

---

## Sommaire

<b>Composition du groupe de travail</b> . . . . .	<b>5</b>
<b>Lettre de mission</b> . . . . .	<b>7</b>
<b>Introduction</b> . . . . .	<b>9</b>
<b>Chapitre 1</b>	
<b>Recensement des fichiers</b> . . . . .	<b>13</b>
Les fichiers de la police nationale (sous CHEOPS) . .	<b>15</b>
Le fichier de la Direction de la surveillance du territoire (DST) . . . . .	<b>40</b>
Le Système d'analyse et de liens de la violence associée au crime (SALVAC) . . . . .	<b>42</b>
Le fichier de travail de la police judiciaire (FTPJ) . . .	<b>44</b>
Le Fichier automatisé des empreintes digitales (FAED) . . . . .	<b>44</b>
Les fichiers de la gendarmerie nationale . . . . .	<b>48</b>
ARIANE . . . . .	<b>74</b>
Le Fichier judiciaire national automatisé des auteurs d'infractions sexuelles (FIJAIS) . . . . .	<b>76</b>
Le Fichier national des permis de conduire (FNPC) .	<b>79</b>
AGRIPPA . . . . .	<b>84</b>
<b>Chapitre 2</b>	
<b>Problèmes et dysfonctionnements</b> . . . . .	<b>87</b>
<b>La saisine et l'alimentation</b> . . . . .	<b>97</b>
Les difficultés techniques . . . . .	<b>97</b>
Le respect de la finalité des fichiers selon les textes en vigueur . . . . .	<b>109</b>
<b>Le droit d'accès aux fichiers et les recours administratifs ou contentieux contre les décisions préfectorales</b> . . . . .	<b>115</b>
L'information sur le droit d'accès aux données . . . . .	<b>117</b>
Les demandes de droit d'accès indirect . . . . .	<b>120</b>
Des délais de réponse excessifs . . . . .	<b>123</b>

<b>Chapitre 3</b>	
<b>Recommandations du groupe de travail sur le contrôle des fichiers de police utilisés à des fins administratives . . . . .</b>	<b>127</b>
<b>Propositions générales . . . . .</b>	<b>131</b>
Pour améliorer la transparence des fichiers . . . . .	131
Pour une mise à jour systématique des fichiers d'antécédents judiciaires . . . . .	131
Pour une amélioration du droit d'accès aux données	133
Pour le développement de voies de recours . . . . .	134
Pour une appréciation plus juste des décisions préfectorales . . . . .	138
Poursuivre la démarche « qualité » dans l'alimentation et la mise à jour des fichiers . . . . .	139
Pour une nécessaire évolution du cadre juridique et des outils de travail des forces républicaines de sécurité . . . . .	139
<b>Recommandations particulières sur certains fichiers . . . . .</b>	<b>141</b>
Le fichier ELOI . . . . .	141
Le STIC-Canonge . . . . .	142
Le Fichier alphabétique de renseignements (FAR) . .	142
Le Fichier central automobile (FCA) . . . . .	143
<b>Annexe 1</b>	
<b>Les modalités d'exercice du droit d'accès indirect au STIC . . . . .</b>	<b>145</b>
<b>Table des matières . . . . .</b>	<b>149</b>

---

## **Composition du groupe de travail**

**Alain BAUER**, criminologue, président du conseil d'orientation de l'Observatoire nationale de la délinquance, membre du Collège de la HALDE, président du groupe de travail.

**Michel GAUDIN**, directeur général de la police nationale

**Général Guy PARAYRE**, directeur général de la gendarmerie nationale

**Martine MONTEIL**, directeur central de la police judiciaire

**Pierre BOUSQUET de FLORIAN**, directeur central de la surveillance du territoire

**Joël BOUCHITE**, directeur central des renseignements généraux

**Philippe LAUREAU**, directeur central de la sécurité publique

**Jacques LAMOTTE**, directeur de l'Inspection générale de la police nationale

**Général Edmond BUCHHEIT**, inspecteur de la gendarmerie nationale

**Général Daniel LEMERCIER**, chef du service des opérations et de l'emploi (DGGN)

**Général Serge CAILLET**, sous-directeur de la police judiciaire (DGGN)

**Stéphane FRATACCI**, directeur des libertés publiques et des affaires juridiques

**Jean-Marie HUET**, directeur des Affaires criminelles et des grâces, représenté par Myriam QUEMENER, sous-directrice de la justice générale pénale au ministère de la Justice

**François CORDIER**, procureur de la République adjoint au tribunal de grande instance de Paris

**Alex TURK**, président de la CNIL, représenté par François GIQUEL, vice-président

**Jean-Paul DELEVOYE**, Médiateur de la République, représenté par Serge PETIT

**Pierre TRUCHE**, président de la CNDS, représenté par Jean BONNARD

**Bruno THOUZELLIER**, Union syndicale des magistrats

**Bruno BESCHIZZA**, Synergie officiers

**Joaquim MASANET**, UNSA police

**Sylvie FEUCHER**, Syndicat des commissaires et hauts fonctionnaires de la police nationale

**Maître Franck NATALI**, avocat, président de la Conférence des bâtonniers

**Frédéric PLOQUIN**, journaliste *Marianne*

**Maître Henri LECLERC**, sollicité, n'a pu participer aux travaux

**Christophe SOULLEZ**, chef du département de l'observatoire national de la délinquance, rapporteur du groupe de travail

A également activement contribué au groupe de travail, **Renaud VEDEL**, directeur adjoint du cabinet du directeur général de la police nationale.



MINISTÈRE DE L'INTERIEUR  
ET DE L'AMÉNAGEMENT DU TERRITOIRE

LE MINISTRE D'ÉTAT  
CABUMBOR n° 149

Paris, le 15 JUIN 2006

Monsieur le Président,

En vous confiant la présidence du Conseil d'Orientation de l'Observatoire National de la Délinquance, j'ai délibérément fait le pari de la transparence et de la rigueur scientifique dans l'analyse de la délinquance.

Les chiffres et les analyses publiées ne font plus l'objet de contestations et la rigueur des travaux menés a permis enfin de rompre avec des pratiques anciennes tout en permettant d'analyser l'efficacité retrouvée des services de police et de gendarmerie.

Je souhaite donc vous confier une mission supplémentaire en vous demandant de bien vouloir mettre en place 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.

Votre travail devrait permettre, après un recensement des outils disponibles et des évolutions prévues pour les prochaines années en matière de fichiers de police et de gendarmerie, de proposer les solutions permettant un équilibre entre les impérieuses nécessités de protection des personnes et des biens, de lutte contre le terrorisme et le crime organisé et ma préoccupation constante de protection des libertés individuelles et collectives.

.../...

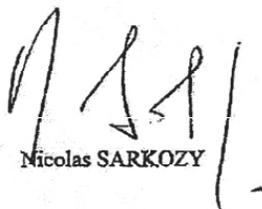
Monsieur Alain BAUER  
Président du Conseil d'orientation OND  
PPG AB Associates  
108 Boulevard Sébastopol  
75003 PARIS

Vous voudrez bien vous entourer des responsables concernés de la Police Nationale, de la Gendarmerie Nationale, de la DLPAJ, des autorités administratives concernées (CNIL, CNDS notamment) et de personnalités qualifiées pour mettre en place ce groupe qui voudra bien me remettre un rapport qui sera bien évidemment rendu public avant la fin de cette année.

Vous pourrez compter sur les personnels de l'INHES pour vous aider dans votre mission. Le Ministère de l'intérieur mettra également à votre disposition une salle de réunion en fonction de vos besoins.

En vous remerciant de votre implication personnelle sur ce dossier, je vous prie de croire, Monsieur le Président, à l'assurance de mes sentiments les meilleurs.

*Le commissaire*

  
Nicolas SARKOZY

---

# Introduction

Il existe en France de nombreux fichiers tenus par l'administration en vue de recenser des personnes en fonction de leur statut (nationaux ou étrangers, par exemple), de comptabiliser les propriétaires de véhicules ou les titulaires de permis de conduire, de dénombrer les personnes condamnées (Fichier du casier judiciaire national) ou encore contribuant à prévenir ou à réprimer les crimes, délits et contraventions.

Ces derniers fichiers sont principalement gérés par les services de police et de gendarmerie. 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 individus surveillés. Il peut aussi s'agir de fichiers contenant des traces et indices (empreintes digitales, par exemple). Ces fichiers, dits de police, jusqu'alors principalement manuels, ont progressivement été automatisés et se sont considérablement développés au cours des dix dernières années, suivant en cela l'évolution des techniques, de l'informatique et de la science tout en répondant à l'évolution parallèle des phénomènes criminels ou terroristes.

C'est une pratique très ancienne dans les services de police et de gendarmerie que de consulter les fichiers de police judiciaire pour les besoins des enquêtes administratives. L'informatisation, souvent considérée comme un risque de diffusion de données personnelles à protéger, peut paradoxalement aussi assurer le traçage de l'interrogateur et présenter ainsi de meilleures garanties pour la protection des données individuelles.

La volonté de l'État d'encadrer la consultation des fichiers de police judiciaire à des fins administratives ainsi que le développement des techniques de traçabilité dans les systèmes d'information de la police nationale ont conduit le législateur à donner un fondement juridique clair de l'usage des fichiers.

Ce fut l'objet de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne et de la loi n° 2003-239 du 18 mars 2003 relative à la sécurité intérieure, qui ont autorisé la consultation de certains

fichiers dans le cadre d'enquêtes administratives, avec l'accord du Conseil constitutionnel <sup>1</sup>.

Si l'article 17-1 modifié de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité permet, dans le cadre de certaines enquêtes administratives préalables fixées par décret en Conseil d'État <sup>2</sup>, la consultation de traitements automatisés de données à caractère personnel, elle ne l'autorise que pour les traitements visés par l'article 21 de la loi n° 2003-239 du 18 mars 2003 sur la sécurité intérieure.

Ces traitements concernent les seuls 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'État, soit les emplois publics ou privés relevant du domaine de la sécurité et de la défense, soit les emplois privés ou activités privées réglementées relevant des domaines des jeux, paris et courses.

Cette réglementation a pris d'autant plus d'importance que le législateur et le Gouvernement ont voulu renforcer la régulation du secteur de la sécurité privée, en pleine croissance et de plus en plus stratégique en raison des risques accrus dans certains points ou réseaux sensibles. Cet impératif de moralisation du secteur est indissolublement lié aux prérogatives nouvellement confiées aux agents de sécurité privée, qu'il s'agisse des fouilles dans les aéroports, des palpations de sécurité dans les stades ou de la surveillance de sites sensibles.

La plupart des fichiers automatisés de données font l'objet d'une déclaration à la Commission nationale informatique et libertés (CNIL) conformément à la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés. Toutefois, 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, l'utilisation de certains fichiers, aux finalités administratives, continue de soulever certains problèmes susceptibles d'attenter aux libertés individuelles et collectives.

C'est en vue de remédier à ces risques que, par lettre de mission du 15 juin 2006, le ministre d'État, ministre de l'Intérieur et de l'Aménagement du territoire, a décidé la création d'un groupe de travail

(1) Décision du Conseil constitutionnel n° 2003-467 DC en date du 13 mars 2003.

(2) Il s'agit en l'occurrence du 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 mentionnées à l'article 21 de la loi n° 2003-239 du 18 mars 2003.

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 ». Il est précisé que « le travail doit permettre, après un recensement des outils disponibles et des évolutions prévues pour les prochaines années en matière de fichiers de police et de gendarmerie, de proposer les solutions permettant un équilibre entre les impérieuses nécessités de protection des personnes et des biens, de lutte contre le terrorisme et le crime organisé et la préoccupation constante [du ministre] de protection des libertés individuelles et collectives ».

Le groupe de travail a donc principalement porté son attention sur les fichiers de police et de gendarmerie et a exclu de son champ de réflexion l'ensemble des fichiers gérés par d'autres administrations, à l'exception du Fichier judiciaire national automatisé des auteurs d'infractions sexuelles et violentes (FIJAIS), tenu par le ministère de la Justice, et du Fichier national des permis de conduire (FNPC), administré par la Direction des libertés publiques et des affaires juridiques (DLP AJ) du ministère de l'Intérieur, mais n'étant pas, *stricto sensu*, considéré comme un fichier de police.

Ne seront pas recensés dans ce rapport :

- les fichiers de la Défense nationale ;
- le Fichier national des immatriculations <sup>3</sup> (FNI) ;
- le Fichier national des cartes d'identité ;
- le Fichier national des passeports ;
- le Fichier réseau mondial visas 2 <sup>4</sup> (RMV 2) ;
- l'application de gestion des dossiers des ressortissants étrangers en France (AGDREF <sup>5</sup>) ;
- le fichier ELOI <sup>6</sup> ;
- le Fichier national des personnes incarcérées <sup>7</sup> ;
- le Casier judiciaire national <sup>8</sup> ;
- le Fichier des naturalisations <sup>9</sup> ;
- les fichiers de l'Office français de protection des réfugiés et apatrides <sup>10</sup> ;
- le Répertoire national d'identification des personnes physiques <sup>11</sup> ;
- le Fichier du recensement ;

(3) Lois : n° 90-1131 du 19 décembre 1990 – articles L. 225-1, L. 330-1, L. 330-2 à L. 330-4 et R. 322-1 à R. 322-18 du code de la route – Arrêtés du 5 novembre 1984 relatif à l'immatriculation des véhicules, du 20 janvier 1994 et du 28 décembre 1994 et du 22 septembre 2003 – Délibérations Cnil : n° 93-104 du 30 novembre 1993.

(4) Arrêté du 22 août 2001.

(5) Décret du 29 mars 1993.

(6) Arrêté du 30 juillet 2006 relatif à l'informatisation de la procédure d'éloignement.

(7) Arrêté du 28 octobre 1996 portant création d'un fichier national automatisé de personnes incarcérées.

(8) Loi du 4 janvier 1980 relative à l'automatisation du casier judiciaire ; Décret du 6 novembre 1981.

(9) 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.

(10) 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.

(11) Décret n° 82-103 du 22 janvier 1982. Géré par l'Insee.

- les fichiers d'état civil ;
- le Fichier national des comptes bancaires (FICOBA <sup>12</sup>) ;
- le Fichier national des chèques irréguliers <sup>13</sup> (FNCI) ;
- le Fichier central des chèques <sup>14</sup> (FCC) ;
- le Fichier national des incidents de remboursement des crédits aux particuliers <sup>15</sup>.

(12) Géré par la Direction générale des impôts. 1<sup>er</sup> 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).

(13) Loi du 30 décembre 1991 relative à la sécurité des chèques et des cartes de paiement. Géré par la Banque de France.

(14) Créé en 1955 et géré par la Banque de France.

(15) Loi du 30/12/1989 intégrée au code de la consommation (art. L. 333-4 et L. 333-5).

---

## Chapitre 1

---

# Recensement des fichiers



---

## **Les fichiers de la police nationale (sous CHEOPS)**

Le Système de circulation hiérarchisée des enregistrements opérationnels de la police sécurisés (CHEOPS) fédère et permet de donner accès, sous une même configuration, à différentes applications de police :

- le Système de traitement des infractions constatées (STIC) ;
- le Fichier des véhicules volés (FVV) ;
- le Fichier des personnes recherchées (FPR) ;
- le Fichier des renseignements généraux (FRG) ;
- le Fichier national transfrontières (FNT) ;
- le Fichier des brigades spécialisées (FBS) ;
- le Fichier informatisé du terrorisme (FIT) ;
- le Fichier national du faux monnayage (FNFM) ;
- le Fichier national automatisé des empreintes génétiques (FNAEG).

## **Le Système de traitement des infractions constatées (STIC)**

Réf. : décret n° 2001-583 du 5 juillet 2001 modifié par le décret n° 2006-1258 du 14 octobre 2006 ; décret n° 2002-424 du 28 mars 2002 ; loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure. Voir également en annexe la circulaire du ministère de la Justice du 6 juillet 2001.

### Historique

Issu du plan Joxe de 1985, le projet STIC vise à moderniser le traitement de l'information judiciaire en s'appuyant sur l'informatisation des services territoriaux de police urbaine (actuels services territoriaux de sécurité publique). L'objectif annoncé était de mettre à la disposition de tout policier exerçant une mission de police judiciaire un outil d'aide à l'enquête, une meilleure connaissance de la délinquance, une assistance bureautique et une gestion de la documentation. Les développements ont été engagés en 1992 pour une première expérimentation sur sites en 1994, le déploiement ayant été achevé en 1998. Le système s'est appuyé sur des

applications préparatoires existantes, STIC-FCE conçu à l'origine comme outil statistique, STIC-AS, fichier des antécédents et stupéfiants des SRPJ ainsi que STIC-Canonge. Le projet a été découpé en plusieurs phases pour parvenir à une automatisation aussi complète que possible du traitement des procédures judiciaires :

- 1997 : prise en compte des objets bien identifiés ;
- 1998 : intégration à l'architecture CHEOPS du MIAT ;
- 1999 : module de comptabilisation et de consultation de la statistique institutionnelle (états 4001) et mise en œuvre des recherches couplées STIC/Schengen ;
- 2001 : enregistrement et consultation des suites judiciaires ;
- 2004 : mise en œuvre de la version graphique du STIC et du Canonge, de la fonction de consultation en matière de police administrative et du dispositif d'épurement automatique des données.

Le projet est actuellement redimensionné pour répondre aux impératifs de mutualisation des moyens entre police et gendarmerie nationales qui doivent aboutir à une convergence des systèmes de documentation criminelle respectifs STIC pour la police nationale et JUDEX pour la gendarmerie nationale.

## Présentation <sup>1</sup>

Le Système de traitement des infractions constatées (STIC) est une application mise en œuvre par la police nationale qui permet notamment 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 de ces données dans la base nationale du STIC ne peut se faire qu'à partir des bases locales du STIC-FCE (faits constatés et élucidés), outil de constitution des états statistiques qui repose sur différentes grilles suivant la nature des infractions : grille de type « C » (pour « constaté ») qui reçoit les informations relatives à la commission des faits et à la victime, grille de type « E » (pour « élucidé ») qui contient les données relatives au mis en cause, aux circonstances de temps et de lieu de son interpellation.

Le STIC, accessible sous l'architecture réseau CHEOPS, constitue un outil d'aide à l'enquête, offre une information sur la criminalité et assure la gestion de la documentation et l'assistance bureautique.

Le STIC collecte et rassemble dans une base informatique nationale les renseignements sur :

- les procédures judiciaires ;
- les infractions, leurs circonstances de lieux et de temps et les modes opératoires utilisés ;
- les personnes mises en cause et les victimes ;
- les objets volés ou remarqués.

(1) NB : les informations ci-dessous prennent en compte les modifications apportées par le nouveau décret STIC du 14 octobre 2006 publié au JORF du 15 octobre 2006.

Il est consulté en mode d'interrogations simples, de recherches complexes ou de rapprochements judiciaires.

Une fonction spécifique – la recherche couplée STIC/Schengen au moyen d'une transaction unique – permet également d'avoir accès aux objets dits Schengen (armes, billets de banque, documents) signalés auprès des services de la gendarmerie nationale et des pays signataires de la convention Schengen.

La base nationale est alimentée de façon journalière au travers du logiciel STIC-FCE (faits constatés et élucidés), à partir de micro-ordinateurs implantés dans tous les services de police produisant des procédures. Elle est accessible à tout utilisateur habilité.

Le traitement des informations nominatives s'effectue sous le contrôle du procureur de la République territorialement compétent.

## Nature des informations contenues dans le STIC

L'article 2 du décret prévoit que les informations contenues dans le STIC sont relatives aux procédures concernant des crimes, des délits ainsi que les contraventions de cinquième classe prévues 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, R. 645-4 à R. 645-12 du Code pénal.

Ces informations peuvent concerner soit les personnes, sans limitation d'âge, 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 de ces infractions, soit les victimes de ces infractions.

L'article 4 précise les catégories d'informations relatives à l'identité des personnes mises en cause ou des victimes et celles relatives aux faits objets de la procédure qui devront être enregistrées.

## Durée de conservation des informations

### Informations concernant les personnes mises en cause

#### *Cas des majeurs*

Les informations concernant le mis en cause majeur sont en principe conservées vingt ans. Par dérogation, elles sont conservées pour une durée moindre, de cinq ans, lorsque la personne est mise en cause pour l'un des délits prévus par le Code de la route, ou 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, ainsi que pour les contraventions énumérées à l'article 2 du décret. La durée de conservation est par ailleurs portée à 40 ans lorsque la personne est mise en cause pour certaines infractions présentant une particulière gravité et figurant sur la liste jointe en annexe I du décret.

### ***Cas des mineurs***

Les informations concernant le mis en cause mineur sont conservées cinq ans. Par dérogation, elles sont conservées :

- dix ans lorsque la personne est mise en cause pour l'une des infractions figurant sur la liste jointe en annexe II du décret ;
- vingt ans lorsque la personne est mise en cause pour l'une des infractions figurant sur la liste jointe en annexe III du décret.

### ***Prorogation des délais***

En cas de mise en cause dans une ou plusieurs nouvelles infractions avant l'expiration de l'un des délais ci-dessus 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.

### **Informations concernant les victimes**

La durée de conservation des informations concernant les victimes est au maximum de quinze ans, sous réserve des dispositions de l'article 9 du décret.

Cette durée est toutefois prolongée jusqu'à la découverte des objets, lorsque l'infraction porte sur des œuvres d'art, des bijoux ou des armes.

### **La mise à jour des informations**

Une mise à jour des données à caractère personnel peut être effectuée après transmission par l'autorité judiciaire des suites judiciaires favorables aux mis en cause ou suite à une sollicitation d'une victime ou d'un mis en cause. Dans le premier cas, elles entraînent une suppression ou l'ajout d'une mention dans le traitement <sup>2</sup>.

### **Qui peut consulter ce fichier ?**

Seules les personnes habilitées peuvent interroger le STIC. Il s'agit des personnels de la police nationale, de la gendarmerie nationale et des services des douanes qui exercent des missions de police judiciaire. Ils appartiennent pour la police nationale à la Direction centrale de la sécurité publique, des renseignements généraux, à la police aux frontières, la préfecture de police de Paris, à la direction centrale des CRS, à la direction centrale de la police judiciaire ainsi qu'aux services plus spécialisés tels que la DST, ou des services rattachés au ministère de l'Intérieur (par exemple : unité de lutte antiterrorisme). Les personnels investis de missions de police administrative ont un accès restreint aux informations de façon strictement encadrée pour les seules enquêtes listées par décret en Conseil d'État. Les magistrats du parquet ainsi que les magistrats instructeurs pour les recherches relatives aux infractions dont ils sont saisis peuvent également avoir accès aux informations. Enfin, les organismes de

(2) Voir également la deuxième partie.

coopération internationale en matière de police judiciaire et les services de police étrangers, dans les conditions énoncées à l'article 24 de la loi sur la sécurité intérieure peuvent également être destinataires des données.

La traçabilité des interrogations est assurée, les traces de toutes les interventions effectuées étant conservées trois ans.

En mai 2005, près de 90 000 personnes étaient habilitées à accéder au STIC dans le cadre d'une mission de police judiciaire, de police administrative ou de fonctions de gestion du fichier.

## Le cadre de saisie informatique

Le STIC est alimenté de façon quotidienne par trois canaux différents :

- le STIC-FCE : à partir des procès-verbaux papier issus du logiciel de rédaction des procédures (LRP), les secrétariats des services de police resaisissent dans l'application locale STIC-FCE les données principales relatives à la procédure (faits, infractions, victimes, mis en cause et compteurs 4001). Par une opération manuelle, les données de la base locale du STIC-FCE sont extraites dans un fichier pour alimenter le STIC. Par une fonction spécifique du STIC dite de « *concentration FCE* », les données contenues dans ce fichier sont transmises au serveur central du STIC en vue de leur intégration dans la base de données factuelles et statistiques 4001. Sur le serveur central, une fonction d'intégration traite quotidiennement (deux fois par jour actuellement) les données transmises par tous les services de police pour les intégrer dans la base de données factuelles (dite de référence) et statistiques 4001 ;
- l'application OMEGA de la préfecture de police : les mises à jour (création, modification, suppression) sur les procédures enregistrées par les services de police de Paris et la Petite Couronne sont transmises quotidiennement pour être intégrées dans le STIC ;
- la mise à jour en temps réel à partir d'un poste de travail directement connecté à l'application STIC *via* CHEOPS pour créer, enrichir, supprimer et radier tout élément d'un dossier de procédure (archive, procédure, fait, infraction, manière d'opérer, nature de lieu, victime, mis en cause et objets).

Parallèlement à la transmission informatisée des informations, la documentation papier relative aux procédures intégrées est transmise par courrier aux services régionaux de documentation criminelle pour qu'ils procèdent aux mises à jour.

## Prochaines évolutions

### À court terme

Le décret n° 2001-583 du 5 juillet 2001 portant création STIC vient d'être modifié par le décret n° 2006-1258 du 14 octobre 2006. Il a, en effet, tiré les conséquences des dispositions introduites par les articles 21, 22, 24 et 25 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, concernant la finalité du traitement, les catégories de données à

caractère personnel enregistrées, leur modalité de mise à jour ainsi que les personnes qui en sont destinataires.

La liste des destinataires a ainsi été complétée par les agents des douanes exerçant des missions de police judiciaire et par tous autres personnels investis par la loi d'attributions de police judiciaire. Sont également nommées les autorités hiérarchiques qui habilite l'ensemble des personnels pouvant accéder au STIC, en l'occurrence le directeur général de la police nationale, le directeur général de la gendarmerie nationale et le directeur général des douanes et des droits indirects, et par délégation, les personnels de catégorie A ou ayant le rang d'officier placés sous l'autorité de ceux-ci.

Par ailleurs, conformément à l'article 25 de la loi pour la sécurité intérieure, les personnels investis de missions de police administrative, individuellement et limitativement habilités par le préfet, pourront consulter cette application. L'accès à l'information reste toutefois limité à la seule connaissance de l'enregistrement de l'identité de la personne concernée dans le STIC en tant que mis en cause.

Dans le cadre des engagements internationaux en vigueur, le traitement pourra aussi être constitué de données à caractère personnel issues de traitements gérés par des organismes de coopération internationale en matière de police judiciaire ou des services de police étrangers s'ils présentent un niveau de protection suffisant de ces données.

Enfin, cette modification du décret STIC a mis l'accent sur les droits des personnes concernées. Les victimes d'infractions seront dorénavant informées de l'enregistrement de leurs données à caractère personnel et de leurs droits d'accès et d'opposition afférents.

### **À moyen terme**

Les applications préparatoires LRP, STIC-FCE et Canonge disparaîtront et leurs fonctionnalités seront reprises par le nouveau système intégré comportant les applications :

- ARDOISE (Application de recueil de la documentation opérationnelle et des informations statistiques sur les enquêtes) qui permettra l'alimentation de la base nationale ARIANE et également la gestion de la documentation au plan local ;
- les traitements statistiques sont, pour la DGPN, assurés par deux applications distinctes (Stats OP et stats 4001) ;
- ARIANE (Application de rapprochements, d'identification et d'analyse pour les enquêteurs) qui se substituera à la base nationale du STIC dans ses fonctions de recherches et de rapprochements criminels en incluant les dossiers des Canonge locaux. Cette application est mutualisée avec la DGGN et se substituera à JUDEX.

---

*Au 1<sup>er</sup> janvier 2006, le STIC recensait 28,9 millions de procédures, 32 millions d'infractions, 22,5 millions de victimes, 9,8 millions d'objets. Au 31 août 2006, il regroupait 4 750 030 fiches de mis en cause. En 2005, le STIC a fait l'objet de 12 035 200 consultations.*

---

## Une application particulière : le Canonge graphique

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 1<sup>er</sup> 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 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 5<sup>e</sup> classe peuvent être enregistrées dans le CANONGE. La signalisation des témoins ou autres personnes est proscrite.

En 2005, le STIC-CANONGE a fait l'objet de 209 249 consultations.

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 : six 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 douze types différents : blanc (caucasien) ; méditerranéen ; gitan ; moyen-oriental ; nord-africain maghrébin ; asiatique eurasiens ; amérindien ; indien (Inde) ; métis-mulâtre ; noir ; polynésien ; mélanésien-canaque.

<b>Nom du fichier</b>	STIC CANONGE
<b>À quoi sert-il ?</b>	<ul style="list-style-type: none"> <li>- Identification de malfaiteur à partir d'un signalement fourni par une victime, un témoin.</li> <li>- Identification dans une base texte et photographique, constituée à l'aide des notices individuelles, d'individus déjà mis en cause dans une procédure judiciaire.</li> </ul>
<b>Que trouve-t-on ?</b>	<ul style="list-style-type: none"> <li>- La photographie du malfaiteur.</li> <li>- L'identité complète et l'adresse du mis en cause.</li> <li>- Les infractions pour lesquelles le mis en cause a été signalisé, les références des procédures, les complices éventuels.</li> <li>- Les éléments de signalement du mis en cause : sexe, type, âge apparent, taille, corpulence, cheveux, couleur des yeux, accent, signe particulier..</li> </ul>
<b>Mode d'interrogation</b>	<ul style="list-style-type: none"> <li>- Programme de requête simplifiée regroupant les critères fournis par le témoin ou la victime.</li> <li>- À partir des critères de recherches correspondant à ceux énumérés ci-dessus permettant de constituer une sélection d'individus, afin d'en présenter les photographies</li> </ul>

## **Le Fichier des véhicules volés (FVV)**

Réf. : arrêté du 15 mai 1996 (*JO* du 18 mai 1996) modifié par l'arrêté du 2 septembre 2005 (*JO* du 28 septembre 2005).

### Historique

Les véhicules volés étaient gérés localement par les services régionaux de police judiciaire sur leur ressort. Dix-huit fichiers manuels étaient ainsi exploités, rendant peu opérationnelle leur utilisation en raison de la lenteur des transmissions et des difficultés de mises à jour.

La décision d'automatiser le traitement des données relatives aux véhicules volés et surveillés afin d'avoir un seul fichier relié à des terminaux d'interrogation, mis à jour très rapidement, a été prise par la DGPN en 1974. Les premiers échanges quotidiens avec la gendarmerie ont été instaurés en 1982 par le biais de bandes magnétiques. En 1994, des échanges en temps réels entre les deux bases police (PN) et gendarmerie (GN) ont été complètement automatisés. Cette même année a été créé le Fichier des bateaux volés, complété en 1996 par les aéronefs pour devenir le Fichier des bateaux et aéronefs (FBA).

La liaison avec le système d'information Schengen (SIS) permettant son alimentation directe à partir du FVV est intervenue en 1995.

Les dernières évolutions notables du logiciel ont été réalisées en 2002 et 2004 avec la mise en exploitation d'une version graphique (ergonomie *Windows*) pour les interrogations simples et multicritères. L'inscription automatisée des véhicules volés en France dans la base de données de l'OIPC-Interpol (ASF) a été mise en exploitation en mars 2004.

Cette application fait actuellement l'objet d'une refonte dans le cadre d'un projet commun de mutualisation des bases de données PN/GN. La nouvelle application FOVeS (Fichier des objets et des véhicules signalés) permettra notamment de prendre en compte les évolutions du système Schengen.

## Présentation générale du FVV

Cette application, accessible sous l'architecture réseau CHEOPS, permet la gestion sur le plan national des véhicules, bateaux, aéronefs signalés volés par leur propriétaire ou mis sous surveillance à la demande d'un service de police ou de gendarmerie. L'application autorise également sous certaines conditions la mise sous surveillance des plaques d'immatriculation volées.

Le FVV est actuellement constitué de trois bases (ou sous-fichiers) :

- le Fichier des véhicules soumis à immatriculation volés ou surveillés (FVI) ;
- le Fichier des véhicules non soumis à immatriculation volés ou surveillés portant un numéro identifiant (FVN) ;
- le Fichier des bateaux et aéronefs volés ou surveillés (FBA).

Le FVV communique au Fichier national des automobiles (FNA intégré au Fichier national des immatriculations de gestion des cartes grises), en temps réel, les déclarations de vol et de surveillance pour tous les véhicules. Inversement le FNA met quotidiennement à disposition du FVV la liste des véhicules volés ou surveillés dont le numéro d'immatriculation, le numéro de série, voire la marque est erronée, ainsi que la liste des véhicules surveillés au FVV ayant fait l'objet d'une transaction au FNA.

D'autre part, une liaison avec le système d'information Schengen (SIS) permet son alimentation par le FVV. À l'inverse, 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 FVV.

## Les modifications intervenues en 2005

L'arrêté du 2 septembre 2005 portant modification de l'arrêté du 15 mai 1996 relatif au Fichier des véhicules volés (FVV) tire les conséquences des articles 22, 23, 24 et 27 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure (LSI) en améliorant les conditions d'inscription dans le fichier et en autorisant l'accès à d'autres services concourant à des missions de sécurité intérieure.

Les agents des douanes chargés des missions traditionnelles de contrôle dévolues à cette administration ainsi que les agents des services des douanes judiciaires désignés par l'article 28-1 du Code de procédure pénale peuvent désormais accéder au FVV.

La modification de l'arrêté du 15 mai 1996 susvisé intègre également le dispositif prévu à l'article 24 de la loi du 18 mars 2003 sur la sécurité intérieure qui autorise la cession réciproque d'informations entre les fichiers français et ceux d'organismes ou de services de police étrangers, sous certaines conditions juridiques.

## Le cadre de saisie informatique

Depuis 1994, date de décentralisation des mises à jour du FVV par les services territoriaux de sécurité publique, le FVV est alimenté par tous les services de la police nationale et complété par des cessions en temps réel de données du fichier de la gendarmerie nationale, ce système d'échange réciproque des données avec le fichier équivalent de la gendarmerie nationale assurant l'identité du contenu des deux bases de données.

Le FVV peut être consulté par toute personne habilitée à partir de postes de travail multifonctions ou de terminaux embarqués (TESA).

---

Au 31 août 2006, le FVV regroupait 491 223 fiches. Les services de la police nationale se sont connectés 4 286 657 fois en 2005.

---

## Le Fichier des personnes recherchées (FPR)

Réf. : arrêté du 15 mai 1996 (*JO* du 18 mai 1996) ; arrêté du 2 septembre 2005 modifiant l'arrêté du 15 mai 1996 (*JO* du 15 octobre 2005) relatif au Fichier des personnes recherchées géré par le ministère de l'Intérieur et le ministère de la Défense.

## Historique

Les personnes recherchées en vertu de décisions de justice, de décisions administratives, ou dans le cadre d'enquêtes de police judiciaire ont depuis toujours figuré dans une documentation qui était mise à la disposition des services de police et de gendarmerie pour leur permettre d'appliquer les mesures de recherches. D'abord sous forme de « bulletins périodiques » puis de « fiches signalétiques » qui ont alimenté jusqu'à 300 fichiers manuels locaux, les recherches de personnes ont fait l'objet d'un fichier automatisé en 1969.

Les premiers échanges avec le fichier, créé par la gendarmerie nationale en 1980, ont été instaurés en 1982 par le biais de bandes magnétiques. Ces échanges ont été automatisés en temps réel en 1993.

Une liaison avec le système d'information Schengen permet l'alimentation du C-SIS (système central) automatiquement à partir du FPR ainsi que la consultation du N-SIS depuis 1995.

Le logiciel a régulièrement fait l'objet de modifications (ajout de services émetteurs, mise en place de statistiques, éditions de sous-produits, etc.), les dernières évolutions ayant concerné :

- 2002 : mise en œuvre de la fiche « X » des personnes non identifiées destinée à améliorer les recherches de personnes disparues et de la fonction de recherches sous interface graphique ;
- 2005 : mise en conformité du FPR avec la loi sur la présomption d'innocence, la LSI du 18 mars 2003 et la loi Perben II du 9 mars 2004 ;
- 2006 : intégration de la photographie pour les personnes disparues.

## Présentation générale du FPR

Cette application, accessible sous l'architecture réseau CHEOPS, permet la gestion sur le plan national des personnes faisant l'objet d'une mesure de recherche administrative ou judiciaire, à chaque catégorie de recherche correspondant un type de fiche particulier. Chaque fiche comporte une conduite à tenir en cas de découverte de la personne recherchée. Cette conduite à tenir donne des instructions précises qui conditionnent l'action des services de police sur le terrain ou l'action administrative dans le cadre de la délivrance de documents.

Police et gendarmerie alimentent ce fichier au travers de deux systèmes parallèles. La mise à jour des bases de données s'effectue « au fil de l'eau » par un échange en temps réel entre les deux administrations.

Une liaison avec le système d'information Schengen permet l'alimentation du C-SIS (système central) automatiquement à partir du FPR ainsi que la consultation du N-SIS (système national).

Les applications réglementaires portant sur les titres d'identité et de séjour consultent automatiquement le FPR avant délivrance du titre CNI, DELPHINE (passeports), VISA, et AGDREF (dossiers des ressortissants étrangers en France également dénommée FNE).

## Les modifications intervenues en 2005

L'arrêté du 2 septembre 2005 portant modification de l'arrêté du 15 mai 1996 relatif au Fichier des personnes recherchées (FPR) tire les conséquences des articles 22, 23 et 24 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure (LSI) en étendant son champ d'application à de nouvelles peines et mesures de sûreté prescrites par les autorités judiciaires et en autorisant l'accès à d'autres services concourant à des missions de sécurité intérieure.

Les agents des douanes chargés des missions traditionnelles de contrôle dévolues à cette administration ainsi que les agents des services des douanes judiciaires désignés par l'article 28-1 du Code de procédure pénale peuvent désormais accéder au FPR.

La modification de l'arrêté du 15 mai 1996 susvisé intègre également le dispositif prévu à l'article 24 de la loi du 18 mars 2003 sur la sécurité intérieure qui autorise la cession réciproque d'informations entre

les fichiers français et ceux d'organismes ou de services de police étrangers, sous certaines conditions juridiques.

La modification de l'arrêté du 15 mai 1996 innove enfin sur deux points : l'enregistrement de la photographie des personnes recherchées et l'inscription dans le traitement des personnes découvertes sans identité (cadavre non identifié, amnésique, nouveau-né).

### Le cadre de saisie informatique

Le service central de documentation criminelle (DCPJ/SDPTS/SCDC) qui assure la direction d'application du FPR et qui, à ce titre, élabore et contrôle sa doctrine d'utilisation, est également un vecteur important des enregistrements effectués dans la base de données en complément des inscriptions effectuées par les services territoriaux de police judiciaire.

Le FPR peut être consulté par toute personne habilitée à partir de postes de travail multifonctions ou de terminaux embarqués.

---

Le Fichier des personnes recherchées a fait, en 2005, l'objet de 39 millions de consultations qui ont donné lieu à plus de 44 000 découvertes par les services de police et les unités de gendarmerie. Au 31 août 2006, le FPR contenait 280 679 fiches.

---

## **Le Fichier des renseignements généraux (FRG)**

Réf. : décret n° 91-1 051 du 14 octobre 1991.

### Historique

La CNIL a autorisé dans son avis conforme du 24 juillet 1991 pris à l'occasion du décret n° 91-1051 en date du 14 octobre 1991, les renseignements généraux, à collecter, conserver et traiter les informations nominatives relatives aux personnes majeures faisant apparaître leurs activités politiques, philosophiques, religieuses ou syndicales, pour les finalités précisées par ce texte et strictement limitées

### Présentation

Ce fichier est notamment régi par le décret n° 91-1 051 du 14 octobre 1991 portant application aux fichiers informatisés, manuels ou mécanographiques gérés par les services des renseignements généraux des dispositions de l'article 31, alinéa 3, de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Les fichiers des renseignements généraux ne peuvent faire mention des opinions politiques, religieuses ou syndicales.

Il existe toutefois des cas particuliers concernant :

- les personnes fichées pour terrorisme ;
- les élus et personnes jouant un rôle significatif, ou ayant accès à certaines informations sensibles.

Les activités politiques, philosophiques, religieuses ou syndicales, ainsi que les caractéristiques physiques particulières, objectives et inaltérables peuvent être mentionnées pour : les personnes fichées pour atteinte à la sûreté de l'État ou terrorisme, les personnes ayant eu des contacts directs et répétés avec ces dernières.

Les activités politiques, philosophiques, religieuses ou syndicales peuvent être mentionnées pour : les élus, anciens élus et personnes ayant sollicité un mandat électoral ou jouant un rôle politique, social, religieux ou économique significatif ; les personnes ayant accès à des informations sensibles (Défense nationale, par exemple) ou sollicitant un accès à ces informations.

La réorientation des missions des renseignements généraux en novembre 1995 a conduit à ce que ces informations ne soient plus collectées.

Il existe un droit d'accès indirect à sa fiche des renseignements généraux par l'intermédiaire de la CNIL. Toutefois, le ministre de l'Intérieur peut s'opposer à la communication de ces informations si celles-ci peuvent nuire à la sûreté de l'État ou à la Défense nationale.

Il existe également un droit de rectification en cas d'erreurs de faits et de mentions illégales (indication de condamnations amnistiées, etc.).

## Le cadre de saisie informatique

Le FRG se décline en deux applications, le RGD (application centrale des personnes physiques) et le RGA (application centrale des personnes morales). La saisie informatique s'effectue par chaque service RG (service déconcentré ou direction centrale).

Il s'agit d'une indexation centrale informatique de l'ensemble des dossiers qui a pour objet, d'une part, d'éviter la redondance de dossiers entre les services, une personne pouvant être connue à différents niveaux (départemental, régional, central) et, d'autre part, de garantir, lors des demandes de consultation, l'exhaustivité des recherches et de sécuriser les consultations en gérant les habilitations des consultants.

Les dossiers sont enregistrés au moyen d'un numéro délivré automatiquement par le système informatique. Parallèlement, un numéro de dossier individuel est attribué par le service détenteur de l'information indexée.

La consultation du dossier nécessite une prise de contact avec le service qui a constitué le dossier dont la référence apparaît sur l'application informatique.

## **Le Fichier national transfrontières (FNT)**

Réf. : arrêté du 29 août 1991.

### **Fonctionnement actuel du FNT**

Le Fichier national transfrontières, créé par l'arrêté du 29 août 1991, a pour finalité la prévention des atteintes à la sûreté de l'État ou à la sécurité publique à l'occasion de l'exercice des contrôles frontaliers.

Ce fichier est alimenté par certaines données inscrites sur les cartes de débarquement et d'embarquement renseignées par les passagers en provenance ou à destination de certains pays sensibles dont la liste est établie par l'unité de coordination de lutte antiterroriste (UCLAT). Cette liste comprend actuellement vingt-neuf pays.

Ces fiches manuscrites collectées lors du contrôle transfrontalier sont transmises périodiquement à un service de la police aux frontières implanté à Pantin (93). Ses effectifs y procèdent à la saisie manuelle dans le FNT des principales informations contenues dans ces cartes.

Une fois traitées, les cartes sont ensuite conservées pour pouvoir être consultées manuellement sur une période de trois ans, leur destruction intervenant ensuite par incinération.

Les catégories d'informations nominatives enregistrées dans le FNT sont les suivantes :

- nom ;
- nom de jeune fille ;
- prénom ;
- date et lieu de naissance ;
- nationalité ;
- date et aéroport d'arrivée ;
- date et aéroport de départ.

Outre la Direction centrale de la police aux frontières, les destinataires de ces informations sont la direction de la surveillance du territoire, la Direction générale de la sécurité extérieure, la Direction de la protection et de la sécurité de la défense, la Direction centrale des renseignements généraux et la Direction centrale de police judiciaire

Le FNT ne présente plus actuellement un grand intérêt sur le plan opérationnel. Cette situation tient essentiellement à son mode d'alimentation. En effet, le processus d'acheminement et d'informatisation des fiches d'embarquement et de débarquement demeure très aléatoire. Cet état de fait est de plus amplifié par l'accroissement des délais de saisie résultant de l'augmentation constante des flux de voyageurs et du traitement de ces fiches pour la plupart illisibles ou incomplètes.

### **La modernisation en cours du fichier**

La base juridique de la modernisation du FNT est l'article 7 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme

et portant dispositions diverses relatives à la sécurité et aux contrôles transfrontières qui autorise le ministère de l'Intérieur à constituer des traitements automatisés de données personnelles relatives aux passagers des transporteurs aériens, maritimes et ferroviaires aux fins de contrôle des frontières, de la lutte contre l'immigration clandestine et de la prévention et répression des actes terroristes.

L'alimentation automatique du FNT à partir « *de la bande de lecture optique des documents de voyage, de la carte nationale d'identité et des visas des passagers* » va optimiser l'efficacité du système par :

- l'amélioration de la fluidité du traitement des flux de voyageurs lors des contrôles transfrontières ;
- l'enregistrement en temps réel des données à caractère personnel des passagers ;
- l'exactitude des informations collectées ;
- l'élimination des informations incomplètes ou erronées ;
- l'information immédiate des services destinataires.

Le projet d'arrêté portant modification de l'arrêté du 29 août 1991 est actuellement en cours de contreseing, la CNIL ayant délibéré le 14 septembre 2006.

## **Le Fichier des brigades spécialisées (FBS)**

### Historique

Depuis 1991, date de mise en exploitation du FBS (version 1.0), cette application a successivement fait l'objet d'une version micro reprenant l'ergonomie *Windows* (janvier 1997), d'un passage sous architecture CHEOPS (juin 2000), et de deux versions ayant successivement permis de créer de nouvelles rubriques (version 2.2. en janvier 2002) et d'améliorer les possibilités de recherches et de restitution des réponses (version 2.3.1 en mars 2006).

Frappée d'obsolescence technique et fonctionnelle, la refonte de cette application a été engagée jusqu'à la finalisation d'un cahier des charges prenant en compte les besoins des utilisateurs en juin 2005. La poursuite des travaux est actuellement en attente d'une priorisation de ce projet.

### Présentation

Le Fichier des brigades spécialisées (FBS) a été créé au bénéfice des 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 d'argent, grande délinquance financière, immigration clandestine.

Ce fichier de travail géré par un ordinateur central permet d'échanger, sous le contrôle permanent des services qui les fournissent, des informations relatives à ces activités criminelles et à leurs auteurs.

L'objectif de ce fichier est d'enregistrer, classer et exploiter de manière optimale les informations collectées à l'occasion de la surveillance du milieu criminel ; de permettre les échanges entre les services spécialisés en assurant la confidentialité nécessaire ; d'autoriser tous les croisements de recherches possibles entre les informations mêmes incomplètes de la base.

## Le cadre de saisie informatique

Ce système d'information national à caractère confidentiel est une application sécurisée qui utilise l'architecture CHEOPS du ministère de l'Intérieur et de l'Aménagement du territoire. Seuls les personnels disposant d'une habilitation spéciale ont accès au FBS. L'application fonctionne 24 heures sur 24, 7 jours sur 7, et permet des mises à jour en temps réel par les services utilisateurs (offices centraux de police judiciaire ou de la DCPAF, brigades centrales de la préfecture de police de Paris, directions interrégionales de police judiciaire).

Les besoins exprimés par les utilisateurs du FBS ont conduit à engager un projet de refonte de ce dernier, prenant en compte la nouvelle dimension de « *fichier de travail* ». Un projet de cahier des charges fonctionnel a été établi. Toutefois, il apparaît nécessaire de donner à ce type de fichiers une base législative distincte de l'article 21 de la loi pour la sécurité intérieure en date du 18 mars 2003, qui n'apparaît pas adapté. Tout particulièrement en raison du fait que ces fichiers ne sont jamais utilisés dans le cadre des enquêtes administratives : ils sont exclusivement alimentés et consultés pour les besoins de la police judiciaire, pour la lutte contre la criminalité organisée.

---

*Au 31 décembre 2005, le FBS contenait 174 593 fiches. En 2005, 108 965 consultations ont été enregistrées.*

---

## Le Fichier automatisé du terrorisme (FIT)

Réf. : décret n° 91-1 052 du 14 octobre 1991.

### Historique

En 1982, suite à la vague d'attentats terroristes commis à Paris, le Gouvernement a décidé d'instituer un fichier sur le terrorisme. Or, le seul fichier informatisé existant en ce domaine était le fichier VAT (Violences attentats terrorisme) géré par les renseignements généraux.

Vu l'urgence, le ministre de l'Intérieur décida de s'appuyer sur le VAT et de regrouper les renseignements détenus par chacun des services luttant contre le terrorisme et de leur en permettre directement l'accès.

Ainsi a été créé le Fichier central du terrorisme (FCT) qui répondait à un double objectif : constituer un fichier de travail unique rassemblant toutes les informations importantes émanant de tous les services impliqués dans la lutte antiterroriste et permettre aux services à vocation plus large d'apporter leur concours à la lutte antiterroriste.

Cette application a été légalisée par le décret n° 1052 du 14 octobre 1991, le FCT prenant le nom de FIT.

## Présentation

Le Fichier automatisé du terrorisme a été créé par le décret n° 91-1 052 du 14 octobre 1991 relatif au fichier informatisé du terrorisme mis en œuvre par les services des renseignements généraux du ministère de l'Intérieur.

La Direction centrale des renseignements généraux du ministère de l'Intérieur est autorisée à mettre en œuvre un fichier informatisé des personnes pour l'accomplissement exclusif de sa mission de lutte contre les entreprises individuelles ou collectives ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur.

La finalité exclusive de ce traitement est la centralisation des informations qui concernent les personnes qui peuvent, en raison de leur activité individuelle ou collective, porter atteinte à la sûreté de l'État ou à la sécurité publique par le recours ou le soutien actif apporté à la violence, ainsi que les personnes entretenant ou ayant entretenu des relations directes et non fortuites avec celles-ci.

Pourront, en tant que de besoin, faire l'objet d'un traitement automatisé les informations ayant trait à l'état civil, l'adresse et la profession des personnes visées à l'article 2 ainsi que les références du ou des dossiers les concernant.

Ces informations pourront être complétées par les éléments suivants, nécessaires à l'identification de l'intéressé :

- signalement ;
- comportement ;
- numéros de téléphone ;
- motif du signalement ;
- identité des personnes entretenant ou ayant entretenu des relations directes et non fortuites avec la personne faisant l'objet du présent traitement automatisé ainsi que ses déplacements et antécédents judiciaires (notamment date et lieu de détention) lorsque ces derniers ne sont pas suivis d'une décision de non-lieu, de relaxe ou d'acquiescement.

Dans la mesure où le FIT est mis en œuvre conformément aux dispositions prévues par le décret 91-1051 du 14 octobre 1991, ce fichier

peut également faire apparaître les signes physiques, particuliers, les activités politiques, philosophiques, religieuses, ou syndicales.

La Direction centrale des renseignements généraux est chargée de la modification et de la mise à jour des informations enregistrées dans le traitement automatisé et les dossiers manuels auxquels il renvoie. Il est en outre procédé, sous le contrôle de la Commission nationale de l'informatique et des libertés (CNIL), tous les cinq ans, à un examen de la justification et du bien-fondé des informations nominatives détenues. La Direction centrale des renseignements généraux rend compte chaque année à la CNIL de ses activités de vérification, de mise à jour et d'apurement de ses fichiers et de ses dossiers.

Le droit d'accès aux informations visées à l'article 3 s'exerce auprès de la CNIL, conformément aux dispositions de l'article 39 de la loi du 6 janvier 1978 susvisée.

Il est interdit de connecter ce fichier avec tout autre fichier.

### Le cadre de saisie informatique

La DCRG a la charge de l'alimentation du FIT, en fonction des données qui lui sont transmises par les autres services.

Les dossiers sont enregistrés au moyen d'un numéro délivré automatiquement par le système informatique. Parallèlement, un numéro de dossier individuel est attribué par le service détenteur de l'information.

Les renseignements saisis sont les suivants : état civil, signalement dont signes particuliers, adresse, profession, organisation politique ou syndicale, moyen de déplacement, antécédents judiciaires, comportement, relations, numéro de dossier, ainsi qu'une rubrique texte.

Jusqu'en 1997, la base FIT était incluse dans la base RGD. À la demande de la CNIL, il a été procédé à la séparation des deux bases en octobre 1997.

Pour certains membres du groupe de travail, il apparaît surprenant que ce fichier ne soit pas accessible directement par informatique par la sous-direction antiterroriste de la Direction centrale de la police judiciaire.

### Modalités de droit d'accès

En application du décret n° 1051 du 14 octobre 1991, article 5, seuls les fonctionnaires des renseignements généraux dûment habilités et dans la limite du besoin d'en connaître peuvent obtenir communication de la totalité des informations collectées.

En revanche, les fonctionnaires des autres services de police et de gendarmerie ne peuvent obtenir communication que des seules informations relatives à la violence politique ou au terrorisme, ainsi que des informations relatives à des personnes faisant ou ayant fait l'objet d'une enquête d'habilitation.

La communication est subordonnée à une demande écrite qui précise l'identité du consultant, l'objet et les motifs de la consultation.

Les utilisateurs disposent de différents profils leur permettant soit une simple consultation, soit une consultation et éventuellement une modification ou une suppression des dossiers.

## **Le 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 1<sup>er</sup> 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 (indicateurs 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.

---

Les enquêteurs spécialisés et habilités ont réalisé 44 358 consultations entre octobre 2002 et le 31 août 2006. Au 31 août 2006, 10 503 faits de fausse monnaie sont regroupés dans la base.

---

## **Le Fichier national automatisé des empreintes génétiques (FNAEG)**

Réf. : loi n° 98-468 du 17 juin 1998 ; décret d'application n° 2000-413 du 18 mai 2000 ; loi n° 2001-1062 du 15 novembre 2001 (décret d'application du 30 avril 2002) ; loi n° 2003-239 du 18 mars 2003 sur la sécurité intérieure ; décret n° 2004-470 du 25 mai 2004.

### **Historique**

La recherche d'éléments spécifiques propres à chaque individu susceptibles de favoriser son identification constitue un des fondements de la criminalistique. Certains noms désormais célèbres sont demeurés attachés à cette quête (Alphonse BERTILLON, Francis GALTON, Edmond LOCARD...).

Parmi ceux-ci, Sir Alec JEFFREYS aura, sans doute, franchi une étape décisive en 1985, grâce à la mise en œuvre d'une technique d'analyse permettant de déterminer une empreinte génétique à partir de l'ADN d'un individu.

La nécessité d'une exploitation efficace des résultats analytiques, dans le cadre de l'enquête judiciaire, a rapidement conduit à la mise en œuvre de fichiers informatisés susceptibles de centraliser ce nouveau type d'information en une base de données unique, afin d'en rationaliser la gestion.

Ainsi, le Royaume-Uni a mis en œuvre le premier fichier d'empreintes génétiques en avril 1985. Géré par le Forensic Science Service (FSS), sa base de données compte actuellement plus de 3 millions de personnes.

## Présentation

Créé par la loi n° 98-468 du 17 juin 1998 (décret d'application n° 2000-413 du 18 mai 2000) relative à la répression des infractions sexuelles ainsi qu'à la protection des mineurs, le Fichier national automatisé des empreintes génétiques (FNAEG) a rapidement bénéficié d'une extension de son champ d'application aux principaux crimes d'atteintes aux personnes et aux biens en vertu de l'article 56 de la loi n° 2001-1062 du 15 novembre 2001 (décret d'application du 30 avril 2002) relative à la sécurité quotidienne.

La loi n° 2003-239 du 18 mars 2003 sur la sécurité intérieure a clairement fait du Fichier des empreintes génétiques un outil d'identification criminelle « généraliste », à l'instar des choix criminalistiques faits dans d'autres pays étrangers, notamment la Grande-Bretagne. La biométrie génétique présente en effet pour certaines enquêtes judiciaires des perspectives opérationnelles supérieures à la biométrie digitale. Il est plus difficile pour un délinquant de trouver des modes opératoires permettant d'éviter de laisser tout matériau génétique comme indice que d'éviter de laisser des empreintes digitales exploitables. La destruction de traces et indices génétiques est également beaucoup plus compliquée.

Le législateur a donc défini un régime équilibré. Si le recours à la biométrie génétique intéresse potentiellement l'ensemble des catégories de crimes et délits (article 706-54, alinéa 3 et 706-55 du CPP), la loi encadre strictement les données pouvant faire l'objet d'une inscription définitive au sein du fichier. En outre, la loi délimite précisément les modalités de recours à la biométrie au cours des enquêtes judiciaires. Tout d'abord en fixant une condition légale, à savoir qu'il existe au moins une raison plausible de soupçonner qu'une personne a commis un crime ou un délit. Mais ce n'est que si les soupçons sont étayés par des indices graves et concordants que l'empreinte génétique peut faire l'objet d'une conservation dans le fichier. En outre, dans ce dernier cas, s'il n'y a pas eu condamnation, des voies de recours sont ouvertes et l'effacement peut être ordonné si la conservation n'apparaît plus nécessaire au regard des finalités du fichier.

Désormais donc, outre la centralisation des empreintes génétiques issues des traces biologiques et celles des personnes condamnées dans le cadre d'une des infractions mentionnées à l'article 706-55, la loi prévoit :

- l'enregistrement de l'empreinte génétique (article 706-54 alinéa 2) des personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient commis l'une des infractions mentionnées à l'article 706-55 du CPP. Avant 2003, elles ne pouvaient qu'être l'objet d'une comparaison avec les empreintes déjà insérées dans la base de données ;
- la (simple) comparaison (sans enregistrement) de l'empreinte génétique (article 706-54 alinéa 3) des personnes à l'encontre desquelles il existe une ou plusieurs raisons plausibles de soupçonner qu'elles ont commis un crime ou un délit. L'ensemble des crimes et des délits sont ici concernés et non pas seulement ceux prévus par l'article 706-55 du CPP ;

– l’enregistrement du profil génétique des personnes disparues ou décédées (article 706-54 alinéa 4 du CCP) dans le cadre des procédures de recherche des causes de la mort ou des causes d’une disparition prévues par les articles 74, 74-1 et 80-4 du CPP.

Par ailleurs, la loi consacre le pouvoir propre de l’officier de police judiciaire (sans autorisation préalable d’un magistrat et quel que soit le cadre juridique) de procéder ou faire procéder à un prélèvement sur un individu et de demander son inscription au fichier après avoir requis une personne habilitée aux fins d’analyses (article 706-56 du CPP). Dans ce cadre, il n’est plus nécessaire que la personne requise soit inscrite sur une liste d’expert. Il convient toutefois de préciser que cette faculté ne concerne que les empreintes génétiques des condamnés et des suspects de l’article 706-54 alinéas 2 et 3.

Le nouveau texte prévoit également, pour les mêmes officiers de police judiciaire, la possibilité de consulter ou faire consulter le fichier (par le seul état civil) afin de s’assurer, avant tout prélèvement, que la personne concernée n’y est pas déjà inscrite. En outre, il autorise les transferts télématiques des informations dans la base de données afin d’en assurer une meilleure alimentation.

Enfin, la sanction du refus de prélèvement ne vise plus les seuls condamnés, elle s’étend désormais aux mis en cause et aux suspects (article 706-56, II).

Le décret n° 2004-470 du 25 mai 2004 est venu apporter quelques précisions à ces nouvelles dispositions. Celles-ci concernent principalement : la suppression du deuxième prélèvement sur les individus. Pour prendre en compte cette situation nouvelle, un marché national, portant sur un nouveau kit de prélèvement buccal, est en cours d’élaboration ; les prélèvements qui peuvent être effectués, avec leur accord, sur les ascendants et descendants des personnes disparues dont le matériel biologique n’aurait pu être récupéré.

Le FNAEG est un fichier commun à la police et à la gendarmerie. Cependant, en application du décret n° 2000-413 du 18 mai 2000 (modifié par le décret n° 2004-470 du 25 mai 2004), le FNAEG est mis en œuvre par la direction centrale de la police judiciaire.

L’institut de recherches criminelles de la gendarmerie nationale assure l’exploitation du service central de préservation des prélèvements biologiques qui assure la conservation des prélèvements effectués sur les scènes d’infraction, après leur analyse.

Les profils génétiques, insérés dans le fichier, sont issus de l’analyse des segments d’ADN dont la liste est fixée par l’article A38 du CPP (arrêté du 14 février 2002).

Les délais de conservation des enregistrements dans le fichier varient :

- 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.

Les empreintes génétiques peuvent être effacées sur instruction du procureur de la République agissant d'office ou à la demande de la personne concernée, quand leur conservation n'apparaît plus nécessaire compte tenu de la finalité du fichier.

Outre les pouvoirs dont dispose la CNIL en vertu de la loi informatique et libertés, le fichier est placé sous le contrôle d'un magistrat du parquet hors hiérarchie, assisté par un comité composé de trois membres, tous étant nommés par le garde des Sceaux, ministre de la Justice.

## Le cadre de saisie informatique

Seuls les fonctionnaires de l'unité gestionnaire du FNAEG (rattachée au service central d'identité judiciaire de la sous-direction de la police technique et scientifique sise à Écully), sont habilités à assurer la saisie et l'exploitation des données (profils génétiques et mentions administratives ou procédurales) ainsi que la consultation de la base à la demande des magistrats et des services d'enquête (article R. 53-18, 1<sup>er</sup> alinéa)

Les fonctionnaires affectés à l'unité précitée accèdent à l'application, *via* l'interface CHEOPS, grâce à un code qui leur est propre. Au niveau des personnels de l'unité gestionnaire, l'interface précitée définit deux types de profils :

- un profil d'administrateur (administration et modification éventuelle de certains paramètres logiciels, gestion des opérateurs de saisie...);
- un profil d'opérateur de saisie (toute opération d'alimentation et de consultation).

Toute opération effectuée sur la base de données fait l'objet d'une traçabilité dans le système.

Concrètement, lorsque le scellé (contenant du matériel biologique prélevé sur la scène d'infraction ou sur une personne) est transmis au laboratoire, l'OPJ ou le magistrat joint un formulaire de demande d'analyse et d'inscription dans le FNAEG du résultat analytique (empreinte génétique) sur lequel sont portées différentes mentions procédurales et administratives relatives au prélèvement.

À l'issue de son analyse, le laboratoire transmet à l'unité gestionnaire du fichier le formulaire précité auquel il joint une fiche sur laquelle est consignée l'empreinte génétique extraite.

Après avoir vérifié la conformité légale ou réglementaire de la demande (type d'infraction, exhaustivité des informations...), l'unité procède à l'insertion dans la base du FNAEG (enregistrement ou simple consultation), des données portées sur les deux documents.

Dès l'insertion dans le fichier, le moteur de recherche de l'application balaie la base et propose d'éventuels rapprochements. À l'issue de cette opération, le résultat (positif ou négatif) est communiqué au requérant sous forme de rapport.

Depuis la loi du 18 mars 2003 et son décret d'application en date du 25 mai 2004, les OPJ (ou APJ placés sous leur autorité) peuvent vérifier dans le FNAEG si une personne susceptible de faire l'objet d'un prélèvement n'y est pas déjà inscrite (une telle consultation ne peut concerner que les seuls états civils <sup>3</sup>).

En outre, les magistrats, les personnes habilitées à procéder à des analyses génétiques et les OPJ peuvent désormais transmettre, par voie télématique, les informations destinées à alimenter le fichier.

Cette dernière mesure revêt une importance capitale en termes de fluidité des flux et d'alimentation. En effet, l'actuel support papier, en tant qu'unique vecteur de l'information, n'est plus compatible avec la très forte montée en puissance du FNAEG et constitue, de fait, une entrave qu'il convenait de supprimer.

En conséquence, le système a fait l'objet de modifications logicielles afin d'intégrer l'interface sécurisée CHEOPS et de permettre, par voie télématique, à partir du poste de travail des fonctionnaires concernés :

- la consultation du fichier par les OPJ et APJ ;
- la transmission, par les OPJ, des informations relatives aux prélèvements.

L'accès à l'application se fait par l'intermédiaire de l'interface précédemment évoquée, au travers de deux profils spécifiques relatifs aux prérogatives qui s'attachent à chaque catégorie de fonctionnaires concernés (agent ou officier de police judiciaire).

Pleinement opérationnel depuis le 17 juillet 2006, ce nouveau type de transfert est appelé à se substituer, progressivement, à l'actuel processus « papier » décrit ci-dessus. Complément indispensable à l'allègement des procédures administratives et à la suppression des doubles saisies, les transmissions télématiques des données en provenance des laboratoires viendront, dans l'avenir, compléter le dispositif. Toutefois, plus complexes dans leur mise en œuvre, elles ne pourront probablement pas être effectives avant la fin de l'année 2007. Dès lors, à titre provisoire, un procédé de transfert par médias (CD-ROM) sera expérimenté à compter du mois de novembre 2006.

---

*Au 31 octobre 2006, près de 350 000 profils étaient enregistrés dans le FNAEG. En 2005, 100 833 consultations ont été effectuées.*

---

(3) L'objet de la consultation par état civil du fichier est d'éviter les doubles prélèvements biologiques d'un même individu comme le précise le I de l'article 706-56 du code de procédure pénale et l'article R. 53-18 du même code issu du décret n° 2004-470 du 25 mai 2004 relatif au fichier national automatisé des empreintes génétiques.

## 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 la 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 (FPR – notamment celles relatives à des mandats 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 être mis en œuvre à l'horizon 2008 et inclure pour les

vingt-cinq États membres de l'espace Schengen (les dix nouveaux États membres entrés dans l'UE en 2004 doivent rejoindre « l'espace Schengen » en 2008) de nouvelles catégories d'objets (bateaux, avions, équipements industriels, moteurs de hors-bord, 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.

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 31 août 2006, la base nationale comptait : 80 620 billets de banque ; 164 716 documents vierges ; 68 741 armes ; 1 890 159 documents d'identité délivrés ; 199 819 véhicules ; 159 688 personnes recherchées. Les opérateurs du Sirène France ont effectué 145 000 consultations en 2005.*

---

---

## **Le fichier de la Direction de la surveillance du territoire (DST)**

### Présentation

Le fichier de la DST comporte trois catégories principales d'informations concernant les personnes physiques, les personnes morales

et les données documentaires, accessibles à partir des postes de travail reliés au réseau informatique de la direction.

L'application est installée sur un réseau spécifique protégé et aucune donnée n'est intégrée automatiquement dans les serveurs. Les informations sont propres à la DST et ont été saisies au fil des ans par le personnel des différents services de la direction.

La saisie est locale : chaque rédacteur saisit, sous le contrôle de sa hiérarchie directe, ses propres données dans la mesure où il est le plus qualifié pour décider de la pertinence des informations méritant d'être archivées.

Des criblages automatisés sur des individus sont effectués, soit systématiquement (demandes de visas), soit à la demande. Les réponses sont imprimées sur des listings qui sont adressés pour avis aux différentes divisions concernées avant toute transmission à l'extérieur.

Pour assurer le contrôle d'accès aux données, la notion de « groupe de travail », qui correspond à une fonction ou à une entité de travail, a été introduite. Les différents droits (saisie, consultation, effacement, rectification) sont attribués à ces groupes d'agents spécialement habilités, ayant besoin d'en connaître, suivant les instructions de chaque chef de service.

Avant qu'une information saisie ne soit introduite dans le système d'information, elle doit être validée par une autorité hiérarchique sous forme de signature électronique. Un dernier contrôle, portant sur la forme, est effectué par un service spécialisé.

Toutes les opérations effectuées (recherches, consultations, saisies, effacements, édition des données) sont tracées sous le contrôle d'un bureau de la sécurité informatique.

Le fichier de la DST n'est pas soumis au même régime juridique que les autres fichiers de la police nationale, dans la mesure où ses activités sont soumises au secret de défense nationale et qu'elle est investie d'une mission de renseignement consistant notamment à gérer des sources humaines et à recevoir des informations classifiées des services étrangers. C'est pourquoi les autres services de police et de gendarmerie n'ont pas un accès direct à ce fichier et que les interrogations extérieures doivent faire l'objet d'une appréciation d'opportunité selon une procédure hiérarchique formelle, quant à la nature des informations susceptibles d'être fournies.

## Les dispositions juridiques

Le particularisme du fichier de la DST a été pris en compte par la loi informatique et libertés du 6 janvier 1978 qui prévoit certaines dérogations pour les fichiers dits « de souveraineté » qui intéressent notamment la sûreté de l'État et la défense.

- Formalités déclaratives simplifiées permettant de ne pas faire figurer les données les plus sensibles. Les données essentielles, qui permettent à la CNIL d'exercer sa mission de contrôle, sont bien sûr maintenues. (Cette disposition abrogée par la loi modificative du 6 août 2004 a été réintroduite pour la loi antiterroriste du 23 janvier 2006, article 13).

- Exemption du contrôle sur pièces et sur place par les agents de la CNIL prévu par l'article 44 de la loi informatique et libertés.

- Modalités particulières pour la mise en œuvre du droit d'accès indirect accordé aux particuliers qui souhaitent savoir s'ils figurent dans un fichier et/ou faire rectifier les données les concernant.

Dans cette hypothèse, deux membres de la CNIL procèdent sur place aux vérifications utiles mais la CNIL ne peut communiquer aucune donnée à l'intéressé sans l'accord du responsable du traitement (article 41). Ces dispositions dérogatoires, strictement définies, permettent de concilier le respect des libertés fondamentales et les impératifs de confidentialité et d'efficacité.

---

*Le nombre de fiches ne peut être divulgué car il est couvert par le secret de la défense nationale. Le nombre de consultations au profit d'autres administrations et services de sécurité nationaux a dépassé, en 2005, le million (1 057 233).*

---

---

## **Le Système d'analyse et de liens de la violence associée au crime (SALVAC)**

La loi n° 2005-1549 du 12 décembre 2005 relative au traitement de la récidive des infractions pénales a créé un cadre législatif spécifique, nécessaire pour la création des fichiers d'analyse criminelle. Elle constitue la base légale de SALVAC. Un projet de décret, accompagné des annexes administratives et techniques, est en cours de mise au point. Après accord interministériel, il sera transmis à la CNIL pour avis, avant saisine du Conseil d'État.

### **Présentation**

Le fichier SALVAC a été créé en janvier 2003. Il vise à opérer des rapprochements aux fins d'établissement de liens entre les informations contenues dans les procédures judiciaires et de mise en évidence du caractère sériel des infractions, en vue d'en identifier les auteurs.

Sont exclusivement concernées les procédures en relation avec des infractions d'une particulière gravité (infractions de meurtre, d'assassinat, d'empoisonnement, d'actes de tortures et de barbarie, d'enlèvement et séquestration, de viol, d'agression sexuelle, d'atteinte sexuelle sur mineur, lorsqu'elles constituent un crime ou un délit puni de plus de cinq ans d'emprisonnement ; infractions de destruction, dégradation ou

détérioration d'un bien par l'effet d'une substance explosive ou d'un incendie commis volontairement, lorsqu'elles constituent un crime ou un délit puni de plus de sept ans d'emprisonnement).

### Le cadre de saisie informatique

Les données à caractère personnel inscrites dans le fichier sont de plusieurs ordres :

- pour la victime et le mis en cause : état civil, adresse(s), lieux fréquentés, numéro(s) de téléphone, phénotype, description physique, photographie, mode de vie ;
- pour le suspect : état civil, adresse, photographie ;
- pour les tiers (témoins et relations de l'agresseur) : nom, adresse, photographie.

Certaines données sensibles (article 8 de la loi du 6 janvier 1978) peuvent également être mentionnées pour le mis en cause et la victime : origine ethnique, vie sexuelle, adhésion à un groupe si cela a une importance pour l'enquête.

Les informations enregistrées sont conservées pour une durée de quarante ans (sous réserve des modalités d'effacement).

### Les destinataires des informations

L'ensemble des données est accessible aux personnels spécialement habilités et individuellement désignés de la police et de la gendarmerie nationales, chargés de procéder à leur enregistrement et à leur analyse (soit une quinzaine de personnels).

Les résultats des rapprochements peuvent être communiqués aux magistrats et enquêteurs pour l'affaire dont ils sont saisis ainsi qu'aux organismes de coopération internationale en matière de police judiciaire et aux services de police étrangers.

### Modalités du droit d'accès aux informations

Les données de ce fichier sont soumises aux règles du droit d'accès indirect auprès de la Commission nationale de l'informatique et des libertés.

### Les souhaits d'évolution

Le formulaire de 34 pages à remplir par le directeur d'enquête n'est pas toujours renseigné correctement. Une réflexion pourrait être utilement engagée en vue de mettre ce fichier sous CHEOPS avec un remplissage obligatoire de « champs » avec validation successive.

---

*Au 31 août 2006, SALVAC contenait 6 352 dossiers.*

---

---

## **Le 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 (CNIL) 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 STIC, le ministère de l'Intérieur a privilégié la présentation du dossier STIC devant la CNIL, prioritaire. Celui n'ayant abouti qu'en 2001 après plus de quinze 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* » (cf. p. 29).

---

## **Le Fichier automatisé des empreintes digitales (FAED)**

Réf. : décret n° 87-249 du 8 avril 1987 ; décret n° 2005-585 du 27 mai 2005.

### Historique

Utilisées par les Chinois dès le V<sup>e</sup> siècle, les empreintes digitales ont fait l'objet de nombreux travaux et études expérimentales, au cours

du XIX<sup>e</sup> siècle, notamment en France sous l'impulsion du professeur Lacassagne, de Galton en Angleterre qui testa avec succès aux Indes un système dactyloscopique, et de Vucetich qui, en Argentine, inventa un procédé simple et rationnel de classement.

Alphonse BERTILLON les introduisit, en 1894, dans son système d'identification criminelle basé jusqu'alors sur l'anthropométrie et la photographie. En 1902, pour la première fois en France, il identifiait l'auteur d'un homicide (Henri-Léon SCHEFFER) à partir de ses seules traces digitales laissées sur une vitrine fracturée qu'il avait comparées avec les empreintes de l'intéressé classées au fichier anthropométrique dactyloscopique.

Durant des décennies, les fichiers dactyloscopiques ont fait l'objet d'un traitement manuel. Dans les années 1980, le ministère de l'Intérieur s'est engagé dans l'exploitation informatisée de ce type de données qui, au terme d'essais validés sur une application baptisée PSO (petit système opérationnel), débouchait sur la première version du FAED, officiellement mise en service en 1992 à la direction centrale de la police judiciaire. Deux ans plus tard, la préfecture de police de Paris et la gendarmerie nationale se connectaient au FAED.

Le FAED a été créé par un décret n° 87-249 du 8 avril 1987.

## Présentation

C'est un fichier commun à la police et à la gendarmerie nationales qui a pour mission de détecter les emprunts d'identité ou les identités multiples et de permettre l'identification des traces digitales et palmaires relevées sur les scènes d'infraction.

Il est mis en œuvre par la direction centrale de la police judiciaire.

Le décret initial précité énonce que peuvent y être enregistrées :

- les traces relevées dans le cadre d'une enquête en flagrant délit, en préliminaire, en exécution d'une commission rogatoire ou d'un ordre de recherche délivré par une autorité judiciaire ;
- les empreintes relevées dans le même cadre sur des personnes contre lesquelles il existe des indices graves et concordants de nature à motiver leur inculpation ;
- les empreintes relevées dans les établissements pénitentiaires en vue de s'assurer de l'identité des personnes détenues dans le cadre d'une procédure pour crime ou délit et d'établir les cas de récidive.

Les informations ainsi enregistrées ne peuvent pas être conservées plus de vingt-cinq ans.

Les dispositions du décret n° 2005-585 du 27 mai 2005 ont complété les dispositions du décret du 8 avril 1987.

Outre les cadres juridiques précédemment définis, peuvent désormais être enregistrées dans le fichier les traces relevées à l'occasion

d'une enquête ou d'une instruction pour recherche des causes d'une disparition inquiétante ou suspecte (articles 74-1 et 80-4 du CCP).

Par ailleurs, le texte prévoit l'enregistrement :

- des empreintes palmaires ;
- des clichés anthropométriques ;
- des traces et empreintes digitales et palmaires transmises par des services de police étrangers ou des organismes de coopération internationale en application d'engagements internationaux.

Le décret réactualise, en outre, les modalités juridiques des signalements de personnes poursuivies dans le cadre d'enquêtes préliminaires ou de flagrance et sur commission rogatoire adoptant la notion « *de personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer, comme auteur ou comme complice, à la commission d'un crime ou d'un délit* », par équivalence à celle du Fichier national automatisé des empreintes génétiques (FNAEG).

L'article 7-1 du décret définit les modalités d'effacement des empreintes lorsque leur conservation n'apparaît plus nécessaire compte tenu de la finalité du fichier. La mise en œuvre de la procédure, à la demande des personnes concernées, est du ressort du procureur de la République.

Outre la CNIL, le fichier est placé sous le contrôle du procureur général de la cour d'appel dans le ressort de laquelle est situé le service gestionnaire.

## Le cadre de saisie informatique

Les relevés d'empreintes digitales et palmaires sur les personnes ou le prélèvement de traces sur les scènes d'infraction, destinées à alimenter le FAED, sont effectués, dans les services d'enquête, par des personnels formés, *a minima*, à la réalisation d'actes simples en identité judiciaire.

L'alimentation et la consultation du fichier automatisé des empreintes digitales sont, quant à elles, limitées aux seuls fonctionnaires dûment habilités des services d'identité judiciaire du ministère de l'Intérieur et des unités de recherche de la gendarmerie nationale (article 8 du décret 87-249 du 8 avril 1987 modifié par le décret 2005-585 du 27 mai 2005). Les habilitations sont délivrées par la direction d'application du FAED (SDPTS/SCIJ).

Ces personnels exercent uniquement sur les sites dédiés à cette tâche, à savoir :

- trois sites centraux situés à : Écully (69) pour la Direction centrale de la police judiciaire (DCPJ) ; Paris pour la préfecture de police ; Rosny-sous-Bois (93) pour la gendarmerie nationale ;
- dix-neuf sites régionaux répartis dans les services territoriaux de la DCPJ.

Chaque fonctionnaire habilité accède au système grâce à un code d'accès qui lui est propre et bénéficie d'un niveau d'habilitation qui

lui est accordé en fonction des différentes tâches qu'il est susceptible d'accomplir. Il existe actuellement treize niveaux (dont deux spécifiques aux services territoriaux de la DCPJ) permettant d'accéder à la base FAED au travers de ses différentes fonctionnalités.

Concernant l'enregistrement dans le système des données signalétiques relatives aux personnes, les fiches « *décadactylaires* » (qui supportent les doigts et les paumes des individus prélevés) font l'objet d'un contrôle de légalité (motif de signalisation) ainsi que d'un contrôle qualité (mentions alphanumériques et relevés digitaux), avant toute insertion en base de données.

Les données alphanumériques (état civil...) font l'objet d'une double saisie à l'issue de laquelle les empreintes digitales qui leur sont associées sont numérisées par scanner et intégrées dans le système. Lors de l'insertion, ce dernier propose d'éventuels rapprochements avec des fiches déjà présentes en base de données. L'opérateur juge alors de la pertinence de ces rapprochements par un examen des dessins digitaux (la validation d'une proposition du système n'étant prononcée qu'après détermination de douze points de concordance entre deux mêmes doigts)

À l'issue de leur insertion dans le fichier, les fiches précitées font l'objet d'un archivage.

Concernant les traces, celles-ci sont insérées dans le FAED par des personnels (« traceurs ») ayant bénéficié d'une qualification spécifique. Après définition de leurs points particuliers, elles sont également numérisées par scanner et insérées dans le système. En retour, ce dernier propose à l'opérateur un certain nombre de rapprochements avec des empreintes digitales d'individus insérées en base de données. Comme précédemment, le « traceur » juge de la pertinence de ces rapprochements par un examen des dessins digitaux et valide une éventuelle identification dans le strict respect des principes précédemment énoncés (détermination de douze points de concordance entre la trace et l'empreinte proposée).

Depuis la fin du premier semestre 2006, après une période d'expérimentation débutée en 2004, des bornes de signalisation sont déployées dans les services de police. Elles ont pour but d'accroître l'efficacité du système en proposant des réponses aux services enquêteurs, pendant le temps de la garde à vue (détection éventuelles d'identités multiples ou identification d'une trace relevée sur une scène d'infraction). Ces matériels permettent la transmission directe des informations signalétiques (données alphanumériques et empreintes), dans la base du FAED, par voie télématique. Ils se substituent ainsi au traditionnel support papier et sont de deux types :

- bornes T1 qui procèdent à la numérisation des empreintes par apposition des doigts sur un bloc optique (sans recours à l'encre traditionnelle) ;
- bornes T4 permettant la numérisation des documents encrés ainsi que le transfert des traces papillaires prélevées sur les lieux d'infraction vers un site régional du FAED en vue de leur exploitation.

Fin 2006, 110 bornes sont opérationnelles (20 T1 et 90 T4). Leur installation, qui a débuté le 20 juin 2006, s'inscrit dans la mise en

œuvre d'un plan pluriannuel (2006-2009) qui doit permettre, à terme, d'en implanter 320 sur le territoire national (50 T1 et 270 T4).

Les personnels de l'identité judiciaire appelés, dans les services, à utiliser ces matériels, sont formés par le Service central d'identité judiciaire de la sous-direction de la police technique et scientifique au fur et à mesure de leur déploiement et reçoivent une habilitation spécifique à leur emploi.

---

*Au 31 août 2006, 2 398 727 individus étaient fichés au FAED.  
En 2005, près de 204 252 consultations ont eu lieu.*

---

---

## **Les fichiers de la gendarmerie nationale**

### **JUDEX**

Réf. : décret n° 2006-1411 du 17 novembre 2006 (JO du 20 novembre 2006).

#### **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 (8 339 000 fiches) et JUDEX-Personnes mises en cause (2 833 000 fiches), 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 constatés et portés 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 et de la police nationales, et prochainement de la douane, 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 5<sup>e</sup> 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 d'attributions 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 infractions 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, de consultation et d'épure

### 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.

#### **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 7 500 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 émane 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.

Ce type de consultation ne permet pas de disposer, pour quelques mois encore, d'une traçabilité des demandes.

#### ***Par réseau intranet gendarmerie***

Ce mode est disponible pour les seules unités reliées par le réseau intranet gendarmerie. À partir du mois de septembre 2006, toutes les unités de gendarmerie seront progressivement 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.

#### **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 alphanumérique 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.

D’octobre 2005 à septembre 2006, le STRJD a traité 1 936 dossiers et en a présenté 1 028 à la CNIL.

Les délais de constitution des dossiers se sont fortement allongés du fait de la saisine des parquets par le STRJD et non plus par la CNIL.

Sur la même période de temps, 360 demandes ont été faites en direction des parquets.

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’épurement**

Les règles d’épurement 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 le 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 le 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'épurement des données à caractère personnel est réalisé sur les bases départementales et sur la base nationale par un traitement automatisé.

### Évolution fonctionnelle ou juridique

Le système JUDEX est en fin de vie opérationnelle et technique. Il doit être remplacé à l'horizon de la fin 2007 par l'application ARIANE commune à la police et à la gendarmerie nationales.

---

*JUDEX rassemble 2,8 millions de fiches concernant des personnes mises en cause et plus de 8,3 millions de fiches affaires. JUDEX est consulté près de 7 500 fois par jour.*

---

## **Le Fichier des objets signalés (FOS)**

### Présentation et finalité

L'application FOS 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 les noms, prénoms et 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'épurement

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'épurement des données est réalisé automatiquement par l'application en fonction des durées de conservation des objets.

## Situation juridique actuelle

Créé comme une base de données sous-ensemble de JUDEX (c'est pourquoi ce fichier est encore appelé JUDEX-objets), 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 fusionnera le FOS et le STIC objets à l'horizon 2007.

## Évolution fonctionnelle ou juridique

Le dossier de déclaration de FOVES sera transmis à la CNIL au cours de l'année 2007.

---

*En septembre 2006, la base contenait 2 473 000 objets. On dénombre 450 consultations de la base par jour.*

---

## **Le fichier de traitement des images des véhicules volés (FTIVV)**

### 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). 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 cette base 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'épurement

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 de la CTIVV. 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'épurement de données n'est encore prévue pour cette base nouvelle encore en cours de déploiement.

### Situation juridique actuelle

Le fichier de la CTIVV est en cours de déclaration auprès de la CNIL.

Toutefois, une circulaire prévoit que seul le STRJD peut exploiter les enregistrements photographiques à des fins judiciaires. Ces informations n'ont actuellement valeur que de simple renseignement judiciaire.

### Évolution fonctionnelle ou juridique

Aucune évolution n'est envisagée.

---

*La base contient plus de 3 000 images en septembre 2006.*

---

## **ANACRIM**

### 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) fonctionne sur la base de fichiers temporaires d'investigations criminelles.

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 :

- d'assister le directeur d'enquête dans le cadre des affaires complexes, en permettant la gestion et l'exploitation d'un grand nombre d'informations, afin d'orienter judicieusement les 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.) ;
- 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 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 de l'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.

## Modes d'alimentation, de consultation et d'épurement

### Alimentation

D'une manière générale, les données intégrées dans les fichiers temporaires sont importées manuellement par les analystes criminels à partir du seul contenu des procédures.

Les données fournies sous forme de listes informatiques (réponses aux réquisitions adressées par les opérateurs téléphoniques ou les services bancaires notamment) peuvent toutefois être directement intégrées dans les bases de données.

Chaque information comporte les références de la pièce de procédure dont elle est extraite.

### Modes de consultation

L'utilisation des fichiers temporaires ANACRIM a donc pour seul objectif et intérêt la mise en évidence, parmi l'ensemble des informations contenues, de certains éléments déterminants pour l'enquête ainsi que leurs relations éventuelles.

Les résultats de l'analyse des données se présentent sous la forme de tableaux relationnels et de graphiques permettant de les visualiser instantanément.

### Modalités d'épurement

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 pour leur part détruits.

## 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) énonce les dispositions relatives aux traitements automatisés d'informations.

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.

Afin de faciliter la constatation des crimes et délits présentant un caractère sériel.

### Évolution fonctionnelle ou juridique

La loi n° 2005-1549 du 12 décembre 2005 relative au traitement de la récidive des infractions pénales dispose qu'un décret d'application doit être pris en Conseil d'État.

À ce jour, ce décret n'a pas encore été publié.

L'intérêt et le besoin de pouvoir mettre en œuvre l'analyse criminelle dans le cadre d'enquêtes autres que celles visées à l'article 30 de la loi n° 2005-1549 du 12 décembre 2005 sont avérés.

Il est donc souhaitable, puisque l'outil existant s'avère performant, de faire évoluer la législation vers un élargissement du champ d'utilisation de ces fichiers, qui ne revêtent qu'un caractère temporaire.

## **Le Service central de préservation des prélèvements biologiques (SCPPB)**

Réf. : arrêté ministériel du 13 septembre 2002.

### Présentation et finalité

Le traitement automatisé dénommé Service central de préservation des prélèvements biologiques a pour finalité d'assurer la gestion des prélèvements biologiques prélevés :

- 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 au service ou unité requérants, au scellé, 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 décret du 18 mai 2000.

### Modes d'alimentation, de consultation et d'épure

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.

### 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.

### Évolution fonctionnelle ou juridique

Il est envisagé de procéder, à l'instar du FNAEG, à la transmission par voie électronique des réquisitions.

---

*Au 1<sup>er</sup> septembre 2006, 5 404 scellés sont conservés au SCPPB.*

---

## **Le Fichier des avis de condamnations pénales (FAC)**

Ce fichier obsolète est en cours d'abandon.

### Présentation et finalité

Le Fichier des avis de condamnations pénales a été créé en 1982 sous la forme d'un fichier manuel local destiné à compléter le fichier

alphabétique de renseignement des brigades (*cf.* fiche FAR) avec les renseignements collectés auprès des greffes des tribunaux.

Ne font l'objet d'une inscription au FAC que les condamnations exécutoires inscrites au bulletin n° 2 du casier judiciaire.

### Nature des informations contenues

Le FAC comprend les données identitaires de la personne condamnée ainsi que les éléments relatifs à la condamnation (nature du jugement, tribunal l'ayant prononcé, peine infligée, infraction réprimée et date des faits).

### Destinataires des informations

Peuvent être destinataires :

- de l'intégralité des informations, les unités de gendarmerie ;
- d'extraits du fichier, les services ou organismes habilités (préfecture, police nationale).

### Modes d'alimentation, de consultation et d'épurement

L'alimentation, la consultation et l'épurement sont réalisés manuellement à partir des informations collectées auprès des greffes ou lors de la promulgation des lois d'amnistie.

### Évolution fonctionnelle ou juridique

Une demande d'accès au casier judiciaire sera formulée auprès de la chancellerie.

Concernant la demande d'accès au casier judiciaire, le ministère de la Justice tient à rappeler que le Code de procédure pénale organise strictement la restitution sélective par le Casier judiciaire national des informations relatives aux condamnations qui y sont mémorisées et gérées au regard des règles d'effacement qu'il édicte.

S'agissant du bulletin n° 2 des personnes physiques et morales, seuls des motifs administratifs strictement énumérés par les articles 776 et 776-1 et R79 du Code de procédure pénale peuvent fonder la demande des autorités administratives et organismes assimilés expressément autorisés par les mêmes textes qui en font une énumération exhaustive.

L'analyse du contenu de ces motifs permet de constater que la délivrance du bulletin n° 2 n'est autorisée aux administrations concernées que pour les renseigner sur la moralité ou la capacité professionnelle des candidats aux divers emplois qu'elles gèrent et professions qu'elles contrôlent.

C'est dans ces conditions que la demande de délivrance de bulletin n° 2 fondée sur un motif d'exercice de la police judiciaire ne saurait prospérer au plan juridique en l'état des textes, étant précisé que leur

modification devrait suivre la procédure du décret en Conseil d'État après avis de la CNIL, en application de l'article 779 du Code de procédure pénale.

Par ailleurs, l'analyse de la nature même de l'activité de police judiciaire conduit à la même conclusion dans la mesure où, si les activités administratives sont accomplies par les administrations de manière autonome – comme l'activité de recrutement propre à la gendarmerie ou à la police nationale – en revanche celles relevant de la police judiciaire s'effectuent sous la direction et le contrôle du procureur de la République en application des articles 12 et 41 du Code de procédure pénale.

Dans le cadre de l'exercice de ses prérogatives de direction de la police judiciaire comme dans ses autres activités judiciaires, le procureur est autorisé à tout moment à accéder au relevé intégral des condamnations qu'exprime exclusivement le bulletin n° 1.

C'est ainsi que l'accès par les officiers de police judiciaire aux informations détenues par le Casier judiciaire national pour l'exécution de leurs missions de police judiciaire doit s'exprimer dans le cadre des pouvoirs de direction et de contrôle de celle-ci dévolus au procureur.

## **PULS@R**

### Présentation et finalité

PULS@R est une évolution de l'application Bureauque brigade 2000, déclarée à la CNIL. Centralisée, elle permet aux unités territoriales de la gendarmerie nationale de gérer sur le plan administratif le service et les registres (courrier et procès-verbaux) et de partager l'information sur la connaissance de la circonscription de l'unité (lieux et personnes particuliers).

L'application PULS@R sera déployée au sein des unités sur la période second semestre 2006/second semestre 2007.

### Nature des informations contenues

PULS@R pourrait contenir certaines informations 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 l'auteur et le type d'infraction relevée ;
- le message d'information statistique : les éléments d'identité et la qualité de la personne (victime ou mis en cause) appréciée au moment de la transmission de la procédure vers l'autorité destinataire (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 vérifier ces 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 (trente jours après l'accident) en vue d'alimenter l'ONISR ;

– le dossier de circonscription : données concernant les 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...);

– le cahier de renseignement : il pourrait comporter des informations nominatives.

### Destinataires des informations

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

### Modes d'alimentation, de consultation et d'épurement

L'alimentation et la consultation se font à partir de n'importe quel poste de travail connecté au réseau intranet.

Les règles d'épurement sont en cours de définition en fonction des objectifs poursuivis par chacun des modules de l'application.

### Situation juridique actuelle

Le dossier de déclaration à la CNIL est en cours de finalisation.

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

## **La Bureautique brigade 2000 (BB2000)**

Réf. : arrêté ministériel en date du 28 octobre 1992, modifié par l'arrêté du 13 mai 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 l'auteur 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 (trente jours après l'accident) en vue d'alimenter l'ONISR ;
- le dossier de circonscription : données concernant les 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 (ONISR).

## Modes d'alimentation, de consultation et d'épure

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'épure varient en fonction des modules :

- le registre : épurement au terme de deux ans échus ;
- les amendes forfaitaires : épurement au terme de deux ans échus ;

- le message d'information statistique : épurement automatique de la partie nominative dès transmission du message ;
- le BAAC : épurement 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).

## Évolution fonctionnelle ou juridique

Cette application sera remplacée par l'application PULS@R sur la période 2006-2007.

## **COG-RENS**

### Présentation et finalité

Le projet COG-RENS permettra à l'horizon 2008 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.

Le dossier de déclaration de COG-RENS sera transmis à la CNIL dès que le périmètre de cette application sera finalisé.

### Nature des informations contenues

Le système COG-RENS comprendra tous les documents non 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, Reuter...).

Il est destiné à contenir des fiches descriptives d'événements, de personnes, d'organisations, de moyens ou de lieux.

Il permettra de stocker toutes les autres données structurées (données issues des formulaires de collecte d'informations structurées, fiches d'appel et d'intervention produites par les centres opérationnels et les brigades...).

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 les applications PULSAR et COG-RENS.

## Modes d'alimentation, de consultation et d'épurement

Seuls les personnels habilités de la gendarmerie auront accès aux informations contenues dans les bases.

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<sup>4</sup> se fera par des interfaces de saisies spécifiques : la fiche renseignement, la fiche entité, le compte-rendu opérationnel, les sources externes formelles.

La consultation pourra se faire par l'Intranet.

L'épurement des données, qui ne pourra qu'être automatisé pour maintenir un niveau de mise à jour efficient, fait l'objet de règles qui sont en cours de définition dans le cadre de l'étude de COG-RENS.

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 événements ARAMIS.

## **Le Fichier alphabétique de renseignements (FAR)**

### Présentation et finalité

Se présentant sous forme de fiches manuscrites individuelles gérées localement, le Fichier alphabétique de renseignements (FAR) avait pour vocation de permettre aux militaires des unités opérationnelles d'acquies 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 dispositions légales relatives au respect des libertés individuelles, obligent la gendarmerie nationale à refondre ce système.

Au terme de la période transitoire, fixée avant octobre 2010, le FAR sera supprimé.

### Nature des informations contenues

Les informations contenues sont relatives à l'état civil de la personne, les procédures dont elle a fait l'objet (judiciaire, administrative, police route...) ainsi que tout autre renseignement utile pouvant faciliter le travail des unités opérationnelles (comportement, possession d'armes, propriétaire de chiens dangereux...).

(4) Mise en oeuvre par exemple en cas d'événements d'ordre public d'ampleur nationale et qui visent à établir régulièrement un bilan des troubles en cours.

## 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 principale ;
- 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'épurement

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'épurement 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'épurement des fiches ne donnent plus satisfaction en raison du volume de fiches à traiter, estimé à 60 millions sur l'ensemble du territoire national.

## Évolution fonctionnelle ou juridique

Dès 2008, les renseignements exclusivement administratifs seront intégrés dans le nouveau système COG-RENS (*cf.* fiche spécifique). Les fiches détenues dans les brigades seront détruites avant octobre 2010.

## Droit d'accès aux informations

Le droit d'accès au FAR s'effectue indirectement. Le requérant adresse une demande au président de la CNIL qui saisit par courrier le chef du STRJD. La procédure décrite dans la fiche JUDEX est identique pour le FAR.

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 l'estime à 60 millions de fiches. Le nombre de consultations n'est pas comptabilisé.*

---

## **Le Fichier des personnes nées à l'étranger (FPNE)**

### Présentation et finalité

Créé en 1975, le Fichier des personnes nées à l'étranger est un fichier nominatif manuel. À l'instar du fichier alphabétique de renseignements (FAR), il est constitué de fiches cartonnées individuelles.

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'épurement

La gestion des fiches du FPNE, y compris les opérations d'épurement, est entièrement manuelle. Chaque militaire établit une fiche dès lors qu'une personne née à l'étranger entre en contact avec une unité de gendarmerie. Ce document est alors expédié au STRJD qui en fait retour après exploitation. L'organisme central conserve un volet détachable de la fiche cartonnée, insérée dans le fichier alphabétique de renseignements.

L'administration pénitentiaire communique au STRJD les avis d'écrou. Les fiches existantes sont renseignées en conséquence. Au besoin, de nouvelles fiches sont créées.

Si les militaires de l'unité détentrice des fiches peuvent accéder directement à ces informations, les autres gendarmes doivent saisir le STRJD aux fins de communication.

Les conditions d'épurement sont similaires à celles du FAR : les personnes décédées ou ayant plus de 80 ans ne doivent plus faire l'objet d'une fiche, de même que les personnes identifiées à une date antérieure à 10 ans étant SDRF au moment du contrôle, ou domiciliées à l'étranger.

## Situation juridique actuelle

À l'issue de la période de mise en conformité des fichiers manuels dont l'échéance est octobre 2010, ce fichier sera définitivement supprimé.

## Évolution fonctionnelle ou juridique

La période transitoire évoquée *supra* sera mise à profit pour fixer les modalités de la reprise des données.

## Droit d'accès aux informations

Le droit d'accès au FPNE s'effectue indirectement. Le requérant adresse une demande au président de la CNIL qui saisit par courrier le chef du STRJD. La procédure décrite dans la fiche JUDEX est identique pour le FPNE.

Le nombre de demandes ne peut être précisé.

---

*À ce jour, le FPNE, fichier mécanographique, comporte environ 7 millions de fiches. Le nombre de consultations n'est pas comptabilisé.*

---

## **Le fichier ARAMIS**

### Présentation

L'application ARAMIS 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 événements en cours, de leur évolution et de leur implication.

### Nature des informations contenues

Essentiellement orientée vers la gestion et le suivi de l'évènement, ARAMIS contient certaines données effectivement nominatives (nom, 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 (*cf. infra*).

## 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'épure

L'alimentation des bases de données peut être effectuée par toute unité disposant d'un terminal RUBIS, ou de l'application ARAMIS.

La consultation des données, dans la gestion immédiate d'une intervention, est réalisée par l'opérateur du CORG. Les cellules RENS, au niveau des groupements et des régions, peuvent consulter la base « *événements* » (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. À chaque niveau hiérarchique ou pour chaque type de module, des droits sont ouverts pour une catégorie d'unité.

L'épurement des données personnelles est automatisé au terme d'un délai de trois mois, sans qu'il y ait d'archivage.

## Évolution fonctionnelle ou juridique

Le système de gestion de l'intervention et de suivi des événements sera géré prochainement par l'application COG-RENS qui conduira à la disparition d'ARAMIS.

## **Le Fichier de suivi des titres de circulation délivrés aux personnes sans domicile ni résidence fixe (SDRF)**

Réf. : arrêté interministériel du 22 mars 1994 modifié par l'arrêté du 28 février 2005.

## Présentation et finalité

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

## 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.

### 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 fixe. 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.

### Modes d'alimentation, de consultation et d'épurement

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.

La consultation par les unités de gendarmerie est effectuée *via* le réseau intranet. Par contre, les demandes de renseignements provenant d'organismes extérieurs sont traitées à l'échelon central (STRJD). Elles doivent être adressées par voie postale ou télématique authentifiée, précisant l'identité du consultant, l'objet, le motif de la consultation et les éléments de réponse souhaités. Dans le cadre d'enquêtes judiciaires, ce fichier ne peut être consulté que par le biais de réquisitions adressées au STRJD, gestionnaire du fichier.

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.

### Droit d'accès

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.

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

### Évolution fonctionnelle ou juridique

La circulaire relative au fichier des titres de circulation délivrés aux personnes sans domicile ni résidence fixe 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 comportait 168 200 fiches en septembre 2006. De janvier à septembre 2006, 49 400 consultations ont été réalisées.

---

## **Le Fichier de suivi des personnes faisant l'objet d'une rétention administrative**

Réf. : arrêté interministériel du 19 décembre 1994 modifié par l'arrêté du 30 juillet 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, mettent 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'épure

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 deux ans, les informations sont effacées.*

---

## Évolution fonctionnelle ou juridique

Le MIAT expérimente aujourd'hui le système ELOI, développé par la DCPAF à Lognes (77), qui permettra une gestion commune interservices (police, gendarmerie, administration pénitentiaire et préfecture) des étrangers. Dès la mise en œuvre du système ELOI, les fichiers de suivi des personnes faisant l'objet d'une rétention administrative seront détruits.

## **Le Fichier de la batellerie**

Ce fichier n'a fait l'objet d'aucune déclaration.

### Présentation et finalité

Le Fichier de la batellerie a été créé en 1942 afin d'assurer le suivi des marinières ainsi que celui des bateaux affectés au transport fluvial de marchandises et des compagnies fluviales. Fichier manuel géré par la brigade de Conflans-Sainte-Honorine (78) jusqu'à la dissolution de celle-ci, il est aujourd'hui détenu, au titre des archives, par le STRJD à Rosny-sous-Bois (93).

### Nature des informations contenues

Riche de 52 000 fiches, ce fichier recense des informations concernant les marinières, leur famille, leurs ouvriers, leur bateau et leur employeur. Il regroupe également des informations concernant les compagnies fluviales.

### 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.

### Modes d'alimentation, de consultation et d'épurement

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

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

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

## Évolution fonctionnelle ou juridique

Le besoin d'un suivi des activités du milieu fluvial perdurant, ce fichier, tombé en désuétude, est conservé en l'état dans l'attente d'une décision relative à la création d'un fichier informatique prenant en compte l'apparition de secteurs nouveaux tels que la navigation commerciale de passagers ou de plaisance et celui des bateaux-logements.

En raison de la désuétude des données qu'il contient, ce fichier n'est plus consulté aujourd'hui.

---

## ARIANE

La direction des libertés publiques et des affaires juridiques du ministère de l'Intérieur et la Direction des affaires juridiques du ministère de la Défense ont entrepris la réalisation du dossier de déclaration de l'application à la CNIL. L'application sera créée par décret en Conseil d'État après avis de la CNIL. Le décret portera abrogation des décrets STIC et JUDEX.

## 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 réalisation débutera à compter d'octobre 2006. La mise en œuvre opérationnelle devrait intervenir à l'horizon de la fin de l'année 2007 ou au début de l'année 2008.

## Nature des informations contenues

Les informations contenues dans ARIANE respecteront les mêmes règles que les applications STIC et JUDEX actuelles (*cf.* fiches STIC et JUDEX). En revanche, l'origine des informations (police ou gendarmerie) ne sera plus distinguée.

## Destinataires des informations

Les règles actuelles valables pour les applications STIC et JUDEX seront appliquées pour ARIANE. À noter notamment qu'il est prévu un accès direct au profit des parquets.

## Modes d'alimentation, de consultation et d'épure

### 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'épure

Les règles d'épure 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 épures de façon automatique.

---

## **Le 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 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 1<sup>er</sup> 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.

### **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 et par la loi du 4 avril 2006 renforçant la prévention et la répression des violences au sein du couple ou commises contre les mineurs.

La mise en œuvre du FIJAIS a été assurée par un comité interministériel (Justice, Intérieur, Défense) de pilotage présidé par le ministre 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 assure un regroupement semestriel de ses référents désignés par le procureur général de chaque cour d'appel.

Le ministère de la Justice est responsable et gestionnaire du FIJAIS. Il est tenu par le service du casier judiciaire national (CJN) 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 énoncées à l'article 706-47 du Code de procédure pénale, mais également, concernant ces mêmes infractions, les personnes ayant exécuté une composition pénale, mises en examen par une juridiction d'instruction ou 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).

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.

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.

À 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 doivent, tous les six mois, se présenter en personne afin de justifier de leur adresse. Le séjour à l'étranger d'une personne inscrite ne fait pas cesser ses obligations.

Le non-respect de ces obligations constitue une infraction pénale punie d'une peine d'emprisonnement de deux ans et de 30 000 euros d'amende.

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 : préfetures.

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 leur identité ainsi que par le gestionnaire.

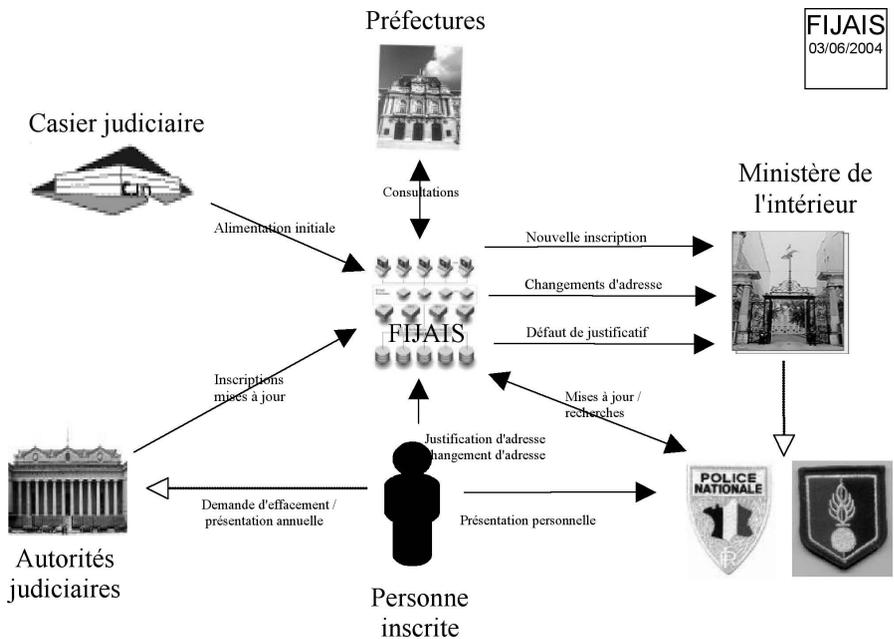
Le gestionnaire du FIJAIS, avant de valider l'inscription d'une personne, vérifie son identité au vu du Répertoire national d'identification des personnes physiques. Il procède aux effacements ou refuse les enregistrements non conformes à la loi ou au règlement.

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.

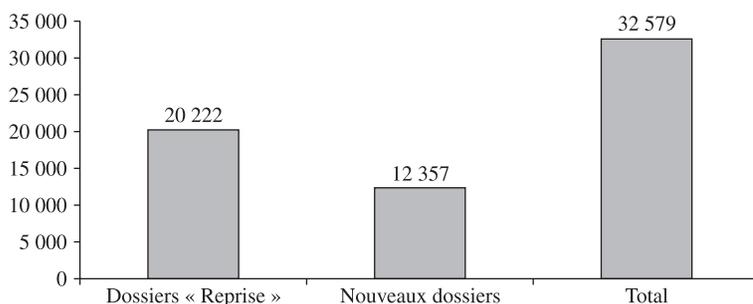
Tout accès au FIJAIS est tracé et archivé durant trois ans.

### Schéma général de fonctionnement



Le FIJAIS est une application *Web* conçue sur un principe de client léger. Les utilisateurs bénéficient d'un accès sécurisé (identifiant, mot de passe), l'ensemble des échanges, cryptés et tracés étant réalisé au travers du réseau inter-administration ADER, à partir des portails propres à chaque administration (CHEOPS et serveur gendarmerie) en fonction de leur habilitation.

## Données statistiques



---

*À l'entrée en service, l'application comprenait 20 222 dossiers enregistrés au titre de la reprise de l'article 216-II de la loi du 9 mars 2004. Au 31 juillet 2006, 31 827 dossiers sont actifs sur 33 527 dossiers enregistrés au 10 août 2006.*

---

---

## Le Fichier national des permis de conduire (FNPC)

Réf. : arrêté du 20 décembre 1972.

### Présentation du fichier – Historique

Au sein du ministère de l'Intérieur et de l'Aménagement du territoire – Direction des libertés publiques et des affaires juridiques, sous-direction de la circulation et de la sécurité routières, le service du Fichier national des permis de conduire, 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 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 SNPC comprend des données centrales et des données locales.

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

- Dans tous les cas :
  - l'état civil : nom, nom d'usage, prénoms, date et lieu de naissance ;
  - l'adresse ;
  - le 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.

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 et des commissions spéciales dites « *de suspension du permis de conduire* » : nom, prénom, adresse des membres, organismes représentés, qualité de délégué permanent de la commission de suspension ;
- 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 préfetures

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 ;
- la saisie des décisions judiciaires de 5<sup>e</sup> classe et des délits dans le SNPC.

Les préfetures 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-préfetures

Elles ont un rôle identique aux préfetures 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.

À 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 au SNPC ainsi que les informations relatives à la sanction prévue. Le 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 restreint des dossiers contenus dans SNPC, c'est-à-dire aux informations relatives à l'existence, les catégories et la validité du permis de conduire.

## **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. Le 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)**

Les DDE peuvent jouer un rôle semblable à celui d'une préfecture. Elles sont raccordées à un CII et peuvent effectuer en temps réel les opérations suivantes :

- mise à jour du 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 au SNPC par une liaison sécurisée, *via* le réseau ADER.

## **La gendarmerie**

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

## **L’Imprimerie nationale**

L’Imprimerie nationale a en charge, à partir du 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 DLPAJ**

La DLPAJ intervient au travers du service du 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 le 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 (ensemble, 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) et les forces de l’ordre lors des contrôles routiers (en application de l’article L. 225-5 du Code de la route).

## **Prochaines évolutions envisagées**

L’architecture fonctionnelle et technique de l’actuelle application réglementaire 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 outre, la base de données est

quasiment saturée, compte tenu de la nécessité d'y intégrer l'augmentation exponentielle du nombre d'infractions relevées dans le cadre du système de contrôle-sanction automatisé.

En conséquence, un projet de refonte globale de cette application informatique doit être initié au cours du second semestre 2006.

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 2009, offrira donc une meilleure qualité de service aux usagers et permettra un renforcement de la lutte contre la violence routière, la fraude et le contournement des mesures restrictives prises au niveau national. Parallèlement, des économies importantes devraient être générées en maintenance évolutive.

---

## **AGRIPPA**

### Objectifs

La réglementation relative aux armes à feu repose sur de nombreux textes et notamment les articles du Code de la défense fixant le régime des matériels de guerre, armes et munitions et le décret n° 95-589 du 6 mai 1995 relatif à l'application du décret du 18 avril 1939.

C'est pour l'application efficace de ces textes que le ministère de l'Intérieur et de l'Aménagement du territoire est amené à mettre en œuvre une application nationale de gestion du répertoire informatisé des propriétaires et possesseurs d'armes (AGRIPPA).

Cette application doit permettre une gestion rigoureuse des demandes d'autorisation d'acquisition et de détention d'armes ainsi que des récépissés de déclaration délivrés par l'autorité administrative.

### Processus de l'application

L'application AGRIPPA de gestion des armes soumises à autorisation ou déclaration se compose de quatre modules fonctionnels :

- un module d'aide à la classification des armes et munitions enregistrées ;
- un module de gestion des autorisations ;
- un module de gestion des déclarations ;
- un module de gestion des cartes européennes d'armes à feu.

Le traitement automatisé est alimenté par les sites en charge de la gestion des armes (préfectures et sous-préfectures).

Déployée le 8 février 2006, la version 1.9 du logiciel AGRIPPA permettra un accès en consultation des données aux services de la police et gendarmerie nationales, *via* leurs portails informatiques sécurisés.

Un profil d'habilitation spécifique offrira à ces services, dans le cadre de leurs attributions et sous la responsabilité de l'autorité hiérarchique, la possibilité de consulter les informations relatives :

- aux détenteurs d'armes, d'éléments d'arme et munitions ;
- aux titres de détention (autorisation, déclaration et carte européenne d'arme à feu) ;
- aux matériels (arme, élément d'arme, matériel divers) en possession des détenteurs ;
- aux données du catalogue des armes de l'application informatique.

L'utilisateur disposera de modalités de recherches simples, affinées ou reposant sur plusieurs critères.

## Évolution

Le décret n° 2005-1463 du 23 novembre 2005 introduit dans le décret n° 95-589 du 6 mai 1995 un chapitre VII intitulé « La saisie d'arme et de munitions » qui détermine les modalités d'application des articles L. 2336-4 et L. 2336-5 du Code de la défense.

Cette modification de la réglementation suppose la création d'un module fonctionnel de gestion de l'instruction des saisies administratives d'armes prononcées par l'autorité préfectorale.



---

## Chapitre 2

---

# Problèmes et dysfonctionnements



Il convient tout d'abord de rappeler que la loi du 6 janvier 1978 modifiée dispose que tout traitement automatisé de données à caractère personnel ne doit comporter que des données « *exactes, complètes et, si nécessaire, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées* » (article 6,4).

Les difficultés pouvant affecter l'usage des fichiers de sécurité dépendent au premier chef de la nature des données qu'ils contiennent.

Tout d'abord, certains fichiers recueillent des données que l'on peut qualifier, par commodité de langage, de « *techniquement neutres* ». C'est le cas du FAED ou du FNAEG, puisque les empreintes digitales ou génétiques sont des éléments biométriques propres à chaque individu. La gestion de ces fichiers prévoit d'ailleurs un protocole d'alimentation et de validation scientifiquement établi et rigoureux : formation des agents procédant aux relevés des empreintes d'un individu, spécialisation plus grande encore des agents chargés du recueil des traces anonymes sur les scènes d'infraction, séparation des chaînes de traitement respectives des traces anonymes et des analyses des individus pour les empreintes génétiques, vérification (légalité et qualité) par des spécialistes avant inscription dans le fichier, etc.

Aux erreurs matérielles de saisies près dans les champs autres que les données biométriques, ces fichiers ne connaissent aujourd'hui qu'une seule dimension significative en termes d'exercice du droit d'accès : celle de l'usurpation de l'identité d'une tierce personne par une personne signalisée. Dans ce cas, les éléments centraux du fichier (empreintes digitales ou génétiques) sont corrects, mais pas les données nominatives relatives à l'identité. Lors d'une demande de droit d'accès, le titulaire réel de l'identité est invité à se soumettre à un prélèvement aux seules fins de vérification et de rectification (ses données personnelles n'étant pas conservées). Cette procédure ne soulève pas à ce jour de difficulté particulière.

Le législateur a défini un régime encadré et équilibré autorisant le recours aux empreintes génétiques comme outil criminalistique au service de l'enquête judiciaire. Le prélèvement et la simple comparaison par rapport à la base génétique du fichier (article 706-54, alinéa 3 du CPP) n'est possible que s'il existe une raison plausible de soupçonner qu'une

personne a commis un crime ou un délit. En revanche, la conservation du profil génétique dans la base n'est possible que si des indices graves et concordants sont réunis et que l'on se situe dans le champ des infractions limitativement énumérées par l'article 706-55 du CPP. Le législateur a également prévu des voies de recours et, sous certaines conditions, l'effacement lorsque la conservation n'est plus nécessaire à l'enquête au regard de la finalité du fichier. Dès lors, inévitablement, des recours plus nombreux seront formés au fur et à mesure de la montée en régime du fichier, qui comprend aujourd'hui 350 000 profils.

Rappelons toutefois que cela ne concerne en rien la problématique des enquêtes administratives préalables à la délivrance de diverses autorisations ou agréments professionnels, puisque les fichiers d'identification FAED et FNAEG, à finalité exclusivement judiciaire, ne sont jamais consultés au cours de ce type d'enquêtes.

Sont également « *techniquement neutres* » les données conservées dans le fichier national transfrontières (simple lecture automatisée des données du titre de voyage et indication des coordonnées de l'entrée ou de la sortie du territoire). Ces informations ne sont accessibles, outre les besoins de la lutte contre l'immigration irrégulière, que pour la lutte antiterroriste. Celle-ci ne recouvre qu'un champ très limité des enquêtes administratives préalables à la délivrance d'une autorisation administrative. Ainsi, ce fichier ne sera consulté que si des informations préalablement recueillies au cours de l'enquête administrative justifient sa consultation.

D'autres fichiers encore recueillent également des données que l'on peut qualifier de « *techniquement neutres* ». C'est par exemple le cas du fichier des personnes recherchées, dans la mesure où y sont inscrites des mesures judiciaires ou administratives à exécuter ou au respect desquelles il faut veiller. La problématique des données erronées se concentre principalement sur les erreurs matérielles de saisies ou, indirectement, sur le bien fondé des décisions, administratives ou judiciaires, qui ont servi de support à l'inscription dans le FPR, ainsi que dans son équivalent européen interconnecté, le SIS. La problématique est similaire s'agissant du fichier des véhicules volés.

Il convient ensuite d'examiner la situation des fichiers des services de renseignements dans lesquels prédominent les éléments « *qualitatifs* ». Toutefois, la jurisprudence administrative a clairement fixé les règles applicables en matière d'utilisation des fichiers des services de renseignement à l'occasion de décisions administratives, qu'il s'agisse de décisions relatives au droit au séjour des étrangers ou même à des refus d'habilitation ou d'agrément. C'est le cadre fixé par cette jurisprudence qui est par exemple appliqué dans le dossier de la sécurité aéroportuaire.

- Application du cadre législatif de la loi n° 79-587 du 11 juillet 1979 (motivation des actes administratifs) : la motivation est obligatoire pour « *les décisions qui restreignent l'exercice des libertés publiques ou, de manière générale, constituent une mesure de police* », qui « *infligent une sanction, ou retirent ou abrogent une décision créatrice de droits* ».

- En cas de procédure contentieuse, la motivation peut être étayée par une note des services de renseignement établie à partir des informations conservées par les services dans leurs fichiers. Cette note est reconnue par le juge comme ayant une valeur probante sous la condition qu'elle soit suffisamment précise et circonstanciée. Toutefois, cette valeur probante n'est pas automatique et le magistrat examine tous les éléments qui lui sont apportés par le requérant (CE, 3 mars 2003, ministère de l'Intérieur contre RAKHIMOV).

Par ailleurs, et dans la période d'activité du groupe de travail, des interrogations sont apparues quant aux modalités d'application du fichier ELOI (voir annexe – texte sur le fichier ELOI), notamment pour l'enregistrement des visiteurs des personnes concernées (en particulier leurs défenseurs). De même, la presse nationale a rapporté l'existence d'un fichier développé par une brigade de gendarmerie pour disposer d'informations sur les travailleurs saisonniers employés localement. Ce fichier a été aussitôt détruit en application des textes en vigueur dans la gendarmerie. Une enquête de commandement a été diligentée par la hiérarchie. L'autorité judiciaire a été informée.

Enfin, il y a la situation du STIC et de JUDEX, deux fichiers alimentés quasiment en temps réel par les officiers de police judiciaire lorsqu'ils transmettent les conclusions de leurs enquêtes au magistrat compétent, procureur ou juge d'instruction. Les données enregistrées résultent de l'appréciation des faits par l'OPJ qui les qualifie. Mais cette qualification peut être complétée, réformée ou infirmée par l'autorité judiciaire, aussi bien par le procureur de la République, le juge d'instruction que par la juridiction de jugement.

Les membres du groupe de travail ont constaté que, dans le cadre de l'utilisation administrative des fichiers de police judiciaire, ces deux fichiers sont ceux qui posent plus de difficultés, eu égard aux conséquences importantes qui peuvent en résulter pour les individus.

\* \* \*

L'article 17-1 de la loi 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, introduit dans l'ordre juridique par l'article 28 de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, autorise la consultation des fichiers dits d'antécédents judiciaires dans le cadre d'enquêtes administratives (STIC et JUDEX<sup>1</sup>). 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.

(1) Au 1<sup>er</sup> janvier 2005, le fichier STIC comportait 5 millions d'individus mis en cause et le fichier JUDEX 2 500 000 de personnes inscrites en qualité de mises en cause.

Aux termes de l'article 17-1 ainsi modifié, la consultation des fichiers de police judiciaire est possible dans le cadre d'enquêtes préalables aux décisions administratives de recrutement, d'affectation, d'agrément, ou d'habilitation concernant soit les emplois publics participant à l'exercice des missions de souveraineté de l'État, soit les emplois publics ou privés du domaine de la sécurité et de la défense.

La consultation des fichiers de police judiciaire est également prévue pour l'autorisation d'accès à des zones protégées en raison de l'activité qui s'y exerce et les autorisations concernant les matériels ou produits présentant un caractère dangereux (exemple : port d'armes).

Le décret n° 2005-1124 du 6 septembre 2005 (abrogeant le décret n° 2002-424 du 28 mars 2002, modifié par le décret n° 2005-307 du 24 mars 2005), précise la liste des emplois du secteur public et du secteur privé pouvant donner lieu à la consultation de ces fichiers de police judiciaire : agents de police municipale, agents de surveillance et de gardiennage, convoyeurs de fonds, membres des services d'ordre des organisateurs de manifestations sportives, récréatives, ou culturelles... En 2005, plus de 120 000 enquêtes administratives ont été effectuées dans le cadre de la loi du 12 juillet 1983 sur la sécurité privée et plus de 70 000 dans le seul domaine aéroportuaire.

La consultation du STIC n'est pas propre aux métiers de la sécurité privée, mais s'effectue aussi pour l'accès à de nombreux emplois régaliens, ou pour travailler dans des zones protégées au titre de la défense nationale (pour des raisons militaires ou civiles comme les activités économiquement très sensibles).

L'article 17-1 de la loi du 21 janvier 1995 précitée prévoit en outre la consultation de ces fichiers pour « *l'instruction des demandes d'acquisition de la nationalité française et de délivrance et de renouvellement des titres relatifs à l'entrée et au séjour des étrangers ainsi que pour la nomination et la promotion dans les ordres nationaux* ».

Lors de l'examen, en octobre 2002, du projet de loi pour la sécurité intérieure, la CNIL avait souligné que l'extension des cas de consultation des fichiers de police judiciaire à des fins administratives risquait de leur faire jouer : « *Le rôle d'un casier judiciaire parallèle moins contrôlé, alors même que leur objet, leurs conditions d'accès, les modalités structurelles de leur alimentation et les délais inévitables de toute mesure d'effacement ou de mise à jour doivent en faire seulement un instrument de police judiciaire sauf dans quelques cas bien précis et rigoureusement contrôlés.* »

Le Conseil constitutionnel, dans sa décision sur la loi de sécurité intérieure (n° 2003-467DC) en date du 18 mars 2003, a validé ce dispositif en déclarant « *qu'aucune norme constitutionnelle ne s'oppose par principe à l'utilisation à des fins administratives de données nominatives recueillies dans le cadre d'activités de police judiciaire* » et que ces consultations étaient assorties de garanties suffisantes au regard du respect des libertés individuelles.

La loi et le règlement prévoient en effet différentes garanties pour la consultation des fichiers de police judiciaire dans le cadre d'enquêtes administratives.

L'article 6 du décret du 5 juillet 2001 modifié par le décret n° 2006-1258 du 14 octobre 2006 sur le STIC prévoit à cet égard une limitation des informations accessibles.

Ainsi, les consultations effectuées dans le cadre d'enquêtes administratives ne permettent pas d'accéder aux informations relatives aux victimes ni à celles concernant les personnes mises en cause ayant bénéficié d'une suite judiciaire favorable (non-lieu et classement sans suite motivés par une insuffisance de charges).

Cependant, contrairement à l'article 6 du décret du 5 juillet 2001 d'origine qui limitait la consultation à des fins administratives (dans des cas exceptionnels) aux seules informations qui se rapportaient à des procédures judiciairement closes, l'article 25 de la loi 18 mars 2003 précitée étend cette possibilité de consultation aux données portant sur des procédures judiciaires en cours.

Deux décrets pris en application de l'article 21 de la loi du 18 mars 2003 précitée ont été élaborés. Le décret n° 2006-1258 du 14 octobre 2006 modifiant le décret STIC n° 2001-583 a été publié le 15 octobre 2006. Le décret 2006-1411 du 17 novembre 2006 portant création du système JUDEX a été publié le 20 novembre 2006. Ces deux textes au contenu similaire ont fait l'objet d'un avis de la CNIL comportant un certain nombre de réserves (délibération du 8 septembre 2005). Ils ont fait l'objet d'un examen par le Conseil d'État qui a retenu certaines des préconisations de la CNIL.

Dans son avis rendu sur les fichiers STIC et JUDEX le Conseil d'État s'est prononcé en faveur du renforcement de certaines garanties :

- **Sur l'information du procureur**

Comme le précisait l'article 2 du décret n° 2001-583 du 5 juillet 2001 portant création du STIC, en vigueur au moment des débats devant le Conseil d'État « *les informations nominatives relatives aux personnes mises en cause et aux victimes ainsi que la qualification des faits telles qu'elles sont enregistrées dans le STIC, sont transmises au procureur de la République en même temps que la procédure* ».

Le contrôle du procureur de la République porte donc sur des données enregistrées au STIC au regard de la procédure qui lui est transmise.

La transmission de la procédure constitue en effet, un préalable essentiel à ce contrôle puisque seule sa lecture permettra au procureur de la République de procéder à l'analyse juridique des faits nécessaire à leur qualification, d'estimer la suffisance des charges susceptibles d'être retenues à l'encontre d'une personne enregistrée comme mise en cause dans le fichier, etc.

Les avis rendus par l'assemblée générale du Conseil d'État le 9 mars 2005 n'ont pas prévu que le procureur de la République soit informé des données susceptibles d'être enregistrées et qu'il les valide préalablement à leur enregistrement.

Le Conseil d'État a indiqué que le procureur de la République, pour être mis en mesure d'exercer son contrôle sur les données devait en être destinataire dès leur enregistrement : « *Le traitement des données à caractère personnel est opéré sous le contrôle du procureur de la République territorialement compétent conformément aux dispositions de l'article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure. À cette fin, l'ensemble des données lui sont transmises lorsqu'elles sont enregistrées.* » (Articles 3 des projets de décrets STIC et JUDEX).

Le Conseil d'État a ainsi estimé nécessaire que les données à caractère personnel soient transmises au procureur de la République lorsqu'elles sont enregistrées sans que cette information soit subordonnée à la transmission des actes de la procédure.

Il est apparu néanmoins que les modalités proposées de contrôle des données par le procureur de la République auraient pour effet de le rendre inopérant si ce magistrat devait d'apprécier la pertinence des informations collectées sans avoir à sa disposition les actes de la procédure afférente aux dites informations.

C'est la raison pour laquelle le Gouvernement a préféré à cette proposition celle retenue dans les projets de décrets initiaux soumis à l'examen du Conseil d'État. Aux termes de celle-ci, les données à caractère personnel relatives aux personnes mises en cause ou aux victimes ainsi que la qualification des faits sont transmises au procureur de la République, lorsqu'elles sont enregistrées, en même temps que la procédure.

- **Sur l'information des victimes**

Le Conseil d'État a estimé nécessaire que les victimes d'infractions soient informées de leur droit d'accès et d'opposition au maintien de leurs données, lorsque l'auteur des faits a été définitivement condamné, dans les fichiers STIC ou au JUDEX. La forme de cette information n'a pas été précisée. Le Gouvernement a pris en compte cette recommandation dans sa rédaction des décrets.

- **Sur le recours devant le procureur général**

Comme l'a rappelé le Conseil constitutionnel dans sa décision n° 2003-467 DC du 13 mars 2003, les dispositions de la loi du 18 mars 2003, dont celles de son article 21, doivent s'articuler avec celles de la loi du 6 janvier 1978 précitée.

Il en résulte, y compris dans l'hypothèse où la demande de droit d'accès indirect est adressée au procureur de la République, qu'il appartient au responsable du traitement en application de celle-ci de prendre ou non la décision d'effacement ou de rectification et non au procureur de la République lui-même à la suite de leurs échanges. Il s'ensuit que la réponse du magistrat adressée au requérant à la suite de sa demande

doit être regardée comme une mesure d'information attestant de son contrôle opéré sur les mentions enregistrées dans les fichiers et non comme une décision.

La portée du recours exercé devant le procureur général en cas de silence du procureur de la République aurait donc été limitée. De surcroît il ne peut être automatiquement déduit du silence du procureur de la République une absence de dialogue entre ce magistrat et le gestionnaire du fichier, dialogue qui constitue le préalable nécessaire à toute décision d'effacement ou de rectification de données obsolètes ou erronées

Le Gouvernement a donc écarté l'instauration d'un tel recours hiérarchique auprès du procureur général.

**• Le Conseil d'État a recommandé au Gouvernement de préciser dans les projets de décret les modalités d'habilitation des personnes ayant accès à ces fichiers et de prévoir une traçabilité des inscriptions et des consultations de ces fichiers.**

Début 2008, il est prévu une fusion entre les fichiers STIC et JUDEX avec la création d'un fichier de police judiciaire commun.

\* \* \*

Au 1<sup>er</sup> janvier 2006, 87 856 agents étaient habilités à accéder au STIC dans le cadre d'une mission de police judiciaire, de police administrative ou de fonctions de gestion du fichier. Le décret STIC prévoit que, pour accélérer le traitement des demandes liées à des enjeux professionnels, les agents des préfectures pourront avoir accès (après habilitation individuelle et de manière « traçée ») au STIC sur le mode « connu/inconnu ». Ceci devrait permettre de traiter sans délai les décisions ne posant aucun problème et de recentrer les services de police et de gendarmerie sur les enquêtes administratives approfondies car impliquant des antécédents de police judiciaire.

---

*Pour le ministère de l'Intérieur, le STIC et JUDEX sont les seuls outils disponibles suffisamment réactifs pour permettre aux services de police et de gendarmerie d'assurer avec toute l'efficacité requise leurs missions de sécurité. En effet, outre les procédures judiciaires closes, ils comprennent aussi les données relatives aux procédures judiciaires en cours, contrairement au fichier du casier judiciaire. En raison des délais de jugement et des voies de recours juridictionnelles, l'efficacité des enquêtes administratives serait fortement compromise si l'interrogation du STIC ne pouvait intervenir et une partie très significative des risques ne pourrait être prise en compte par les décisions administratives.*

*M. Y., 46 ans, s'est vu refuser un agrément préfectoral pour exercer la profession d'agent de sécurité privée, l'enquête administrative et la consultation du STIC ayant permis de révéler que cette personne avait été mise en cause dans différentes affaires d'ivresse publique manifeste et de violences.*

*M. S., 20 ans, souhaitait devenir transporteur de fond alors que l'enquête administrative a révélé des antécédents dans des affaires de stupéfiants, port illégal d'arme et vol simple.*

*L'agrément préfectoral d'agent de sécurité privée a également été refusé à M. D., 51 ans. Ce dernier était mis en cause dans des affaires de violences volontaires, vol à l'étalage, vol par ruse, recel et escroquerie.*

*L'enquête administrative et la consultation du STIC a permis au préfet de refuser à M. A., 36 ans, l'agrément qui lui était nécessaire pour diriger une société de gardiennage. M. A. était en effet mis en cause dans sept affaires judiciaires comprenant notamment la conduite malgré l'annulation du permis, menaces, harcèlement et vol.*

*M. C., 35 ans, était mis en cause dans treize affaires judiciaires comprenant notamment un vol de véhicule, vol avec arme blanche, vol avec arme, faux en écriture, usage de chèques volés. Au vu de ces éléments, sa demande d'agrément d'agent de sécurité lui a été refusée.*

---

Il reste que des problèmes se posent, en particulier pour la mise à jour des données, et que la mise en œuvre du droit d'accès à ces deux fichiers par l'intermédiaire de la CNIL fait apparaître un certain nombre de dysfonctionnements.

---

*Les chiffres et les tableaux qui figurent dans les pages suivantes, émanant de la CNIL, de la DGPN et de la DGGN, proviennent pour l'essentiel des contrôles faits à l'occasion de l'exercice par les citoyens de leur droit d'accès dit « indirect », car assuré pour leur compte par la CNIL (articles 41 et 42 de la loi du 6 janvier 1978 modifiée), mais la définition de certaines notions, la période retenue ou l'échelle de regroupement statistique peuvent être différentes selon les sources.*

---

---

# La saisine et l'alimentation

---

## Les difficultés techniques

### La qualité inégale de l'alimentation du STIC

Outre les dysfonctionnements liés à l'accès, la qualité inégale de l'alimentation du STIC est à relever dans certains cas, en raison :

- d'erreurs matérielles pures et simples (sur des millions de saisies annuelles) ;
- d'insuffisance du contrôle hiérarchique sur la bonne tenue des fichiers. Cela peut conduire par exemple à des retards de classement, d'où la nécessité de supprimer les doubles saisies pour gagner en fiabilité et en productivité ;
- d'aléa lié à l'expérience des agents qui renseignent le fichier (connaissance plus ou moins grande du droit pénal et de la procédure pénale, qualités de synthèse) ;
- d'insuffisances des contrôles hiérarchiques dans la stricte application de la charte CHEOPS : radiation systématiques des accès des personnels mutés ou partis en retraite, vérification des profils de consultations « *anormalement élevés* », contrôles aléatoires, etc.

### L'absence d'archives correspondant à la totalité de la durée d'inscription au STIC

À ce jour, la suppression des archives au-delà d'un certain délai est une des causes de la suppression des mentions dans le STIC. Elle découle généralement de la destruction des archives locales par les services de police confrontés à un manque de locaux disponibles pour la conservation des procédures papier, une fois qu'elles ne présentent plus d'utilité opérationnelle directe et à partir du moment où l'archivage des originaux est assuré par les greffes des tribunaux.

Dès lors que le service régional de documentation criminelle n'est pas en mesure de transmettre l'archive complète d'une procédure judiciaire requise dans le cadre du droit d'accès indirect et qu'elle ne peut être récupérée auprès des services d'enquête locaux, le gestionnaire du STIC procède à l'effacement des données à caractère personnel du requérant relatives à la procédure considérée. Les greffes des parquets ne sont pas sollicités pour retrouver une archive. On notera que ces effacements sont donc réalisés au « *bénéfice du doute* », l'hypothèse la plus favorable devant bénéficier au requérant, victime ou mis en cause.

	2003	2004	2005
Nbre dossiers traités	526	774	890
Nbre total rectifications	98	213	160
<i>dont absence d'archives</i>	25 (25 %)	86 (40 %)	67 (42 %)

Source : DGPN (DCPJ).

Note : Il convient de préciser que le nombre de dossiers traités comprend les personnes inconnues au fichier (245 sur 890 en 2005) et les personnes qui n'y figurent que comme victimes.

Ces dysfonctionnements sont très directement liés à des choix stratégiques passés, à savoir l'absence de conservation numérisée des procédures judiciaires.

Selon le ministère de l'Intérieur, lors de l'édiction du décret STIC en 2001, la CNIL, qui disposait alors d'un pouvoir d'avis conforme, a demandé la suppression pure et simple de la finalité de gestion des archives de procédures judiciaires du traitement, alors qu'elle aurait pu limiter la mise ne œuvre de cette finalité à la seule période de conservation légale des données. Au-delà, les règles applicables aux archives nationales s'appliquent (article 4-1 de la loi du 3 janvier 1979 modifiée par la loi du 12 avril 2000).

Pour la CNIL, cette interprétation est erronée, la Commission n'ayant en aucune façon remis en cause la nécessité de conserver les dossiers de procédure pendant les durées de conservation des données telles que fixées par le décret... Au-delà de cette durée de conservation, la Commission a surtout rappelé que l'archivage des dossiers relevait de la loi de 1979 sur les archives.

Ces problèmes d'archivage disparaîtront progressivement avec la mise en œuvre à l'horizon 2008 d'ANADOC (Application nationale d'archive de la documentation d'enquête de la police nationale) qui assurera l'archivage direct sans ressaisie des procédures judiciaires et administratives rédigées sous ARDOISE (Application de recueil de la documentation opérationnelle et des informations statistiques sur les enquêtes) et leur mise à disposition de tous les services. Naturellement, l'accès à ces informations devra faire l'objet d'une gestion des droits et d'une sécurisation appropriée, qui sera définie par un acte réglementaire préalablement soumis à l'avis de la CNIL.

## La durée de conservation du STIC

L'activation du programme d'épure automatique mis en œuvre au cours du mois d'octobre 2004 a abouti à la suppression de 1 241 742 « *fiches mis en cause* » et de 49 483 « *fiches victimes* ».

Depuis, la chaîne d'épure opère automatiquement au début de chaque mois la mise à jour pour toutes les données dont la durée de

conservation arrive à expiration dans le mois en cours. En 2005, près de 170 000 fiches ont ainsi été apurées.

	2003	2004	2005
<i>Dossiers traités</i>	526	774	890
Total rectifications	98	213	160
<i>dont délai conservation épuisé</i>	41	61	23*
En %	42 %	27 %	14 %

Source : DGPN (DCPJ).

(\*) dont 13 dans les fichiers manuels et 10 requalifications emportant une durée de conservation minorée.

Conséquent, le nombre de rectifications en raison du délai de conservation expiré a chuté depuis fin 2004. Il tient désormais pour l'essentiel à l'incidence de la requalification pénale des faits (délits requalifiés en faits contraventionnels de 5<sup>e</sup> classe) entraînant une correction dans la durée de conservation des informations criminelles (passage d'une durée de vingt ans à cinq ans).

Exemples : le taux d'incapacité totale de travail (ITT) à l'occasion de violences volontaires déterminera la durée de conservation fixée à :  
 – vingt ans si l'ITT est supérieure à huit jours ;  
 – cinq ans si l'ITT est inférieure ou égale à huit jours.

De même, en fonction du résultat des dommages causés par des dégradations volontaires sur des biens privés, la durée de conservation, qui par défaut est définie à vingt ans, tombera à cinq ans s'il n'en résulte qu'un dommage léger (depuis septembre 2006, la qualification pénale de « *dommages légers* » figure au lexique permettant l'alimentation du STIC).

## L'apurement des données dans JUDEX

Dans JUDEX, les services de la gendarmerie nationale ont mis en œuvre à partir de décembre 2006 un logiciel d'apurement automatique alors que cela a été fait à partir d'octobre 2004 pour le STIC. C'est ce qui explique pour une large part que ce fichier, même s'il donne lieu à des demandes de droit d'accès indirect beaucoup moins nombreuses que le STIC, contient lui aussi un nombre significatif de données inexactes ou incomplètes. Ainsi, au cours des dix séances d'investigations menées dans le cadre du droit d'accès indirect par la CNIL entre le 1<sup>er</sup> janvier et le 30 juin 2006, sur soixante et onze dossiers de personnes « *mises en cause* » dans JUDEX, vingt-huit fiches devaient être totalement ou partiellement effacées pour expiration des délais et vingt-quatre supprimées ou mises à jour en raison de suites judiciaires ayant une incidence (non-lieu, relaxe, etc.).

---

## **Les rectifications apportées d'initiative au fichier JUDEX**

*En plus des contrôles exécutés à la demande de la CNIL, deux types de contrôle sont effectués au STRJD concernant les informations relatives aux personnes.*

Ainsi, la base « personnes » du système JUDEX fait l'objet d'un contrôle quotidien sur tous les documents nouveaux entrés dans la base. Ce contrôle consiste en la détection automatisée :

- des doublons d'identité, ceux-ci pouvant évidemment générer des erreurs dans l'imputation des faits ;
- des mots inconnus du système, notamment sur les champs « signalement », « surnom », « profession », le caractère inconnu de ces mots étant souvent révélateur d'une erreur dans la saisie de l'information.

*De septembre 2005 à août 2006, 61 894 interventions ont été ainsi réalisées sur la base « personnes » au titre des doublons d'identité et 18 047, essentiellement dans la rubrique relative au signalement des individus, au titre des mots nouveaux. Ces 79 941 interventions ont abouti à 33 907 modifications des données enregistrées.*

*Par ailleurs, depuis 2005 a été entreprise une vaste opération de vérification des infractions correspondant à certains index dont l'appellation générique, modifiée depuis, a pu induire en erreur les enquêteurs lors de la saisie des données. Correctes sur le plan de l'imputation de l'affaire à la personne, ces fiches peuvent en revanche être erronées dans le champ permettant le calcul de la durée de conservation de l'information. Ces opérations de vérification, manuelles, seront terminées courant 2007 et auront porté sur plus d'un million de fiches.*

*Concernant le dépassement de la durée de conservation, pour la Direction générale de la gendarmerie nationale, cette situation est en cours de régularisation par des opérations de grande ampleur d'épure du fichier, opérations qui devraient être terminées au moment de l'entrée en fonction du système ARIANE. Au pire, si l'épure n'était pas terminée à la date de mise en service d'ARIANE, seule la partie épurée de JUDEX sera versée dans la nouvelle base. Du point de vue de l'effacement des données à échéance de leur durée de conservation, la situation sera donc totalement normalisée au moment du changement de système, fin 2007 ou début 2008.*

---

Bien consciente du caractère particulièrement sensible des données à caractère personnel qui sont traitées dans ses fichiers judiciaires, notamment au STRJD où sont regroupées toutes ces données, la gendarmerie nationale s'est engagée dans la mise en œuvre d'une démarche d'assurance qualité en matière de traitement de l'information judiciaire.

Le groupe « assurance qualité » créé au STRJD a ainsi reçu mission :

- d’auditer le processus de réception et de traitement des demandes et de détecter les éventuelles failles qui pourraient y exister en matière de contrôle de la légalité de celles-ci ;
- d’auditer de même les processus du contrôle d’opportunité des demandes.

À l’issue des audits, le processus d’assurance qualité sera mis en œuvre en trois phases :

- planification : élaboration participative de protocoles de fonctionnement et de protocoles de contrôle dont le collationnement permettra l’édition du « manuel qualité » du service ;
- mise en œuvre systématique des protocoles dans l’exécution du service quotidien ;
- contrôle du respect des protocoles et, au besoin, mise en œuvre de mesures correctives.

Assortie de l’élaboration d’indicateurs de contrôle et de performance et garante d’une totale transparence des modalités de fonctionnement du service, cette démarche d’assurance qualité permet de garantir le caractère parfaitement sécurisé et légaliste de l’action qui y est conduite. Sa conclusion logique sera l’éventuel engagement d’une procédure de certification sur la base de la norme ISO 27 001 (référentiel norme ISO 17799).

## **Les personnels habilités à consulter les fichiers de police judiciaire**

Les personnels habilités à consulter les fichiers sont définis dans l’article 21 de la loi 2003-239 du 18 mars 2003 sur la sécurité intérieure et dans les articles 5 et 6 du décret du 5 juillet 2001 modifié qui réglementent cette question. Il s’agit essentiellement des personnels des services de la police nationale et de la gendarmerie nationale et des agents des douanes spécialement habilités qui exercent des missions de police judiciaire ainsi que des magistrats du parquet et d’instruction.

Par ailleurs, certaines données figurant dans le fichier STIC peuvent être consultées dans le cadre de missions de police administrative ou de sécurité par des agents de la police et de la gendarmerie nationale individuellement désignés et spécialement habilités par le directeur de la police nationale ou le directeur de la gendarmerie nationale.

Les décrets STIC et JUDEX prévoient que « *la consultation peut également être effectuée par des personnels investis de missions de police administrative spécialement habilités par le préfet. Dans ce cas, l’accès à l’information est limité à la seule connaissance de l’enregistrement de l’identité de la personne concernée dans le traitement* ».

En raison du très grand nombre d’utilisateurs potentiels et de la sensibilité des fichiers concernés, la CNIL (délibération du 8 septembre 2005) souligne « *qu’il est impératif que des règles d’habilitation rigoureuses de ces personnels soient définies* ».

Par instruction du 9 mai 2006, le directeur général de la police nationale a rappelé à l'ensemble des services de police les règles relatives aux fichiers de police contenues dans la charte pour la sécurité du système d'information du ministère de l'Intérieur et dans le règlement de sécurité CHEOPS.

Déjà par télégramme du 24 mars 2004, précisé par une note du 15 avril 2005, le directeur de cabinet du ministre d'État, ministre de l'Intérieur et de l'Aménagement du territoire, a rappelé la rigueur devant entourer la conduite des enquêtes administratives et l'instruction des dossiers d'agrément pour l'accès aux métiers de la sécurité privée. Il a notamment renouvelé les instructions concernant la célérité relative au traitement des déclarations et des demandes et le fait qu'une simple mention sur un fichier de police ne saurait conduire à émettre un avis défavorable. Il précise « *qu'il importe d'examiner la situation de chaque intéressé à partir des éléments relevés par le casier judiciaire et le fichier de police, eux-mêmes appréciés par rapport aux fonctions devant être exercées et en tenant compte de leur gravité, de leur ancienneté, des suites judiciaires qui, le cas échéant, leur ont été données et leur éventuelle répétition* ». Il insiste également sur la nécessité de « *motiver les décisions qui doivent comporter des considérations de droit et de fait* ».

## La question des mises à jour

### Données générales

S'agissant des « *mis en cause* » (auteurs), il doit être relevé que si, en 2003, 93 fiches ont été mises à jour ou supprimées suite à l'intervention de la CNIL (soit 43 % des personnes mises en cause dont la fiche a été vérifiée) ce chiffre est tombé à 32 % en 2004 (66 fiches sur 208), du fait notamment de la mise en place en octobre 2004 du logiciel d'apurement du STIC.

### Nombre de saisines relatives au STIC clôturées au 1<sup>er</sup> septembre 2006

Année d'origine de la saisine	2003	2004	2005 <sup>1</sup>	Total
Pas de fiche	189	127	129	445
Fiche victime uniquement	149	98	93	340
Fiche victime et fiche auteur sans modification	58	74	11	143
Fiche auteur uniquement sans modification	63	68	6	137
Suppression totale ou mise à jour fiche auteur	93	66	40	199
Total fiche auteur	214	208	57	479
% de suppression ou MAJ/total fiche auteur	43 %	32 %		
Total	552	433	279	1 264

(1) Compte tenu du nombre limité de saisines clôturées en 2005, aucune interprétation ne peut être donnée quant au nombre de fiches supprimées ou mises à jour.

Ce chiffre relativement bas s'explique par deux raisons :

- au 1<sup>er</sup> août 2005, un relevé de conclusion signé par les Ministères de l'Intérieur, de la Défense et de la Justice a été mis en place. La PJ devait donc saisir les procureurs avant les premières investigations pour toutes les saisines arrivées après le 1<sup>er</sup> août 2005 ;
- les fiches STIC examinées avant le 1<sup>er</sup> août 2005 ou dont la date de saisine de la CNIL était antérieure au 1<sup>er</sup> août 2005 ne peuvent être clôturées tant que la CNIL n'aura pas recueilli l'accord de communication.

Source : CNIL.

Le tableau ci-après présente les motifs pour lesquels des suppressions ou des mises à jour ont été effectuées dans le cadre de l'exercice du droit d'accès, que ce soit à la demande expresse de la CNIL ou à l'initiative du gestionnaire du fichier lors du travail préparatoire à l'examen du dossier par le commissaire désigné par la CNIL. En 2003 et 2004, les motifs de ces mises à jour ou effacements tenaient en premier lieu à l'absence de mise à jour ou d'effacement en raison de suites judiciaires favorables et en second lieu au non-respect des durées de conservation fixées par le décret du 5 juillet 2001.

### Motifs de la suppression ou de la mise à jour

Année d'arrivée de la saisine à la CNIL	Nombre d'affaires		
	2003	2004	2005
<b>Les mises à jour</b>			
Mise à jour pour non-lieu	4	3	1
Mise à jour pour classement sans suite pour insuffisance de charges	19	13	5
Requalification de l'infraction		6	
<b>Les suppressions</b>			
Infraction non constituée	5		2
Enregistré à tort comme mis en cause	22	19	13
Expiration de la durée de conservation	46	35	17
Relaxe-acquittement	5	6	2
Absence d'archive du dossier de procédure	3	5	2
Erreur d'enregistrement	2	3	3
Divers		1	0
<b>Nombre d'affaires <sup>1</sup></b>	106	91	45
<b>Nombre de requérants</b>	93	66	40

(1) Étant entendu qu'un individu peut être signalé dans le STIC pour plusieurs affaires.

Source : CNIL.

Il s'avère donc que des décisions administratives ont pu être prises à l'encontre des intéressés sur la base de renseignements inexacts.

Ces statistiques mettent tout d'abord en lumière les dysfonctionnements liés à l'absence d'une procédure de transmission régulière par les parquets des suites judiciaires favorables au gestionnaire du STIC, pourtant prévue et demandée par la CNIL et le Médiateur de la République à plusieurs reprises.

S'agissant du respect des durées de conservation dans le fichier STIC, il doit être relevé que le logiciel, mis en place en 2004, a permis d'éliminer plus de 1,2 million de fiches du STIC au moyen d'un épurement automatique. Désormais, les données dont la durée de conservation arrive à expiration dans le mois en cours sont effacées. Le ministère de l'Intérieur considère que l'automatisme de l'épurement des informations apporte une garantie nouvelle et significative d'amélioration du fonctionnement du STIC. La CNIL indique que cette cause de signalement injustifié devrait disparaître.

S'agissant des autres motifs (problème de requalification de l'infraction, infraction non constituée, enregistrement à tort comme mis en cause, absence d'archive) elles semblent relever à la fois d'erreurs de saisie à la source et du contrôle insuffisant des parquets sur le contenu des fiches STIC. Sur ce dernier point, le fait que les parquets ne disposent pas de terminaux d'accès au STIC leur permettant en temps réel de vérifier le contenu des fiches STIC, de procéder notamment à la requalification des faits, constitue assurément un obstacle à l'exercice effectif de leur contrôle.

Les résultats des investigations conduites en 2006 par la CNIL dans le cadre du droit d'accès indirect montrent que, pour le premier semestre 2006, sur près de 300 dossiers vérifiés lors d'une première investigation, 21 % avaient fait l'objet d'une mise à jour ou d'une suppression pour erreurs d'enregistrement ou requalification (à la lecture du dossier de procédures en possession de la PJ), plus d'une centaine devant faire l'objet d'une vérification complémentaire au vu des suites judiciaires demandées aux parquets compétents, ce qui entraînera d'autres suppressions ou mises à jour (un cas sur trois au premier semestre 2006).

<b>Analyse des investigations relatives au fichier STIC pour les personnes mises en cause (du 1<sup>er</sup> janvier 2006 au 30 juin 2006)</b>				
	Fiche sans modification	Suppression ou mise à jour	Demande de suites judiciaires	Total
1 <sup>ère</sup> investigation	111	57	104	272
%	41 %	21 %	38 %	100 %
2 <sup>ème</sup> investigation	41	19	-----	60
%	68 %	32 %	-----	100 %

Source : CNIL.

### L'absence de transmission régulière par les parquets des suites judiciaires

L'article 21-III de la loi 2003-239 du 18 mars 2003 relative aux fichiers STIC et JUDEX et les articles 3 des décrets n° 2001-583 du 5 juillet 2001 modifié portant création du STIC et n° 2006-1411 portant création du JUDEX prévoient que la mise à jour des fichiers au regard des suites judiciaires relève de la compétence du procureur de la République territorialement compétent qui doit transmettre au gestionnaire du fichier certaines décisions de justice n'ayant pas abouti à des poursuites ou à des condamnations.

Le ministère de la Justice rappelle que l'article 21-III de la loi du 18 mars 2003 relative à la sécurité intérieure précise les suites judiciaires donnant lieu à la mise à jour des données à caractère personnel inscrites dans les fichiers de police judiciaire dits d'antécédents. Il s'agit, d'une part, des décisions de relaxe et d'acquiescement devenues définitives qui doivent donner lieu à l'effacement des données enregistrées, sauf si le procureur en ordonne le maintien pour des raisons liées aux finalités du fichier (exemple : cas de relaxe motivée sur le fondement de l'article 122-1 du Code pénal). Il s'agit d'autre part des décisions de classement sans suite

pour insuffisances de charges et de non-lieu qui doivent compléter les données inscrites dans les fichiers par l'apposition d'une mention sauf si le procureur de la République en prescrit l'effacement. Le champ des suites judiciaires donnant lieu à la mise à jour ou à l'effacement des données enregistrées est bien moins large que celui des décisions prises par les procureurs de la République qui n'aboutissent pas à la mise en œuvre de l'action publique ou à des condamnations.

Les outils statistiques du ministère de la Justice ne lui permettent pas d'indiquer le nombre de suites judiciaires transmises au gestionnaire du fichier STIC. Pour ce qui concerne le fichier JUDEX, il ne peut qu'être réaffirmé que des instructions seront données aux magistrats des parquets afin d'en assurer la mise à jour dès lors que le décret qui en porte la création aura été publié.

Pour information, au cours de l'année 2005 <sup>2</sup> :

- 24 867 relaxes ont été prononcées dont 21 368 par les tribunaux correctionnels et 3 499 par les chambres des appels correctionnels. Il est toutefois nécessaire de préciser qu'une relaxe confirmée par une cour d'appel est comptabilisée deux fois puisque sa comptabilisation au niveau des juridictions de première instance intervient avant son caractère définitif ;
- 295 acquittements concernant des accusés majeurs et 29 concernant des accusés mineurs ont été prononcés ;
- 129 623 classements sans suite pour absence d'infractions et 221 723 classements sans suite pour infraction insuffisamment caractérisée ont été pris ;
- 3 940 ordonnances de non-lieux ont été prises.

En pratique, la transmission de ces informations ne s'opère pas de façon immédiate et systématique.

Il semble que certains parquets aient des difficultés à mettre en œuvre cette procédure de manière optimale.

À l'occasion de l'examen des projets de décrets STIC et JUDEX pris en application de l'article 21 de la loi du 18 mars 2003 précitée, la CNIL, dans sa délibération du 8 septembre 2005, « s'étonne [...] que le projet de décret ne comporte aucune précision quant aux diligences qui incombent dès lors aux procureurs ; elle estime en conséquence que doivent figurer dans le projet de décret, les modalités de transmission des informations nécessaires à la mise à jour et à l'effacement des données ».

Afin de pallier partiellement ce défaut de transmission, dans sa délibération, la CNIL, « tout en prenant acte que le projet de décret prévoit que la consultation du fichier à des fins administratives ne peut porter ni sur les données relatives aux victimes ni sur les données concernant des personnes mises en cause ayant fait l'objet d'une mise à jour ordonnée par le procureur de la République, [...] estime toutefois que des dispositions

(2) Ces chiffres confondent les procédures police et gendarmerie et il n'est pas possible de distinguer le nombre de décisions qui auraient eu plus particulièrement vocation à alimenter les fichiers de l'une ou l'autre institution.

*doivent être prévues afin que le résultat de la consultation ne puisse être communiqué à l'autorité compétente qu'après que le responsable du fichier s'est assuré auprès du procureur de la République compétent qu'aucune décision judiciaire n'est intervenue qui appellerait la mise à jour de la fiche de l'intéressé ou encore qu'aucune requalification judiciaire n'est intervenue qui justifierait la rectification des informations figurant sur cette fiche ».*

Cette proposition de la CNIL n'a cependant pas été retenue par le Gouvernement pour deux raisons :

- elle conduirait, tout d'abord, à faire intervenir une autorité judiciaire, le procureur de la République, dans le cours d'une enquête administrative et lui conférer un pouvoir d'intervention ;
- elle aboutirait, de surcroît, au prolongement des délais de réponse aux intéressés, voire même de blocage de la procédure administrative en cas de silence du procureur de la République, alors qu'il existe déjà des critiques sur ce point.

Cependant, la CNIL a pu relever, à l'occasion d'une visite effectuée très récemment dans une préfecture de la région parisienne, que les services préfectoraux appelés à réaliser les enquêtes administratives requises dans le cadre des procédures d'agrément aux emplois de sécurité étaient particulièrement soucieux de s'assurer de la fiabilité des informations contenues dans le STIC et vérifiaient les informations fournies dans le cadre de la consultation du STIC en consultant notamment les parquets sur les suites judiciaires données aux faits relatés dans la fiche STIC.

Selon le ministère de la Défense, la proposition de la CNIL n'apparaît pas réalisable car elle serait trop lourde à mettre en œuvre. En effet, pour chaque demande de consultation le gestionnaire du fichier serait contraint de saisir les différents parquets concernés.

Le ministère de l'Intérieur précise qu'une telle procédure, par sa durée et sa longueur, causerait de graves difficultés au secteur économique de la sécurité privée, qui doit faire face à des besoins de mains d'œuvre rapidement variables.

S'agissant du contrôle des parquets sur le contenu des fiches STIC, le fait que ceux-ci ne disposent pas de terminaux d'accès au STIC leur permettant en temps réel de vérifier le contenu des fiches STIC, de procéder notamment à la requalification des faits, constitue assurément un obstacle à l'exercice effectif de leur contrôle. Pourtant, pour assurer l'efficacité du contrôle et de la mise à jour des données par les magistrats du parquet, le ministère de la Justice avait prévu par circulaire en date du 6 juillet 2001 (*Bulletin officiel du ministère de la Justice* n° 83 du 1<sup>er</sup> juillet-30 septembre 2001) la mise en place progressive au sein de chaque tribunal de grande instance de postes de travail informatiques permettant d'accéder directement au fichier STIC.

Si l'accès aux fichiers, par l'implantation de terminaux de consultation dans les juridictions, peut être utile au contrôle exercé par le procureur de la République sur les données enregistrées, il n'en reste pas moins que l'autorité judiciaire ne pourra être mise en mesure de faire face

à ses obligations dès lors qu'elle aura à disposition un outil lui permettant d'assurer une transmission automatisée des suites judiciaires concernées aux gestionnaires des fichiers.

Le système CASSIOPEE, qui devrait être déployé dans les juridictions (sauf région parisienne et l'ensemble des cours d'appel) entre 2007 et fin 2008, autorisera une telle transmission dans l'application ARIANE.

Lorsque la transmission des suites judiciaires intervient, la mise à jour du STIC est traitée prioritairement par les services régionaux de documentation criminelle.

### État des mises à jour dans le STIC réalisées à partir des suites judiciaires transmises par les parquets

Suites judiciaires	2003	2004 (+ 10 %)	2005 (+ 1,7 %)
Classement sans suite	8 216	8 771	8 293
Non-lieu	479	753	1 097
Relaxe ou acquittement.	687	839	1 148
<b>Total</b>	<b>9 382</b>	<b>10 363</b>	<b>10 538</b>

Source : DGPN (DCPJ).

Selon la CNIL, il serait nécessaire de comparer ces chiffres avec le nombre total de classements sans suite, non-lieu, relaxes ou acquittements (à titre d'exemple, 3 850 non-lieux ont été prononcés en 2004).

### Les questions de requalification judiciaire

Des rectifications dans le STIC peuvent également avoir pour origine des enregistrements infondés ou devenus sans fondement à la suite d'une requalification judiciaire des faits. Ils recouvrent un ensemble d'anomalies telles que :

- l'inscription non autorisée par le décret (délits requalifiés en faits contraventionnels comme les violences volontaires sans ITT) ;
- l'inscription d'une personne physique en lieu et place d'une personne morale : il s'agit pour l'ensemble de ces dossiers de personnes connues en qualité de victime ;
- l'inscription d'une personne physique qui ne répond pas à la définition du mis en cause.

	2003	2004	2005
Nbre dossiers traités	526	774	890
Nbre total rectifications	98	213	160
dont enregistrements infondés	32 (33 %)	40 (20 %)	32 (20 %)

Source : DGPN (DCPJ).

Outre les inscriptions devenues sans fondement en raison d'une requalification « à la baisse » des faits ou d'une mesure de classement en raison de l'insuffisance de charges ou du caractère insuffisamment caractérisé de l'infraction, une part de ces anomalies trouve son origine dans une insuffisance de la qualité de rédaction des comptes rendus d'enquête après identification (CREi.), indispensables à l'alimentation et à la gestion du STIC, et qui peuvent parfois présenter des inexactitudes et/ou imprécisions au regard des mentions portées dans la procédure qu'ils accompagnent.

Il appartient à l'opérateur de saisie chargé de l'enrichissement du STIC et au procureur de la République (rendu destinataire du CREi, en même temps que de la procédure), dans son pouvoir de contrôle du fichier, de vérifier les informations inscrites sur le CREi. L'exactitude des mentions est toutefois rarement vérifiée à ce stade.

La mise en œuvre coordonnée des applications ANADOC et ARDOISE permettra de corriger également cette catégorie de dysfonctionnements <sup>3</sup>.

Dans le cadre de l'instruction des demandes de droit d'accès indirect, la CNIL a eu connaissance de plusieurs cas de personnes licenciées (alors qu'elles étaient employées depuis de nombreuses années dans la société de sécurité) ou refusées à l'embauche en raison d'un signalement dans le STIC pour des infractions qui, après lecture de la procédure, ne relevaient pas, de son point de vue ni d'ailleurs de l'avis du parquet compétent, des cas justifiant que la personne ne soit pas recrutée ou soit licenciée. Par exemple, des cas de signalement pour violences conjugales (dont il s'avérait à la lecture de la procédure qu'il s'agissait d'un différend réglé par la voie d'un classement sans suite) ou pour des infractions telles que des atteintes à la dignité de la personne (qui relevaient plutôt d'un problème relationnel entre un professeur et son élève).

---

**Exemple 1 :** *en mars 2004, un élève ingénieur s'est vu refuser un stage dans la centrale nucléaire de Chooz sur la base d'informations portées sur un fichier émanant d'un service de gendarmerie et se rapportant à une procédure antérieure « pour coups et blessures volontaires ». Ce jeune homme, en septembre 2002, au cours d'une partie de chasse avec un ami, avait été interpellé par un gendarme qui avait reproché aux deux hommes d'avoir blessé une personne qui se trouvait dans son jardin. Le dossier, qui se rapportait à des « coups et blessures involontaires » transmis au procureur de la République compétent, avait été clos bien avant mars 2004 par un simple rappel à la loi. D'une part, cette fiche portait une erreur de qualification du délit involontaire et non pas volontaire et, d'autre part, « l'inscription aurait été supprimée sur l'initiative du commandant local ».*

(3) Cf. aussi chapitre 3 : *Les propositions et recommandations.*

**Exemple 2 :** suite à une saisine, la CNDS a estimé que la relaxe d'un professeur de lettres poursuivi pour outrage et diffamation, relaxe prononcée par le tribunal en ce qui concerne l'outrage et par la cour sur les deux chefs d'inculpation, devrait entraîner la suppression dans les fichiers des données concernant ce professeur.

**Exemple 3 :** M<sup>me</sup> K., agent de sécurité, âgée de 24 ans, n'a pu être embauchée dans une société de sécurité et de gardiennage en septembre 2004. Elle était signalée dans le STIC pour une infraction à la législation relative aux animaux dangereux (elle promenait son chien dans la rue, non muselé et non tenu en laisse). Ce signalement a été supprimé car il y avait eu une erreur d'enregistrement, cette infraction relevant d'une contravention de 2<sup>e</sup> classe.

**Exemple 4 :** un requérant occupait un emploi en CDI dans une société de gardiennage, mais la PAF de l'aéroport a refusé son agrément. Il a saisi la CNIL le 28 février 2005 d'une demande d'effacement de sa fiche de police judiciaire.

Lors des investigations menées par le magistrat de la CNIL, le 18 juillet 2006, il a été constaté que M. X était signalé dans le STIC comme mis en cause dans une affaire de menaces d'atteinte à personnes sous condition ; l'affaire a été classée sans suite pour infraction insuffisamment caractérisée. Le parquet ayant demandé l'effacement de la fiche, le 21 juillet 2006, les services de police judiciaire, seize mois après la saisine de la CNIL, ont confirmé la suppression à la CNIL.

---

---

## **Le respect de la finalité des fichiers selon les textes en vigueur**

### **La finalité des fichiers de police judiciaire**

Dans un dossier relatif à une infraction au Code de la route suivi d'une poursuite pour outrage et rébellion à l'encontre de deux époux, la CNDS avait dénoncé la remise d'un rapport administratif sur cette affaire, où le commandant avait écrit en caractères gras pour attirer l'attention qu'un témoin, dont la déclaration n'était pas conforme à celle des policiers, « a fait l'objet d'une procédure pour travail clandestin par les services de la SPAF de Toulouse le 1<sup>er</sup> janvier 1999 ».

Le 27 juin 2006, dans ses observations sur l'avis rendu par la Commission, le ministère de l'Intérieur a précisé que « la référence à la procédure judiciaire mettant en cause un témoin se trouve dans le texte

*d'un rapport de synthèse établi à l'issue d'une enquête interne, à la demande du directeur départemental de la sécurité publique saisi des récriminations des époux O ».*

Le ministre de l'Intérieur admet que « *cette référence ne s'inscrit pas strictement dans le cadre des dispositions du décret 2001-583 du 5 juillet 2001 portant création du Système de traitement des infractions constatées (STIC) et de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne* ».

Il a été indiqué à la Commission qu'un rappel adressé aux personnels concernés viserait « *le cadre législatif et réglementaire portant sur l'utilisation en police judiciaire et en police administrative des données du STIC* ».

## **L'utilisation malveillante**

Certains fonctionnaires peuvent parfois utiliser les informations des fichiers de police à des fins personnelles et non prévues par les textes. Il appartient alors aux services d'inspection de sanctionner ces dérives.

Selon l'Inspection générale de la police nationale, l'examen des dossiers disciplinaires des dernières années montre différentes motivations individuelles dans les manquements à l'obligation de discrétion professionnelle :

- la curiosité « malsaine » mais sans toujours d'intention malveillante (exemple : savoir si telle ou telle personnalité, tel ou tel voisin, est connu des services de police) ;
- la recherche d'informations pour régler des litiges personnels (vérification de la plaque minéralogique d'un véhicule trop fréquemment stationné devant son domicile, pression sur un voisin avec lequel on est en conflit, rechercher l'adresse de son ex-femme, etc.) ;
- la divulgation d'informations pour obtenir un avantage ou une contrepartie, monétaire ou non (corruption pure et simple, ancien policier usant de son réseau relationnel et reconverti à la retraite dans une « officine », grande entreprise souhaitant (irrégulièrement) vérifier la moralité d'un candidat à un poste sensible avant de le recruter et par ailleurs en contacts réguliers avec les services de police).

Les seuls dysfonctionnements, très marginaux, constatés en matière d'accès à l'information judiciaire de la gendarmerie relèvent de la défaillance humaine, la traçabilité et la sécurité des fichiers n'ayant jamais été mise en cause. Ils sont numériquement très marginaux rapportés au nombre de consultations et de personnels.

	2005	2006
Faits ayant donné lieu à enquête ou information judiciaire*	4	9
Nombre de personnels concernés	4	12
* Atteinte à l'intégrité des fichiers, violation de secret, corruption		

Source : DGGN.

## Les fichiers de police comme unique élément des enquêtes administratives

L'article 10 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifié par la loi du 6 août 2004, énonce « qu'aucune [...] décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité ».

La consultation des fichiers à l'occasion d'une enquête administrative est toujours facultative et ne lie pas l'autorité administrative. Elle n'épuise ni ne résume l'enquête administrative. Celle-ci doit donc prendre en compte l'interrogation des fichiers, vérifier les informations qui y sont portées et toujours exercer un jugement de mise en relation entre les informations recueillies et l'objet de l'enquête administrative. En outre, enquête administrative et décision administrative ne doivent pas se confondre.

L'autorité administrative doit apprécier *in concreto* si la nature des mentions portées par ces fichiers peut légalement fonder sa décision. Ainsi, en ce qui concerne l'agrément des agents de sécurité, il ressort de la jurisprudence que l'autorité administrative se doit d'apprécier avec précision la compatibilité avec les fonctions, au regard des mentions factuelles présentes dans le STIC et, éventuellement, selon les motifs de la condamnation pénale avec les fonctions d'agents de sécurité (TA Versailles 3 juin 2005, Frédéric H n° 0500761).

Les faits pouvant être pris en compte dans le cas d'un refus d'agrément ou d'habilitation sont définis de manière large : « *comportements* » et « *agissements* ». Avant la loi antiterroriste, les dispositions propres à la sécurité privée indiquaient que seuls les « *actes* » contraires à l'honneur, à la probité, aux bonnes mœurs ou de nature à porter atteinte à l'ordre public ou à la sécurité des personnes pouvaient être pris en compte. Or, ce terme conduisait la jurisprudence à adopter une interprétation restrictive, exigeant que des infractions aient été préalablement commises. Or, ceci est apparu totalement inadapté à la problématique de la menace terroriste contemporaine, avec des individus pratiquant un islamisme radical avec des trajectoires de passage à l'acte terroriste rapide sans nécessairement de passé délinquant. Le terme « *comportement* » a donc été substitué au terme « *acte* ». Même s'il s'agit d'un raccourci excessivement simplificateur, on peut considérer que le terme « *acte* » se rapporte plutôt aux infractions enregistrées dans le STIC, alors que le terme de « *comportement* » est plus englobant et permet d'inclure les informations contenues dans la documentation des services de renseignement.

Or, la CNIL a pu constater (rapport d'activité 2004) que souvent les enquêtes administratives se limitent, sans véritable appréciation, à la seule consultation des fichiers de police judiciaire.

Cette consultation constitue dans certains cas l'élément essentiel et probant de l'enquête conditionnant la décision d'embauche ou d'agrément (CAA de Versailles du 2 novembre 2004 n° 02VE01956 : annulation d'une décision préfectorale de refus d'agrément en vue de

l'acquisition d'une arme de 4<sup>e</sup> catégorie fondée uniquement sur des mentions figurant au STIC et qui se sont par ailleurs révélées erronées).

Une partie des difficultés rencontrées découle du fait que le service instructeur n'exerce pas toujours correctement le contrôle d'opportunité. Ce rôle instructeur doit s'exercer à deux niveaux :

- à celui du service de police ou de l'unité de gendarmerie, lorsqu'il réalise l'enquête administrative. Il doit jouer pleinement son rôle de conseiller technique de l'autorité préfectorale pour la sécurité ;
- à celui du service de la réglementation de la préfecture, lorsqu'il instruit la décision administrative.

Ainsi, indépendamment de la qualité de la mise à jour et de la précision des fichiers de police, l'instruction du dossier requiert l'exercice du jugement, car la compétence préfectorale n'est jamais liée.

De même, en vue de respecter la stricte proportionnalité entre le respect des libertés individuelles et « *la protection de la sécurité des personnes et la défense des intérêts fondamentaux de la nation* », des instructions précises encadrant l'action des services instructeurs ont été prises : télégramme NOR/INT/D/04/00035/C du 24 mars 2004 et circulaire DLPAJ NOR/INT/D/05/00047/C du 15 avril 2005.

Encore convient-il de s'assurer qu'une procédure de retour « *correctif* » existe à partir de l'analyse des cas individuels « *défaillants* », c'est-à-dire ceux qui ont donné lieu à un recours suivi d'une rectification de la position de l'administration. Et que ce recours soit administratif (hiérarchique auprès du ministre, auprès du Médiateur, auprès de la CNIL dans le cadre du droit d'accès indirect aux fichiers) ou contentieux.

Il convient donc de consolider la performance des services instructeurs en attirant l'attention des préfets, DDSP et commandants de groupement sur ces cas dans le cadre d'un retour « *pédagogique* ». Or, aujourd'hui, les circuits administratifs inévitablement complexes ne permettent qu'imparfaitement l'harmonisation de la position de tous les services instructeurs : les dossiers analysés par le Médiateur sont directement adressés aux préfets ; les recours hiérarchiques sont instruits par la DLPAJ ; les « *recours indirects* » que constituent les demandes de droit d'accès sont instruits par la CNIL avec le soutien de la DGPN.

---

**Exemple 1 :** *une requérante s'est vu refuser son renouvellement d'habilitation à l'aéroport de Beauvais-Tillé. Elle a donc saisi la CNIL le 8 avril 2004 d'une demande de droit d'accès indirect aux fichiers de police judiciaire. À l'issue de ses investigations opérées en février 2005, la CNIL a demandé le 1<sup>er</sup> mars 2005 au procureur la suite judiciaire de l'affaire de vol en réunion datant de 2000, affaire pour laquelle elle était signalée dans le STIC. Sept mois après, le TGI a informé la CNIL que l'affaire avait fait l'objet d'un classement sans suite le 11 septembre au motif que le préjudice était peu important.*

*Cette rubrique ne rentre pas dans le cas des suppressions prévues dans le décret STIC ce qui fait que cette information sera maintenue dans le STIC pendant vingt ans.*

**Exemple 2 :** *un requérant employé à la RATP au sein du service interne de sécurité GPSR s'est vu refuser le renouvellement de son agrément parce qu'il était connu dans le STIC pour une affaire de violence volontaire entraînant une ITT de plus de huit jours ; le procureur de la République du TGI de Bobigny a informé la CNIL que cette affaire avait fait l'objet d'un classement sans suite résultant d'un désistement du plaignant. Cette mention sera maintenue quarante ans dans le STIC.*

**Exemple 3 :** *un requérant travaillant depuis plus de quatorze ans dans le domaine de la sécurité-incendie, a été licencié suite à un transfert de société par le directeur de la nouvelle société. En effet, il était signalé dans le STIC dans une affaire de violences volontaires par conjoint datant de 1999. Il avait bénéficié d'un classement sans suite par désistement de la plaignante, ce qui n'est pas un cas de suppression. Cette mention sera maintenue pendant vingt ans dans le fichier de police judiciaire.*

---

## **La consultation du fichier pour des contraventions de 5<sup>e</sup> classe**

Une consultation systématique à des fins administratives des fichiers de police judiciaire s'agissant des personnes mises en cause pour des faits relevant de certaines contraventions de 5<sup>e</sup> classe, qui à l'évidence ne mettent pas en cause « *la protection de la sécurité des personnes ou la défense des intérêts fondamentaux de la nation* », conditions exigées par le législateur pour justifier la consultation administrative de ces fichiers, est-elle opportune ?

Toutefois, toutes les contraventions de 5<sup>e</sup> classe ne pourraient être exclues du champ d'interrogation. En effet, les violences légères ou les dégradations volontaires légères sont alternativement contraventionnelles ou délictuelles en fonction du préjudice subi. Or, il pourrait apparaître nécessaire, au regard de l'esprit qui a prévalu à la mise en place de ce système de contrôle, de pouvoir disposer de telles informations eu égard à la nature des infractions commises même contraventionnelles.

Dans le cadre de l'instruction des demandes de droit d'accès indirect, la CNIL a eu connaissance de plusieurs cas de personnes licenciées (alors qu'elles étaient employées depuis de nombreuses années dans la société de sécurité) ou refusées à l'embauche en raison d'un signalement dans le STIC pour des infractions qui, après lecture de la procédure, ne relevaient pas de son point de vue ni d'ailleurs de l'avis du parquet compétent postérieurement saisi des faits de cas justifiant que la personne ne soit pas recrutée ou soit licenciée. Par exemple des cas de signalement pour

violences conjugales (dont il s'avérait à la lecture de la procédure qu'il s'agissait d'un différend réglé par la voie d'un classement sans suite) ou pour des infractions telles que des atteintes à la dignité de la personne (qui relevaient plutôt d'un problème relationnel entre un professeur et son élève).

À cet égard, la situation risque de s'aggraver, d'une part, avec l'élargissement considérable de la liste des enquêtes donnant lieu à consultation des fichiers de police judiciaire que consacre le décret du 6 septembre 2005 et, d'autre part, avec l'extension possible du champ d'application du fichier STIC à l'ensemble des contraventions de 5<sup>e</sup> classe contre les biens, contre les personnes et contre la nation, l'État ou la paix publique.

À l'égal des mesures techniques prises pour exclure la consultation des fiches concernant les victimes des dispositions du même ordre pourraient être adoptées pour restreindre la consultation administrative des signalements concernant des personnes mises en cause dans des affaires relevant de certaines contraventions de 5<sup>e</sup> classe, voire de certains délits.

Il serait également souhaitable de s'interroger sur l'opportunité ou non d'élargir la liste des cas de classements sans suite ou de sanction judiciaire « modérée » (rappel à la loi, alternative aux poursuites, composition pénale) justifiant une mise à jour du STIC par complément d'information. 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.

---

*Pour le ministère de l'Intérieur, il convient de rappeler que le préfet apprécie la compatibilité des éléments ressortant de l'enquête avec ces dispositions notamment selon les instructions générales contenues dans la circulaire du 24 mars 2004 : « L'incompatibilité s'apprécie au regard de la gravité des faits commis, de leur éventuelle répétition, de leur ancienneté ainsi que de leur nature et des rapports entre celle-ci et l'activité envisagée », réitérées par la circulaire du 15 avril 2005 : « Une simple mention au casier judiciaire ou sur un fichier de police ne saurait vous conduire à émettre un avis défavorable. Il importe en effet d'examiner la situation de chaque intéressé à partir des éléments relevés par le casier judiciaire et le fichier de police, eux-mêmes appréciés par rapport aux fonctions devant être exercées et en tenant compte de leur gravité, de leur ancienneté, des suites judiciaires qui, le cas échéant, leur ont été données et de leur éventuelle répétition. » Le refus d'agrément par un préfet ne saurait reposer sur le seul critère d'une inscription dans le STIC au titre des contraventions de 5<sup>e</sup> classe ou d'une catégorie de délits. Dès lors, leur exclusion a priori du champ de l'enquête administrative ne se justifie pas.*

---

---

# **Le droit d'accès aux fichiers et les recours administratifs ou contentieux contre les décisions préfectorales <sup>4</sup>**

Les statistiques produites par la CNIL ne portent que sur des dossiers vérifiés par la Commission dans le cadre de l'instruction des demandes de droit d'accès indirect qui lui sont présentées, conformément à l'article 41 de la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004. En effet, toute personne souhaitant exercer son droit d'accès à ce fichier doit s'adresser à la CNIL qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation ou à la Cour des comptes, pour mener pour le compte du requérant les investigations.

En cas d'accord du ministère de l'Intérieur et du procureur de la République territorialement compétent, l'intéressé reçoit la fiche récapitulative des informations enregistrées dans le STIC. Une présentation de la procédure d'instruction des demandes de droit d'accès indirect au STIC figure en annexe 1. Cette procédure est complexe et donc souvent longue, d'autant plus que le requérant a fait l'objet de multiples inscriptions dans des ressorts juridictionnels différents. Elle nécessite l'intervention, outre de la CNIL, d'autant de services de police et d'autant de parquets qu'il y a d'inscriptions relatives à des affaires commises dans des ressorts différents <sup>5</sup>.

Parce que les requérants ne motivent pas toujours leur demande, ce qui n'est d'ailleurs pas une obligation, il est difficile de donner des chiffres précis sur le nombre de saisines motivées par un refus d'embauche, d'agrément ou un licenciement ou pour d'autres raisons. Mais les demandes de droit d'accès résultent en majorité de telles situations et ce, essentiellement dans le domaine de la sécurité et du gardiennage.

Les lettres de notification des décisions préfectorales indiquent les voies de recours, administratives ou contentieuses.

Les personnes qui se voient opposer une décision négative, qui parfois travaillent déjà depuis plusieurs années dans le secteur de la

(4) Cf. aussi annexe 1 : *Les modalités d'exercice du droit d'accès indirect au STIC.*

(5) *En 2005, les commissaires en charge du droit d'accès indirect ont procédé à 98 missions de vérifications et à 27 missions au premier semestre 2006.*

sécurité privée, saisissent fréquemment la CNIL. Elles espèrent ainsi soit obtenir rapidement la suppression de leur fiche STIC, lorsqu'elles savent qu'elles sont signalées, et ainsi intégrer ou réintégrer rapidement leur emploi, soit, à tout le moins, obtenir la garantie qu'elles pourront tenter de trouver un emploi dans le domaine de la sécurité sans s'exposer à nouveau à un refus préfectoral.

Une des difficultés est que le public distingue souvent mal l'exercice des droits d'accès aux fichiers de police prévus par les articles 41 et 42 de la loi informatique et libertés, de l'exercice d'un recours contre la décision préfectorale négative, le premier n'étant d'ailleurs pas exclusif du second.

Ainsi, il est fréquent que des personnes sollicitent l'effacement des données les concernant à titre « *d'indulgence* » en indiquant regretter des « *erreurs passées* » ou des « *erreurs de jeunesse* », alors même qu'elles reconnaissent avoir commis des actes délictuels. Elles le font souvent auprès d'une autorité incompétente, l'autorité administrative, alors que la loi dispose que le traitement des données nominatives contenues dans le STIC s'exerce sous le contrôle du procureur de la République. En outre, il n'est pas souhaitable qu'un problème rencontré à l'occasion d'une procédure administrative rende définitivement inutilisable à des fins de police judiciaire des antécédents judiciaires.

Il est donc souhaitable que les requérants identifient mieux la voie la plus adaptée pour que ceux d'entre eux qui sont légitimes dans leurs demandes obtiennent rapidement gain de cause :

- le droit d'accès et de rectification, ou le recours spécifique effectué devant le procureur de la République, devrait être privilégié dans les cas où l'autorité judiciaire n'a pas retenu l'infraction ou l'a requalifiée à la baisse, et que l'autorité administrative n'en a pas tenu compte dans sa décision, soit à tort, soit qu'elle n'était pas en mesure de le faire, faute de complément ou de rectification du fichier ou de réponse du parquet sollicité ;
- la voie du recours administratif puis, le cas échéant, contentieux, devrait être privilégiée lorsque les faits délictuels ou criminels sont établis. Dans ce cas, si le requérant estime que la décision préfectorale est disproportionnée au regard de l'ancienneté, de la faible gravité et de l'absence de répétition des faits, il s'agit de la voie la plus rapide pour que la décision soit réformée. En outre, cela évitera l'engagement d'une procédure d'accès indirect vouée à l'échec, longue pour le requérant, et qui surcharge inutilement les services de la CNIL, les services de police et de gendarmerie et les services judiciaires ;
- dans certains cas, le requérant devrait engager parallèlement les deux procédures, principalement lorsqu'il dispose de la preuve, à la lecture de la motivation de la décision préfectorale, que cette dernière s'est appuyée sur la consultation d'une inscription non mise à jour et dont les suites judiciaires n'ont pas été recoupées. À l'appui de sa demande, il produirait utilement la décision du tribunal classant sans suite la procédure judiciaire reprochée pour insuffisance de charges. Le recours gracieux étant la procédure pouvant être le plus rapidement traitée, si sa demande est légitime, son problème professionnel serait très rapidement résolu et la rectification

des fichiers surviendrait après que l'ensemble des vérifications nécessaires ait été réalisé.

La loi dispose qu'une autorité administrative, saisie à tort d'une demande pour laquelle elle n'est pas compétente, est tenue de la transmettre directement à l'autorité compétente. Tout en accusant réception de la demande au requérant, elle réoriente celle-ci pour en accélérer le délai de traitement. Ce principe s'applique aussi bien aux administrations qu'aux autorités administratives indépendantes et même aux magistrats qui agiraient dans le cadre d'une procédure administrative et non au titre de l'activité judiciaire.

Au total, le nombre de saisines de la CNIL concernant le STIC est limité si on le rapporte au nombre total de fiches de mises en cause ou de victimes enregistrées. On compte ainsi 1 000 saisines dans le cadre du droit d'accès indirect clôturées au cours de l'année 2005 pour 4,5 millions de personnes mises en cause et 22,5 millions de fiches de victimes au 1<sup>er</sup> janvier 2006. Cependant, l'analyse des dossiers révèle soit des dysfonctionnements du fichier, soit des dysfonctionnements dans l'usage qui en est fait à des fins administratives.

---

## **L'information sur le droit d'accès aux données**

### La position de la CNIL

Pour la CNIL, alors que le législateur, en particulier par la loi du 18 mars 2003, a expressément reconnu aux personnes inscrites dans les fichiers de police judiciaire un certain nombre de droits tels que la possibilité de demander sous certaines conditions la rectification des données en cas de requalification judiciaire et, s'agissant des victimes, l'effacement des données les concernant, ces droits ne sont, en pratique, pas ou peu exercés, faute d'être connus.

En effet, à l'exception, notable, des personnes appelées à travailler dans le domaine de la sécurité et du gardiennage, pour lesquelles les notifications de refus d'agrément adressées par les préfets mentionnent généralement les voies de recours qui leur sont offertes et notamment la possibilité d'exercer leur droit d'accès en s'adressant à la CNIL (les modèles de lettres joints à l'instruction adressée le 15 avril 2005 aux préfets par le ministre de l'Intérieur ne mentionnent plus cette voie de recours), celle-ci constate qu'aucune mesure d'information n'a en effet été prévue à l'égard des personnes mises en cause.

Toutefois, l'article 2 du décret 6 septembre 2005 précitée prévoit que *« les personnes qui font l'objet d'une enquête administrative mentionnée dans la liste fixée à l'article 1<sup>er</sup> 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 par l'article 19 de la loi 12 avril 2000 susvisée. Dans les autres cas, l'intéressé est informé lors de la notification de la décision administrative le concernant ».*

Certes, la loi informatique et libertés prévoit une dérogation à l'obligation générale d'information des personnes s'agissant des traitements de données ayant pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales.

Toutefois, dès lors que ces fichiers de police judiciaire jouent un tout autre rôle en matière de police administrative et en fait d'emploi, la CNIL estime que l'information des personnes sur l'existence et les conditions d'exercice de ces droits ainsi que sur leur droit d'accès doit être reconnue et garantie par des mesures spécifiques telles que l'affichage dans les locaux des commissariats, des mentions sur les dépôts de plaintes...

Par ailleurs, il doit être souligné que la communication aux intéressés des informations les concernant n'est effective que depuis août 2005 (soit plus de quatre ans après l'entrée en vigueur du décret du 5 juillet 2001) et met en œuvre une procédure particulièrement longue et complexe puisqu'elle nécessite le double accord du ministère de l'Intérieur et du parquet.

Se pose d'ailleurs la question de maintenir, s'agissant de la communication aux intéressés du contenu de leur fiche, cette procédure d'accord préalable, alors même qu'une instruction du 15 avril 2005 adressée par le ministre de l'Intérieur aux préfets leur fait désormais obligation de motiver leur décision de refus et d'indiquer précisément les raisons de celui-ci et notamment les faits pour lesquels ils sont signalés dans le STIC. Dès lors donc que les intéressés connaissent les motifs pour lesquels ils sont fichés (au moins pour ce qui concerne les personnes employées ou susceptibles de l'être dans le cadre d'activités de sécurité privée), on peut légitimement s'interroger sur l'intérêt qu'il y a à requérir le double accord du ministère de l'Intérieur et du parquet.

Il en est de même s'agissant des victimes : dès lors qu'elles ont déposé plainte pour tel ou tel fait et que la procédure qui s'ensuit donne lieu à signalement dans le STIC, il est difficile de comprendre les raisons pour lesquelles elles ne pourraient pas accéder directement au contenu de leur fiche.

## La position du ministère de l'Intérieur

L'information sur les modalités de droit d'accès indirect dans le cadre des articles 41 et 42 de la loi informatique et libertés consiste à rappeler que la CNIL peut mener, au nom de la personne requérante, des investigations afin de procéder aux vérifications et aux éventuelles modifications sur les données enregistrées qui s'imposent (mise à jour, effacement).

Ce rappel ne saurait être confondu avec le droit à l'information prévu à l'article 32 de cette même loi qui impose au responsable du traitement d'informer, au moment de la collecte des données, les personnes figurant dans celui-ci de l'identité du responsable du traitement, de la finalité qu'il poursuit, des destinataires qu'il comprend et des droits dont la personne concernée dispose au regard de cet enregistrement de données. Le VI de cet article 32 prévoit très clairement que ce droit à l'information est exclu pour les traitements de données ayant pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales.

Bien que non obligatoire en vertu de la loi, une procédure d'information des victimes sera mise en œuvre très prochainement en application du décret en Conseil d'État régissant le STIC, publié le 15 octobre 2006.

S'agissant des mis en cause, le ministère de l'Intérieur est très attaché à l'application du droit actuel, confirmé par le législateur en 2004 après avis de la CNIL sur le projet de loi, qui tient compte de la spécificité des fichiers de police.

Informers systématiquement les personnes mises en cause que des informations les concernant sont conservées dans les fichiers de police judiciaire serait très lourd sur le plan procédural, alors que le formalisme de la procédure judiciaire présente déjà beaucoup d'inconvénients. Dans certaines enquêtes, cela serait impraticable, sauf à mettre en péril leur efficacité : ainsi, une inscription dans le STIC ne découle pas nécessairement d'un placement en garde à vue. L'inscription est légitime dès lors qu'il existe des indices graves ou concordants qui peuvent être réunis sur la base d'informations obtenues auprès de tiers, par exemple des mis en cause complices, ou encore des témoins, ou encore sur la base d'indices matériels. Un « *droit à l'information* » pourrait compromettre certaines enquêtes, entraîner la destruction de preuves ou entraîner la fuite des auteurs mis en cause.

De plus, une information sur le fait qu'une consultation des fichiers de police pourra être mise en œuvre est systématiquement délivrée, dans le récépissé de demande, à toute personne sollicitant une décision administrative impliquant une enquête administrative pouvant donner lieu à consultation de fichiers. Dès lors que cette règle prévue par l'article 2 du décret du 6 septembre 2005 précité s'applique, il serait disproportionné de bouleverser le fonctionnement des fichiers de police judiciaire.

Informers les personnes concernées à chaque fois qu'une procédure de consultation à des fins administratives est mise en œuvre suffit à atteindre l'objectif qui est de garantir les droits des personnes à l'occasion de la consultation des fichiers de police judiciaire à des fins administratives. Le Conseil d'État a validé ce raisonnement lors de l'examen du projet de décret modifiant le décret n° 2001-583 du 5 juillet 2001 portant création du Système de traitement des infractions constatées.

Concernant la mention expresse par les préfets des modalités de droit d'accès aux fichiers de police en cas de refus d'agrément lié à une activité privée, il s'agit d'insérer, dans les réponses qui sont apportées aux

candidats, en plus des voies et délais de recours administratifs ou contentieux, les modalités de droit d'accès indirect au STIC. Cela vise le droit d'accès en rectification ou d'effacement des données devant le procureur de la République (article 3 du décret STIC 2001 modifié) et le recours indirect devant la CNIL (article 8 du décret STIC 2001 modifié).

Sur la suppression du double accord du ministère de l'Intérieur et du parquet, concernant la transmission des informations à l'intéressé dans le cadre d'une demande de DAI, la CNIL a saisi le ministère de l'Intérieur le 18 juillet 2006. Ces propositions sont en cours d'expertise.

Le ministère de la Justice précise que les décrets relatifs au STIC et à JUDEX ne soumettent cet accès à l'accord du procureur que dès lors que la procédure n'est pas judiciairement close. Le fait, lorsque la procédure est close, de ne plus soumettre cet accès à l'accord du procureur de la République, devrait permettre aux requérants d'accéder plus rapidement aux informations sollicitées.

S'agissant enfin de la proposition de la CNIL d'instaurer un droit d'accès direct aux données pour les victimes, le ministère de l'Intérieur considère qu'il n'est pas souhaitable d'introduire une sécabilité de l'exercice du droit d'accès au fichier STIC (droit d'accès indirect pour les mis en cause et droit d'accès direct pour les victimes). En effet, si une personne exerce un droit d'accès direct auprès du gestionnaire et qu'il s'avère qu'elle n'est pas signalée dans le fichier comme victime mais comme mis en cause, le gestionnaire devra la renvoyer devant la CNIL par application du droit d'accès indirect. Par ailleurs, le maintien d'une procédure unique clairement définie de l'exercice du droit d'accès indirect par l'intermédiaire de la CNIL assure une meilleure gestion, un gain de temps et une plus grande lisibilité des modalités d'exercice de droit d'accès pour le citoyen. Le Conseil d'État a également confirmé cette analyse lors de l'examen du projet de décret modifiant le décret n° 2001-583 du 5 juillet 2001 portant création du système de traitement des infractions constatées dénommé STIC.

---

## **Les demandes de droit d'accès indirect**

### **Les demandes de droit d'accès au STIC**

Les demandes de droit d'accès aux fichiers de police formulées par les particuliers auprès de la CNIL ont connu une augmentation significative en 2004 (803) et 2005 (1003), suite à l'entrée en vigueur de la loi pour la sécurité intérieure, qui a modifié l'article 17-1 de la loi du 21 janvier 1995 (consultation des fichiers d'antécédents judiciaires en soutien des enquêtes administratives de moralité). La tendance pour l'année 2006 semble toutefois marquer une décrue.

**Nombre des dossiers reçus par la DCPJ/SDPTS en distinguant les demandes visant tous les fichiers (DAI global, y compris le STIC) et celles ne visant que le STIC (DAI – STIC <sup>1</sup>)**

	2003	2004	2005	Au 01/10/06
D.A.I global	269 (47 %)	823 (80 %)	1 137 (87 %)	724 (90 %)
D.A.I - S.T.I.C	306 (53 %)	202 (20 %)	169 (13 %)	84 (10 %)
<b>Total</b>	<b>575</b>	<b>1 025</b>	<b>1 306</b>	<b>808</b>

(1) On n'évoque ici que les demandes d'accès aux fichiers de police judiciaire, y compris effectué pour les contentieux de police administrative. La CNIL reçoit d'autres demandes d'accès indirects aux fichiers de police, ceux des fichiers des renseignements généraux ou de la DST par exemple.

Source : DGPN (DCPJ).

Les exercices du droit d'accès indirect « globaux » représentent ainsi, depuis 2004, plus de 80 % des demandes totales. La garantie est plus forte pour les citoyens, mais la procédure plus complexe à instruire.

Sur la période 2003-2005, la proportion des personnes exerçant leur droit d'accès indirect effectivement connues (auteur et/ou victime) s'est accrue, passant de 54 % en 2003 à 72 % en 2005. Cette évolution reflète la part prise par les saisines de la CNIL suite à une décision préfectorale de refus ou de retrait dans le cadre de leur activité privée de surveillance, de gardiennage et de transport de fonds. C'est majoritairement parce que l'on conteste une décision prise après consultation des fichiers que l'on demande à accéder aux fichiers, en préalable et/ou en parallèle à un recours hiérarchique.

Les « rectifications » effectuées par le gestionnaire du fichier à l'occasion de l'exercice du droit d'accès indirect sont à rapporter au nombre de dossiers traités dans l'année : ainsi, en 2005, sur 1 306 DAI transmises par la CNIL, 890 ont été traitées et ont provoqué un total de 160 rectifications (soit 18 %).

Il faut analyser ces chiffres en regard du nombre d'enquêtes administratives réalisées pour l'ensemble des domaines soumis à enquête de moralité, dont celles relevant de l'application de la loi du 12 juillet 1983 sur la sécurité privée (plus de 120 000 en 2005) et celles spécifiquement réalisées en matière aéroportuaire (plus de 70 000 l'an passé).

---

*Pour la Direction générale de la police nationale, s'il est parfaitement normal que le DAI, en cas d'erreur dans les informations figurant dans le fichier, débouche sur des mesures correctives, il est regrettable que, dans l'opinion publique, le « taux de rectification suite à DAI » ait parfois été transformé en « indicateur de qualité des fichiers ». Cette interprétation peut causer un grave et injuste problème d'image concernant les fichiers, et partant, de légitimité. Prendre comme dénominateur l'ensemble des dossiers qui posent problèmes ne permet pas d'obtenir un indicateur de qualité scientifiquement rigoureux et pertinent.*

*La CNIL estime pour sa part :*

*– que pour apprécier la fiabilité d'un fichier du point de vue de la loi informatique et libertés (notamment son article 6) et vu les conséquences de données inexactes pour les personnes concernées, il convient de considérer le nombre des « rectifications » faites par rapport aux fiches qui sont présentes dans le fichier, donc en ne tenant pas compte des saisines qui ont pour réponse « inconnu au fichier » (environ ? des saisines) ;*

*– qu'il y a lieu d'analyser distinctement les fiches de ceux qui sont « mis en cause » comme auteurs et les fiches des simples victimes, les conséquences d'une anomalie n'étant pas évidemment pas les mêmes dans les deux cas.*

*Dans tous les cas, le but n'est pas d'établir des indicateurs de qualité, mais d'identifier les problèmes et d'en rechercher les causes. C'est pourquoi les données chiffrées présentées par la CNIL dans la première partie ci-dessus doivent être considérées comme le reflet de réels dysfonctionnements constatés dans l'état actuel de ces fichiers.*

---

## **Les demandes de droit d'accès à JUDEX**

Pour vérifier la nature des éléments détenus dans les fichiers judiciaires que la gendarmerie nationale met en œuvre, la CNIL saisit par courrier le service technique de recherches judiciaires et de documentation (STRJD), administrateur fonctionnel des principaux d'entre eux.

Depuis fin septembre 2005, aux termes d'un relevé de conclusions DGGN-DGPN-DACG validé le 26 juillet 2005 par le président de la CNIL, le STRJD est chargé d'effectuer auprès des parquets les demandes de suites judiciaires pour les affaires qui lui sont adressées par la commission.

Pour chaque saisine reçue de la CNIL, la cellule « *Droit d'accès indirect* » du STRJD instruit donc le dossier en procédant à des opérations de trois types :

- l'exploitation du système JUDEX, du fichier des personnes recherchées et du fichier des personnes nées à l'étranger ;
- la vérification par message auprès des FAR des brigades des lieux de domicile, de naissance et de commission de l'infraction. À la demande CNIL, cette vérification peut être étendue à d'autres départements ;
- la demande auprès des procureurs de la République compétents pour connaître les suites judiciaires de toutes les affaires indexées dans la base JUDEX au nom de la personne concernée, que celle-ci y soit présente en qualité d'auteur ou de victime.

Après collecte de tous les éléments de réponse, la CNIL avisée par le STRJD s'y déplace pour que lui soit présenté le dossier ainsi constitué.

En année glissante, d'octobre 2005 (date d'entrée en vigueur de la nouvelle procédure prévue par le relevé de conclusions) à septembre 2006, 1 936 dossiers ont été reçus par la gendarmerie selon la typologie suivante.

Dossiers	Oct/Déc 2005	Janv/Sept 2006	Total
Dossiers reçus	1264	672	1936
Personne inconnue de la gendarmerie	985	499	1484
Personne connue « auteur »	220	106	326
Personne connue « victime »	44	41	85
Personne connue « auteur » et « victime »	15	26	41
Suppression à l'initiative du STRJD	51	34	85
Dossiers présentés à la CNIL	787	241	1028
Modifications en séance	172	24	196
Suites judiciaires (retour STIC)	233	27	260

Source : DGGN.

Nota : les chiffres pour trois mois en 2005 sont nettement plus importants que pour neuf mois en 2006 en raison de la reprise en septembre 2005 d'un important arriéré détenu par la CNIL.

## Des délais de réponse excessifs

Les statistiques présentées ci-après peuvent présenter des différences avec celles produites par le ministère de l'Intérieur, dans la mesure où la CNIL et le ministère de l'Intérieur n'ont pas la même définition de la notion de « *saisine clôturée* » : en effet pour la CNIL la saisine n'est considérée comme clôturée que lorsque l'intéressé a été rendu destinataire de la lettre de notification du président de la CNIL lui indiquant les résultats des vérifications opérées et le cas échéant lui communiquant sa fiche (après accord du ministère de l'Intérieur et du parquet). En outre, les premières saisines reçues par la CNIL nécessitent parfois une demande de renseignements complémentaires auprès du requérant (en particulier pour obtenir les dates et lieux de naissance) avant de pouvoir être transmises au ministère de l'Intérieur.

Les statistiques de la CNIL mettent en lumière un premier dysfonctionnement touchant à l'exercice des droits des personnes.

Les délais de réponse aux demandes de droit d'accès indirect transmises par la CNIL sont actuellement de l'ordre de plusieurs mois.

Ainsi, au 1<sup>er</sup> septembre 2006, les services de la CNIL étaient en attente de la réponse des services de police judiciaire pour 470 dossiers datant de 2005 et pour 45 datant de 2004 <sup>6</sup>. A cela s'ajoute l'attente de la confirmation par les services de la police nationale, d'une mise à jour ou d'une suppression des informations pour 38 dossiers, de la suite judiciaire pour 155 dossiers, de l'accord de communication au requérant pour 218 dossiers.

Ainsi, en définitive, pour les personnes mises en cause signalées dans le STIC qui nécessitent une demande de suites judiciaires auprès des parquets, l'ensemble de la procédure peut atteindre deux ans.

Au 1 <sup>er</sup> septembre 2006	2003	2004	2005	2006*
Dossiers en cours	37	370	724	604
Dossiers clôturés	552	433 (54 %)	279 (28 %)	31
Total	589	803	1003	635

Source : CNIL.

(\*) Ces chiffres ne concernent que le premier semestre 2006.

Or, le décret du 20 octobre 2005 pris pour l'application de la loi du 6 janvier 1978 modifiée prévoit, en son article 87, que la CNIL notifie au demandeur le résultat de ses investigations dans un délai de quatre mois à compter de sa saisine. Ce texte prévoit aussi que le responsable du traitement dispose, pour réaliser ses investigations, d'un délai de trois mois à compter de la transmission de la demande de droit d'accès par la Commission. Ce délai ne suspend pas celui de quatre mois qui s'impose à la CNIL.

Les modalités actuelles d'instruction des demandes par le ministère de l'Intérieur et la lenteur des réponses des parquets ne permettent donc pas en l'état à la Commission de respecter les termes de l'article 87 du décret précité. Même si les moyens en personnel du ministère de l'Intérieur ont été récemment renforcés, la CNIL considère que ceux-ci restent insuffisants pour traiter les demandes dans les délais. Au-delà, le retard constaté dans le traitement des dossiers provient aussi des parquets qui, compte tenu de leur charge de travail et du manque de moyens en personnel, ne peuvent aujourd'hui transmettre leurs réponses aux demandes de suites judiciaires dans les délais impartis. Est à cet égard tout à fait significative la réponse faite à la CNIL par la Direction de la police judiciaire en août 2006, faisant état de l'impossibilité pour le parquet de Paris d'informer le ministère de l'Intérieur des suites judiciaires et de l'accord de communication requis dans le traitement de onze dossiers transmis au printemps 2006.

De son côté, la CNIL connaît elle-même un certain retard dans le traitement des dossiers, ne disposant actuellement que deux personnes pour assurer la gestion de l'instruction des demandes.

(6) À ces chiffres, il convient d'ajouter les 604 dossiers envoyés au ministère de l'Intérieur depuis le 1<sup>er</sup> janvier 2006.

**Saisines relatives au STIC : état d'avancement des dossiers en cours au 1<sup>er</sup> septembre 2006**

Saisines arrivées à la CNIL en	2004	2005	TOTAL
<b><i>En attente de la 1<sup>ère</sup> investigation</i></b>			
Recherches en cours à la PJ	45	470	515
Dossiers prêts à être examinés	46	122	168
<b><i>En attente de la 2<sup>ème</sup> investigation</i></b>			
Attente par la CNIL de la mise à jour de la fiche STIC	11	27	38
Attente par la CNIL de la réponse du Procureur pour suites judiciaires	36	37	73
Attente par la PJ de la réponse du Procureur pour suites judiciaires	70	12	82
Investigation pour recueillir accord	31	15	46
Communication fiche STIC Procureur pour communication fiche STIC	131	41	172
Total	370	724	1094

Source : CNIL.



**Recommandations  
du groupe  
de travail sur  
le contrôle des  
fichiers de police  
utilisés à des fins  
administratives**



Le groupe de travail n'a pas eu pour mission de débattre de l'utilité des fichiers judiciaires dont chacun s'accorde à reconnaître la nécessité et l'importance dans le cadre de la prévention et la répression de la criminalité et du terrorisme, sous réserve d'un légitime contrôle.

Pour l'essentiel, les travaux du groupe de travail ont permis de constater que l'utilisation de certains des fichiers de police judiciaire dans le cadre de procédures administratives, malgré les contrôles de la Commission nationale informatique et libertés (CNIL) et les opérations d'apurement importantes réalisées par les services de police et les unités de gendarmerie, révélait des dysfonctionnements et pouvaient attenter aux libertés individuelles ou nuire à l'efficacité de l'action publique.

Certes, la consultation de ces fichiers permet d'éviter l'accès à certains emplois ou zones sensibles à des personnes présentant un risque pour la sécurité publique, mais aussi pour les libertés individuelles, par exemple en raison de la croissance rapide du secteur de la sécurité privée.

À l'inverse, les imperfections des fichiers ou l'usage parfois inapproprié qui en est fait peuvent entraîner des conséquences très défavorables pour certaines personnes, en premier lieu pour le libre accès à un emploi ou le maintien dans un poste de travail.

Ainsi, une des problématiques majeures apparues au cours des débats du groupe de travail a concerné la mise à jour des fichiers. En effet, au regard des dispositifs informatiques actuels, certaines fiches du STIC ou du fichier JUDEX ne sont pas toujours actualisées faute de transmission des suites judiciaires ou des requalifications judiciaires par le parquet vers les services de police et les unités de gendarmerie. Il peut donc arriver, par exemple, que dans le cadre d'une enquête administrative, un emploi soit refusé à une personne sur la base d'une information contenue dans le STIC concernant sa mise en cause pour une infraction, alors même que celle-ci a fait l'objet d'un non-lieu, décision qui n'aurait pas été portée à la connaissance du gestionnaire du fichier.

C'est donc l'usage à des fins autres que judiciaires de ces fichiers de police et de gendarmerie qui continue de poser problème. Il convient de mettre en œuvre des ajustements complémentaires afin que le cadre fixé par le législateur en 2001 et 2003 pour encadrer cet usage soit parfaitement respecté et l'ensemble des droits des personnes garantis.

À partir du recensement général des fichiers utilisés par diverses administrations pour lutter contre les différentes formes de criminalité réprimées par la loi (routière, criminalité organisée ou terrorisme...), le groupe de travail a constaté que plusieurs d'entre eux pouvaient être utilisés pour des raisons administratives et qu'il convenait donc, en s'appuyant sur les réflexions de la CNIL, de la CNDS et du Médiateur de la République, de fixer une recommandation générale plutôt que des dispositifs particuliers.

Les différentes recommandations du groupe de travail ont donc d'abord pour objet de renforcer les garanties individuelles en s'assurant que des informations non actualisées, inexactes ou dont la date de validité de conservation est expirée, soient écartées des fichiers et ne risquent plus ainsi de nuire à l'employabilité des personnes.

Elles visent également à rappeler que les décisions préfectorales, prises après consultation du STIC ou du fichier JUDEX, doivent faire l'objet d'une véritable instruction prenant en compte la gravité, la répétition et l'ancienneté des faits. La mention dans un fichier de police ne saurait automatiquement entraîner une décision défavorable et le préfet doit motiver sa décision sur des faits et non sur cette inscription.

Enfin, plusieurs recommandations concernent l'amélioration du droit d'accès aux données et le développement des voies de recours et portent sur des fichiers spécifiques.

---

# Propositions générales

---

## Pour améliorer la transparence des fichiers

### 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, 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 DAI* » ne soit pas transformé en « *indicateur de qualité des fichiers* ».

### 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 fichier 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.

---

## Pour une mise à jour systématique des fichiers d'antécédents judiciaires

### 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 la médiature de la République.

#### 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.

#### 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*.

## 6 – Réfléchir aux modalités de prise en compte des contraventions de 5<sup>e</sup> classe

Le groupe de travail recommande qu'une réflexion de fond puisse être engagée sur les modalités de prise en compte des contraventions de 5<sup>e</sup> classe dans le cadre des enquêtes administratives.

## 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.

---

## **Pour une amélioration du droit d'accès aux données**

### 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.

## 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 le développement de voies de recours

### 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<sup>1</sup>). 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.

(1) D'une manière générale au regard des articles 41 et 42 de la loi du 6 janvier 1978 modifiée par la loi du 4 août 2004 et d'une manière spécifique au regard des dispositions prévues dans le décret n° 2001-583 du 5 juillet 2001 modifié par le décret n° 2006-1258 du 14 octobre 2006 portant création du STIC et le décret n° 2006-1411 du 17 novembre 2006 portant création du système judiciaire de documentation et d'exploitation dénommé JUDEX.

## 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.

---

*Selon le Médiateur de la République, il résulte de l'article 21-III de la loi du 18 mars 2003 sur la sécurité intérieure que le traitement des données contenues dans les fichiers de police judiciaire est sous le contrôle du procureur de la République territorialement compétent qui peut demander qu'elles soient effacées, complétées ou rectifiées en cas de requalification judiciaire ou d'intervention d'une mesure de classement sans suite pour insuffisance de charges, d'une décision de non-lieu, ou de décisions de relaxe ou d'acquiescement devenue définitive.*

*À cet égard, l'article 4 alinéa 5 du décret du 14 octobre 2006 sur le STIC prévoit que les demandes de mise à jour au regard des suites judiciaires lui sont adressées soit directement, soit indirectement par l'intermédiaire de la CNIL qui saisit le responsable du traitement. Celui-ci dans un second temps soumet cette demande au procureur de la République territorialement compétent.*

*L'article 21-III de la loi précitée précise qu'en cas de « décision de relaxe ou d'acquiescement 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 ».*

*S'agissant des décisions de non-lieu et de classement sans suite pour insuffisance de charges, le même article prévoit qu'elles font l'objet d'une mention « sauf si le procureur de la République ordonne l'effacement des données ». Ainsi, le refus d'effacement constituant une décision faisant grief à l'intéressé, il conviendrait de rendre la législation compatible avec les exigences du droit européen et 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 conséquence, à l'initiative du Médiateur de la République, le groupe de travail propose de lancer une réflexion sur la mise*

*en place de voies de recours à l'encontre de ces décisions de refus d'effacement prises par le procureur de la République. Ces voies de recours pourraient se traduire par l'introduction, soit d'un recours hiérarchique devant le procureur général, soit d'un recours judiciaire devant la juridiction ayant prononcé la relaxe, le non-lieu, ou l'acquiescement.*

***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 CNIL.*

*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 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'État, s'agissant du fichier des renseignements généraux. Ainsi, la Haute Assemblée a 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 le 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.*

---

## 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 5<sup>e</sup> 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 prend acte de la position débattue au sein du groupe de travail.

En effet, le groupe de travail a rappelé que les condamnations ne sont pas inscrites dans ces traitements automatisés qui ont pour objet l'inscription de faits commis par une personne ou ayant donné lieu à un dépôt de plainte. Il a également rappelé le principe de stricte séparation des procédures administrative et judiciaire qui s'oppose à l'intervention d'un tribunal judiciaire – sauf hypothèse rare d'une question préjudicielle – dans l'instruction d'une demande d'agrément préfectoral.

La suppression de données à caractère personnel à l'occasion d'une enquête administrative aurait également, par voie de conséquence, la

suppression de ces données au titre de la police judiciaire. Si elle était limitée au champ de la police administrative, cette même suppression au titre d'une enquête administrative serait, par voie de conséquence, étendue à toutes les enquêtes. Dans un cas comme dans l'autre, cette suppression priverait l'autorité administrative de la possibilité de réaliser utilement les enquêtes administratives légalement ou réglementairement prescrites.

Enfin, le groupe de travail a indiqué que les fichiers STIC et JUDEX étaient des fichiers de police judiciaire et n'avaient pas vocation à faciliter « *la réinsertion* » sociale des personnes mais, notamment à prévenir les crimes et délits dans le cadre de missions de police administrative ou à rechercher les auteurs des infractions dans le cadre de la police judiciaire.

---

## **Pour une appréciation plus juste des décisions préfectorales**

### **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.

### **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.

### **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.

---

## **Poursuivre la démarche « qualité » dans l'alimentation et la mise à jour des fichiers**

### 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.

### 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.

---

## **Pour une nécessaire évolution du cadre juridique et des outils de travail des forces républicaines de sécurité**

### 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.

## 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 les décisions administratives nécessitant des enquêtes administratives et la consultation des fichiers de police interviennent.

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, la médiation de la République et la CNDS (suivant la décision prise en application de la proposition 3).

---

# Recommandations particulières sur certains fichiers

---

## Le fichier ELOI

Le fichier ELOI (éloignement) supporte les deux applications suivantes :

- SUEDEE (Suivi des étrangers devant être éloignés) ;
- SIRSEI (Système d'information en réseau du suivi des étrangers incarcérés).

L'application SIRSEI est accessible uniquement par le personnel de préfecture.

Lorsque un préfet prend un arrêté de reconduite frontière, un dossier SUEDEE est établi et envoyé au CRA (Centre de rétention administrative) pour le remplissage des parties incombant à la police, notamment la rubrique « *visite* ».

Cette rubrique permet d'identifier tout visiteur de l'éloigné. Elle comprend la date de début et fin de visite, l'heure de début et de fin de visite, le nom et prénoms, l'adresse, la ville, le code postal et le lien de parenté du visiteur.

Créé durant la période de fonctionnement du groupe de travail, le fichier ELOI a fait l'objet d'une attention particulière et d'une recommandation sur la non inscription de l'avocat comme visiteur dans le fichier SUEDEE.

Le groupe de travail, informé des échanges entre le ministère de l'Intérieur (qu'il avait également saisi par l'intermédiaire de son président) et les organisations professionnelles d'avocats, prend acte avec satisfaction des courriers du 18 octobre 2006 au président du Conseil national des barreaux et du 9 novembre 2006 au président du Syndicat des avocats de France, indiquant que « *le terme de »visiteur« doit naturellement s'entendre comme excluant les personnes qui, en raison de la nature de leurs fonctions, doivent s'entretenir avec un étranger en situation irrégulière* », et précisant que cette exclusion s'applique « *aux avocats, mais aussi aux députés, aux sénateurs ou aux membres d'institutions comme le Comité européen pour la prévention de la torture et des peines ou traitements inhumains ou dégradants ou la Commission nationale de contrôle des centres et locaux de rétention administrative et des zones d'attente* <sup>2</sup> ».

(2) Cette liste n'est pas exhaustive.

---

## Le STIC-Canonge

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 :

- type européen (nordique, caucasien, méditerranéen) ;
- type africain/antillais ;
- type métis ;
- type maghrébin ;
- type moyen-oriental ;
- type asiatique
- type indo-pakistanaï ;
- type latino-américain ;
- type polynésien ;
- type mélanésien (dont notamment canaque...).

Le groupe de travail recommande d'adopter cette nouvelle classification.

---

*Toutefois, la CNIL estime pour sa part prématuré de se prononcer sur la typologie proposée, compte tenu de la réflexion qu'elle vient d'engager sur la mesure de la diversité des origines et dans l'attente du rapport qui lui sera remis en janvier prochain par le groupe de travail qu'elle a constitué.*

---

---

## Le Fichier alphabétique de renseignements (FAR)

L'obsolescence du FAR, liée principalement à sa gestion très lourde, ainsi que les dispositions légales relatives au respect des libertés individuelles, obligent la gendarmerie nationale à refondre ce système.

Au terme de la période transitoire, fixée avant octobre 2010, le FAR sera supprimé.

Le groupe de travail recommande que, dans l'attente de la suppression prévue par la Direction générale de la gendarmerie nationale en 2010, le FAR soit déclaré à la CNIL et fasse l'objet des procédures réglementaires adaptées.

---

## **Le Fichier central automobile (FCA <sup>3</sup>)**

Bien que les objectifs de ce fichier ne soient pas directement couverts par la mission, le groupe de travail recommande que le ministère des Transports, gestionnaire de ce fichier, prévoit, sur le formulaire de demande de carte grise, une mention permettant au titulaire de refuser que les éléments fournis soient communiqués à des opérateurs privés.

(3) Le FAC est un fichier national (pour la France métropolitaine) établi à partir des données de cartes grises. Il permet un suivi des immatriculations et des parcs à partir des informations transmises par les préfetures. C'est un fichier national informatisé qui recense les véhicules immatriculés sur le territoire français. Le fichier a été créé en 1950, il était géré initialement par l'INSEE. Depuis 1973, le ministère des transports (SES) en assure la maîtrise d'ouvrage. Dans le cadre d'une convention, sa gestion est déléguée à l'Association auxiliaire de l'automobile (AAA). Arrêté du 11 octobre 1983 relatif au Fichier national informatisé des véhicules immatriculés sur le territoire français.



# Les modalités d'exercice du droit d'accès indirect au STIC <sup>1</sup>

Il faut noter d'abord qu'un certain nombre de saisines visent l'ensemble des fichiers de police, de la gendarmerie et du renseignement. Même si la saisine se limite aux fichiers de police judiciaire, compte tenu de la multiplicité des fichiers concernés pour une demande de droit d'accès indirect aux fichiers de police judiciaire, la CNIL communique au préalable à la DCPJ les noms des requérants avec leur date et lieu de naissance.

La Direction de la police judiciaire vérifie l'existence d'une fiche ou d'un dossier non seulement dans le STIC mais aussi dans le fichier manuel central et dans les fichiers locaux de la sécurité publique.

## **1 – Si le requérant est effectivement connu des services de police judiciaire du ministère de l'Intérieur, la PJ :**

- rapatrié au ministère de l'Intérieur les dossiers de procédure conservés par les directions départementales et régionales pour les mis en cause ;
- saisit le procureur de la République du tribunal compétent pour connaître la suite judiciaire des affaires mentionnées et recueillir son accord de communication en cas de maintien de la fiche STIC qu'il soit mis en cause ou victime.

L'article 21 de la loi du 18 mars 2003 pour la sécurité intérieure confère en effet au procureur de la République territorialement

(1) Article 41 : Par dérogation aux articles 39 et 40, lorsqu'un traitement intéresse la sûreté de l'État, la défense ou la sécurité publique, le droit d'accès s'exerce dans les conditions prévues par le présent article pour l'ensemble des informations qu'il contient. La demande est adressée à la commission qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de la commission. Il est notifié au requérant qu'il a été procédé aux vérifications. 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'État, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant. Lorsque le traitement est susceptible de comprendre des informations dont la communication ne mettrait pas en cause les fins qui lui sont assignées, l'acte réglementaire portant création du fichier peut prévoir que ces informations peuvent être communiquées au requérant par le gestionnaire du fichier directement saisi.

compétent un pouvoir d'appréciation s'agissant de la mise à jour, voire de l'effacement, de la fiche du requérant dans les fichiers de police judiciaire.

Si la procédure a fait l'objet d'une décision de classement sans suite pour insuffisance de charges ou de non-lieu, le procureur de la République doit préciser à la police judiciaire s'il ordonne ou non l'effacement des informations concernant le requérant dans les fichiers de police judiciaire. En cas de refus, la fiche doit cependant être mise à jour par la mention de la décision de classement ou de non-lieu.

Si la procédure a fait l'objet d'une décision de relaxe ou d'acquiescement devenue définitive, les informations concernant l'intéressé doivent en principe être effacées, sauf si le procureur de la République en prescrit le maintien dans les fichiers de police judiciaire.

Ces premières démarches prennent en moyenne actuellement plus d'un an si la personne est connue en tant que mise en cause.

**2 – Une réunion est organisée soit au ministère de l'Intérieur soit dans les locaux de la PJ à Écully afin que les membres de la CNIL qui ont la qualité de magistrats puissent examiner les différentes pièces du dossier (compte rendu d'enquête, pièces du FAED et/ou Canonge, procès-verbaux d'audition et éventuellement des documents plus anciens non répertoriés dans le STIC).**

Si le requérant a demandé accès à plusieurs fichiers, les services de la CNIL s'assurent que l'ensemble des dossiers relevant de la DGPN relatifs au requérant sont rassemblés pour la réunion d'investigations (renseignements généraux et/ou police judiciaire et/ou sécurité publique).

Dans le cadre des investigations, le magistrat de la CNIL examine successivement :

- la qualification des faits ;
- les durées de conservation des données telles qu'elles ont été définies dans le décret n° 2001-583 du 5 juillet 2001 portant création du système de traitement des infractions constatées ;
- les mises à jour ou suppressions éventuelles des données concernant :
  - les personnes ayant bénéficié d'un non-lieu ;
  - les personnes mises en cause qui ont bénéficié d'une décision judiciaire de classement sans suite motivée par l'insuffisance des charges ;
  - les personnes ayant bénéficié d'une décision de relaxe ou d'acquiescement devenue définitive ;
  - éventuellement la requalification des faits à la lecture de la procédure ;
  - les erreurs d'enregistrement (infraction ne devant pas être enregistrée dans le STIC ou dans JUDEX, personne signalée comme « auteur » alors qu'elle n'était que victime, plainte au nom d'une personne morale et enregistrée au nom de la personne physique qui a procédé au dépôt de la plainte...).

Lors de la réunion d'investigations, les services de police judiciaire remettent à la CNIL les fiches STIC qui ont recueilli l'accord de communication du ministère de l'Intérieur et du procureur de la République.

S'il y a lieu de demander une suppression, le président de la CNIL saisit la DGPN et sollicite son accord pour en informer le requérant. Si la radiation a déjà été effectuée par les services de police judiciaire, lors de l'examen du dossier, les services de police judiciaire présentent au magistrat de la CNIL l'ancienne et la nouvelle version de l'enregistrement. Le président de la CNIL saisit la Direction de la police judiciaire afin d'obtenir son accord pour informer le requérant de cette suppression.

La CNIL demande aux services de police judiciaire de transmettre les signalements rectifiés aux services préfectoraux concernés dès lors que le signalement initial a pu être utilisé notamment dans le cas des habilitations, des assermentations ou d'embauches.

**3 – Enfin le président de la CNIL notifie au requérant** qu'il a été procédé aux vérifications demandées dans les fichiers visés dans la saisine initiale et communique les fiches STIC si le procureur a donné son accord. En cas de refus de communication ou de refus de suppression du ministère de l'Intérieur suite à la demande du procureur de la République, il lui est en outre précisé qu'un recours devant le tribunal administratif lui est ouvert dans un délai de deux mois à compter de la date de réception du courrier envoyé en recommandé avec accusé de réception. C'est à ce stade que la saisine est considérée comme « *clôturée* ».



---

## Table des matières

<b>Sommaire</b> . . . . .	<b>3</b>
<b>Composition du groupe de travail</b> . . . . .	<b>5</b>
<b>Lettre de mission</b> . . . . .	<b>7</b>
<b>Introduction</b> . . . . .	<b>9</b>
<b>Chapitre 1</b>	
<b>Recensement des fichiers</b> . . . . .	<b>13</b>
Les fichiers de la police nationale (sous CHEOPS) . . . . .	<b>15</b>
Le Système de traitement des infractions constatées (STIC) . . . . .	<b>15</b>
Le Fichier des véhicules volés (FVV) . . . . .	<b>22</b>
Le Fichier des personnes recherchées (FPR) . . . . .	<b>24</b>
Le Fichier des renseignements généraux (FRG) . . . . .	<b>26</b>
Le Fichier national transfrontières (FNT) . . . . .	<b>28</b>
Le Fichier des brigades spécialisées (FBS) . . . . .	<b>29</b>
Le Fichier automatisé du terrorisme (FIT) . . . . .	<b>30</b>
Le Fichier national du faux monnayage (FNFM) . . . . .	<b>33</b>
Le Fichier national automatisé des empreintes génétiques (FNAEG) . . . . .	<b>34</b>
Le fichier d'information Schengen (SIS) . . . . .	<b>39</b>
Le fichier de la Direction de la surveillance du territoire (DST) . . . . .	<b>40</b>
Le Système d'analyse et de liens de la violence associée au crime (SALVAC) . . . . .	<b>42</b>
Le fichier de travail de la police judiciaire (FTPJ) . . . . .	<b>44</b>
Le Fichier automatisé des empreintes digitales (FAED) . . . . .	<b>44</b>
Les fichiers de la gendarmerie nationale . . . . .	<b>48</b>
JUDEX . . . . .	<b>48</b>
Le Fichier des objets signalés (FOS) . . . . .	<b>54</b>
Le fichier de traitement des images des véhicules volés (FTIVV) . . . . .	<b>55</b>
ANACRIM . . . . .	<b>56</b>
Le Service central de préservation des prélèvements biologiques (SCPPB) . . . . .	<b>59</b>
Le Fichier des avis de condamnations pénales (FAC) . . . . .	<b>60</b>

PULS@R . . . . .	<b>62</b>
La Bureautique brigade 2000 (BB2000) . . . . .	<b>63</b>
COG-RENS . . . . .	<b>65</b>
Le Fichier alphabétique de renseignements (FAR) . . . . .	<b>66</b>
Le Fichier des personnes nées à l'étranger (FPNE). . . . .	<b>68</b>
Le fichier ARAMIS . . . . .	<b>69</b>
Le Fichier de suivi des titres de circulation délivrés aux personnes sans domicile ni résidence fixe (SDRF). . . . .	<b>70</b>
Le Fichier de suivi des personnes faisant l'objet d'une rétention administrative . . . . .	<b>72</b>
Le Fichier de la batellerie. . . . .	<b>73</b>
ARIANE. . . . .	<b>74</b>
Le Fichier judiciaire national automatisé des auteurs d'infractions sexuelles (FIJAIS). . . . .	<b>76</b>
Le Fichier national des permis de conduire (FNPC) . . . . .	<b>79</b>
AGRIPPA. . . . .	<b>84</b>

## **Chapitre 2**

### **Problèmes et dysfonctionnements . . . . . 87**

#### **La saisine et l'alimentation . . . . . 97**

Les difficultés techniques . . . . . **97**

La qualité inégale de l'alimentation du STIC. . . . . **97**

L'absence d'archives correspondant à la totalité de la durée  
d'inscription au STIC . . . . . **97**

La durée de conservation du STIC. . . . . **98**

L'apurement des données dans JUDEX . . . . . **99**

Les personnels habilités à consulter les fichiers de police  
judiciaire . . . . . **101**

La question des mises à jour. . . . . **102**

Le respect de la finalité des fichiers selon les textes  
en vigueur. . . . . **109**

La finalité des fichiers de police judiciaire. . . . . **109**

L'utilisation malveillante . . . . . **110**

Les fichiers de police comme unique élément des enquêtes  
administratives . . . . . **111**

La consultation du fichier pour des contraventions de 5<sup>e</sup> classe . **113**

#### **Le droit d'accès aux fichiers et les recours administratifs ou contentieux contre les décisions préfectorales . . . . . 115**

L'information sur le droit d'accès aux données. . . . . **117**

Les demandes de droit d'accès indirect . . . . . **120**

Les demandes de droit d'accès au STIC . . . . . **120**

Les demandes de droit d'accès à JUDEX. . . . . **122**

Des délais de réponse excessifs . . . . . **123**

### Chapitre 3

## **Recommandations du groupe de travail sur le contrôle des fichiers de police utilisés à des fins administratives . . . . . 127**

### **Propositions générales . . . . . 131**

Pour améliorer la transparence des fichiers . . . . . **131**

1 – Améliorer la communication publique . . . . . **131**

2 – Rendre publique, chaque année, une information sur  
la consultation des fichiers de police et de gendarmerie  
à des fins administratives . . . . . **131**

Pour une mise à jour systématique des fichiers  
d'antécédents judiciaires . . . . . **131**

3 – Créer un rendez-vous annuel technique . . . . . **131**

4 – Mettre en place un groupe de travail police-justice-  
gendarmerie . . . . . **132**

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 . . . . . **132**

6 – Réfléchir aux modalités de prise en compte  
des contraventions de 5<sup>e</sup> classe . . . . . **133**

7 – Diffuser une nouvelle circulaire du ministère de la Justice . . . **133**

Pour une amélioration du droit d'accès aux données **133**

8 – Mieux informer les victimes des garanties légales  
et réglementaires protectrices prévues à leur égard . . . . . **133**

9 – Archiver et numériser les procédures judiciaires pour éviter  
le risque de décisions erronées ou insuffisamment argumentées . **134**

Pour le développement de voies de recours . . . . . **134**

10 – Mieux informer les personnes sur les voies de recours  
existantes. . . . . **134**

11 – Réfléchir à la création d'une voie de recours contre  
les décisions du parquet en matière de conservation  
ou d'effacement des décisions . . . . . **135**

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 . . . . . **137**

Pour une appréciation plus juste des décisions  
préfectorales . . . . . **138**

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 . . . . . **138**

14 – Mieux harmoniser les motivations des décisions préfectorales **138**

15 – Améliorer la traçabilité des consultations . . . . . **138**

Poursuivre la démarche « qualité » dans  
l'alimentation et la mise à jour des fichiers . . . . . **139**

16 – Poursuivre la formation des personnels. . . . . **139**

17 – Poursuivre la démarche « qualité » de la gendarmerie  
et de la police nationales . . . . . **139**

Pour une nécessaire évolution du cadre juridique et des outils de travail des forces républicaines de sécurité . . . . .	<b>139</b>
18 – Ouvrir une réflexion sur l'évolution nécessaire des outils de travail des forces républicaines de sécurité . . . . .	<b>139</b>
19 – Prendre en compte la dimension européenne . . . . .	<b>140</b>
<b>Recommandations particulières sur certains fichiers . . . . .</b>	<b>141</b>
Le fichier ELOI . . . . .	<b>141</b>
Le STIC-Canonge . . . . .	<b>142</b>
Le Fichier alphabétique de renseignements (FAR) . . . . .	<b>142</b>
Le Fichier central automobile (FCA) . . . . .	<b>143</b>
 <b>Annexe 1</b>	
<b>Les modalités d'exercice du droit d'accès indirect au STIC . . . . .</b>	<b>145</b>