurs dans les fichiers, et produit dans les procédures.

Apparaissent des mentions du type « bien connu » ou « défavorablement connu » des services de police qui servent en fait à asseoir une prévention voir une culpabilité.

Le déséquilibre entre défense et accusation, au profit de cette dernière, est encore accentué.

De leur coté les personnes fichées ne le découvrent qu'à la l'occasion d'un refus d'embauche, voir d'un licenciement, d'un refus d'habilitation ou de visa, voir d'une garde à vue.

Propositions

- Seule la Loi, après avis favorable de la CNIL, peut créer un fichier de police ou de gendarmerie (CNCDH., avis sur les nouveaux projets de décrets relatifs aux fichiers des Renseignements Généraux, 6 juin 1991).
- Réduction des délais de conservation, disproportionnés, en particulier au regard des durées de prescription de l'action publique, et mise en place d'une procédure d'effacement identique pour tous les fichiers.
- Promotion du rôle de la CNIL, notamment en renforçant ses moyens.
- Création dans chaque département de relais de la CNIL par l'intermédiaire des conciliateurs de justice.
- Mise en place dans chaque préfecture d'une borne de consultation directe des fichiers par les personnes concernées.
- Création d'une procédure d'injonction de modification(s) en cas de mentions erronée(s) : LRAR à la CNIL qui fera procéder à la modification nécessaire, et, à défaut de réponse de cette dernière ou de refus, saisine du Président du tribunal de grande instance statuant en référé.
- Information des personnes de leur mise en fiche et sur les conséquences que peut entraîner ce fichage.
- Suppression obligatoire et automatique, par le parquet, de toute fiche après décisions de classement sans suite, de non-lieu, de relaxe et d'acquittement, quelles qu'elles soient, immédiatement après l'expiration du délai de recours du Parquet Général.
- Mise en place effective, et au plus vite du système CASSIOPEE, et de l'installation de terminaux d'accès aux fichiers dans les parquets.
- Interdiction des consultations administratives en cas de procédure close par une médiation ou par condamnation pour toute contravention.

Il s'agit de chercher à harmoniser notre législation avec l'article 8 de la Charte des droits fondamentaux de l'UE, ainsi rédigé : *« Toute personne a droit à la protection des données à caractère personnel la concernant. Ces données doivent être traitées loyalement, à des fins déterminées, et sur la base du consentement de la personne concernées ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne à le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification ».*

3. COMMISSION NATIONALE CONSULTATIVE DES DROITS DE L'HOMME (CNCDH)

Les recommandations qui suivent se fondent à la fois sur les avis de la CNCDH sur le sujet et sur les positions qui ont pu être exprimées, sur cette base, lors d'auditions devant des parlementaires, par exemple récemment devant la mission d'information sur les fichiers de police mise en place au sein de la Commission des lois de l'Assemblée nationale.

Ces recommandations sont d'ordre général, dans la mesure où la CNCDH n'a qu'une très partielle connaissance des fichiers de police et de gendarmerie, de leur nombre, de leur contenu, des conditions de leur mise en œuvre et de leur exploitation. Cette très mauvaise connaissance du paysage général des fichiers de police et de gendarmerie est du reste assez partagée – une illustration en a été donnée récemment au sujet du fichage des mineurs - ; ceci est assez préoccupant et incite la CNCDH à recommander qu'une véritable politique de communication soit mise en œuvre, comme cela avait été demandé dans le rapport du groupe de travail de 2006 (recommandations 1 et 2). Il ne serait pas inutile non plus qu'un large débat ait lieu au Parlement, alors que la tendance est celle d'une inflation du nombre de fichiers en même temps qu'un contrôle *a priori* n'est pas exercé par la CNIL.

Dans un contexte d'évolution rapide et remarquable de la technique, la tendance veut que l'on cherche à tirer toujours plus de profit des possibilités que celle-ci offre, alors même que les possibilités d'interconnexions de fichiers, de tris et de croisements de données qui sont collectées en masse ne manquent pas de poser des questions. La CNCDH souhaite rappeler que dans ce contexte, un fichage doit au préalable être précédé d'une réflexion sur son caractère indispensable et qu'il faut veiller à ce que le minimum de données sur le minimum de personnes soient traitées.

Il ne serait en effet pas superflu de rappeler, en exergue de recommandations plus ciblées, quelques principes de base, avant tout ceux de finalité du fichier, et de proportionnalité et de pertinence quant aux données collectées. En outre, des recommandations sur la durée de conservation et les garanties à apporter quant aux destinataires des informations, sur le droit d'accès, de rectification et d'opposition, sur la mise à jour de données exactes et complètes devraient être rappelées dans le rapport du groupe de travail.

Sur la question du fichage des mineurs en particulier, la CNCDH souhaite qu'une recommandation incite à la prudence et que de solides garanties soient apportées au respect des durées de conservation des données et à leur effacement. Les discussions qui ont eu lieu, au cours d'une des réunions du groupe de travail, sur l'examen périodique des données contenues dans un fichier et concernant un mineur, devraient être reprises sous la forme d'une recommandation ; une révision au maximum tous les ans semble à la CNCDH le minimum que l'on puisse demander. Pour autant, la CNCDH reste circonspecte quant à la possibilité de ficher des mineurs et s'interroge sur l'information qui en est faite aux parents ou tuteurs légaux.

Sur certaines informations saisies dans le STIC Canonge relatives au filtre « type » de la partie signalement

La question des types ethno-raciaux ou des données sur les « caractères physiques susceptibles de révéler l'origine raciale ou ethnique », pour reprendre la formule de la CNIL dans son *rapport du 15 mai 2007 sur la mesure de la diversité et la protection des données personnelles*, croise aujourd'hui celle des « statistiques ethniques ». La CNCDH n'a pas rendu d'avis sur la question mais a procédé, dans le cadre des travaux annexes à la publication du rapport annuel sur le racisme, l'antisémitisme et la xénophobie, à un certain nombre d'auditions sur la question. Elle ne s'oppose pas au principe de la mesure de la diversité et se range aux positions exprimées par la CNIL, à savoir que pour le cas particulier des fichiers de police judiciaire utilisés en particulier pour les recherches criminelles, le fait qu'ils comportent des données sur les types ethno-raciaux peut se concevoir au vu de leur finalité. Pour autant, dès lors qu'il s'agit de créer, à des fins de mesure de la diversité, un référentiel national « ethno-racial », elle souhaite insister sur le danger que l'utilisation de critères ethniques à grande échelle pourrait constituer (risque accru de discrimination qui pourrait résulter d'une telle « catégorisation », accentuation des clivages, des préjugés, voire des discriminations au lieu d'aider à les réduire. Mais la progression du métissage dans la population française joue en faveur de cette position de prudence, la pertinence des « types » tels qu'ils existent étant appelée à se réduire.

Reste entière la question particulière du travail de la police lorsqu'elle recherche quelqu'un, question sur laquelle la CNCDH n'est pas particulièrement fondée à se prononcer.

Le fait que les critères ethno-raciaux semblent utilisés dans très peu de fichiers est dans une certaine mesure rassurant. La CNCDH a également entendu les arguments de la police nationale expliquant qu'un Canonge national n'aurait pas d'intérêt en cela qu'il noierait le témoin et que les bases locales qui fonctionnent actuellement correspondent à une échelle réaliste de recherche d'individus, hors les crimes les plus graves.

Reste quelques questions, qui découlent du récit d'utilisations inadéquates du STIC Canonge : pour la catégorie « gitan », qui existe actuellement et correspond à un type méditerranéen[24], il arrive que les modes opératoires et non l'apparence physique soit à l'origine de son choix pour l'inscription dans le fichier. Cet exemple incite la CNCDH à insister à nouveau sur la nécessité de veiller à ce que la formation des « canongistes » et plus largement des personnels de la police fasse l'objet d'une attention particulière et qu'elle soit l'occasion d'interventions, lors de séminaires, de représentants des institutions en charge, en France, de la protection et de la promotion des droits de l'homme, ainsi que de la lutte contre les discriminations.

Sur la question en particulier de la déclinaison des types, il semble difficile de faire d'autres propositions que celles qui ont fait l'objet d'une recommandation dans le rapport de 2006, dans la mesure où celles-là même n'ont pas encore été mises en œuvre. Pour autant, la référence à un type « métis » semble à tout le moins difficilement applicable, sauf à dire qu'elle ferait l'objet d'une définition très précise de la part des formateurs au Canonge et que cette même définition vaudrait pour l'ensemble des destinataires d'informations tirées de ce fichier.

Une possibilité d'identification par nuances de couleur de peau a été proposée. Elle semble ne pas pouvoir se substituer entièrement à celle par « type » dans la mesure où ce qu'il recouvre ne se limite pas à la couleur de la peau.

[24] cf. échange téléphonique entre Judith Klein (CNCDH) et Eric Brendel, le vendredi 28 novembre 2008

4. COMMISSION NATIONALE INFORMATIQUE ET LIBERTES (CNIL)

CNIL.

Le Président

Monsieur Alain BAUER
Président
OBSERVATOIRE NATIONAL DE LA
DELINQUANCE - INHES
CONSEIL D'ORIENTATION
LES BORROMEES
3 AVENUE DU STADE DE FRANCE
93218 SAINT-DENIS-LA-PLAINE CEDEX

Paris, le – 5 DEC. 2008

N/Réf. : AT/YPA/SV/GDP/MMR/ACB/CE081241
A rappeler dans toute correspondance.

Monsieur le Président,

Vous avez souhaité que la CNIL exprime sa position sur les projets de recommandations élaborées dans le cadre des travaux du groupe que vous présidez et qui seront adoptées, en principe, lors de la prochaine séance.

Vous comprendrez aisément que, en tant qu'autorité administrative indépendante, notre Commission ne peut participer à un vote dans le cadre d'un groupe de travail mis en place sous l'égide du pouvoir exécutif.

Je sais que vous ne verrez dans cette position nulle méfiance à l'égard de ces travaux et de vous-même mais la simple traduction de l'esprit même de la loi de 1978 modifiée en 2004.

C'est pourquoi notre représentant, Monsieur Jean-Marie Cotteret, sera présent lors de la prochaine réunion du groupe mais ne participera pas au vote.

Bien entendu, nous sommes toujours disponibles pour apporter, chaque fois que cela est nécessaire, notre appréciation technique dans le cadre de nos compétences. C'est la raison pour laquelle, vous trouverez ci-joint une note technique d'observations sur certaines propositions établies par mes services.

Persuadé que vous comprendrez l'esprit qui anime ma démarche, je vous prie de croire, Monsieur le Président, en l'expression de mes sentiments les meilleurs.

Bien cordialement Alex Türk

Alex TÜRK

PJ

Commission Nationale de l'Informatique et des Libertés
3 rue Vivienne CS 30223 75083 PARIS Cedex 02 - Tél: 01 53 73 22 22 - Fax: 01 53 73 22 00 - www.cnil.fr
RÉPUBLIQUE FRANÇAISE

Observations sur les propositions de recommandations

Note technique

NB : la présente note, élaborée par les services, présente un certain nombre d'observations techniques sur les propositions de recommandations formulées dans la première version du projet de rapport du groupe de travail sur les fichiers de police et de gendarmerie, mis en place par le ministère de l'intérieur. Son contenu ne doit pas être analysé comme l'expression de la position officielle de la CNIL.

Recommandation n°1

La première des recommandations a pour objet l'institutionnalisation du groupe de contrôle sur les fichiers de police et de gendarmerie. A l'appui de cette proposition, il est fait état de la nécessité à ce que les fichiers considérés ne puissent être « *créés et utilisés que dans un cadre strictement défini par la loi et la réglementation et pour une finalité conforme aux principes de proportionnalité et de garantie des libertés individuelles et collectives* ». A cet égard, il convient de rappeler qu'il s'agit d'une prérogative de la CNIL. En effet, en application de l'article 26 de la loi du 6 janvier 1978, modifiée par la loi du 6 août 2004, elle doit notamment être saisie pour avis de tous les projets d'actes réglementaires portant création de ce type de traitements.

De même, conformément à l'article 44 de la même loi, elle procède au contrôle de la mise en œuvre de ces derniers et veille à l'effectivité du droit d'accès des personnes, en application des dispositions des articles 38 et suivants de la loi précitée. A titre indicatif, la Commission a réalisé près de 2 700 vérifications en 2008 et a reçu près de 5 444 demandes de droit d'accès aux fichiers de police cette même année. Dans ces conditions, la création d'un nouvel organisme de contrôle reprenant tout ou partie des missions de la CNIL n'apparaît pas pertinente. En effet, son activité parallèle pourrait à la fois obérer la lisibilité du contrôle des fichiers de police et de gendarmerie et, sans doute, son efficacité.

Recommandation n°2

Le groupe souhaite fournir à la population une information pédagogique sur les fichiers de police, leur utilité etc. Si de telles animations venaient à voir le jour elles devraient être complétées par une information sur le droit des personnes à l'égard de ces fichiers.

Recommandations n°5 et 12

Le groupe de travail appelle de ses vœux la désignation d'un expert « informatique et libertés » au sein des services de police et de gendarmerie (recommandation n°5) et la mise en place d'un contrôleur interne au sein de la DGPN et de la DGGN spécialisé dans la protection des données (recommandation n°12). Si l'on ne peut que souscrire à l'idée selon laquelle il conviendrait de diffuser une « *culture informatique et liberté dans les services opérationnels* », il importe de clarifier le rôle de ces experts et contrôleurs par rapport à celui des correspondants à la protection des données à caractère personnel, tels que définis à l'article 22 de la loi du 6 janvier 1978, et dont le groupe propose la création au sein des directions générales de la police et de la gendarmerie.

Recommandation n°6

Le groupe de travail propose au ministère de l'intérieur de recourir systématiquement aux procédures dites de « déclarations-cadres ». Outre que cette dénomination n'apparaît pas dans la loi « Informatique et Libertés », il paraît utile de préciser que, s'agissant des fichiers de police et de gendarmerie, ceux-ci ne peuvent pas faire l'objet d'une simple déclaration et doivent être autorisés par un acte réglementaire.

Toutefois, il est prévu aux termes du IV de l'article 26 de la loi « Informatique et Libertés » que « *les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires peuvent être autorisés par un acte réglementaire unique* », ce qui va dans le sens de la recommandation considérée. Une telle procédure a d'ailleurs été mise en œuvre pour les fichiers de police municipale, la Commission s'étant prononcée sur un projet d'arrêté correspondant, toujours en attente de publication.

Recommandations n°8 et 9

Elles participent d'une volonté d'amélioration des modalités techniques de contrôle des fichiers de police et de gendarmerie et rejoignent en cela les préoccupations de la Commission, laquelle a notamment obtenu ces dernières années que soient mises en œuvre de véritables politiques de traçabilité des accès auxdits fichiers. Leur mise en œuvre serait d'ailleurs de nature à faciliter l'accomplissement des missions de vérification et de contrôle sur site effectuées par la CNIL. A cet égard, il convient de noter que, au cours de l'année 2008, 1158

demandes de droit d'accès indirect au STIC ont fait l'objet de procédures de vérification sur place et que 19 missions de contrôle du STIC ont eu lieu[25].

Recommandation n°13

Elle évoque la désignation d'un magistrat en charge du contrôle des fichiers d'antécédents judiciaires. Il est nécessaire d'indiquer que la Commission n'a pas été rendue destinataire de l'avant-projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure. Il ne lui est donc pas possible d'apprécier, à ce stade, la portée et les implications de cet article 6, auquel il est fait référence. En tout état de cause, il importerait de clarifier l'articulation de l'action dudit magistrat avec celle de la CNIL, même s'il est souhaitable que les magistrats soient plus étroitement associés au suivi des fichiers d'antécédents judiciaires, en particulier s'agissant de leur mise à jour.

Recommandation n°14

S'agissant du renforcement du contrôle des fichiers d'antécédents judiciaires, la publication prochaine de l'arrêté conjoint du ministre de l'intérieur et du garde des sceaux, cité plus haut, ainsi que d'une autorisation unique prise par la Commission devrait contribuer à fixer un cadre juridique à la mise en œuvre de ces traitements en voie de développement. Par ailleurs, la CNIL procède régulièrement à des missions de contrôle des traitements mis en œuvre par les services de police municipale, soit dans le cadre de son programme annuel de contrôle soit en suite de plaintes.

Recommandations n°15 et 16

S'agissant du développement de la formation des fonctionnaires de police et des militaires de la gendarmerie (recommandation n°15) et, le cas échéant, des agents administratifs (recommandation n°16) en matière de protection des données, l'association plus étroite encore de la CNIL à ce processus paraît nécessaire. La CNIL intervient déjà dans le cadre de la formation dispensée par les écoles de police et est disposée à accroître son investissement.

En ce qui concerne les agents administratifs, il convient de souligner que la possibilité qui leur est donnée, au niveau des SRPJ, de prendre part à la saisie de telle ou telle information dans le STIC ne saurait être envisagée que si elle s'effectue sous l'autorité et le contrôle d'un officier de police judiciaire.

Recommandation n°17

Le groupe de travail recommande de modifier la loi « Informatique et Libertés » afin de permettre la reconnaissance d'une phase d'expérimentation pour les fichiers relevant de son article 26. Il convient de souligner que rien n'interdit actuellement la possibilité de recourir à une phase d'expérimentation. C'est un dispositif expérimental qui a, notamment, été retenu s'agissant du placement sous surveillance électronique mobile (PSEM), du système de pré-plainte en ligne, du fichier des passagers aériens (FPA) ou encore, dans un autre domaine, du dossier pharmaceutique.

En outre, si l'on comprend la nécessité de pouvoir adapter, dans certains cas, les modalités de présentation des dossiers techniques correspondant aux traitements déclarés, la généralisation du recours aux déclarations simplifiées serait de nature à obérer l'effectivité du contrôle *a priori* exercé par la CNIL puisqu'elle ne bénéficierait alors d'aucune information sur les caractéristiques techniques du fichier (son degré de sécurité etc.).

Recommandation n°21

Il convient tout d'abord de rappeler que la CNIL s'est toujours montré réservée sur le principe même de la consultation du STIC à des fins strictement administratives. En outre, compte tenu du nombre déjà très important des agents habilités à consulter les données qu'il contient, une nouvelle extension de la liste des destinataires du traitement pourrait être de nature à accroître les risques d'utilisation abusive.

Recommandation n°25

Dans ses recommandations du 16 mai 2007 sur la mesure de la diversité et la protection des données, la Commission **avait émis de fortes réserves** sur la création d'une nomenclature nationale de catégories « ethno-raciales » et estimé que la décision de principe de créer une telle nomenclature, si elle devait être utilisée de façon obligatoire, relèverait du Législateur, sous le contrôle du Conseil Constitutionnel.

[25] Un rapport général de contrôle du STIC sera d'ailleurs prochainement rendu public.

Recommandation n°26

La Commission a rendu son avis sur le projet de décret en Conseil d'Etat portant création du traitement « EDVIRSP » le 20 novembre dernier. La délibération correspondante sera publiée en même temps que ledit décret. A ce jour et conformément à la loi, il n'est donc pas possible d'en révéler le contenu.

5. HAUTE AUTORITE DE LUTTE CONTRE LES DISCRIMINATIONS (HALDE)

a) Avis sur EDVRISP

Le fichier EDVIGE, tel que prévu dans le décret initial le créant, était destiné à remplacer le fichier « RG » instauré par le décret n°91-1051 du 14 octobre 1991 dans la mesure où il devait l'abroger, à la date du 31 décembre 2009.

Etant donné que le nouveau projet de décret créant le fichier EDVIRSP tient compte, selon les termes mêmes de la Ministre, des différentes observations formulées lors des consultations qu'elle a organisées, on peut penser qu'il est destiné à se substituer au fichier EDVIGE et, lui aussi, à remplacer le fichier « RG » de 1991.

Toutefois, ces hypothèses ne sont pas mentionnées dans le nouveau projet de décret puisque ce dernier ne précise pas s'il modifie, complète ou se substitue à celui de juillet qui a mis en place EDVIGE.

Or, en attendant que le gouvernement procède à l'abrogation du décret n°2008-632 créant EDVIGE, ce dernier est toujours en vigueur et permet la collecte de très nombreuses informations. **Le Collège recommande qu'il soit précisé, dans le nouveau projet de décret, dans quelles conditions le fichier EDVIRSP remplacera le fichier « RG » à partir du 31 décembre 2009 et qu'il soit procédé à la suppression des informations collectées dans EDVIGE qui n'auront plus lieu d'être dans EDVIRSP du fait des modifications que ce dernier instaure.**

La mise en œuvre des fichiers relève du champ de compétence de la Commission nationale de l'informatique et des libertés. Toutefois, dans la mesure où ces données portent notamment sur les opinions politiques, les activités syndicales et les convictions religieuses mais aussi, de manière plus dérogatoire, sur des données sensibles, l'utilisation de ces données était susceptible d'entrer dans le champ de compétence de la haute autorité si elle devait servir de fondement à des décisions administratives défavorables, telles que, par exemple, un refus d'autorisation pour exercer certaines activités.

Or, cette utilisation est prévue par la seconde finalité du fichier EDVIRSP qui autorise, conformément à la loi n°95-73 du 21 janvier 1995 et au décret n°2005-1124 du 6 septembre 2005, le recensement d'informations dans le cadre d'enquêtes administratives pour l'exercice de fonctions soumises à autorisation (emploi de sécurité notamment).

Dans le but de réaliser ces enquêtes, les services de police ont accès aux informations collectées au titre de la première finalité, liée à la sauvegarde de la sécurité publique. A ce titre, des données nominatives sensibles, constituant des critères de discrimination prohibés (origine ethnique et raciale, opinions politiques, religieuses etc.) vont pouvoir être collectées. Il en résulte que, dans la mesure où coexistent en réalité deux fichiers poursuivant des objectifs distincts (enquêtes administratives et sauvegarde de la sécurité publique) dans un unique traitement automatisé, une telle interconnexion peut conduire à fonder des décisions administratives discriminatoires en fonction d'activités militantes jugées potentiellement dangereuses. En d'autres termes, le cœur de compétence de la haute autorité s'exerce sur la seconde finalité du fichier et ce, au regard de la nature des données collectées. Toutefois, au regard des conséquences liées à la connexion, de fait, des deux finalités du fichier, la haute autorité porte également une appréciation concernant la finalité liée à la sécurité publique.

Si des aspects positifs peuvent indéniablement être constatés dans les dispositions du nouveau projet de décret au regard des dispositions du décret créant EDVIGE, son objet - tel que circonscrit par ses deux finalités (1) - demeure néanmoins beaucoup plus large que le fichier « RG » de 1991, et pose problème notamment au regard des données susceptibles d'être recensées (2) et des personnes concernées (3).

1. Des finalités de recensement insuffisamment définies (article 3 du nouveau projet de décret)

Alors que le fichier EDVIGE poursuit trois finalités distinctes, le projet du fichier EDVIRSP ne vise plus que deux d'entre elles, à savoir un objectif lié à la sécurité publique et un objectif d'enquêtes administratives pour l'exercice de certaines fonctions soumises à autorisation.

L'objectif controversé de connaissance, dans le cadre de ce qui est nécessaire au Gouvernement dans l'exercice de ses responsabilités est ainsi abandonné. Pour mémoire, les personnes fichées dans ce cadre étaient celles ayant sollicité, exercé ou exerçant un mandat politique, syndical, économique, social, religieux ou qui jouent un rôle institutionnel significatif.

S'il convient de prendre acte de cette disparition, comme des précisions données concernant les deux autres finalités au regard de la protection du droit à la vie privée, il n'en demeure pas moins que le double objet du fichier EDVIRSP reste beaucoup plus large que celui du fichier « RG » de 1991. Il convient d'analyser le

risque de discrimination lié à la deuxième finalité et si l'ingérence dans la vie privée est suffisamment justifiée ou, au contraire, excessive au regard des articles 8 et 14 de la CEDH.

a) Un objectif d'enquêtes administratives pour l'exercice de certaines fonctions soumises à autorisation)

Selon le décret de 1991, les enquêtes menées devaient *« apprécier la vulnérabilité des personnes [sollicitant de telles autorisations] à des pressions exercées par des personnes susceptibles [elles-mêmes] de porter atteinte à la sûreté de l'Etat ou à la sécurité publique »*.

Dans le fichier EDVIGE, les conditions et la nature des enquêtes administratives susceptibles d'être réalisées dans ce cadre, ainsi que les fonctions pour lesquelles la Direction centrale de la sécurité publique **(**DCSP) peut faire de telles enquêtes, ne sont pas précisées. En conséquence, la limite de conservation des données à 5 ans, à ce titre, n'est pas une véritable garantie.

Le dernier alinéa de l'article 3 du projet de décret instituant EDVIRSP apporte ces précisions en mentionnant que ces enquêtes sont celles réalisées dans le cadre des dispositions de l'article 17-1 de la loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité dont le décret d'application[26] énumère les enquêtes administratives donnant lieu à la consultation de traitements automatisés de données personnelles. Il s'agit :

- des emplois publics participant à l'exercice des missions de souveraineté de l'Etat ;
- des emplois privés ou publics relevant du domaine de la sécurité ou de la défense ;
- les activités ou emplois privés réglementés relevant des domaines des jeux, paris et courses ;
- les autorisations d'accès à certaines zones en raison de l'activité qui s'y exerce (zones militaires, aérodromes, zones portuaires) ;
- la fabrication, la production ou le port de matériels présentant un danger pour la sécurité publique (explosifs, armes etc.).

Les emplois, ainsi que les personnes concernées, se chiffrent en centaines de milliers.

Certes, cette précision circonscrit les possibilités de constituer une « fiche » à l'occasion d'enquêtes administratives, il n'en demeure pas moins qu'au regard du décret de 2008 instituant EDVIGE, tout comme au regard du projet de décret instituant EDVIRSP, l'objet de ces enquêtes s'est sensiblement élargi. Il s'agit désormais de déterminer si *« le comportement des personnes intéressées est compatible avec l'exercice des fonctions ou des missions envisagées »*, ce qui implique un contrôle plus approfondi que celui prévu par le décret de 1991 qui était, l'*« appréciation de la vulnérabilité des personnes sollicitant de telles autorisations à des pressions exercées par des personnes susceptibles elles-mêmes de porter atteinte à la sûreté de l'Etat »*.

En conséquence, les informations recherchées pourront être plus étendues et porteront davantage atteinte au droit au respect de la vie privée. Cet état de fait est d'autant plus préoccupant que ces informations (religion, origine ethnique etc.) pourraient, en outre, fonder des décisions administratives de refus d'agrément ou d'autorisation et conduire à des entraves à une activité économique.

Or, la possibilité d'enquête et d'utilisation de données sensibles pour les réaliser, pourra se faire tant dans le cadre d'activités susceptibles de porter vraisemblablement atteinte à la sécurité publique (détention d'explosifs, fonctionnaires de police) que d'activités plus communes, telles celles des fonctionnaires des finances, voire « légères » en matière de sécurité, comme l'autorisation de faire courir des lévriers de courses ou l'agrément des arbitres des parties de pelotes basques (Cf. article 1er II du décret n°2005-1124 cité en note de bas de page).

Cet état de fait appelle deux observations. En premier lieu, on peut s'interroger sur la pertinence d'enquêtes administratives rendues nécessaires pour certaines activités dont on voit mal en quoi elles sont particulièrement susceptibles de porter atteinte à la sécurité publique. En second lieu, il peut être déduit du fait que la deuxième finalité du fichier EDVIRSP n'étant pas entièrement liée à un objectif de sécurité publique, deux fichiers poursuivant des objectifs distincts cohabitent, en réalité, dans un unique traitement automatisé. Ceci semble, d'une part, contraire au principe de spécialité des finalités des fichiers au regard de la loi Informatique et Libertés mais, d'autre part et surtout, de nature à permettre une interconnexion de fait qui peut conduire à fonder des décisions administratives discriminatoires en matière d'emploi notamment fondées sur des activités militantes jugées potentiellement dangereuses.

[26] Décret n°2005-1124 du 6 septembre 2005 fixant la liste des enquêtes administratives donnant lieu à la consultation des traitements de données personnelles.

Au demeurant, une fois que le rapport de police - rapport de moralité - est diffusé à l'autorité administrative compétente pour apprécier si le comportement de la personne est compatible avec les fonctions sollicitées et fonder sa décision, les éléments qu'il contient échappent au dispositif de contrôle prévu par le fichier de police lui-même *(Cf. recommandations infra, p. 9, c).*

b) Un objectif lié à la sécurité publique

Pour mémoire, la finalité liée à la sécurité publique dans le fichier de 1991 autorisait le fichage de *« personnes qui peuvent, en raison de leur activité individuelle ou collective, porter atteinte à la sûreté de l'Etat ou à la sécurité publique par le recours ou le soutien actif apporté à la violence ».*

L'article 3 du nouveau projet de décret créant EDVIRSP apporte quelques précisions au regard de ce qui était prévu dans EDVIGE puisqu'il ne vise que les personnes dont *« l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique ».* La notion de « groupe » disparaît même si la notion « d'activité collective » tend à l'en rapprocher. L'avancée la plus importante réside dans le fait que ces personnes seront fichées pour le trouble que leur activité est susceptible de porter atteinte à la *sécurité* publique et non plus à l'*ordre* public, notion bien plus large.

Le champ recouvert par les termes *« activité (…) indiquant qu'elles peuvent porter atteinte à la sécurité publique »* demeure néanmoins beaucoup plus vaste que celui du fichier « RG » de 1991. En effet, si le motif d'entrée dans le fichier relatif au *« risque d'atteinte à la sécurité publique »* existait déjà dans le précédent traitement automatisé de 1991, il était bien plus précis : cette atteinte éventuelle, potentielle à la sécurité publique était définie par le type d'action utilisé par les personnes, à savoir le recours ou le soutien actif à la violence, ce qui ne constitue en aucun cas *toute* atteinte à la sécurité publique.

Bien au contraire, la sécurité publique se définissant[27] comme *« l'élément de l'ordre public caractérisé par l'absence de périls pour la vie, la liberté ou le droit de propriété des individus »*, il peut lui être porté atteinte (ou risqué de lui être porté atteinte), en l'absence de tout recours ou soutien actif à la violence.

Par ailleurs, la suppression de la notion de *« sûreté de l'Etat »,* présente en 1991, renforce le sentiment d'abaissement du niveau de risque potentiel que doivent constituer les individus pour être fichés.

La notion floue de risque d'atteinte à la sécurité publique, en l'absence de définition plus précise, contient des risques d'appréciations et d'interprétations très subjectives de la part des personnes compétentes pour un tel recensement. Concrètement, l'ensemble du mouvement social (militantisme syndical, associatif et politique) risque d'être jugé comme potentiellement attentatoire à la sécurité publique et, de ce fait, légitimement fiché. C'est d'ailleurs ce que vise explicitement la ministre de l'Intérieur dans la note explicative du fichier EDVIGE qu'elle a jointe à la haute autorité pour justifier la prise en compte des mineurs dans le recensement : *« cette évolution résulte de la place accrue des jeunes dans le militantisme et dans les formes organisées de délinquance ».*

Pour la Cour européenne des droits de l'Homme, une ingérence de cette nature dans la vie privée doit être prévue par la loi, étant entendu que la forme juridique de cette base en droit importe peu (un décret peut être conforme à cette exigence), à condition que cette « loi » soit accessible et prévisible pour le justiciable. Pour ce faire, la Cour a considéré que la phrase *« prévue par la loi » « ne se borne pas à renvoyer au droit interne mais concerne aussi la qualité de la loi. (...). Le droit interne doit offrir une certaine protection contre les atteintes arbitraires de la puissance publique aux droits garantis par la Convention. Or, le danger d'arbitraire apparaît avec une netteté singulière là où un pouvoir de l'exécutif s'exerce en secret (…) elle doit définir l'étendue et les modalités d'exercice d'un tel pouvoir avec une netteté suffisante - compte tenu du but légitime poursuivi – pour fournir une protection adéquate contre l'arbitraire ».*

Or, le décret attaqué, faute de définir avec une précision suffisante, l'étendue et les conditions du fichage des personnes visées au regard des finalités poursuivies, ne semble pas apporter les garanties adéquates et suffisantes de nature à satisfaire les exigences de l'article 8 de la CEDH. Dans la mesure où l'atteinte aux libertés individuelles protégées par l'article 8 est réalisée à partir d'éléments qui tombent sous l'empire de l'article 14 de la Convention, elle revêt, de surcroit, un caractère discriminatoire.

En l'absence de toute définition des activités indiquant qu'elles peuvent porter atteinte à la sécurité publique, le fichier EDVIRSP est indéniablement doté d'une finalité bien plus large que son prédécesseur de 1991. **Le Collège considère que l'ingérence dans la vie privée permise par ce nouveau fichier est excessive concernant ce premier objectif, et recommande que la formule du décret de 1991 soit reprise *in extenso*, ce qui conduirait à encadrer davantage la possibilité de collecter des informations - parfois constitutives de données sensibles - par les services concernés.**

[27] Gérard Cornu, *Vocabulaire juridique*, PUF

L'insuffisance de la définition de ces finalités pose d'autant plus problème que, pour la poursuite de ces dernières, des données sensibles revêtant un caractère discriminatoire vont pouvoir être enregistrées dans le fichier.

2. Des données sensibles revêtant un caractère discriminatoire enregistrées dans le traitement automatisé EDVIRSP (articles 2 et 4 du décret)

La nature des données collectées (a), leur conservation (b), leurs destinataires (c) et la possibilité d'y accéder et/ou de les modifier (d) sont susceptibles d'entrer en contradiction avec les stipulations des articles 8 et 14 de la CEDH.

a) La nature des données susceptibles d'être collectées

L'article 1er du projet de décret instituant EDVIRSP, à l'instar du décret de 1991, rappelle l'interdiction qui pèse sur les services de police compétents en matière de renseignements, résultant du I de l'article 8 de la loi du 6 janvier 1978, *« de collecter ou de traiter des données à caractère personnel qui font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci »*.

Le fichier « RG » de 1991 permettait, par dérogation à ce principe, de collecter et conserver des informations nominatives sensibles limitativement énumérées, à savoir :

- les signes physiques particuliers, objectifs et inaltérables (ces informations ne pouvaient être collectées qu'au titre des personnes susceptibles de porter atteinte à la sécurité publique, pas au titre des enquêtes administratives)
- les activités politiques, philosophiques et religieuses ou syndicales (quelle que soit la finalité poursuivie par le fichier).

Le fichier EDVIRSP instaure quant à lui une dérogation bien plus large par la possibilité, offerte à l'article 4 du projet de décret, de collecter et conserver des informations nominatives personnelles et ce, quelle que soit la finalité du fichier[28], à savoir :

- les informations ayant trait à l'état civil et à la profession, adresses physiques, numéros de téléphone et adresses électroniques ;
- signes physiques particuliers et objectifs, photographie ;
- activités publiques, comportements et déplacements ;
- titres d'identité ;
- immatriculation des véhicules ;
- informations patrimoniales ;
- antécédents judiciaires ;
- données relatives à l'environnement de la personne, notamment aux personnes entretenant ou ayant entretenu des relations directes et non fortuites avec elle.

En outre, la dérogation s'ouvre à l'ensemble des données dites sensibles, sans énumération et par simple renvoi à l'article 8[29] de la loi CNIL, à l'exception des données liées à l'orientation sexuelle et la santé (collecte que permet actuellement le décret instituant EDVIGE).

Au regard du projet de décret, cette possibilité de collecter et conserver ces données sera effective tant pour les personnes susceptibles de porter atteinte à la sécurité publique que pour celles faisant l'objet d'une enquête administrative. Il s'agit :

- des origines raciales ou ethniques ;
- des opinions politiques, philosophiques, religieuses.

[28] A l'exception, en ce qui concerne la finalité liée aux enquêtes administratives des signes physiques, des déplacements et de l'immatriculation des véhicules

[29] Pour mémoire, l'article 8 I de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés dispose : *« il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou la vie sexuelle de celles-ci »*.

La notion de « signes physiques distinctifs objectifs », utilisée par le décret de 1991, ne recouvre pas la notion d' « origines raciales ou ethniques », désormais opérationnelle depuis la création du fichier EDVIGE : inscrire qu'une personne a la peau noire dans un but de reconnaissance plus aisée par les forces de police ne revient pas, ni en termes d'atteinte à sa vie privée, ni en termes d'utilisations de données sensibles, à rechercher, puis inscrire son origine dite raciale en créant une catégorie comme, par exemple, « Afrique subsaharienne » ou « Antilles ».

Or, l'objet du projet de décret est bien d'offrir la possibilité de mentionner, indépendamment de tout signe physique objectif, l'origine ethnique ou « raciale » des personnes fichées et ce, alors même qu'elles font l'objet d'une simple enquête administrative en vue d'exercer certaines fonctions. En effet, dans le cas contraire, l'article 2 du projet de décret aurait explicitement exclu la possibilité de collecter une telle donnée, à l'image de ce qu'elle a fait concernant l'orientation sexuelle et la santé.

En outre, l'autorisation de collecter et conserver des informations relatives aux *opinions* politiques, philosophiques et religieuses diffère de celle existant dans le fichier « RG » de 1991 qui prévoyait que les *activités* politiques, philosophiques et religieuses puissent être prises en compte. Enquêter puis mentionner les *opinions*, notion relevant du for intérieur de chacun, est indéniablement plus attentatoire aux libertés que mentionner les *activités* de cet ordre qui, par la force des choses, ont davantage un caractère public.

Enfin, en 1991, qu'il s'agisse des données objectives ou des activités politiques, philosophiques et religieuses, le décret posait, en son article 4, une interdiction d'en faire état dans les rapports d'enquêtes administratives ou de moralité. Cette garantie d'absence de diffusion de données si personnelles au-delà des seules forces de police compétentes en la matière est absente du projet de décret créant EDVIRSP. L'atteinte portée au droit fondamental au respect de la vie privée semble, d'une part, excessive au regard des buts recherchés (la reconnaissance physique d'une personne ou la vérification de la compatibilité de ses activités avec certaines fonctions) et, d'autre part, susceptible de créer une stigmatisation à portée discriminatoire pour les individus qui en font l'objet.

Il résulte de ce qui précède que le Collège recommande, en premier lieu, d'exclure de la dérogation prévue à l'article 2 du projet de décret les données liées à l'origine ethnique des personnes fichées, à l'instar de ce qui est prévu pour les données relatives à la santé ou la vie sexuelle des intéressés. Il s'avère que la notion de « signes physiques particuliers et objectifs » est suffisante pour parvenir aux buts poursuivis par le traitement automatisé.

En second lieu, le Collège recommande que le cadre de la dérogation prévue pour les données relatives aux opinions politiques et religieuses soit précisé dans un sens plus restrictif en liant ces données, non seulement à une activité et non plus aux seules opinions, mais aussi à l'activité violente ou extrémiste. Seule la collecte et la conservation de ces données permettraient de ne pas excéder le but poursuivi par le fichier.

Enfin, le Collège recommande que les données relatives aux comportements et aux déplacements ne soient pas collectées au titre de la seconde finalité du fichier.

b) Conservation de ces données et les destinataires du traitement

Dans le cadre qui vient d'être décrit, la durée de 5 ans de conservation de ces données dans l'hypothèse d'un fichage pour enquête administrative paraît excessive, notamment en raison du fait que ce délai court à compter de la fin de l'enquête administrative (pour une personne qui n'aura finalement pas été autorisée) ou bien à compter de la cessation des activités (pour une personne ayant exercé les fonctions sollicitées), ce qui peut représenter plusieurs décennies.

L'objectif du recensement des informations étant d'apprécier la compatibilité du comportement de la personne avec les fonctions ou missions sollicitées, **le Collège recommande que ces informations soient détruites dans un délai plus bref, par exemple deux ans, et ce, à compter de la décision administrative adoptée, alors que le texte actuel permet cette conservation pendant une durée qui peut dépasser 40 ans si les informations portent sur un fonctionnaire effectivement recruté à l'issue de l'enquête administrative.**

En ce qui concerne les informations collectées dans le cadre de la finalité liée à la sécurité publique, aucun délai de conservation n'est mentionné, ce qui paraît, *a fortiori*, disproportionné au regard du but recherché. Quelles seront en effet l'utilité et la pertinence d'informations relatives au passage momentané d'une personne, devenue âgée, dans un mouvement susceptible de porter atteinte à la sécurité publique ?

c) Les destinataires de ces informations

Au regard de l'article 6 du projet de décret, les destinataires de l'ensemble de ces informations sont bien plus nombreux dans EDVIRSP qu'ils ne l'étaient dans le fichier de 1991 (article 5).

En dehors des fonctionnaires de police appartenant aux services de renseignements et dûment habilités, le projet de décret prévoit que le fichier EDVIRSP peut être consulté par tout agent de la police nationale et de la gendarmerie (en 1991, il s'agissait « des services de police et de gendarmerie »), sur demande expresse de son chef de service (en 1991, la demande ne pouvait être agréée que par « le Directeur central ou le responsable du service départemental des RG »).

Bien évidemment, la diffusion à un plus grand nombre de personnes de telles données personnelles est de nature à renforcer l'atteinte au droit au respect à la vie privée protégé par l'article 8 de la CEDH.

Le rétablissement de la garantie de traçabilité posée à l'article 9 du projet de décret, qui avait disparu pour le fichier EDVIGE, et selon laquelle les consultations du fichier EDVIRSP font l'objet d'un enregistrement comprenant l'identifiant du consultant, la date et l'heure de la consultation et la conservation de ces éléments pendant deux ans peut dissuader les consultations abusives de telles données.

Cette garantie est cependant à relativiser dans la mesure où les données mobilisées par un agent de police sont nécessairement communiquées à l'autorité administrative compétente pour fonder la décision envisagée.

En conséquence le Collège recommande que des garanties de traçabilité et de destruction des données, comparables à celles imposées aux services de police, soient prévues à l'égard du destinataire final (l'administration par exemple) lequel reste en possession, en dehors de tout contrôle, des données qui lui ont été transmises.

d) Droit d'accès et de rectification des informations.

Plus un droit d'accès et de rectification de ces données personnelles - et parfois sensibles - est aisé pour les citoyens, plus il est de nature à atténuer le caractère excessif des atteintes à la vie privée auquel un tel fichier peut conduire.

Or, force est de constater que l'article 8 du nouveau projet de décret reprend l'article 5 du décret créant EDVIGE en affirmant que le droit d'accès aux données du fichier s'exerce de manière indirecte, par l'intermédiaire d'un commissaire de la CNIL qui effectue les investigations utiles et fait procéder aux modifications nécessaires, par exemple la rectification ou l'effacement de données inexactes et ce, conformément à l'article 41 de la loi Informatique et Libertés concernant les fichiers de police et de gendarmerie. Pour les autres fichiers, l'article 39 de la même loi prévoit un accès direct auprès du responsable du fichier.

Pourtant, dans la mesure où le troisième paragraphe de l'article 41 prévoit une dérogation au principe de l'accès indirect aux informations détenues dans les fichiers de police et de gendarmerie *« lorsque la commission constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'Etat, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant »*, **le Collège recommande que soit prévu, en amont, dans le décret, cet accès direct concernant les données recensées au titre de la deuxième finalité du fichier (enquêtes administratives) par la personne qui sollicite l'autorisation ou l'agrément.**

En effet, il est regrettable que, parallèlement à un renforcement considérable des informations contenues dans le fichier, rien de nouveau n'ait été créé en matière de contrôle du traitement automatisé et de protection des droits des citoyens ce qui serait pourtant de nature à rendre moins disproportionnée l'ingérence réalisée dans leur vie privée.

Par ailleurs, **le Collège recommande que le Gouvernement informe systématiquement les candidats à des fonctions et/ou missions pouvant faire l'objet d'une enquête administrative qu'ils seront inscrits dans le fichier de police EDVIRSP ainsi que les objectifs de ce dernier, la durée d'inscription des données, les modalités de consultation, de modification et d'effacement de celles-ci dont elle pourrait user.**

Les personnes visées par le fichier. Le cas des mineurs (article 2 du projet de décret)

Alors que le fichier « RG » de 1991 permettait la collecte, la conservation et le traitement de données nominatives pour les seuls majeurs, le fichier EDVIGE, tout comme le projet de décret instituant EDVIRSP autorise un traitement concernant des mineurs de plus de 13 ans et ce, en dehors de toute condamnation pénale ou simple mise en cause.

Certes, la limite importante précisée dans le projet de décret instituant EDVIRSP doit être notée, à savoir la conservation de ces données jusqu'à la majorité des enfants, l'effacement de ces données, ayant lieu à cette

date. Ce « droit à l'oubli », non prévu dans EDVIGE, est d'autant plus légitime qu'un mécanisme comparable existe, à certaines conditions, pour les mentions dans le casier judiciaire et ce, afin de préserver notamment l'avenir professionnel des mineurs. Toutefois, cet effacement peut être reporté aux 21 ans de l'intéressé si un nouvel élément, justifiant un nouvel enregistrement intervient entre ses 16 et 18 ans.

L'ensemble des critiques exposées dans cette note sont *a fortiori* valables pour les mineurs. En dehors des réserves émises par la Défenseure des enfants dans son avis précité, le Comité des droits de l'Homme (organisme compétent pour l'application du Pacte international relatifs aux droits civils et politiques) a lui-même, par décision du 22 juillet 2008, estimé que seul le fichage des mineurs délinquants pouvait répondre à un objectif raisonnable aux regard des stipulations du Pacte.

Le Collège de la haute autorité recommande l'abandon du fichage des mineurs dont les activités indiquent qu'ils sont susceptibles de porter atteinte à la sécurité publique.

b) Avis sur le STIC-CANONGE

L'avis de la haute autorité a été sollicité par le groupe de travail sur les fichiers de police et de gendarmerie concernant la rubrique « signalement » du fichier STIC-Canonge. Outre les six rubriques principales peuvent qui peuvent être renseignées (état civil ; sexe ; âge, taille ; surnom et alias ; fait historique ; signalement ; pilosité, yeux, cheveux ; signes particuliers ; photos anthropométriques), une partie « signalement » comporte un filtre sur le « type », lequel distingue 12 types différents :

- Blanc (caucasien) ;
- Méditerranéen ;
- Gitan ;
- Moyen-oriental ;
- Nord africain Maghrébin ;
- Asiatique Eurasien ;
- Amérindien ;
- Indien (Inde) ;
- Métis-Mulâtre ;
- Noir ;
- Polynésien ;
- Mélanésien-canaque.

Dans le cadre de l'instruction menée dans le dossier Edvige, le Président de la haute autorité a réaffirmé que la mise en œuvre des fichiers relevait du champ de compétence de la Commission nationale de l'informatique et des libertés. Il a toutefois rappelé que, dans la mesure où ces données portent notamment sur les opinions politiques, les activités syndicales et les convictions religieuses mais aussi, de manière plus dérogatoire, sur des données sensibles, l'utilisation de ces données était susceptible d'entrer dans le champ de compétence de la haute autorité si elle devait servir de fondement à des décisions administratives défavorables, telles que, par exemple, un refus d'autorisation pour exercer certaines activités. L'article 1er de la loi n°2004-1486 portant création de la haute autorité dispose en effet que cette dernière est compétente pour connaître de toutes les discriminations, directes ou indirectes, prohibées par la loi ou par un engagement international auquel la France est partie.

Les risques de généralisation de l'utilisation de tels « types » dans le travail quotidien des services de police conduisent la haute autorité à se prononcer sur l'avis sollicité par le groupe de travail.

En matière de fichiers de police, la haute autorité a déjà eu à se prononcer, dans la délibération 2008-233 du 20 octobre 2008, aux termes de laquelle le Collège a recommandé d'exclure de la dérogation prévue à l'article 2 du projet de décret les données liées à l'origine ethnique des personnes fichées. Il a précisé que la notion de « signes physiques particuliers et objectifs » était suffisante pour parvenir aux buts poursuivis par le traitement automatisé.

En l'espèce, la question qui se pose est celle de la définition des « signes physiques particuliers et objectifs ».

Or, à l'occasion de sa première réunion en 2006, le groupe de travail sur les fichiers avait préconisé une nouvelle déclinaison :

- type européen (nordique, caucasien, méditerranéen) ;
- type africain/antillais ;
- type métis ;
- type maghrébin ;
- type moyen-oriental ;
- type asiatique ;
- type indo-pakistanais ;
- type latino-américain ;
- type polynésien.

A ce jour, et au vu des éléments échangés au sein du groupe de travail, les services de police n'ont pas mis en œuvre cette nouvelle liste et ce, pour des problèmes techniques (difficulté à requalifier le stock des données par ces nouveaux types).

La typologie ainsi proposée, comme celle qui existe déjà, fait davantage référence à l'origine dite « ethnique » des personnes qu'à leurs caractéristiques physiques objectives.

La reprise du terme « latino-américain » utilisé aux Etats-Unis et en Grande-Bretagne pour définir une catégorie ethno-raciale semble particulièrement éloquente à ce sujet, tout comme le type « africain/antillais » qui s'apparente plus à l'origine réelle ou supposée des intéressés qu'à leur description physique.

En outre, rien n'interdit que la collecte de ces données permette de réaliser des statistiques à partir d'informations présentes dans le STIC tendant à établir, par exemple, que l'appartenance à telle origine ethnique est sur-représentée parmi certains auteurs de crimes ou délits.

Or, en dehors des fichiers de police, la haute autorité a également formulé un avis sur les fichiers d'une autre nature, notamment ceux de gestion, dans les entreprises. Dans la délibération n°2006-31 du 26 février 2006, **le Collège affirmait son opposition aux comptages ethniques et précisait que devaient *« notamment être prohibés tous dispositifs basés sur des données anthropomorphiques ».***

En conséquence, **la haute autorité réitère ses recommandations initiales, issues de la délibération de février 2006 précitée, en matière d'utilisation de données sensibles liées à l'origine collectées par les fichiers de police et donne donc un avis défavorable à la classification proposée.**

c) Courrier du Président de la HALDE à Alain Bauer

Le Président

Paris, le 8 décembre 2008

N/Réf : AD /2008-4234-001

Monsieur le Président,

Par courrier du 2 octobre 2008, vous avez invité la haute autorité de lutte contre les discriminations et pour l'égalité à participer au groupe de travail sur les fichiers de police et de gendarmerie mis en place en juin 2006 par Monsieur Nicolas SARKOZY, alors Ministre de l'Intérieur, et réactivé en septembre dernier par son successeur, Madame Michèle ALLIOT-MARIE.

Dans le cadre de cette réflexion, la haute autorité a eu l'occasion de remettre deux avis au groupe de travail, l'un portant sur le projet de décret instituant le fichier EDVIRSP, l'autre concernant la classification du type « signalement » dans le fichier STIC-Canonge.

Mercredi 3 décembre 2008, vous avez bien voulu transmettre à la haute autorité un avant-projet du rapport qui sera remis à Madame la Ministre et qui recensera les recommandations formulées par le groupe.

A ce stade de la rédaction du rapport, les avis donnés par la haute autorité figurent dans la partie intitulée « expressions libres » et non dans celle dédiée aux « recommandations », ce qui ne permet pas suffisamment de souligner les divergences d'appréciations qui existent entre les avis formulés par la haute autorité et les préconisations du groupe, adoptées à la majorité de ses membres.

En premier lieu, j'appelle votre attention sur plusieurs points concernant les recommandations relatives au fichier EDVIRSP, page 11 du pré-rapport.

Les développements relatifs à l'utilisation des données personnelles liées à l'origine et aux opinions politiques, philosophiques ou religieuses (article 2 du décret EDVIRSP) vont dans le sens des préconisations de la haute autorité dans sa délibération n°2008-233 du 20 octobre 2008 qui vous avait été notifiée.

En revanche, sur plusieurs points, certaines dispositions méritent d'être précisées et ce, dans le corps même du texte relatif aux recommandations. En effet, l'absence de mention selon laquelle le groupe ne s'est prononcé qu'à la majorité, et non à l'unanimité de ses membres, laisse penser que l'ensemble des membres partagent les recommandations préconisées, ce qui n'a pas été le cas.

Ainsi, la proposition tendant à modifier l'article 3 du décret EDVIRSP pour réintroduire la finalité « personnalités » qui était présente dans le fichier EDVIGE, mais avait disparu dans EDVIRSP, est contraire aux recommandations de la haute autorité adoptées par la délibération n°2008-233 précitée. L'argument selon lequel cette réintroduction dans le décret permettrait d'éviter l'existence de fichiers non déclarés ne permet pas de considérer que les recommandations du Collège n'ont pas à être maintenues.

En conséquence, il me paraît important qu'à la fin du paragraphe sur l'article 3 du décret EDVIRSP page 11, soit précisé la phrase suivante : « La HALDE s'était au contraire félicitée de l'abandon de la finalité liée aux "personnalités" et considère que le mélange des finalités visant des catégories de personnes fichées pour des raisons différentes dans EDVIRSP est éminemment dangereux ».

De même, concernant l'enregistrement des mineurs, les recommandations du groupe sont bien en-deçà de celles de la haute autorité qui avait préconisé, dans la même délibération, l'abandon de leur fichage. Il est en effet écrit dans le pré-rapport que la question devant se poser pour le groupe de travail porte davantage sur la protection renforcée dont doivent bénéficier les mineurs enregistrés que sur le principe même de leur enregistrement.

Je suis attaché à ce qu'à la fin de cette phrase, page 11, il soit mentionné l'indication suivante : « à l'exception de la HALDE qui préconise l'abandon du fichage des mineurs dans le cadre de ce fichier de police administrative ».

Par ailleurs, à la fin de la page 11, il devrait être ajouté que la haute autorité a eu l'occasion de se prononcer sur d'autres aspects du même fichier, notamment en ce qui concerne les règles d'accès aux données et de traçabilité des rapports de moralité dans le cadre des enquêtes administratives.

De manière générale, la HALDE demande à ce que soit mieux garanti et facilité le droit d'accès aux différents fichiers par les personnes concernées et que soient précisées les règles de sécurité et de traçabilité des rapports de moralité ou enquêtes administratives réalisées à partir, notamment, du fichier EDVIRSP.

Enfin, pour chacune de ces mentions, il serait opportun que le rapport renvoie aux textes de la haute autorité, publiés dans le chapitre « expressions libres » qui pourrait plus légitimement être intitulé « observations des membres du groupe ».

Concernant, en second lieu, l'avis relatif au signalement du fichier STIC-Canonge, page 10, les développements y afférant sont conformes à l'avis de la haute autorité en ce qui concerne le refus de toute classification ethno-raciale ainsi que toute utilisation des données en vue de la constitution d'un outil statistique basé sur ces données.

Il est toutefois mentionné que le groupe de travail a préconisé, à la majorité, l'utilisation corrigée de la classification du type « signalement » dans le fichier STIC-Canonge, telle qu'adoptée par le groupe de travail de 2006.

Je vous saurais gré de faire préciser, à cet endroit du texte, que la HALDE a donné un avis défavorable à cette classification, avec un renvoi aux contributions de cette dernière dans le chapitre « expressions libres ». La HALDE ne peut en effet considérer que la classification proposée institue un outil fondé sur des critères objectifs.

De plus, la HALDE préconise que soit établie une liste exhaustive et unique des fichiers de police et de gendarmerie, soumise aux contrôles et garanties de traçabilité et d'accès. La haute autorité souhaite que

puisse être étudié l'effacement dans les fichiers des informations quand elles ne seront plus nécessaires : par exemple les signes physiques concernant les personnes pour lesquelles une photo est obtenue.

Enfin, il me paraît indispensable que chaque fois qu'une information figurant dans un fichier, même couvert par le secret défense, est utilisée pour refuser un droit ou l'accès à un emploi à une personne, une procédure adéquate préalablement définie et dont la personne serait informée permette à un magistrat habilité de vérifier le bien fondé de ce refus au regard de l'information collectée dans le fichier.

Je vous prie d'agréer, Monsieur le Président, l'expression de mes sentiments les meilleurs.

Louis SCHWEITZER

6. LIGUE INTERNATIONALE CONTRE LE RACISME ET L'ANTISEMITISME (LICRA)

La LICRA reconnaît les arguments relatifs à la recherche de l'efficacité du travail d'enquête et d'instruction des instances de police judiciaire, de police administrative et de gendarmerie.

La LICRA est d'autant plus sensible qu'une partie de son action est consacrée à une activité judiciaire aux côtés des victimes de racisme ou de discrimination, dans le cadre de laquelle la recherche des preuves est difficile. Ainsi, son action dépend étroitement de l'efficacité judiciaire en matière d'enquête.

La LICRA entend néanmoins présenter six recommandations concernant les fichiers afin de mieux ménager le délicat équilibre entre les nécessités de la protection des personnes et les impératifs de garantie des libertés publiques.

a) Concernant la classification par « type »

La LICRA souhaite que les fichiers s'en tiennent à un recueil neutre et objectif des données concernant les personnes.

La LICRA s'oppose formellement à la classification actuelle dans le STIC CANONGE d'une déclinaison des personnes en 12 « types », à savoir : Blanc (caucasien), Méditerranéen, Gitan, Moyen-Oriental, Nord africain Maghrébin, Asiatique eurasien, Amérindien, Indien (Inde), Métis-mulâtre, Noir, Polynésien, Mélanésien-canaque.

Cette classification est une déviance inquiétante en ce qui concerne le respect des libertés et, en tout état de cause, elle ne peut conduire à un résultat efficace de l'action policière au regard des finalités d'information générale poursuivies.

En premier lieu, cette classification par « type » n'a aucun sens d'un point de vue ethnologique et conduit à l'admission d'une typologie raciale de l'humanité qu'il convient de combattre fermement.

En second lieu, cette classification ne peut que conduire à des errements et à l'inefficacité puisque fondée sur des évaluations empreintes de la subjectivité de celui qui doit les utiliser.

En dernier lieu, cette classification ne revêt aucune pertinence puisque le même STIC CANONGE permet le signalement des personnes mises en cause ou des victimes en fonction de critères plus neutres et, certainement, plus objectifs, tels que la classification par : sexe, âge apparent, taille, corpulence, cheveux, couleur des yeux, signe particulier.

Quant au fichier JUDEX, les données à caractère personnel se rapportent à des signes physiques particuliers, objectifs et permanents. Ces signes physiques particuliers et objectifs sont suffisants pour remplir les objectifs d'efficacité dans la recherche et l'identification de la personne.

La LICRA recommande donc que les fichiers ne retiennent plus ces classifications par « type » et que de telles données soient supprimées des fichiers à archiver ou à supprimer.

b) Concernant les données relatives aux origines raciales et ethniques

La LICRA s'oppose fermement au recueil de données relatives aux origines raciales et ethniques des personnes dans tous les fichiers.

Outre l'absence d'intérêt pour l'efficacité policière et la sécurité publique de ces données, la LICRA souligne la contradiction du recueil de ces données avec l'ensemble des textes relatifs aux droits de la personne et aux libertés publiques.

La LICRA insiste pour qu'aucune dérogation du I) de l'article 8 de la loi du 6 janvier 1978 ne soit rendue possible en ce qui concerne l'interdiction des données relatives aux origines raciales et ethniques dans les fichiers de police et de gendarmerie et dans le futur fichier EDVIRSP actuellement en discussion.

c) Concernant les données relatives aux opinions politiques, philosophiques ou religieuses

Le I) de l'article 8 de la loi du 6 janvier 1978 interdit de collecter ou de traiter des données qui font apparaître les opinions politiques, syndicales, philosophiques ou religieuses et l'article 26 admet restrictivement des dérogations.

Ainsi, la LICRA peut admettre de telles dérogations lorsque les données concernent plus que la démonstration de simples « opinions » et lorsque ces données sont utiles à des impératifs de défense ou de sécurité publique.

Elle souhaite que ces dérogations ne puissent être rendues possibles qu'au terme d'une intervention du législateur. Le bénéfice de la légitimité démocratique garantit de limiter ces dérogations aux seuls cas absolument nécessaires pour assurer la défense de l'ordre public.

La LICRA recommande qu'aucun futur fichier ne puisse permettre de telles dérogations sauf dans un cadre extrêmement limité et régi par une loi.

d) Concernant les données relatives à la santé ou à la vie sexuelle

La LICRA a pris acte de la volonté du gouvernement de ne pas retenir les données relatives à la santé ou à la vie sexuelle dans les fichiers.

La LICRA tient néanmoins à souligner son désaccord contre toute dérogation à ce principe d'interdiction du recueil et du traitement des données relatives à la santé ou à la vie sexuelle.

e) Concernant la saisine

Le système de traitement des infractions constatées (STIC) permet l'exploitation des informations issues des procès-verbaux établis dans le cadre de procédures judiciaires à des fins de recherches criminelles et statistiques. L'enregistrement des données repose sur des grilles suivant la nature des infractions.

Or, parmi la liste des infractions énumérées dans les annexes des décrets n°2001-583 du 5 juillet 2001 (STIC) et n°2006-1411 du 20 novembre 2006 (JUDEX), sont absentes les mentions relatives à :

- la discrimination, infraction incriminée par les articles 225-1 et 225-2 du code pénal ;
- les crimes et délits commis par voie de presse incriminés au titre de la loi du 29 juillet 1881 sur la liberté de la presse, notamment aux articles 23 et 24 (provocation à la discrimination, à la haine ou à la violence à caractère raciste, apologie de crimes contre l'humanité) ; 24 bis (contestation de crimes contre l'humanité) ; 32 (diffamation publique à caractère raciste) ; 33 (injure publique à caractère raciste) ;

La LICRA recommande que ces infractions soient également traitées et conservées par les fichiers de police et de gendarmerie au même titre que les crimes et délits déjà inclus afin de souligner la gravité de ces actes qui atteignent directement l'ordre public.

En outre, la LICRA souhaite – si ce n'est pas déjà le cas – que dans les fichiers de police et de gendarmerie, soient prises en compte dans une catégorie spécifique, les circonstances aggravantes de la commission d'une infraction à raison de l'appartenance ou de la non appartenance vraie ou supposée, de la victime à une ethnie, une nation, une race ou une religion déterminée.

Par ailleurs, le gouvernement s'est engagé à prendre un nouveau décret remplaçant le décret dit « EDVIGE » et aux termes duquel la notion « d'atteinte à l'ordre public » serait remplacée par la notion « d'atteinte à la sécurité publique, à la sécurité ou à la dignité des personnes, à la sécurité des biens » sachant que la notion de dignité viserait les déclarations racistes ou antisémites (discours du Ministre de l'Intérieur Michèle Alliot-Marie devant la Commission des lois de l'Assemblée nationale le 18 septembre 2008).

La LICRA se félicite d'une telle modification et souhaiterait que cette formulation soit étendue aux autres fichiers de police et de gendarmerie afin que soient distinguées et prises en compte les infractions à caractère raciste ou discriminatoire en termes de traitement des données et de statistiques.

La LICRA recommande la prise en compte des données relatives au caractère raciste ou/et discriminatoire des infractions.

f) Concernant les mineurs

Si la LICRA est consciente des nécessités de prise en compte de la délinquance juvénile, elle tient à faire part de certaines réserves concernant le fichage des mineurs. Elle insiste notamment pour que les fichiers soient en adéquation avec le régime pénal actuel applicable aux mineurs.

La LICRA souhaite qu'une distinction soit opérée entre les données relatives aux mis en cause entre 13 et 16 ans et celles relatives aux mis en cause entre 16 ans et 18 ans. Elle souhaite également l'aménagement d'un droit à l'oubli à la majorité.

7. MEDIATEUR DE LA REPUBLIQUE

Les fichiers de police judiciaire et administrative figurent parmi les instruments privilégiés dont disposent les pouvoirs publics pour assurer la mission fondamentale de sécurité, condition de l'exercice de nos libertés individuelles et collectives.

Dans la mesure où ils portent sur des données personnelles sensibles, il est indispensable qu'ils fassent l'objet de garanties juridiques fortes. En effet, d'une part, ils ne sont pas à l'abri de défaillances techniques ou humaines, et d'autre part, ils peuvent se révéler, même en l'absence de toute défaillance, menaçants pour les libertés si les conditions de leur utilisation n'ont pas été strictement définies et encadrées.

La Commission nationale de l'informatique et des libertés est au premier chef l'autorité compétente sur ces sujets. Néanmoins, le Médiateur de la République reçoit régulièrement des réclamations, émanant de particuliers, qui mettent en cause la fiabilité des données contenues dans les fichiers de police dits d'antécédents (STIC et JUDEX) et que l'administration est amenée à consulter lors de la délivrance d'agréments pour l'exercice de certaines activités de sécurité ou l'utilisation de certains matériels dangereux.

Afin d'éviter que des personnes puissent se voir refuser un emploi ou licenciées sur la base de mentions injustifiées, erronées ou périmées portées dans ces fichiers, le Médiateur de la République a adressé, en octobre 2005, aux ministres compétents, une proposition de réforme tendant au renforcement des garanties judiciaires attachées à la consultation des fichiers de police judiciaire à des fins d'enquêtes administratives.

En novembre 2006, les travaux du groupe de travail présidé par M. Alain Bauer, président du conseil d'orientation de l'Observatoire national de la délinquance, ont débouché sur une série de propositions visant à améliorer la transparence des fichiers de police judiciaire.

Associé à ce groupe de réflexion, le Médiateur de la République s'est à l'époque félicité de ces recommandations, qui reprenaient largement les mesures préconisées dans sa proposition.

Ce rapport recommandait en effet :

- la création d'un rendez-vous judiciaire annuel pour permette à tous les parquets de vérifier la bonne transmission des suites judiciaires favorables aux gestionnaires ;

- la mise en place d'un groupe technique visant à étudier les conditions d'interconnexion des données entre les traitements ARIANE et CASSIOPÉE ;

- l'indication des voies de recours pour l'effacement ou la rectification en cas de notification d'une décision défavorable après enquête donnant lieu à consultation de STIC et JUDEX ;

- la conduite d'une réflexion sur la création d'une voie de recours contre les décisions du parquet en matière de conservation ou d'effacement des décisions.

Deux ans après la remise de ce rapport, de sensibles progrès ont été accomplis, notamment sur la motivation des décisions préfectorales ou l'indication des voies et délais de recours.

En revanche, certaines recommandations semblent avoir fait long feu. Il en va ainsi du rendez-vous annuel technique ou de la réflexion sur la création d'une voie de recours contre les décisions du parquet, qui n'ont jamais eu lieu.

L'occasion du débat sur la création des fichiers Edvige/Edvirsp représente donc une opportunité à saisir pour s'interroger à nouveau sur la qualité et l'utilisation des informations contenues dans l'ensemble des fichiers de police judiciaire et administrative de notre pays.

Le Médiateur de la République fait entièrement sienne la volonté exprimée dans la lettre du 30 septembre 2008 par laquelle Madame la ministre de l'Intérieur, de l'outre-mer et des collectivités locales missionne à nouveau le président du groupe de travail en vue de « *mieux définir l'équilibre entre l'efficacité de la protection des personnes et l'attention de tous les instants que requiert la protection des libertés* » et de « *renforcer l'acceptabilité des fichiers au sein de la population* ».

Il réaffirme son attachement à la création d'un groupe de contrôle permanent afin qu'aucune information erronée ou caduque contenue dans STIC et JUDEX ne soit intégrée dans le système ARIANE.

Le Médiateur de la République insiste, à nouveau, sur la nécessité d'informer celles des personnes relaxées ou acquittée qui font l'objet par décision du procureur d'une inscription dans STIC et JUDEX, de l'existence de cette décision, et de leur ouvrir une voie de recours.

En effet, il est rappelé que l'article 21-III de la loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure prévoit que « *le traitement des informations nominatives est opéré sous le contrôle du procureur de la*

République compétent qui peut demander qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire ».

Si la rectification pour requalification judiciaire est de droit lorsque la personne concernée la demande, en revanche, en cas de décision de relaxe ou d'acquittement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées *« sauf si le procureur de la République en prescrit le maintien pour des raisons liées à la finalité du fichier, auquel cas elle fait l'objet d'une mention* » (même article).

Le législateur a ainsi confié en cette matière au procureur de la République un pouvoir décisionnel, qu'il exerce selon son appréciation, qui s'impose au responsable du traitement et fait grief à la personne mise en cause.

Or, lorsque cette décision intervient, *elle n'est pas notifiée* à la personne mise en cause et *n'est pas susceptible de recours*. Pourtant, cette décision est susceptible d'avoir pour conséquence un refus d'embauche, d'agrément ou un licenciement, *alors même que la personne a été relaxée ou acquittée*.

Il y a donc bien lieu de prévoir qu'en cas de décision de relaxe ou d'acquittement devenue définitive, la prescription du procureur de la République tendant au maintien des mentions au STIC ou au JUDEX devra être désormais notifiée à l'intéressé et pouvoir faire l'objet d'un recours de sa part devant le procureur général.

La circonstance qu'il existe un droit d'accès indirect, qui ne peut s'exercer qu'a posteriori, ne saurait constituer une raison suffisante pour exonérer l'autorité administrative de la possibilité de voir sa décision contestée sur recours hiérarchique.

Le Médiateur de la République tient par ailleurs à formuler les propositions nouvelles suivantes, tendant à :

- élargir la liste des cas justifiant une mise à jour des fichiers STIC et JUDEX aux sanctions judiciaires « modérées » ;

- garantir une procédure contradictoire lorsqu'un refus d'agrément est envisagé pour un recrutement, à la suite d'une enquête donnant lieu à consultation de fichiers de police ;

- mettre à disposition du grand public une information claire et pédagogique sur ces fichiers.

En ce qui concerne les modalités de signalement permettant de caractériser les personnes mises en cause, le Médiateur de la République restera attentif aux résultats de l'expérimentation sur un département d'un dispositif associant l'actuelle classification par typage avec une nouvelle classification par gamme chromatique. La pertinence de la généralisation éventuelle, après évaluation, d'une classification par gamme chromatique devra impérativement faire l'objet d'un débat approfondi au sein du groupe de contrôle.

Les obstacles techniques ne sauraient en aucun cas justifier le renoncement à la recherche de l'équilibre nécessaire entre efficacité des outils d'investigation et protection des libertés.

En raison de la complexité des moyens techniques mais aussi des craintes que ces outils peuvent générer, il peut exister dans ce domaine un risque de divorce entre une partie de la population et les forces de sécurité, auquel les pouvoirs publics doivent à tout prix parer.

Le seuil d'exigence de qualité en la matière doit être à la hauteur de la sensibilité des informations nominatives détenues.

Afin de contribuer à garantir l'indispensable confiance de la population dans ses services publics chargés de la justice et de la sécurité, le Médiateur de la République insiste pour que les recommandations formulées dans le présent rapport ne restent pas lettre morte.

8. SOS RACISME

SOS racisme s'appui sur la Constitution, la Loi, la récente jurisprudence et les rapports de la CNDS pour refuser toute catégorie ethno-raciale dans le travail d'enquête de la police.

a) Le refus de toute catégorisation ethno-raciale

Les apports de la Constitution

D'après le Préambule de la constitution du 27 Octobre 1946, « Au lendemain de la victoire remportée par les peuples libres sur les régimes qui ont tenté d'asservir et de dégrader la personne humaine, le peuple français proclame à nouveau que tout être humain, sans distinction de race, de religion ni de croyance, possède des droits inaliénables et sacrés. Il réaffirme solennellement les droits et libertés de l'homme et du citoyen consacrés par la Déclaration des droits de 1789 et les principes fondamentaux reconnus par les lois de la République ».

D'après la décision n°2007-557 DC du 15 novembre 2007 du Conseil Constitutionnel sur la loi relative à la maîtrise de l'immigration, à l'intégration et à l'asile : « si les traitements nécessaires à la conduite d'études sur la mesure de la diversité des origines des personnes, de la discrimination et de l'intégration peuvent porter sur des données objectives, ils ne sauraient, sans méconnaître le principe énoncé par l'article 1er de la Constitution, reposer sur l'origine ethnique ou la race [...] ».

En d'autres termes, le Conseil Constitutionnel a rappelé dans cette décision que le préambule de notre Constitution en vigueur depuis 1958, interdit à toute administration, et notamment à la police nationale, de distinguer les individus en fonction de caractéristiques ethno raciales.

La jurisprudence DAYTONA

Par jugement du 27/10/2008, le tribunal de grande instance de Nanterre a condamné la société Daytona, filiale n°1 mondial de la communication et du marketing DDB, à 20.000 euros d'amende, dont 15.000 avec sursis, pour avoir sélectionné les personnels, essentiellement des hôtesses de vente et d'animation, selon un critère "pure white" et pour avoir fiché les origines ethniques de ces salariés mis à disposition de sociétés comme Dior, Guerlain ou Gilette (1 pour les Européens blancs, 2 pour les Maghrébins, 3 pour les Noirs et 4 pour les Asiatiques).

Reconnu coupable du fichage ethno racial de ses collaborateurs, l'ancien directeur général François Leveque a écopé de 3000 euros d'amende (dont 2000 avec sursis). L'ex-directrice du département hôtesses, Caroline Housset, a été condamnée pour discrimination raciale et fichage ethnique à 4000 euros d'amende (dont 2500 avec sursis).

Le Parquet et SOS Racisme ont décidé de faire appel de la condamnation "dérisoire" prononcée par le TGI de Nanterre contre la société Daytona pour "discrimination raciale" et "fichage ethnique". (Le parquet avait réclamé 100 000 € ferme d'amende).

Délibération de la CNIL contre le fichier des juifs du Front National

La CNIL a été saisie d'une plainte relative à l'envoi par le Front National de propagande spécifiquement adressée à un électeur présumé Juif en vue de l'élection présidentielle.

Par délibération n°89-13 du 14 Février 1989, la CNIL a considéré que le Front National avait enfreint les articles 25, 26, 31 et 42 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Pour rappel, l'article 25 de cette loi interdit la collecte des données opérée par tout moyen frauduleux, déloyal ou illicite.

L'article 26 donne le droit à toute personne de s'opposer, pour des raisons légitimes, à ce que des informations nominatives la concernant fassent l'objet d'un traitement.

L'article 31 interdit la collecte d'informations nominatives faisant apparaître, directement ou indirectement, les origines raciales ou les opinions religieuses des personnes sans leur accord exprès, c'est-à-dire écrit.

L'article 42 sanctionne pénalement le non respect de ces dispositions.

En l'espèce, la collecte des noms et adresses des plaignants avait été réalisée à leur insu et les intéressés n'avaient pas eu le droit de s'opposer à ce que ces données fassent l'objet d'un traitement.

La CNIL a considéré qu'en toute vraisemblance les plaignants avaient reçu les correspondances incriminées en raison de leurs opinions religieuses supposées sans en avoir donné leur accord écrit.

Le STIC - CANONGE

Développé dans le cadre du système de traitement des infractions constatées (STIC), le logiciel Canonge permet de rassembler dans un même fond documentaire le signalement des auteurs d'infractions à l'échelon d'une circonscription, d'un département, du ressort territorial d'un SRPJ ou d'une DIPJ, du service central de documentation criminelle.

Il permet de rechercher des auteurs déjà connus des services de police à partir d'éléments de signalements fournis par le témoin ou la victime.

Seules les personnes formellement mises en cause pour crime, pour délit ou pour certaines contraventions de 5è classe peuvent être enregistrées dans le Canonge. La signalisation des témoins ou autres personnes est proscrite.

Concernant la saisie des informations, il existe aujourd'hui 6 rubriques principales parmi lesquelles figure « le signalement ».

Dans la partie « signalement », un filtre sur le « type » distingue 12 types différents : Blanc (caucasien) ; Méditerranéen ; Gitan ; Moyen Oriental ; Nord africain Maghrébin ; Asiatique Eurasien ; Amérindien ; Indien (Inde) ; Métis Mulâtre ; Noir ; Polynésien ; Mélanésien canaque.

Dans le cadre de la réflexion sur l'évolution du fichier STIC CANONGE, et notamment des types mentionnés en vue de l'identification puis de l'interpellation des individus recherchés, il est proposé une nouvelle déclinaison :

1. Type EUROPEEN
- Nordique
- Caucasien
- Méditerranéen
2. Type AFRICAIN/ANTILLAIS
3. Type METIS
4. Type MAGHREBIN
5. Type MOYEN ORIENTAL
6. Type ASIATIQUE
7. Type INDO PAKISTANAIS
8. Type LATINO AMERICAIN
9. Type POLYNESIEN
10. Type MELANISIEN (dont notamment CANAQUE, …)

Cette classification devait permettre à une victime ou un témoin de décrire un individu. Mais cette nouvelle typologie est tout aussi absurde que la précédente.

La démonstration de son absurdité aurait pu être faite avec les récentes violences du 19eme arrondissement de Paris lorsque certains ont voulu qu'on apprenne à reconnaître les juifs parmi les jeunes participants aux violences. Tandis que d'autres voulaient carrément distinguer les séfarades des ashkénazes. Un ancien ministre de l'intérieur allant jusqu'à déterminer lesquels étaient originaires de l'autre côté de la méditerranée en fonction de leurs noms de famille.

La dérive du CANONGE dans ce cas serait de vouloir proposer pour améliorer le travail de la Police du 19ème, le type « juif » avec pourquoi pas la taille du nez comme la police de Vichy avait été formée à reconnaître ceux qui n'avaient pas accepté de porter l'Etoile Jaune.

Mais toutes les autres catégories sont aussi absurdes : Prenons simplement l'exemple du type INDO PAKISTANAIS : il ne peut être considéré comme une race et constituer un signe physique distinctif, les indo-pakistanais se distinguant eux même en une multitudes de catégories.

Par ailleurs, en fonction des connaissances et des sensibilités de chacun, une personne d'origine indienne ou pakistanaise pourra être perçue et décrite comme un individu de type antillais, et inversement. De même, un individu d'origine maghrébine sera considéré comme européen par certains, ou encore de type moyen-oriental ou encore métis, mélanésien, indo-pakistanais ou latino américain ou encore asiatique. Il y a très

souvent un grand écart entre la réalité des origines et la perception des gens. Prenons simplement l'exemple d'Harlem DESIR qui a été des milliers de fois présenté comme un « Beur » par la presse d'extrême droite. Aujourd'hui c'est Dominique SOPO qui est présenté comme antillais par d'autres médias. Prôner une classification est absurde en sachant que les représentations sont très souvent différentes entre les individus et donc entre la personne qui décrit son agresseur et celles qui doivent le rechercher.

Multiplication des comportements discriminatoires de la part des agents de Police et de Gendarmerie

On peut lire dans le rapport de la Commission Nationale de Déontologie de la Sécurité (CNDS) de 2004 :

« La lutte contre les discriminations est devenue aujourd'hui l'une des priorités de la politique du *vivre ensemble* et elle a enrichi le contenu de la citoyenneté, en France et en Europe ».

« Une des manifestations de la discrimination constatée réside dans une perception erronée de la complexité sociale des quartiers d'intervention de la part d'agents. Certains pratiquant volontiers l'amalgame entre populations *visibles*, criminalité et quartiers sensibles, ne perçoivent pas les interpellés comme des citoyens ordinaires, indépendamment de leur appartenance supposée à un groupe ciblé comme groupe à risque ».

Ceux qui sont discriminés par ce type de pratique sont uniquement des jeunes issus de l'immigration. Ce sentiment de persécution, visible à travers les auditions, s'ajoute au sentiment d'une personnalisation des rapports entre les agents et ceux-ci. L'affaire devient donc « personnelle » .

« Des cas de discriminations laissent apparaître une suspicion généralisée à l'égard de groupes pris comme tels sans qu'on prenne la peine de rechercher les responsabilités individuelles dans les incidents ».

« L'utilisation du terme *criminogène* est fréquente dans les réponses faites par le ministère de l'Intérieur. Cela conduit à stigmatiser certains quartiers et à pérenniser des attitudes favorables aux discriminations raciales ».

« Ce travail d'analyse portant sur quatre ans d'exercice de la CNDS a montré le poids de la répétition de cas parfois graves. Il permet aussi de souligner le poids de l'imaginaire et des représentations collectives dans les pratiques des agents de sécurité. Beaucoup de constructions stéréotypées conduisent à nier l'individu en l'amalgamant à un groupe connoté négativement. Cette approche simplificatrice semble liée à une méconnaissance d'une partie de la population française issue de l'immigration ou d'étrangers souvent durablement installés. Amenés, pour la plupart, à participer pleinement à la vie citoyenne, certains ont le sentiment qu'ils ne sont pas considérés comme citoyens à part entière.

Ils peuvent avoir le sentiment que tous les citoyens ne sont pas traités de la même manière, selon que l'on est *puissant ou misérable*, c'est-à-dire dans la version d'aujourd'hui, jeune, *visible* , de couleur, de culture musulmane présumée, de type maghrébin ou gitan, habitant d'un quartier pauvre et ethnicisé ou, au contraire, fréquentant un quartier ou un lieu public où sa seule présence paraît incongrue ou suspecte. Cela vient fortement fragiliser le bien fondé du modèle français de communauté civique et politique construit autour du contrat social, indépendamment des appartenances collectives, communautaires et identitaires, alors que le contrat républicain est aujourd'hui rappelé ».

Conclusion de SOS Racisme

La police comme la gendarmerie et la justice ne doivent pas utiliser la moindre pseudo catégorie ethno-raciale pour décrire les individus recherchés ou les individus arrêtés.

Ceci est illégal au regard de la Constitution et de la Loi mais qui plus est c'est à l'origine de très nombreuses erreurs policières et judiciaires et c'est extrêmement dangereux et générateur de racisme.

b) Observations complémentaires sur le STIC CANONGE

Le fichier STIC CANONGE opère une classification sur la base d'une nomenclature basée sur les appartenances « ethno-raciales » supposées des personnes recherchées.

Mais quelle est la pertinence dans la recherche d'un suspect d'avoir des catégories « ethno-raciales »? Cela perturbe davantage les témoins qu'une simple description physique sur des critères objectifs, et rend donc plus difficile l'élucidation.

De plus l'usage de ces catégories n'est pas sans effets. Lorsque l'État me catégorise et me perçoit à travers le prisme d'une ethnie, d'une race j'ai tendance moi même à reproduire ce schéma. Si la puissance publique me classe sur une base ethno-raciale, cet élément va prendre une place plus importante dans la manière dont je me définis. Dans le rapport à l'autre ces éléments vont aussi déterminer la perception que l'on a de soi et de

celui qui n'appartient pas à ma catégorie. Cela fait donc peser un véritable risque de désagrégation du vivre ensemble.

Par ailleurs, nous vivons dans un pays qui connait de plus en plus le métissage. C'est aujourd'hui une réalité de la démographie française. Les nomenclatures, qui par nature définissent des limites, des bornes nient cet état de fait qu'est le métissage.

Au-delà de ces considérations des problèmes concrets montrent l'impasse de ces nomenclatures : Qui procédera au classement ? sur quelle base ?

Les catégories sont toujours un choix, une subjectivité. Comment fixer les limites d'une catégorie arbitraire à une autre? Les statistiques, type statistiques de la délinquance, lorsqu'elles sont faites sur la base de nomenclatures ethno-raciale ont, dans les pays où elles ont été mises en place, eu un effet stigmatisant qui suscite beaucoup de tensions.

Pour le fichier STIC CANONGE, il serait plus judicieux, pour les raisons mentionnées ci-dessus mais aussi en terme d'efficacité des recherches, qu'il y soit fait référence à la couleur de la peau telle que perçue par les témoins.

Par ailleurs, il faut que cette référence à la couleur de la peau soit telle qu'elle ne permette pas de construire de façon implicite des catégories ethno-raciales propices à l'élaboration de statistiques ethniques à partir du fichier CANONGE.

9. SYNDICAT DES COMMISSAIRES DE LA POLICE NATIONALE (SCPN)

Le SCPN souhaite réitérer sa position de principe selon laquelle la police nationale est une force de police civile, républicaine et citoyenne. L'immense majorité des effectifs de police est absolument respectueuse des droits de l'Homme et la police concourt à la sauvegarde des droits humains et de la défense. Le corps social de la police nationale dispose, en raison de sa variété, de toutes les garanties de pluralisme. De plus, cette variété, appuyée par le fait syndical et le souci déontologique, permet de croire en la présence de contre feux à d'éventuelles pressions ou tentations politiques contraires au respect des droits de l'Homme.

Le SCPN souhaite alerter les membres du groupe sur l'incohérence forte qu'il y aurait à trop restreindre les capacités des fichiers de police et à mettre en cause, à l'échéance, les résultats des forces de police et de gendarmerie face à un bilan négatif de la lutte contre la délinquance et les tensions urbaines. La police nationale et en premier rang ses chefs de service, seront mis en cause en cas d'augmentation des actes de délinquance, alors qu'on leur aura retiré des moyens essentiels au pilotage de leur action et à la détermination des politiques publiques de sécurité.

Propositions

- Concevoir et conserver les fichiers de renseignement comme des instruments de mesure de la menace délinquante et des tensions urbaines. Ces deux forces n'ont pas disparues de la scène urbaine et la société doit conserver une pleine capacité de prévision, d'analyse, de prévention et de répression de la délinquance, y compris juvénile. C'est le sens de la recommandation n°18 issue des travaux de 2006 de ce même groupe de travail sur les fichiers "*ouvrir une réflexion sur l'évolution nécessaire des outils de travail des forces républicaines de sécurité*".
- Conserver un mode écrit et traçable de transmission des poursuites judiciaires (fiche navette) en direction des services enquêteurs, y compris pour les affaires bénéficiant du traitement en temps réel. Les services enquêteurs ne doivent pas supporter les effets du doute en cas d'absence de trace (présomption d'information par la Justice).
- Promouvoir des procédés technologiques d'accès aux fichiers de police garantissant la traçabilité de l'utilisateur réel (biométrie), particulièrement dans les services fonctionnant en horaires de roulement.
- Intégrer, dans les travaux du groupe, le principe de "disponibilité des données", en cours de traduction dans les groupes de travail "Justice Affaires Intérieures" de l'Union européenne.
- Intégrer et valoriser la production issue des travaux de 2006 du groupe de contrôle, dans la recherche d'une typologie acceptable des descriptions des éléments physiques intangibles et objectifs. Rechercher et intégrer les travaux et méthodes utilisées par Interpol dans ses fiches de diffusion.
- Porter le débat sémantique sur les types et éléments physiques intangibles au niveau des agents d'exécution par une politique soutenue de formation et un contrôle hiérarchique des pratiques opérationnelles de terrain.
- Rechercher la plus rapide remise à disposition des services d'information générale d'un outil opérationnel de traitement des données numériques.
- Conserver la capacité de travailler avec des informations utiles dans des domaines sensibles, dans une logique de renseignement, c'est à dire en amont de la commission d'infractions et dans un but de prévention.
- Conserver la capacité de recueillir et d'analyser des informations concernant à des mineurs, tout en assurant un "droit à l'oubli" après la majorité ; cette échéance pouvant être reportée à 21 ans en cas de nouvel élément survenant entre 16 et 18 ans.
- Intégrer formellement au périmètre du champ d'analyse du groupe de contrôle les fichiers mis en œuvre par les polices municipales.

CHAPITRE V – TABLEAU DES FICHIERS DE POLICE ET DE GENDARMERIE

NOM	SERVICE GESTIONNAIRE	CREATION	REFERENCE LEGALE	FINALITE	INFORMATIONS ENREGISTREES	DESTINATAIRES INFORMATIONS	DUREE CONSERVATION	DROITS ACCES	OBSERVATIONS
ARAMIS	Gendarmerie			Informer les autorités hiérarchiques des événements en cours et de leur évolution	- Données nominatives concernant les requérants - Renseignements sur les événements	Patrouilles en cours et leurs autorités hiérarchiques immédiatement supérieures	- 3 mois pour les données relatives aux appelants. - 2 ans pour les fiches d'appel et d'intervention associées - 2 ans ½ pour les messages de renseignements et points de situations		ARAMIS est appelé à être remplacé par le système ATHEN@
BUREAUTIQUE BRIGADE 2000 (BB 2000)	Gendarmerie	1992	Arrêtés ministériels du 28.10.1992 et du 28.05.1993 modifiés par l'arrêté du 13.05.1998	Au niveau local, gestion du service et des registres, partage des informations sur les lieux et personnes particuliers de la circonscription	Dans certains modules, présence de données concernant l'identité, le domicile, l'activité (hors politique ou syndicale)	- Personnels de la Gendarmerie - ONISR, CUB et CEESAR pour les données relatives aux accidents de la circulation	Variable : - Apurement des registres et amendes forfaitaires au terme de 2 ans échus - Apurement des données nominatives des MIS et BAAC dès transmission du message		L'application PULSAR succédera en 2009 à BB 2000.
LOGICIEL DE REDACTION DE PROCEDURES (LRP)	Police		Déclaré à la CNIL en 2001, en même temps que le STIC	Rédiger les procès-verbaux et les rapports administratifs ou judiciaires	Au plan local : informations contenues dans les procès-verbaux	Fonctionnaires de police			Le LRP est associé au STIC.
MAIN COURANTE INFORMATISE E (MCI)	Police	1990	Arrêté du 24.02.1995	Gérer l'emploi des effectifs, les événements et les déclarations des usagers	- Etat-civil des personnes (requérants, témoins, etc.), - Etat-civil et renseignements administratifs concernant les fonctionnaires de police	Fonctionnaires de police habilités Autorités judiciaires, pour certaines informations	Tant qu'elles sont nécessaires eu égard aux finalités du fichier	Droit d'accès direct auprès du commissariat	La procédure de modification du traitement de la main courante informatisée est actuellement en cours.
FICHIER DE GESTION DU SERVICE CENTRAL DE PRESERVATION DES PRELEVEMENT S BIOLOGIQUES (SCPPB)	Gendarmerie		Déclaration à la CNIL en 2002 et arrêté ministériel du 13.09.2002	Assurer la gestion des prélèvements biologiques recueillis sur certaines scènes de crime ou de délit, ou lors de découvertes de cadavres non identifiés voire lors de disparitions de personnes	Informations relatives : - au requérant, - au scellé, - à l'identité de la personne disparue, - au service ou à l'unité ayant effectué le prélèvement,	- SCPPB - Autorités judiciaires - Magistrat du parquet et membres du comité de contrôle	40 ans		
IC@RE	Gendarmerie		Dossier de déclaration déposé en juillet 2008 à la direction des affaires juridiques du ministère de la Défense	- Rédiger les procès-verbaux et rapports - Faciliter et optimiser les tâches des personnels - Alimenter le FVV et JUDEX	Données relatives : - à l'identité de l'OPJ ou APJ - aux destinataires habituels des procédures de l'unité - à l'identité de la victime ou du témoin et du mis en cause - à la personne morale - à la procédure judiciaire (cadre juridique, nature de l'infraction, etc.)	- Enquêteurs au sein d'une même unité territoriale - Magistrats et avocats, sous certaines conditions	Jusqu'à la clôture de la procédure et sa transmission à l'autorité judiciaire		IC@ARE alimentera également la future application CASSIOPEE du ministère de la Justice.
FICHIER NATIONAL DU FAUX MONNAYAGE (FNFM)	Police Gendarmerie	2002		Recenser les affaires relatives au faux monnayage commises sur le territoire national	Données relatives à l'affaire, l'infraction, aux coupures apocryphes saisies, à l'identité des mis en cause et leur signalement	Personnels habilités des SRPJ et des sections de recherche de la gendarmerie			Le FNFM sert également à alimenter le système d'information d'Europol.

FICHIER DE LA BATELLERIE	Gendarmerie	1942	Aucune	Assurer le suivi des mariniers, des compagnies fluviales et des bateaux affectés au transport fluvial de marchandises	- Informations concernant les mariniers, leur famille, leurs ouvriers, leur employeur, leur navire - Informations concernant les compagnies fluviales et entreprises de transport fluvial	- Unités de la Gendarmerie - Services de police ainsi que les administrations (exceptionnellement)	Fiches détruites au décès du marinier (ou lorsqu'il atteint 80 ans) ou à la destruction du bateau		Ce fichier est tombé en désuétude et n'est plus opérationnel aujourd'hui.
FICHIER DES PERSONNES NEES A L'ETRANGER (FPNE)	Gendarmerie	1975	Aucune	Collationner les renseignements relatifs aux personnes nées hors de France	Etat-civil des personnes, procédures dont elles ont fait l'objet, renseignements facilitant le travail des unités opérationnelles	Unités de Gendarmerie	- Destruction de la fiche au décès de la personne, ou lorsqu'elle atteint 80 ans. - 10 ans pour les personnes SDRF au moment du contrôle ou domiciliées à l'étranger	Indirects, par l'intermédiaire de la CNIL	Ce fichier sera supprimé au plus tard en octobre 2010. Il n'est plus alimenté ni consulté depuis septembre 2007.
FICHIER DE SUIVI DES PERSONNES FAISANT L'OBJET D'UNE RETENTION ADMINISTRATIVE	Gendarmerie		Arrêté interministériel du 19.12.1994 modifié par l'arrêté du 30.07.2002	Assurer le suivi des personnes faisant l'objet d'une décision de rétention	Photographie et informations relatives à : - l'identité - la nationalité - le domicile en France des personnes concernées	- Unités de Gendarmerie du lieu d'implantation du centre de rétention administrative, - Membres du CIMADE	2 ans (si la personne concernée ne fait pas l'objet d'une nouvelle mesure de rétention entre temps)	Directs auprès du Groupement de Gendarmerie local ou du responsable de la gestion du CRA	Ce fichier ne concerne que les CRA du Mesnil-Amelot, de Geispolsheim et de Rivesaltes, rattachés aux groupements de Gendarmerie locaux.
FICHIER DES PASSAGERS AERIENS (FPA)	Police	2007	Décret 1630-2006 du 19.12.2006 et arrêté du 19.12.2006	Améliorer le contrôle aux frontières, lutter contre l'immigration clandestine et les actes de terrorisme	Données d'enregistrement des compagnies aériennes (identité, pays de résidence, etc.)	- Agents habilités de la police aux frontières, - Certains services de police spécialisés	- 5 ans pour la lutte contre le terrorisme - 24 heures pour la lutte contre l'immigration clandestine	Droit d'accès direct auprès de la PAF sauf pour la mention « connu » ou « inconnu » du FPR (alors DAI)	Fichier interconnecté avec le FPR et, à l'avenir, avec le SIS.
FICHIER DES VEHICULES VOLES (FVV)	Police Gendarmerie		Arrêté du 15.05.1996, modifié en 2005	Faciliter les recherches de véhicules, bateaux et aéronefs signalés volés ou mis sous surveillance	- Etat-civil et coordonnées du plaignant, - Références de l'assurance, - Caractéristiques du véhicule - Conduite à tenir en cas de découverte	- Fonctionnaires de police et militaires de la gendarmerie habilités - Autorités judiciaires - Autorités administratives - Organismes d'assurance si protocole - Coopération internationale et services de police étrangers	Pour les véhicules volés : le temps de nécessaire à la découverte et la restitution Pour les véhicules signalés : jusqu'à ce que la mesure devienne sans objet	DAI : véhicules signalés Droit d'accès direct : véhicules volés	Le FVV sera progressivement remplacé par le FOVES à compter du 2ème trimestre 2009.
APPLICATION DE GESTION DU REPERTOIRE INFORMATISE DES PROPRIETAIRES ET POSSESSEURS D'ARMES (AGRIPPA)	DLPAJ	2007	Arrêté du 15 novembre 2007	Enregistrer et suivre les autorisations et récépissés de déclaration relatifs aux matériels de guerre ainsi qu'aux armes et munitions des 4ème, 5ème et 7ème catégories	Renseignements sur : - les personnes physiques ou morales (état-civil ou raison sociale, adresse, etc.) - les autorisations et déclarations (date, caractéristique de l'arme, etc.) - les décisions de refus d'autorisation ou de délivrance de récépissé	- Agents habilités du ministère de l'Intérieur et des services préfectoraux - Les données sont consultables par les agents de la police nationale, les militaires de la gendarmerie ainsi que les agents du service des douanes et de la douane judiciaire.	- 20 ans après la fin de la possession de l'arme (sauf en cas de perte ou vol) - 5 ans pour les personnes ayant essuyé un refus d'autorisation	Direct auprès des préfets de département ou du Préfet de police	
FICHIER NATIONAL DES INTERDICTIONS DE STADE (FNIS)	DCSP	2007	Arrêté du 28 août 2007	Prévenir et lutter contre les violences lors de manifestations sportives	Données relatives : - aux personnes (état-civil, adresse, photographie, etc.) - à la mesure d'interdiction (nature, date, champ géographique, etc.)	- Les agents habilités des services de police (DCSP, PP…) - Préfets de département et, à Paris, de police - Autorités judiciaires - Militaires de la gendarmerie habilités - Fédérations sportives agréées - Organismes de coopération inter-nationale en matière de police judiciaire, sous conditions	5 ans à compter de l'expiration de la dernière mesure prononcée	Indirect par l'intermédiaire de la CNIL	

FICHIER NATIONAL TRANS-FRONTIERES (FNT)	Police		Arrêté du 29 août 1991 modifié par l'arrêté du 03 novembre 2006	- Améliorer le contrôle aux frontières et la lutte contre l'immigration clandestine - Prévenir et réprimer les actes de terrorisme	Données relatives à l'état-civil, au pays de provenance ou de destination, à la durée du séjour, au nombre d'entrées, aux documents de voyage et à la bande MRZ	Personnels habilités de la police nationale, la gendarmerie et des douanes	3 ans		
FICHIER ALPHABETIQUE DE RENSEIGNE-MENTS DE LA GENDARMERIE NATIONALE (FAR)	Gendarmerie		- Arrêté du 17.09.92 portant application au FAR des dispositions de l'art 45 de la loi de 78 - Déclaré à la CNIL le 13.10.1993	Connaître de manière approfondie la population résidente, en particulier sur sa dangerosité	- Etat-civil de la personne - Procédures dont elle a fait l'objet - Tout renseignement pouvant faciliter le travail des unités opérationnelles	Personnels des brigades de gendarmerie	Destruction de la fiche : - au décès de la personne, ou lorsqu'elle atteint 80 ans - au déménagement de la personne	Indirect par l'intermédiaire de la CNIL	Ce fichier sera supprimé au plus tard en octobre 2010. Les renseignements administratifs seront intégrés dans le nouveau système ATHENA.
CENTRALISATION DU RENSEIGNEMENT INTERIEUR POUR LA SECURITE DU TERRITOIRE ET LES INTERETS NATIONAUX (CRISTINA)	Police	2008							Décret non publié – secret défense
EDVIRSP	Police		Délibération CNIL du 20 novembre 2008	collecter, conserver et traiter les données concernant : - les personnes susceptibles de porter atteinte à la sécurité publique - les personnes faisant l'objet d'enquêtes administratives	- Etat- civil et profession, - Adresses physiques, - Numéros de téléphone et adresses électroniques, - Signes physiques particuliers et objectifs, - Photographies, - Activités publiques, - Comportement et déplacements, - Titres d'identité, - Immatriculation des véhicules, - Informations patrimoniales, -Antécédents judiciaires - Environnement de la personne	Fonctionnaires spécialement habilités de la direction du renseignement de la préfecture de police	5 ans (3 ans pour les mineurs de 13 ans)	Indirect par l'intermédiaire de la CNIL	Il s'agit ici du projet dans son dernier état transmis à l'avis de la CNIL.
GESTION DU TERRORISME ET DES EXTREMISMES A POTENTIALITE VIOLENTE (GESTEREX)	Police (PP)	2008		- Prévenir les actes de terrorisme - Surveiller les individus, groupes, organisations et phénomènes de société susceptibles de porter atteinte à la sûreté nationale		Fonctionnaires spécialement habilités de la préfecture de police de Paris	Tant qu'elles sont nécessaires eu égard aux finalités du fichier	Indirect par l'intermédiaire de la CNIL	Fichier mis en œuvre par la direction du renseignement de la préfecture de police (DR-PP)
SYSTEME JUDICIAIRE DE DOCUMEN-TATION ET D'EXPLOI-TATION (JUDEX)	Gendarmerie	1986	Décret 2006-1411 du 17/11/2006 Circulaire n° 51992 DEF/GEND/SD PJ/PJ du 10 août 2007	Faciliter la constatation des infractions, le rassemblement des preuves et la recherche des auteurs	Données concernant les personnes impliquées à titre de mis en cause ou de victime dans un crime, un délit ou certaines contraventions de 5ème classe	- Personnels de la Gendarmerie, de la Police nationale, des Douanes, autorités judiciaires, organismes de coopération internationale et services de police étrangers, - Certains personnels investis d'une mission de police administrative	- 20 ans pour les mis en cause majeurs - 5 ans pour les mis en cause mineurs - 15 ans pour les victimes (Pour les mis en cause, ces durées sont susceptibles d'être écourtées ou allongées en fonction de la gravité de l'infraction)	Indirect par l'intermédiaire de la CNIL	JUDEX doit être remplacé à l'horizon fin 2009 par l'application ARIANE, commune à la Gendarmerie et la Police nationales.

SYSTEME DE TRAITEMENT DES INFRACTIONS CONSTATEES (STIC)	Police		Décret 2001-583 du 5/7/2001 (modifié en 2006)	Faciliter la constatation des infractions, le rassemblement des preuves et la recherche des auteurs + statistiques	- Données concernant les personnes impliquées à titre de mis en cause ou de victime dans un crime, un délit ou certaines contraventions de 5ème classe, - Données non nominatives relatives aux infractions, - Informations relatives aux objets	- Personnels de la Police nationale, - Dans certains cas : personnels de la Gendarmerie nationale et de Douanes, - Autorités judiciaires - Certains personnels investis d'une mission de police administrative - Coopération internationale et services de police étrangers	- 20 ans pour les mis en cause majeurs - 5 ans pour les mis en cause mineurs - 15 ans pour les victimes (Pour les mis en cause, ces durées sont susceptibles d'être écourtées ou allongées en fonction de la gravité de l'infraction)	DAI	Fichier placé sous le contrôle d'un magistrat. Le STIC doit être remplacé à l'horizon fin 2009 par l'application ARIANE, commune à la Gendarmerie et la Police nationales.
FICHIER DES BRIGADES SPECIALISEES (FBS)	Police	1991		Collecter des informations sur les délinquants spécialisés et favoriser la coopération des services	Informations collectées à l'occasion de la surveillance du milieu criminel	- Directions interrégionales de la police judiciaire - La plupart des offices centraux de police judiciaire - Les brigades centrales de la préfecture de police	Tant qu'elles sont nécessaires eu égard aux finalités du fichier		
FICHIER DE TRAVAIL DE LA POLICE JUDICIAIRE (FTPJ)	Police	1987	Déclaration à la CNIL en 1991	Collecter des informations sur les délinquants spécialisés	Informations collectées à l'occasion de la surveillance du milieu criminel	Services territoriaux de police judiciaire	Tant qu'elles sont nécessaires eu égard aux finalités du fichier		Constitué de bases locales, sans interconnexions, le FTPJ n'est plus utilisé que par quelques services de PJ.
FICHIER JUDICIAIRE NATIONAL AUTOMATISE DES AUTEURS D'INFRACTIONS SEXUELLES (FIJAIS)	Ministère de la Justice	2004	- Loi n°2004-204 du 09.03.2004, - Articles 706-53-1 à 706-53-12 et R53-8-1 à R53-8-39 du CPP, - Délibération de la CNIL n°2005-039 du 10.03.2005, - Délibération de la CNIL n° 2005-153 du 21.06.2005, - Décret n°2005-627 du 30.05.2005, - Circulaire d'application du 01.07.200, - Loi n°2005-1549 du 12.12.2005, - Circulaire d'application du 27.02.2006, - Loi n°2006-399 du 04.04.2006 - Circulaire d'application du 19.04.2006 - Loi n°2007-297 du 05.03.2007 - Décret n° 2008-1023 du 06.10.2008, -Circulaire d'application du 29.10.2008	Prévenir la récidive des auteurs d'infractions sexuelles ou violentes et faciliter l'identification des auteurs de ces infractions	Données complètes concernant les personnes mises en examen, condamnées ou ayant exécuté une composition pénale pour certaines infractions à caractère sexuel ou violentes		20 ou 30 ans selon la gravité de l'infraction		Fichier géré par le ministère de la Justice Ce fichier concerne également les personnes condamnées à l'étranger ou ayant bénéficié d'un non-lieu, d'une relaxe ou d'un acquittement pour des motifs tenant à l'abolition des facultés de discernement.

FICHIER AUTOMATISE DES EMPREINTES DIGITALES (FAED)	Police et Gendarmerie nationales	1987	Décret 87-249 du 08.04.1987 (modifié en 2005)	- Identifier les auteurs de crimes ou délits grâce aux traces digitales ou palmaires - Détecter les usurpations d'identité et les identités multiples	Traces relevées : - au cours d'enquêtes judiciaires - sur ordres de recherche de l'autorité judiciaire, - lors de disparitions inquiétantes ou suspectes, Empreintes relevées : - sur les personnes mises en cause pour crime ou délit, - sur les personnes détenues	- Personnels habilités de la DCPJ - Personnels des unités de recherche de la Gendarmerie - Coopération internationale et services de police étrangers	- 25 ans pour les empreintes - selon le temps de prescription de l'action publique pour les traces	Droit d'accès direct (DCPJ)	Fichier placé sous le contrôle d'un magistrat. Modification du FAED en cours pour y intégrer les dispositions prévues par le Traité de Prüm.
FICHIER NATIONAL AUTOMATISE DES EMPREINTES GENETIQUES (FNAEG)	Police et Gendarmerie nationales	1998	Loi du 17/06/98 et du 18/03/2003 Décret du 18.05.2000 (modifié en 2004)	Faciliter la recherche des auteurs d'infractions et des personnes disparues	- Traces biologiques non identifiées - Empreintes génétiques des personnes mises en cause ou condamnées pour certaines infractions - Profil génétique de personnes décédées ou disparues pour recherche des causes de la mort ou de la disparition	Magistrats et services d'enquête (de manière indirecte) - coopération internationale et services de police étrangers	- 40 ans pour les condamnés, les personnes décédées ou disparues et les traces, - 25 ans pour les mis en cause et la parentèle des personnes disparues	Droit d'accès direct (DCPJ)	Fichier placé sous le contrôle d'un magistrat. Modification du FNAEG en cours pour y intégrer les dispositions prévues par le Traité de Prüm.
FICHIER DES PERSONNES RECHERCHEES (FPR)	Police Gendarmerie		Arrêté du 15.05.1996 (modifié en 2005)	Répertorier au niveau national les personnes faisant l'objet de recherches judiciaires, et administratives	Etat-civil des personnes et motif de la recherche	- Police nationale, - Gendarmerie, - Douanes judiciaires -Autorités administratives - Autorités judiciaires - Coopération internationale et services de police étrangers	Fiches extraites en cas de découverte ou d'extinction du motif de recherche	Selon la nature des informations : droit d'accès direct ou indirect	
OUTIL DE CENTRALISATION ET DE TRAITEMENT OPERATIONNEL DES PROCESURES ET DES UTILISATEURS DE SIGNATURES (OCTOPUS)	Police (PP)	2008	- Article 26 de la loi du 6 janvier 1978 - Articles 322-1 et R.635-1 du Code Pénal	Rechercher les auteurs de « tags »	Identités des auteurs identifiés, dates et lieux d'infractions, types de support, signatures et/ou « crew »	- Enquêteurs habilités de la préfecture de police - Fonctionnaires de police ou militaires de gendarmerie, sur demande	10 ans à partir du dernier fait enregistré	Indirect par l'intermédiaire de la CNIL	
FICHIER D'INFORMATION SCHENGEN (SIS)	Police								
SYSTEME D'ANALYSE ET DE LIENS DE LA VIOLENCE ASSOCIEE AU CRIME (SALVAC)	Police	2005	Article 21-1 de la loi du 18 mars 2003 Projet de décret et dossier de déclaration en cours d'examen à la CNIL	Identifier les auteurs de crimes ou délits commis en série, dans le domaine de la criminalité violente	Renseignements concernant les suspects, mis en cause et victimes	- Policiers et gendarmes de l'office central pour la répression des violences aux personnes (OCRVP) - Autorités judiciaires - Coopération internationale et services de police étrangers	40 ans		
ANACRIM	Gendarmerie et Police		Loi 2005-1549 du 12.12.2005 et Loi 2003-239 du 18.03.2003	Rechercher et mettre en évidence des relations entre des données issues des enquêtes	Informations issues des procédures établies dans le cadre de certaines enquêtes judiciaires, délictuelles ou criminelles	- Militaires de la Gendarmerie exerçant des missions de police judiciaire, - Autorités judiciaires, - Avocats des mis en cause et des victimes constituées parties civiles	Le temps des investigations		

FICHIER RELATIF A LA CARTE NATIONALE D'IDENTITE	DLPAJ	1987	Décret 55-1397 du 22 octobre 1955	- Limiter les risques de contrefaçon et de falsification - Mettre en œuvre les procédures de délivrance ou renouvellement - Permettre au titulaire d'une carte d'identité de justifier de son identité - Faciliter l'action des policiers et gendarmes lors du franchissement des frontières	- Données personnelles du titulaire de la carte - Informations relatives à la gestion de la demande (date, numéro de carte, etc.)	- Certains fonctionnaires et agents en poste au ministère de l'Intérieur, dans les préfectures ou sous-préfectures, dans les consulats - Agents de la DGGN, DGPN et DGSE en charge de la lutte contre le terrorisme	15 ans	Direct	
FICHIER RELATIF AUX PASSEPORTS (DELPHINE ET TES)	DLPAJ		- Décret 2005-1726 du 30 décembre 2005	- Mettre en œuvre les procédures d'établissement, de délivrance, de renouvellement et de retrait des passeports - prévenir et détecter leur falsification ou contrefaçon	- Données personnelles du titulaire du passeport - Informations relatives à la gestion de la demande	- Certains fonctionnaires et agents en poste au ministère de l'Intérieur, dans les préfectures ou sous-préfectures, dans les consulats - Agents de la DGGN, DGPN et DGSE en charge de la lutte contre le terrorisme	- 15 ans pour les majeurs - 10 ans pour les mineurs	Direct	
FICHIER DE SUIVI DES TITRES DE CIRCULATION DELIVRES AUX PERSONNES SANS DOMICILE NI RESIDENCE FIXE (SDRF)	Gendarmerie		Arrêté interministériel du 22.03.1994 modifié par l'arrêté du 28.02.2005	Assurer le suivi des titres de circulation délivrés aux personnes circulant en France sans domicile ni résidence fixe	- Etat-civil du titulaire du titre, - Photographie, - Informations sur le titre (N°, date, etc.)	- Unités de Gendarmerie - Services de Police - Services préfectoraux	- 6 mois après la sédentarisation du titulaire - Fiches détruites au décès de la personne SDRF ou lorsqu'elle atteint 80 ans	Directs, auprès de la DGGN	
FICHIER NATIONAL DES PERMIS DE CONDUIRE (FNPC)	DLAPJ	1972	Code de la route Arrêté du 20 décembre 1972	Enregistrer et gérer les informations relatives aux permis de conduire	Informations relatives au titulaire (état-civil, adresse, etc.) et au titre (validité, numéro, etc.)	- Agents du service du FNPC - Juges et préfets - Policiers et gendarmes - Intéressé (ainsi que son avocat et son mandataire)			
TRAITEMENT DE DONNEES « PRE-PLAINTE EN LIGNE » (PPL)	Police	En cours d'expérimentation	- Décret du 29 octobre 2008 - Délibération CNIL du 29 avril 2008	Permettre à la victime ou son représentant de faire une déclaration en ligne, pour certaines infractions, et d'obtenir un rendez-vous pour la signature de la plainte.	- Données relatives aux personnes physiques ou morales - Données relatives aux faits rapportés - Données relatives au service de police ou l'unité de gendarmerie - Numéro d'identifiant délivré à la victime	- Fonctionnaires de police habilités - Militaires de la gendarmerie de l'unité choisie pour la signature de la plainte	Données à caractère personnel effacées à la signature de la plainte (à défaut de signature, effacement automatique après 30 jours)		
ATHEN@	Gendarmerie	En projet	Dossier de déclaration déposé en avril 2008 à la direction des affaires juridiques du ministère de la Défense Déclaration CNIL V2 en cours avant envoi à DLPAJ	- Améliorer l'accueil du public et la relation aux usagers - Aider et sécuriser les interventions - Optimiser le traitement du renseignement d'ordre public et de défense	- Données structurées opérationnelles - Données structurées traitant d'événements d'ordre public - Documents structurés de renseignements - Fiches de renseignement sur certaines personnes inscrites d'autorité (violentes, détentrices d'armes ou de chiens dangereux, etc.) ou à la demande de certaines personnes (tranquillité vacances, personnes âgées...)	- Personnels habilités de la gendarmerie	De 2 à 15 ans, selon le type de données		athen@ est destiné à remplacer le FAR et la base aramis.

PULS@R	Gendarmerie	Déploiement prévu en 2009		- Gérer le service et les registres ainsi que les amendes forfaitaires - Générer les messages d'information statistique et les bulletins d'analyse des accidents	Dans certains modules, informations relatives aux personnels, aux victimes (y compris d'accidents) et aux mis en cause	- Personnels de la Gendarmerie - ONISR, CUB et CEESAR pour les données relatives aux accidents de la circulation	Variable selon les modules, sans excéder 3 ans		PULS@R est une évolution de l'application BB 2000, déclarée a la CNIL
APPLICATION DE RECUEIL DE LA DOCUMEN-TATION OPERATION-NELLE ET D'INFOR-MATIONS STATISTIQUES SUR LES ENQUETES (ARDOISE)	Police	Pas encore déployée	Déclaration du traitement en cours (avis CNIL rendu, Conseil d'Etat saisi)	Collecter et archiver les informations recueillies lors des missions de police judiciaire ou administrative	Données issues de procès-verbaux, comptes-rendus d'enquêtes et rapports administratifs ou judiciaires	Fonctionnaires habilités des services de police Militaires de la gendarmerie en fonction dans un service de police Autorités judiciaires	5 ans à compter de la transmission de la procédure à l'autorité judiciaire ou administrative compétente	DAI	
FICHIER DES OBJETS SIGNALES (FOS)	Gendarmerie		Aucune	Vérifier si un objet précisément identifié est signalé volé	Eléments descriptifs textuels ou photographiques de 9 catégories d'objets (armes à feu, documents d'identité, etc.)	- Unités de Gendarmerie - Certains services de la Police nationale - GIR - CCPD - Services policiers et judiciaires européens connectés au SIS			Le FOS doit fusionner avec le STIC objets au sein du FOVES (fichier des objets et véhicules signalés) qui devrait être mis en place au 2ème trimestre 2009.
SYSTEME DE TRAITEMENT DES IMAGES DES VEHICULES VOLES (STIVV)	Gendarmerie		En phase préparatoire de déclaration auprès de la CNIL	Exploiter à des fins judiciaires les photographies prises par les radars automatisés de certains véhicules (volés, mis sous surveillance, etc.)	- Photographies de chaque véhicule concerné - renseignements sur l'infraction (date, heure, lieu, vitesses enregistrée et autorisée)	- Unité de Gendarmerie ou service de Police ayant enregistré le vol ou sollicité la mise sous surveillance - Unité territorialement compétente au lieu de l'infraction	Non prévus pour le moment		L'abandon du système est envisagé, pour éviter une redondance avec le SCTL.
LECTURE AUTOMATISEE DES PLAQUES D'IMMATRI-CULATION (LAPI)	Ministère de l'intérieur, de la défense et du budget	En cours d'expérimentation	Arrêté du 02 mars 2007	Prévenir et réprimer certains types d'infractions : - en matière de terrorisme - criminelles ou relatives à la criminalité organisée - vols ou recels de véhicules volés - contrebande, importation ou exportation en bande organisée - opérations financières définies à l'article 415 du code des douanes	- Photographie du numéro d'immatriculation, du véhicule et des occupants - Pour chaque photographie : date, heure et localisation du dispositif de contrôle automatisé	Fonctionnaires de police, militaires de la gendarmerie et agents des douanes habilités.	De 8 jours à 1 mois	Indirect par l'intermédiaire de la CNIL	Le dossier de pérennisation du LAPI est en cours d'examen par la DLPAJ.
APPLICATION JUDICIAIRE DEDIEE A LA REVELATION DES CRIMES ET DELITS EN SERIE (AJDRCDS)	Gendarmerie	En phase de conception		Faciliter la détection : - des crimes et délits de même nature et imputables à un même auteur ou groupe d'auteurs - des infractions ou comportements délinquantiels polymorphes	Tout type de données ayant un rapport direct avec une affaire judiciaire	- Personnels de la gendarmerie et de la police nationale, servant en unité de recherches et habilités judiciairement - Magistrats, OPJ et APJ chargés des investigations	Variable	Directs, auprès du magistrat référent du fichier	

CELLULE OPERATIONNELLE DE RAPPROCHEMENT ET D'ANALYSE DES INFRACTIONS LIEES (CORAIL)	Police		- Article 26 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés - Article D. 3 du code de procédure pénale	- Mutualisation des diffusions d'informations opérationnelles auprès des enquêteurs (télégrammes via le réseau de commandement (RESCOM), circulaires d'information et de recherche diffusées par la police judiciaire.). - Gestion des GAV - Etablissement de synthèses d'affaires	Données - issues des télégrammes d'information ou de la MCI - d'affaire, ou de synthèse - de gardes à vue - photographiques	OPJ et APJ spécialement habilités des services de police judiciaire situés dans le ressort des DRPJ de Paris et de Versailles	Les données d'affaires sont conservées trois ans lorsque l'auteur n'a pas été identifié et dix ans lorsque l'auteur a été identifié.	Indirect	
APPLICATION DE RAPPROCHEMENTS, D'IDENTIFICATION ET D'ANALYSE POUR LES ENQUETEURS (AR1@NE)	Police Gendarmerie		Déclaration à la CNIL en cours d'élaboration	Faciliter la constatation des infractions, le rassemblement des preuves et la recherche des auteurs + statistiques Permettra une plus grande efficacité dans le cadre des enquêtes impliquant des malfaiteurs récidivistes	Les informations contenues dans ARIANE respecteront les mêmes règles que les applications STIC et JUDEX actuelles.	- Personnels de la Gendarmerie, de la Police nationale, des Douanes, autorités judiciaires, organismes de coopération internationale et services de police étrangers, - Certains personnels investis d'une mission de police administrative	Idem que pour STIC et JUDEX		Par rapport au STIC et à JUDEX, deux nouvelles catégories de données seront intégrées au système : morts suspectes et disparitions inquiétantes.

ANNEXES

ANNEXE 1 - LISTE DES PROFESSIONS POUR LESQUELLES LA CONSULTATION DES FICHIERS D'ANTECENT JUDIXCIAIRE EST AUTORISE

Décret n° 2005-1124 du 6 septembre 2005 pris pour l'application de l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 et fixant la liste des enquêtes administratives donnant lieu à la consultation des traitements automatisés de données personnelles mentionnés à l'article 21 de la loi n° 2003-239 du 18 mars 2003

NOR: INTD0500247D

Le Premier ministre,

Sur le rapport du ministre d'Etat, ministre de l'intérieur et de l'aménagement du territoire,

Vu l'ordonnance n° 58-1270 du 22 décembre 1958 modifiée portant loi organique relative au statut de la magistrature, notamment ses articles 16, 18-1, 21-1, 22, 23, 40, 40-1, 41-10 et 41-17 ;

Vu le code pénal, notamment ses articles 226-3, 413-5 et 413-7 ;

Vu le code de procédure pénale, notamment ses articles 21, 29-1, 529-4, R. 15-33-30, R. 15-34, R. 15-35, R. 16 et R. 57-23 ;

Vu le code général des collectivités territoriales, notamment ses articles L. 2512-16 et L. 2512-16-1 ;

Vu le code des communes, notamment ses articles L. 412-48 et L. 412-49 ;

Vu le code de l'aviation civile, notamment ses articles L. 282-8 et R. 213-4 ;

Vu le code des ports maritimes, notamment son article L. 324-5 ;

Vu le code de la route, notamment son article L. 130-4 ;

Vu le code de la défense, notamment ses articles L. 1332-1, L. 1333-2 et L. 2352-1 ;

Vu la loi du 15 juin 1907 modifiée réglementant le jeu dans les cercles et casinos des stations balnéaires, thermales ou climatiques, notamment ses articles 1er à 3 ;

Vu la loi du 30 juin 1923 portant fixation du budget général des dépenses et des recettes de l'exercice 1923, modifiée par la loi n° 85-1407 du 30 décembre 1985, notamment son article 47 ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée en dernier lieu par la loi n° 2004-801 du 6 août 2004, notamment ses articles 11, 19 et 44 ;

Vu la loi n° 83-628 du 12 juillet 1983 relative aux jeux de hasard, modifiée par la loi n° 2004-204 du 9 mars 2004, notamment son article 2 ;

Vu la loi n° 83-629 du 12 juillet 1983 modifiée réglementant les activités privées de sécurité ;

Vu la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques, modifiée par la loi n° 2004-669 du 9 juillet 2004 ;

Vu la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, modifiée en dernier lieu par la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, notamment son article 17-1 ;

Vu la loi n° 96-542 du 19 juin 1996 relative au contrôle de la fabrication et du commerce de certaines substances susceptibles d'être utilisées pour la fabrication illicite de stupéfiants ou de substances psychotropes, modifiée par l'ordonnance n° 98-728 du 20 août 1998 ;

Vu la loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations, notamment son article 19 ;

Vu la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, notamment ses articles 21, 121 et 131 ;

Vu le décret n° 59-1489 du 22 décembre 1959 modifié portant réglementation des jeux dans les casinos des stations balnéaires, thermales et climatiques, notamment son article 8 ;

Vu le décret n° 71-753 du 10 septembre 1971 pris pour l'application de l'article 1er de la loi du 3 juillet 1970 portant réforme du régime des poudres et substances explosives, modifié par le décret n° 90-154 du 16 février 1990 et le décret n° 96-1046 du 28 novembre 1996 ;

Vu le décret n° 81-512 du 12 mai 1981 relatif à la protection et au contrôle des matières nucléaires, modifié

par le décret n° 94-604 du 19 juillet 1994, notamment son article 3 ;

Vu le décret n° 81-972 du 21 octobre 1981 modifié relatif au marquage, à l'acquisition, à la livraison, à la détention, au transport et à l'emploi des produits explosifs ;

Vu le décret n° 83-922 du 20 octobre 1983 modifié relatif aux sociétés de courses de lévriers autorisées à organiser le pari mutuel, notamment son article 5 ;

Vu le décret n° 87-604 du 31 juillet 1987 relatif à l'habilitation des personnes auxquelles peuvent être confiées certaines fonctions dans les établissements pénitentiaires et complétant l'article R. 79 du code de procédure pénale, modifié par le décret n° 94-965 du 2 novembre 1994 ;

Vu le décret n° 90-153 du 16 février 1990 modifié portant diverses dispositions relatives au régime des produits explosifs ;

Vu le décret n° 93-119 du 28 janvier 1993 relatif à la désignation des agents qualifiés pour la réalisation des opérations matérielles nécessaires à la mise en place des interceptions de correspondances émises par voie de télécommunications autorisées par la loi n° 91-646 du 10 juillet 1991 ;

Vu le décret n° 94-473 du 3 juin 1994 relatif à la désignation dans les territoires de la Nouvelle-Calédonie, de la Polynésie française et des îles Wallis et Futuna des agents qualifiés pour la réalisation des opérations matérielles nécessaires à la mise en place des interceptions de correspondances émises par voie de télécommunications autorisées par la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par voie de télécommunications ;

Vu le décret n° 95-589 du 6 mai 1995 modifié relatif à l'application du décret du 18 avril 1939 fixant le régime des matériels de guerre, armes et munitions ;

Vu le décret n° 97-456 du 5 mai 1997 modifié relatif aux sociétés de courses de chevaux et au pari mutuel, notamment ses articles 12 et 27 ;

Vu le décret n° 97-1135 du 9 décembre 1997 fixant les règles relatives à l'installation et au fonctionnement des casinos, cercles, jeux et loteries en Polynésie française, modifié par le décret n° 2002-814 du 3 mai 2002, notamment ses articles 15, 18 et 26 ;

Vu le décret n° 98-608 du 17 juillet 1998 relatif à la protection des secrets de la défense nationale ;

Vu le décret n° 2000-276 du 24 mars 2000 fixant les modalités d'application de l'article L. 412-51 du code des communes et relatif à l'armement des agents de police municipale ;

Vu le décret n° 2000-376 du 28 avril 2000 modifié relatif à la protection des transports de fonds, notamment son article 10 ;

Vu le décret n° 2005-1122 du 6 septembre 2005 pris pour l'application de la loi n° 83-629 du 12 juillet 1983 réglementant les activités privées de sécurité et relatif à l'aptitude professionnelle des dirigeants et des salariés des entreprises exerçant des activités de surveillance et de gardiennage, de transport de fonds et de protection physique des personnes, notamment son article 4 ;

Vu le décret n° 2005-1123 du 6 septembre 2005 pris pour l'application de la loi n° 83-629 du 12 juillet 1983 réglementant les activités privées de sécurité et relatif à la qualification professionnelle des dirigeants et à l'aptitude professionnelle des salariés des agences de recherches privées, notamment son article 4 ;

Le Conseil d'Etat (section de l'intérieur) entendu,

Décrète :

Article 1

La liste des décisions pouvant donner lieu, lors d'enquêtes administratives préalables, à la consultation, dans les limites fixées au deuxième alinéa de l'article 17-1 de la loi du 21 janvier 1995 susvisée, des traitements automatisés de données personnelles mentionnés à l'article 21 de la loi du 18 mars 2003 susvisée est ainsi fixée :

I. - En ce qui concerne les emplois publics participant à l'exercice des missions de souveraineté de l'Etat et les emplois publics ou privés relevant du domaine de la sécurité ou de la défense :

1° Autorisation ou habilitation :

a) Des personnes physiques ayant accès aux informations et supports protégés au titre du secret de la défense nationale ;

b) Des personnes physiques convoyant des informations ou supports protégés au titre du secret de la défense nationale ;

c) Des personnes physiques employées pour participer à une activité privée de surveillance et de gardiennage, de transport de fonds, de protection physique des personnes ou à une activité de recherches privées, ou suivant un stage pratique dans une entreprise exerçant une telle activité ;

d) Des agents des services internes de sécurité de la Société nationale des chemins de fer français et de la Régie autonome des transports parisiens, préalablement à leur affectation ;

e) Des agents de la Commission nationale de l'informatique et des libertés appelés à participer à la mise en œuvre des missions de vérification de traitements de données à caractère personnel ;

f) Des médiateurs et des délégués du procureur de la République ;

g) Des enquêteurs de personnalité et des contrôleurs judiciaires ;

h) Des agents qualifiés pour la réalisation des opérations matérielles nécessaires à la mise en place des interceptions de correspondances émises par la voie des communications électroniques, autorisées par la loi du 10 juillet 1991 susvisée ;

i) Des personnes mettant en œuvre le dispositif technique permettant le contrôle à distance des personnes placées sous surveillance électronique ;

2° Recrutement des membres des juridictions administratives, des magistrats de l'ordre judiciaire et des juges de proximité ;

3° Recrutement ou nomination et affectation :

a) Des préfets et sous-préfets ;

b) Des ambassadeurs et consuls ;

c) Des directeurs de préfecture chargés de la réglementation et des libertés publiques ;

d) Des chefs des services interministériels des affaires civiles et économiques de défense et de protection civile ;

e) Des directeurs et chefs de service des cabinets des préfets ;

f) Des personnels investis de missions de police administrative spécialement habilités, en application du quatrième alinéa de l'article 17-1 de la loi du 21 janvier 1995 susvisée, à consulter les traitements automatisés de données personnelles mentionnés à l'article 21 de la loi du 18 mars 2003 susvisée ;

g) Des fonctionnaires et agents contractuels de la police nationale ;

h) Des agents des douanes ;

i) Des personnels des services de l'administration pénitentiaire ;

j) Des militaires ;

k) Des officiers de port et officiers de port adjoints ;

l) Des agents de surveillance de Paris ;

4° Agrément :

a) Des agents de police municipale ;

b) Des gardes champêtres ;

c) Des agents de l'Etat ou des communes chargés de la surveillance de la voie publique ;

d) Des agents des services publics urbains de transport en commun de voyageurs mentionnés à l'article L. 130-4 du code de la route ;

e) Des agents des concessionnaires d'une autoroute ou d'un ouvrage routier ouvert à la circulation publique et soumis à péage ;

f) Des agents de la ville de Paris chargés d'un service de police ;

g) Des gardes particuliers ;

h) Des personnes physiques exerçant à titre individuel une activité privée de surveillance et de gardiennage,

de transport de fonds, de protection physique des personnes ou une activité de recherches privées ou dirigeant ou gérant une personne morale exerçant cette activité ;

i) Des agents de surveillance et gardiennage et des agents du service d'ordre des manifestations sportives, récréatives ou culturelles, habilités à procéder à des palpations de sécurité en application des articles 3-1 et 3-2 de la loi du 12 juillet 1983 susvisée ;

j) Des agents de sûreté désignés pour procéder aux contrôles et visites mentionnés aux articles L. 282-8 du code de l'aviation civile et L. 324-5 du code des ports maritimes ;

k) Des agents employés pour exercer une activité privée de transport de fonds, de bijoux ou de métaux précieux ;

l) Des agents des exploitants de transports publics de personnes habilités à relever l'identité et l'adresse des contrevenants, dans les conditions prévues à l'article 529-4 du code de procédure pénale ;

m) Des préposés du titulaire d'une autorisation individuelle d'exploitation d'un dépôt, débit ou installation mobile de produits explosifs, des personnes intervenant dans ces établissements en vue de l'entretien des équipements de sûreté, ainsi que des organismes chargés des études de sûreté ;

II. - En ce qui concerne les emplois privés ou activités privées réglementées relevant des domaines des jeux, paris et courses :

1° Autorisation :

a) De pratiquer les jeux de hasard dans les casinos des stations balnéaires, thermales ou climatiques ;

b) De pratiquer les jeux de hasard dans les cercles de jeux ;

c) De faire courir, d'entraîner, de monter et driver des chevaux de course ;

d) D'exploiter des postes d'enregistrement des paris relatifs aux courses de chevaux ;

e) De faire courir des lévriers de course ;

2° Agrément :

a) Des directeurs et des membres des comités de direction des casinos autorisés, ainsi que des personnes employées dans les salles de jeux des casinos et des cercles de jeux ;

b) Des personnes physiques ou morales qui fabriquent, importent, vendent ou assurent la maintenance des appareils de jeux mentionnés à l'alinéa 5 de l'article 2 de la loi du 12 juillet 1983 susvisée ;

c) Des organismes chargés par les casinos autorisés de gérer des tâches d'intérêt commun comme la centralisation des commandes et le financement groupé d'appareils dont les marques sont agréées ;

d) Des commissaires et des juges des courses de chevaux ;

e) Des arbitres et assesseurs des parties de pelote basque.

III. - En ce qui concerne les zones protégées en raison de l'activité qui s'y exerce, les autorisations d'accès :

1° Aux zones militaires ou placées sous le contrôle de l'autorité militaire ;

2° Aux zones protégées intéressant la défense nationale mentionnées à l'article 413-7 du code pénal ;

3° Aux établissements, installations ou ouvrages d'importance vitale, mentionnés aux articles L. 1332-1 et L. 1332-2 du code de la défense ;

4° Aux zones non librement accessibles des aérodromes, aux zones d'accès restreint, délimitées à l'intérieur des zones portuaires de sûreté et aux installations de la navigation aérienne ;

5° Aux établissements pénitentiaires, pour les personnes autres que les conseils des détenus.

IV. - En ce qui concerne les matériels, produits ou activités présentant un danger pour la sécurité publique, les autorisations ou agréments :

1° De fabrication, de commerce, d'acquisition, de détention, d'importation et d'exportation de matériels de guerre, armes et munitions ;

2° De port d'armes ;

3° De production, d'importation, d'exportation, de commerce, d'emploi, de transport et de conservation des poudres et substances explosives ;

4° D'élaboration, de détention, de transfert, d'utilisation, d'importation, d'exportation et de transport de matières nucléaires ;

5° De fabrication, d'importation, de détention, d'exposition, d'offre, de location ou de vente d'appareils mentionnés à l'article 226-3 du code pénal ;

6° De création d'un aérodrome ou d'une hélisurface privés ou d'utilisation d'une hélisurface, d'une hydrosurface, ou d'une bande d'envol occasionnelle ;

7° De prise de vue aérienne au titre d'une des procédures prévues à l'article D.133-10 du code de l'aviation civile ;

8° De fabrication, transformation et mise à disposition des tiers, à titre onéreux ou gratuit, des substances susceptibles d'être utilisées pour la fabrication illicite de stupéfiants ou de substances psychotropes, mentionnées à l'article 1er de la loi du 19 juin 1996 susvisée.

Article 2

Les personnes qui font l'objet d'une enquête administrative mentionnée dans la liste fixée à l'article 1er sont informées de ce qu'elle donne lieu à la consultation des traitements automatisés de données personnelles prévus par l'article 21 de la loi du 18 mars 2003 susvisée.

Lorsque la décision administrative qui donne lieu à la consultation fait suite à une demande de l'intéressé, celui-ci en est informé dans l'accusé de réception de sa demande prévu à l'article 19 de la loi du 12 avril 2000 susvisée.

Dans les autres cas, l'intéressé est informé lors de la notification de la décision administrative le concernant.

Article 3

Les dispositions du présent décret ne sont pas applicables aux procédures de recrutement en cours à la date de son entrée en vigueur.

Article 4

Le décret n° 2002-424 du 28 mars 2002 pris pour l'application de l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 et fixant la liste des enquêtes administratives pouvant donner lieu à la consultation de traitements autorisés de données personnelles est abrogé.

Article 5

Les dispositions du présent décret sont applicables à Mayotte, en Polynésie française, dans les îles Wallis et Futuna et en Nouvelle-Calédonie.

Article 6

Le ministre d'Etat, ministre de l'intérieur et de l'aménagement du territoire, la ministre de la défense, le garde des sceaux, ministre de la justice, et le ministre de l'outre-mer sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au Journal officiel de la République française.

Fait à Paris, le 6 septembre 2005.

ANNEXE 2 - FORMULAIRE NAVETTE ENTRE LE PARQUET DE PARIS ET LA PREFECTURE DE POLICE EN VUE DE LA MISE A JOUR DU STIC

PREFECTURE DE POLICE

Paris, le 12 novembre 2008

Expéditeur **DIRECTION DE LA POLICE JUDICIAIRE – ETAT MAJOR**
DIVISION DE LA STATISTIQUE ET DE LA DOCUMENTATION CRIMINELLE
36 quai des orfèvres 75001 PARIS

Affaire suivie par , Brigadier Chef de Police
N° de téléphone **N° de télécopieur**

Destinataire **TGI de PARIS Exécution des Peines**
À l'attention de **Section A2 – Bureau 11 bis**
N° de télécopieur

Objet Demande de communication des suites pénales

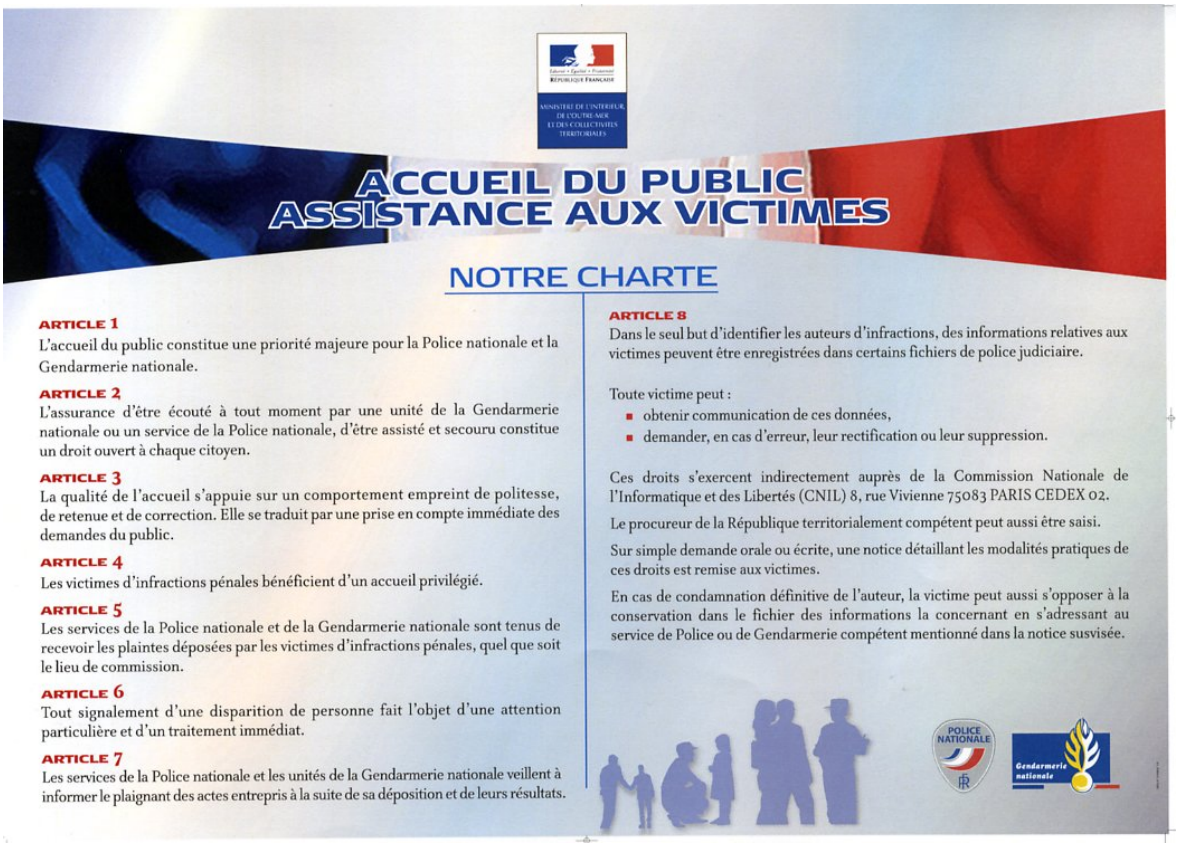
PERSONNE CONCERNEE :
Nom Prénom
Date-lieu de naissance
Adresse

PROCEDURE :
Numéro
service **Brigade des stupéfiants Paris (75)**
qualification **Infraction à la législation sur les stupéfiants**
date-lieu des faits **04 mai 1997 à Paris 11ème (75)**

Classement sans suite pour insuffisance de charges 11 et 21		Autres classements sans suite (motif)	Non lieu		relaxe		acquittement		Condamnations (détail)
MENTION	EFFACEMENT		MENTION	EFFACEMENT	MENTION	EFFACEMENT	MENTION	EFFACEMENT	

Merci de bien vouloir indiquer le motif des autres classements sans suite et le détail des condamnations

ANNEXE 3 - CHARTE D'ACCUEIL DU PUBLIC DE LA POLICE ET DE LA GENDARMERIE NATIONALES



ACCUEIL DU PUBLIC ASSISTANCE AUX VICTIMES

NOTRE CHARTE

ARTICLE 1
L'accueil du public constitue une priorité majeure pour la Police nationale et la Gendarmerie nationale.

ARTICLE 2
L'assurance d'être écouté à tout moment par une unité de la Gendarmerie nationale ou un service de la Police nationale, d'être assisté et secouru constitue un droit ouvert à chaque citoyen.

ARTICLE 3
La qualité de l'accueil s'appuie sur un comportement empreint de politesse, de retenue et de correction. Elle se traduit par une prise en compte immédiate des demandes du public.

ARTICLE 4
Les victimes d'infractions pénales bénéficient d'un accueil privilégié.

ARTICLE 5
Les services de la Police nationale et de la Gendarmerie nationale sont tenus de recevoir les plaintes déposées par les victimes d'infractions pénales, quel que soit le lieu de commission.

ARTICLE 6
Tout signalement d'une disparition de personne fait l'objet d'une attention particulière et d'un traitement immédiat.

ARTICLE 7
Les services de la Police nationale et les unités de la Gendarmerie nationale veillent à informer le plaignant des actes entrepris à la suite de sa déposition et de leurs résultats.

ARTICLE 8
Dans le seul but d'identifier les auteurs d'infractions, des informations relatives aux victimes peuvent être enregistrées dans certains fichiers de police judiciaire.

Toute victime peut :
- obtenir communication de ces données,
- demander, en cas d'erreur, leur rectification ou leur suppression.

Ces droits s'exercent indirectement auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL) 8, rue Vivienne 75083 PARIS CEDEX 02.

Le procureur de la République territorialement compétent peut aussi être saisi.

Sur simple demande orale ou écrite, une notice détaillant les modalités pratiques de ces droits est remise aux victimes.

En cas de condamnation définitive de l'auteur, la victime peut aussi s'opposer à la conservation dans le fichier des informations la concernant en s'adressant au service de Police ou de Gendarmerie compétent mentionné dans la notice susvisée.

ANNEXE 4 - COMMUNIQUE DU SYNDICAT DE LA MAGISTRATURE ET REPONSE D'ALAIN BAUER

AFP – 15/11/2008

Le Syndicat de la magistrature se retire du groupe de travail sur les fichiers présidé par M.Bauer

Le Syndicat de la magistrature indique qu'il ne participera plus aux travaux du groupe de travail sur les fichiers réactivé par la ministre de l'intérieur suite à la forte mobilisation contre EDVIGE.

La place très minoritaire de la « société civile » au sein de ce groupe (c'est-à-dire des personnes ne faisant partie ni de la police ni de la gendarmerie), le choix de ne pas associer aux travaux du groupe le collectif « Non à EDVIGE », la brièveté du calendrier (les conclusions doivent être rendues à la mi-décembre), l'absence de réponses aux questions précises qui sont posées sur les fichiers, font que le Syndicat de la magistrature estime ne pas avoir sa place au sein d'un groupe dont le regard critique et la marge de manœuvre à l'égard du gouvernement apparaissent quasiment nuls.

Le Syndicat de la magistrature poursuit, dans le cadre du collectif « non à EDVIGE », une action militante visant à susciter un débat public salutaire et à contester la prolifération des fichiers.

Commmuniqué d'Alain Bauer, président du groupe de contrôle sur les fichiers de police et de gendarmerie

Suite au communiqué de presse du Syndicat de la Magistrature annonçant son retrait du groupe de travail sur le contrôle des fichiers de police et de gendarmerie, Alain BAUER, Président du groupe de travail, regrette cette démission qui fera chuter le nombre de membres issus de la société civile de 17 sur 22 à 16 sur 21.

Il constate, au regard de la composition du groupe de travail, que les représentants des administrations ne sont qu'au nombre de 5 dont 4 représentants du ministère de l'Intérieur et 1 représentant du ministère de la Justice.

Il souligne la vigilance critique réaffirmée ce matin en réunion par les membres du groupe de travail.

Alain BAUER

Composition du groupe de travail

- Monsieur Alain BAUER, Criminologue, Président
- Monsieur le Directeur Général de la Police Nationale (Frédéric Péchenard)
- Monsieur le Directeur Général de la Gendarmerie Nationale (Général Roland Gilles)
- Monsieur le Préfet de Police (Michel Gaudin)
- Monsieur le Directeur des Libertés Publiques et des Affaires Juridiques (Laurent Touvet)
- Monsieur le Directeur des Affaires Criminelles et des Grâces (Jean-Marie Huet)
- Monsieur le Président de la CNIL (Alex Türk)
- Monsieur le Président de la HALDE (Louis Schweitzer)
- Monsieur le Président de la CNCDH (Joël Thoraval)
- Monsieur le Médiateur de la République (Jean-Paul Delevoye)
- Monsieur le Secrétaire Général de Synergie Police (Bruno Beschizza)
- Monsieur le Secrétaire Général de l'UNSA Police (Henri Martini)
- Madame le Secrétaire Général du SCPN (Sylvie Feucher)
- Monsieur le Président de l'Union Syndicale des Magistrats (Bruno Thouzellier)
- Madame la Présidente du Syndicat de la magistrature (Emmanuelle Perreux)
- Monsieur le Président du Conseil National des Barreaux (Paul-Albert Iweins)
- Monsieur le Président de la Conférence des Bâtonniers (Pascal Eydoux)
- Monsieur le Bâtonnier de Paris (Christian Charrière-Bournazel)
- Monsieur le Président de la LICRA (Patrick Gaubert)
- Monsieur le Président de SOS Racisme (Dominique Sopo)
- Monsieur le Président de SOS Homophobie (Jacques Lizé)
- Monsieur Jean-Marc Leclerc, Journaliste, Le Figaro

ANNEXE 5 - ARTICLE DE COME JACQMIN, MAGISTRAT

Les mineurs pris dans la folie du fichage, par Côme Jacqmin

Article mis en ligne le dimanche 22 avril 2007 - LDH Toulon

Un article de Côme Jacqmin, juge des enfants à Nice paru dans Justice n° 190, avril 2007 - bulletin du Syndicat de la Magistrature [1]

La folie des fichiers n'a pas épargné les mineurs. Ils seront de ce point de vue en première ligne lors de l'entrée en vigueur de la prochaine loi sur la prévention de la délinquance qui prévoit notamment l'échange des fichiers entre l'Education nationale et les municipalités pour contrôler le respect de l'obligation de scolarisation.

S'agissant des fichiers de police, les mineurs sont fichés comme les majeurs, notamment dans le FAED (fichier des empreintes digitales), dans le STIC (système de traitement des infractions constatées), le FIJAIS (fichier des auteurs d'infractions sexuelles), ou le FNAEG (fichier national automatisé des empreintes génétiques). A ceci s'ajoute, arrivé au palais de justice, l'enregistrement dans le fichier du bureau d'ordre puis dans celui du tribunal pour enfants, pour échouer au casier judiciaire...

Des fichiers judiciaires pas plus protecteurs que les fichiers de police

Les fichiers judiciaires ne donnent pas particulièrement l'exemple d'une protection spécifique des mineurs contre l'inévitable érosion du droit à l'oubli qu'engendre cette prolifération. Le fichier du bureau d'ordre et celui du tribunal pour enfants, traditionnellement jamais contrôlés ni apurés, sont sans doute ceux qui prennent le moins en compte cette préoccupation : qui en effet fixe la durée de conservation de ces données ? Qui veille, notamment en cas d'amnistie, à leur effacement ? On peut aussi rappeler d'ailleurs que l'ordonnance de 1945 prévoit, sans plus de précision et sans aucune disposition protectrice autre que le caractère « non public », l'institution d'un registre spécial de toutes les décisions « concernant les mineurs, y compris celles intervenues sur incident à la liberté surveillée, instances modificatives de placement, ou de garde et de remises de garde » (article 38 de l'ordonnance, toujours en vigueur).

Le régime du casier judiciaire lui-même a largement perdu les aspects protecteurs qui résultaient de l'article 769-2 du Code de procédure pénale. Avant son abrogation par la loi Perben II, cet article prévoyait, à l'âge de 18 ans, l'effacement des mentions relatives à des mesures éducatives prononcées en application de l'ordonnance de 1945 ou à des condamnations à des peines d'amende ou d'emprisonnement inférieures à deux mois. Depuis la loi Perben II, les mesures éducatives restent inscrites au bulletin N° 1 du casier judiciaire pendant 3 ans à compter de leur prononcé, y compris après la majorité. Les autres exceptions autrefois prévues ont définitivement disparu, sauf à rappeler que subsistent les dispositions de l'article 770 du Code de procédure pénale qui permettent, à l'expiration d'un délai de trois ans suivant la décision, d'en ordonner spécialement l'effacement.

Certes plus encadré, par un décret du 8 avril 1987, le fichier des empreintes digitales ne réserve pas pour autant un sort plus envieux à la minorité : aucune règle dérogatoire ne s'applique aux mis en cause mineurs dont les empreintes sont relevées et enregistrées. Comme les autres, leurs empreintes digitales seront conservées pendant 25 ans.

Sans exclure les mineurs de leur champ d'application, les fichiers les plus récents leur offrent finalement des garanties supplémentaires.

Les délais de conservation au STIC sont raccourcis à 5, 10 ou 20 ans en fonction de la nature des infractions commises au lieu de 20, ou 40 ans pour les majeurs. S'agissant du FIJAIS, la décision du Conseil constitutionnel du 2 mars 2004 a précisé que l'inscription automatique prévue par l'article 706-53-2 dernier alinéa du Code de procédure pénale ne trouvait à s'appliquer, en ce qui concerne les mineurs, qu'en tenant compte de l'atténuation de peine dont ils bénéficient en application de l'article 20-2 de l'ordonnance du 2 février 1945. Ainsi les mineurs ne sont-ils soumis à l'inscription automatique au FIJAIS que pour des infractions passibles d'une peine de 10 ans d'emprisonnement au moins au lieu de 5. L'article 706-53-10 de ce même code prévoit d'autre part une possibilité d'effacement à la demande de l'intéressé lorsque l'inscription n'apparaît plus nécessaire compte tenu de la finalité du fichier, notamment au regard de l'âge de l'intéressé au moment de l'infraction, disposition qui trouverait particulièrement à s'appliquer aux mineurs.

La Chancellerie et le fichage génétique des mineurs

Le FNAEG, fer de lance de la nouvelle politique de fichage depuis octobre 2004, ne comporte en apparence aucune disposition spécialement protectrice au bénéfice des mineurs. Les règles applicables restent même sur certains points marquées d'un certain flou. Ainsi, hors le cas de personnes condamnées pour crime ou délit

puni de plus de 10 ans d'emprisonnement le prélèvement biologique nécessaire au fichage est soumis au consentement de la personne sur laquelle le prélèvement est effectué. Quid, s'agissant des mineurs de l'information, voire du consentement des détenteurs de l'autorité parentale ?

Pourtant, une note de la direction des affaires et des grâces du 23 juin 2006 attire l'attention sur les limites du champ d'application du fichier aux mineurs, en fonction des sanctions ou mesures prononcées à leur encontre. En effet, l'article 706-54 alinéa 1er du Code de procédure pénale, prévoit l'inscription des personnes « condamnées » pour l'une des infractions énumérées à l'article 706-55. La direction des affaires criminelles et des grâces propose une lecture stricte de ces textes et rappelle que les mesures éducatives prononcées par les juridictions pour mineurs ne constituent pas des condamnations. Dans ces conditions les mineurs concernés n'ont pas vocation à être systématiquement inscrits au FNAEG.

La DACG laisse cependant en suspens, sans doute à l'appréciation souveraine des juridictions, la question de la qualification qu'il convient d'attacher aux sanctions éducatives prononcées par le tribunal pour enfants en application de l'article 15-1 de l'ordonnance de 1945. Constituent-elles des condamnations susceptibles d'entraîner une inscription ? L'article 2 modifié de l'ordonnance semble distinguer d'une part les mesures éducatives (alinéa 1er) et de l'autre les sanctions éducatives et les peines (alinéa 2). De même, sanctions éducatives et peines ne peuvent être prononcées que par le tribunal pour enfants. Cela permet-il pour autant d'assimiler le prononcé d'une sanction éducative à une condamnation au sens de l'article 706-54 du CPP ? Les sanctions éducatives ne sont pas non plus des peines. D'ailleurs, leur non-respect ne peut être sanctionné que par un placement et non par une peine.

Le fichage au FNAEG, inacceptable pour les mineurs au stade de l'enquête

Sans attendre une hypothétique réponse à ces questions, l'interprétation proposée par la Chancellerie invite à des modifications des pratiques des services de police et des juridictions. Le prélèvement biologique et le fichage ADN sont aujourd'hui de plus en plus massivement effectués au stade de la garde à vue, en application de l'article 706-54 alinéa 2 du Code de procédure pénale, dès lors que la personne gardée est à vue est suspectée d'avoir commis une des infractions prévues par l'article 706-55. Une telle pratique est-elle acceptable vis-à-vis de mineurs qui, dans de nombreux cas ne feront l'objet que d'alternatives aux poursuites n'entraînant aucun fichage systématique, ou de mesures éducatives exclues du champ d'application du fichier ? De toute évidence, non. Il conviendrait donc exclure l'application de cette possibilité de prélèvement au stade de l'enquête, pour n'y procéder qu'après l'intervention d'une éventuelle condamnation. Les parquets, chargés non seulement de contrôler la police judiciaire, mais aussi, depuis l'entrée en vigueur de la LOLF, de surveiller les dépenses de frais de justice exposées par les policiers dans le cadre de leurs missions de police judiciaire pourront sans doute donner des instructions aux services de police en ce sens, sur la base de la note de la Chancellerie.

De même, les procureurs de la République, notamment comptables de l'intérêt des mineurs, peuvent-ils, lorsque le fichage aura néanmoins lieu au stade de la garde à vue, se dispenser de faire procéder d'office à l'effacement de l'inscription qui s'avérerait finalement injustifiée au vu des mesures prononcées ? De toute évidence, non. Sauf à vider totalement le texte de son sens, les parquets ne sauraient se réfugier derrière l'ambiguïté de l'alinéa 2 de l'article 706-54 qui prévoit l'effacement à leur diligence ou sur demande de l'intéressé lorsque la conservation des données « n'apparaît plus nécessaire compte tenu de la finalité du fichier ». Enfin, du côté des tribunaux pour enfants, la vigilance devrait aussi être de mise, pour qu'en cas de prononcé d'une simple mesure éducative l'attention du parquet soit attirée sur la nécessité de procéder à l'effacement.

Le droit des fichiers n'a guère épargné les mineurs. Quelques dispositions leur accordent cependant des garanties spécifiques. Encore faudra-t-il que les instances chargées de veiller à leur application leur confèrent toute leur portée.

Côme Jacqmin