



N°1548

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

TREIZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 24 mars 2009.

RAPPORT D'INFORMATION

DÉPOSÉ

en application de l'article 145 du Règlement

PAR LA COMMISSION DES LOIS CONSTITUTIONNELLES, DE LA LÉGISLATION
ET DE L'ADMINISTRATION GÉNÉRALE DE LA RÉPUBLIQUE

sur les fichiers de police

PAR Mme Delphine BATHO et M. Jacques Alain BÉNISTI,

Députés.

SOMMAIRE

	Pages
PRÉAMBULE	9
INTRODUCTION	11
I. CLARIFIER LE CADRE JURIDIQUE	25
A. LES GRANDS PRINCIPES PRÉSIDENT À LA CRÉATION DES FICHIERS DE POLICE.....	25
1. Le cadre juridique international et européen	26
<i>a) Les textes de protection de l'Union européenne</i>	26
<i>b) Les autres instruments internationaux</i>	31
2. Le cadre juridique national	34
<i>a) Protection des données et des personnes : la genèse de la loi du 6 janvier 1978</i>	34
<i>b) Régime de déclaration versus régime d'autorisation : la nécessaire publicité des actes créant des fichiers</i>	35
<i>c) La Commission nationale de l'informatique et des libertés (CNIL) : une autorité de contrôle veillant au respect des libertés publiques</i>	40
B. LA CRÉATION DES FICHIERS : EN FINIR AVEC L'AMBIGUÏTÉ DU CADRE JURIDIQUE ACTUEL.....	42
1. Deux régimes juridiques coexistent actuellement pour créer les fichiers de police	43
2. Entre diversité et absence de base juridique : l'augmentation du nombre de fichiers de police	44
3. Pour un débat public éclairé : les fichiers de police doivent être créés par la loi	46
C. SORTIR DES RELATIONS CONFLICTUELLES ENTRE LA CNIL ET LE MINISTÈRE DE L'INTÉRIEUR.....	49
1. Un dialogue de sourds entre la CNIL et le ministère de l'Intérieur	49
2. L'introduction d'une procédure de mise en application par étapes des fichiers de police sous le contrôle de la CNIL	53

II. MIEUX PROTÉGER LES DONNÉES SENSIBLES	57
A. LES DONNÉES SENSIBLES DANS LES FICHIERS DE RENSEIGNEMENT.....	57
1. Le fichier des renseignements généraux : un cadre juridique progressivement clarifié.....	58
a) <i>Les renseignements généraux : rôle et actions</i>	58
b) <i>Le fichier des renseignements généraux : un outil au service des missions assignées aux RG</i>	60
c) <i>Le fichier des renseignements généraux posait une interdiction de principe de collecter des données sensibles</i>	62
2. Le fichier EDVIGE a opéré une extension notable des données sensibles susceptibles d’être collectées.....	63
a) <i>La création du fichier EDVIGE est liée à la nouvelle architecture du renseignement intérieur</i>	63
b) <i>Le décret créant le fichier EDVIGE opère une extension du champ des données sensibles recueillies</i>	65
3. EDVIRSP : des données collectées et conservées quelle que soit la finalité visée.....	68
a) <i>La réaffirmation de l’interdiction de principe de collecter des données sensibles au sens de l’article 8 de la loi du 6 janvier 1978</i>	69
b) <i>Des données collectées et traitées quelle que soit la finalité visée</i>	70
4. Le « <i>fichier des personnalités</i> ».....	72
B. LA DÉLICATE QUESTION DU FICHAGE DES MINEURS.....	74
1. Les mineurs dans les fichiers de renseignement.....	74
a) <i>Le projet EDVIGE : répertorier les mineurs « susceptibles de porter atteinte à l’ordre public »</i>	75
b) <i>La nécessité d’encadrer et de définir les conditions précises de fichage des mineurs</i>	76
c) <i>Sur la base de critères objectifs clairement définis pour le fichage des mineurs, étendre l’application « Gestion des violences urbaines » (GEVI) sur l’ensemble du territoire</i>	79
d) <i>Le droit à l’oubli : pierre angulaire de la protection des mineurs</i>	81
2. Les mineurs dans les fichiers d’antécédents judiciaires.....	83
C. LE SIGNALEMENT DES PERSONNES : À LA RECHERCHE DES « SIGNES PHYSIQUES PARTICULIERS, OBJECTIFS ET PERMANENTS ».....	84
1. Le STIC-Canonge et son équivalent JUDEX : une identification des personnes recherchées basée sur une typologie ethno-raciale.....	85
2. Les nouvelles classifications proposées par le groupe de travail d’Alain Bauer en 2006 : des amendements à la marge de la typologie Canonge ...	86
3. Identification des personnes recherchées : typologie ethno-raciale <i>versus</i> portrait-robot.....	87

III. GARANTIR L'EXACTITUDE DES FICHIERS	89
A. DES FICHIERS D'IDENTIFICATION QUI ONT DU MAL À INTÉGRER ET À EXPLOITER LE FLUX DES DONNÉES.....	89
1. Une modernisation nécessaire du fichier automatisé des empreintes digitales.....	89
2. Des garanties très sérieuses d'exactitude des données en matière d'empreintes génétiques.....	92
a) <i>Un processus d'alimentation du FNAEG très encadré, afin de garantir l'exactitude des informations</i>	92
b) <i>Vers la fin de la crise de croissance du FNAEG ?</i>	94
c) <i>Préciser davantage les circonstances dans lesquelles un prélèvement peut être effectué</i>	97
B. UNE CHAÎNE D'ALIMENTATION DU STIC COMPLÈTEMENT OBSOLÈTE.....	100
1. Une alimentation initiale à la source de nombreuses erreurs.....	101
a) « Ce sont les personnels administratifs qui vérifient les procédures des actifs. ».....	101
b) <i>L'enjeu du juste moment de l'inscription au STIC</i>	102
c) « Les chiffres seront très différents avec ARIANE ».....	104
2. Des structures de contrôle de la qualité ne pouvant faire face aux flux de procédures.....	106
a) <i>L'ampleur de la tâche d'enrichissement et de contrôle de la qualité</i>	106
b) « Nous sommes défaillants depuis des années et des années. La défaillance n'a été que croissante. ».....	108
3. Prendre dès à présent les décisions nécessaires pour qu'ARIANE soit effectivement un progrès.....	109
a) <i>Le déploiement laborieux de la nouvelle application commune à la police et à la gendarmerie</i>	109
b) <i>Définir des procédures adaptées de contrôle de la qualité des informations saisies</i>	110
c) <i>Garantir l'exactitude du stock d'informations anciennes qui seront transférées vers ARIANE</i>	112
IV. RENDRE LES CONTRÔLES PLUS EFFICACES	115
A. LES INSUFFISANCES DU CONTRÔLE DES FICHIERS D'ANTÉCÉDENTS JUDICIAIRES PAR LES PARQUETS.....	115
1. Un cadre juridique clairement établi.....	115
2. Des mises à jour très insuffisantes en pratique.....	118
a) <i>Une trop faible utilisation de la faculté de requalification lors de la réception des procédures</i>	118
b) <i>La prise en compte inégale et tardive des suites judiciaires</i>	120

<i>c) Garantir un traitement rapide des demandes de mise à jour adressées directement aux parquets</i>	124
3. Le contrôle des fichiers d'antécédents judiciaires par les parquets est-il seulement « un concept » ?	127
D. L'ULTIME RECOURS DU DROIT D'ACCÈS INDIRECT	131
1. Les difficultés rencontrées pour faire face à la croissance des demandes ..	132
<i>a) Un volume croissant de demandes adressées à la CNIL et des délais très longs</i>	132
<i>b) Une procédure complexe : l'exemple du droit d'accès indirect pour les fichiers d'antécédents judiciaires</i>	133
<i>c) Des moyens insuffisants pour des défis toujours plus nombreux : la difficile équation de la CNIL</i>	135
2. L'accès aux données figurant dans les fichiers de renseignement	137
<i>a) Les modalités particulières de communication prévues pour le fichier des renseignements généraux</i>	137
<i>b) Les fichiers de renseignement classés secret-défense</i>	139
V. RESPECTER LES FINALITÉS	143
A. ACCROÎTRE LA LUTTE CONTRE LES CONSULTATIONS ABUSIVES	143
1. Divers degrés d'abus, dans un contexte susceptible d'en accroître la fréquence	144
2. La « tricoche » : un phénomène sévèrement sanctionné	146
3. Améliorer le contrôle d'accès et mettre en place des dispositifs d'alerte précoce	147
B. L'UTILISATION DES FICHIERS D'ANTÉCÉDENTS JUDICIAIRES DANS LE CADRE D'ENQUÊTES ADMINISTRATIVES : D'UNE UTILISATION ANNEXE À UNE PRATIQUE MASSIVE	149
1. Des possibilités très larges de consultation à des fins administratives	149
2. Une exigence particulière de discernement	151
C. LES ENJEUX D'UNE ADAPTATION AUX BESOINS ET DE LA MISE EN PLACE D'UNE VÉRITABLE DÉMARCHE PROSPECTIVE	155
1. Un fichier des brigades spécialisées « à bout de souffle »	155
2. Les expérimentations en cours dans le domaine du rapprochement : « les fichiers c'est utile... quand on sait ce que l'on cherche ! »	156
<i>a) LUPIN et CORAIL : les nouveaux outils de la police pour lutter contre la délinquance sérieuse</i>	156
<i>b) Les ambitions de la gendarmerie nationale</i>	160
<i>c) Un cadre législatif inadapté à l'utilisation accrue des fichiers de rapprochement</i>	161
3. Pour une véritable démarche prospective	162

D. AMÉLIORER L'ENCADREMENT DES TRANSFERTS INTERNATIONAUX DE DONNÉES	167
1. Une première étape minimale d'harmonisation dans le cadre du troisième pilier de l'Union.....	167
2. La lente mise en œuvre du Traité de Prüm	170
3. La longue marche vers l'adoption d'une décision-cadre sur l'utilisation des données passagers	171
VI. CONTRÔLER LA TRANSITION ENTRE FICHIERS DE POLICE ET ACCOMPAGNER LEUR DESTRUCTION ÉVENTUELLE	175
A. LA DIFFICILE TRANSITION ENTRE FICHIERS DE POLICE	175
1. La fusion de deux fichiers de police : une reprise problématique de l'existant.....	175
2. Le démembrement d'un fichier de police : le délicat partage de l'héritage... ..	177
a) <i>La question du partage du FRG entre SDIG et DCRI.....</i>	<i>177</i>
b) <i>L'impossibilité complète d'alimentation : l'imbroglio juridique entourant le retrait d'EDVIGE</i>	<i>178</i>
c) <i>La désorganisation des services à la suite de la réforme des services de renseignements en 2008.....</i>	<i>179</i>
B. ORGANISER LA DESTRUCTION DES FICHIERS DÉSUETS	181
1. Archiver ou détruire, il faut choisir !	182
a) <i>La mission « Archives des renseignements généraux » : donner une seconde vie à des informations ne répondant plus aux besoins opérationnels</i>	<i>182</i>
b) <i>Trier les archives centrales de la préfecture de police : « un monde englouti sous les papiers »</i>	<i>183</i>
2. La fin programmée du FAR : la nouvelle « Arlésienne » ?.....	185
a) <i>Un fichier au fonctionnement obsolète et inadapté.....</i>	<i>185</i>
b) <i>Un fichier auquel la gendarmerie est attachée et dont elle n'arrive pas à se détacher : « c'est la mémoire de la brigade qui va s'en aller ».....</i>	<i>187</i>
c) <i>La fin du FAR : une annonce sans véritable anticipation.....</i>	<i>189</i>
3. La mort des fichiers de police	191
EXAMEN EN COMMISSION	193
SYNTHÈSE DES PROPOSITIONS	207
GLOSSAIRE	219
LISTE DES PERSONNES AUDITIONNÉES	223
LISTE DES DÉPLACEMENTS EFFECTUÉS.....	229
ANNEXES	235

PRÉAMBULE

La mission d'information sur les fichiers de police trouve directement sa source dans les travaux conduits par la commission des Lois dans le cadre des débats sur le fichier de renseignement « EDVIGE » (exploitation documentaire et valorisation de l'information générale). Une série complète d'auditions avait alors été menée et avait été suivie par l'adoption de recommandations figurant dans un rapport d'information du président de la commission, M. Jean-Luc Warsmann ⁽¹⁾.

Ces débats avaient souligné combien le domaine des fichiers de police restait trop peu connu et propice à de réelles inquiétudes des citoyens sur le respect des libertés publiques et la protection de leurs données personnelles. Or, les fichiers sont des outils tout à fait indispensables au travail quotidien des forces de sécurité intérieure, tant en matière d'identification des personnes, de recherche d'antécédents ou de rapprochements à même de faciliter l'élucidation des crimes et délits que dans le cadre des missions de renseignement liées à la sûreté de l'État.

Plusieurs rapports récents ont fait état de dysfonctionnements dans certains fichiers de police ainsi que d'une augmentation sensible de leur nombre comme de la quantité de données collectées. Pour autant, alors même qu'un contrôle démocratique paraît essentiel dans ce domaine, jamais le Parlement jusqu'ici n'avait étudié l'ensemble de cette problématique complexe, afin de disposer d'une vision d'ensemble sur la nature et l'évolution des fichiers de police.

Au demeurant, les travaux officiels sont également restés longtemps très peu nombreux, l'Institut national des hautes études de sécurité n'ayant par exemple jamais réalisé d'études sur cette question, et toujours fort ponctuels. Il a fallu attendre le rapport du groupe de travail sur les fichiers de police, en novembre 2006, pour disposer d'un premier état des lieux. Parallèlement, l'évolution rapide des technologies informatiques, avec les potentialités et les risques qu'elles comportent, amène à s'interroger sur les choix stratégiques que doit faire une démocratie mature dans ce domaine.

Le rapport de la mission d'information constitue donc la première étude réalisée par le Parlement en la matière. Aussi vos rapporteurs ont-ils souhaité entendre l'ensemble des acteurs concernés et rencontrer les utilisateurs et les gestionnaires des fichiers sur leurs lieux de travail.

L'enjeu n'est en effet pas mince : il s'agit de s'assurer du strict respect des droits et libertés des citoyens, mais aussi de la performance des instruments

⁽¹⁾ EDVIGE en débat : les recommandations de la commission des Lois, rapport n° 1126, septembre 2008.

confiés aux gendarmes et policiers pour lutter contre la délinquance et la criminalité. Cette double ambition a continuellement animé vos rapporteurs tout au long de leur mission.

Ils tiennent à remercier l'ensemble des personnes auditionnées pour leurs contributions, ainsi qu'à saluer la disponibilité remarquable dont ont su faire preuve les services de la police, de la gendarmerie et de la justice qui ont été visités. Les personnels rencontrés lors des déplacements ont rendu compte sans fard de leurs conditions de travail réelles et de leurs attentes, et cette sincérité a été particulièrement précieuse.

INTRODUCTION

« Un habitant du Royaume [...] ne pourrait se remuer sans son certificat, il ne pourrait être reçu nulle part sans ce certificat. Les mouvements de l'homme seraient portés sur son certificat. On saurait ce que devient un particulier quelconque depuis le premier moment de sa naissance jusqu'au dernier. De même qu'en une heure de temps le Magistrat de police parvient à déterrer à Paris par le moyen de son bureau et de ses doubles, le particulier le plus ignoré de la capitale, on parviendrait à l'aide du bureau général [...] à découvrir de même le particulier le plus ignoré du Royaume. »

Cette phrase n'a pas été écrite par la plume de l'un des plus grands dictateurs du XX^e siècle ou d'un auteur de science-fiction contemporain. Elle est l'œuvre d'un officier de la Maréchaussée d'Île-de-France du XVIII^e siècle, Guillauté. Ce dernier a rédigé, en 1749, un rapport intitulé *Mémoire sur la réformation de la police en France*, qui avait pour but de réduire les troubles à l'ordre public. Pour ce faire, il avait imaginé d'établir un « feuillet » par maison où seraient recensées toutes les informations concernant les habitants qui y demeurent (nom, âge, origine, qualités notamment). Parallèlement, chaque habitant du royaume aurait dû avoir en sa possession un certificat pour se loger et pour se déplacer. Avec ce double contrôle et grâce à un savant système d'archivage, la Police aurait pu « évanouir la distance » qui sépare les individus des policiers⁽¹⁾.

C'est aux XVIII^e et XIX^e siècles que naît précisément la « société de la surveillance ». La démonstration en est donnée par Michel Foucault qui écrit dans *Surveiller et punir* que s'opère alors « la mise sous contrôle des moindres parcelles de la vie et du corps, dans le cadre de l'école, de la caserne, de l'hôpital ou de l'atelier ». Pierre Rosanvallon a d'ailleurs daté de la fin des années 1760 l'apparition du terme de « surveillance »⁽²⁾.

La volonté de prévenir les troubles à l'ordre public s'incarne alors dans la constitution des premiers fichiers de police. Dès 1752, avait été mis en place un « livre rouge » à Paris, consignait l'identité et le signalement des coupables, ainsi que la nature de leur condamnation, et l'on sait que Fouché était réputé avoir fiché l'ensemble des Français.

Mais ce sont les débuts de la police scientifique qui, au XIX^e siècle, fournissent les moyens de constituer des fichiers efficaces. Ainsi, en 1882 est créé un service anthropométrique puis un service photographique à la préfecture de police. La méthode de signalisation anthropométrique des personnes arrêtées et

(¹) Eric Hailmann, « Comment surveiller la population à distance ? La machine de Guillauté et la naissance de la police moderne ».

(²) Pierre Rosanvallon, *La contre-démocratie*, Paris, Seuil, 2006, p. 42.

la technique de comparaison des empreintes digitales qui y sont élaborées seront copiées partout dans le monde.

C'est également à la fin du XIX^e siècle que sont créés et que se développent les fichiers du contre-espionnage : « *les carnets A recensent alors, dans chaque département les noms des étrangers résidant en France en âge de servir dans les armées et les carnets B ceux des Français soupçonnés d'espionnage ou d'antimilitarisme.* »⁽¹⁾

Depuis lors, **les fichiers et les libertés publiques ont toujours entretenu des rapports conflictuels**, vérifiant la formule d'Alain, selon laquelle la démocratie serait « *un effort perpétuel des gouvernés contre les abus de pouvoir* »⁽²⁾. L'histoire politique de la France est émaillée de scandales mettant en jeu l'existence de fichiers occultes. C'est ainsi que l'affaire des fiches a déclenché l'une des plus grandes crises de la Troisième République. Nommé ministre de la guerre en 1900, le général André entreprend de républicaniser l'état-major des armées. Pour ce faire, il fait établir près de 25 000 fiches sur les opinions politiques et religieuses d'officiers. On peut y lire par exemple « *VLM* » pour « *va à la messe* », « *grand avaleur de bon Dieu* », « *rallié à la République, n'en porte pas moins un nom à particule* », « *a qualifié les maçons et les républicains de canailles, de voleurs et de traîtres* », « *vit maritalement avec une femme arabe* » ou encore « *vieille peau fermée à nos idées* ». Dès la révélation de l'existence de ces fiches, en 1904, le général André est contraint de démissionner⁽³⁾.

*

* *

Si l'existence de fichiers suscitait déjà des craintes au début du XX^e siècle, leur utilisation à des fins de crime contre l'humanité au cours de la deuxième guerre mondiale par le régime de Vichy pèse à l'évidence encore très lourd. De plus, même si les fichiers sont désormais utilisés dans un cadre républicain, **les peurs sont amplifiées par l'apparition somme toute récente des méthodes de traitement informatique**. Celles-ci n'ont pas que des inconvénients puisqu'en même temps qu'elles augmentent les possibilités de collecter, traiter et mettre à disposition des policiers et gendarmes une grande quantité de données, elles permettent d'assurer une traçabilité réelle des consultations qui n'existait pas avec les fichiers papiers. Mais, plus fondamentalement, l'informatisation des fichiers de police donne à nombre de nos concitoyens l'impression que prend progressivement vie le système imaginé par Guillaudé. Se développe alors la peur de voir apparaître un État omniscient, capable de croiser toutes les nombreuses informations qu'il récolte à divers titres. Il est exact que l'informatique est à l'origine d'**une mutation qui dépasse de très loin l'accroissement de la quantité des informations enregistrées**. Une société de la surveillance

⁽¹⁾ Olivier Forcade, « *La République, le renseignement et ses fichiers, 1870-1940* », 2007.

⁽²⁾ Alain, *Propos sur les pouvoirs*, Paris, 1930.

⁽³⁾ François Vinde, *L'affaire des fiches (1900-1904) – Chronique d'un scandale, 1989*.

généralisée est en effet techniquement possible en utilisant les multiples « traces » laissées par les individus lors de la plupart des actes de la vie quotidienne, sans même évoquer l'hypothèse d'une généralisation des interconnexions entre fichiers. Certes, il peut sembler paradoxal que les mêmes individus qui utilisent de plus en plus abondamment les possibilités offertes par l'informatique, parfois jusqu'à l'exhibitionnisme, redoublent d'inquiétudes pour le respect de leur vie privée. Cependant, une telle approche négligerait un fait important : **les fichiers de police sont un instrument de pouvoir**, et il n'est pas anodin que l'État collecte et exploite des informations multiples sur les citoyens. Il y a donc bien une différence de nature considérable entre les informations que chacun rend librement publiques sur Internet et les fichiers de données personnelles constitués et exploités par les forces de sécurité. Pour autant, **interdire aux services de police de vivre avec leur temps et d'utiliser les outils d'aujourd'hui pour traquer délinquants et criminels reviendrait à se tirer une balle dans le pied**, alors qu'il appartient à l'État d'assurer la protection des personnes et des biens. La fiche reste en effet au « cœur du métier » des policiers et gendarmes. Rétablir la confiance des citoyens quant à la protection de leurs libertés suppose, non pas que les forces de sécurité soient privées des nouvelles potentialités offertes par l'informatique, mais que des principes extrêmement clairs les encadrent et qu'un contrôle démocratique constant puisse s'exercer.

Ces dernières années, la **multiplication du nombre de fichiers en service**, souvent désignée sous le terme péjoratif de « prolifération », a pu alimenter les craintes de l'opinion publique. Le premier véritable travail de recensement a été réalisé en novembre 2006 à l'occasion du premier rapport du groupe de travail sur les fichiers de police, présidé par M. Alain Bauer. Il a été complété à l'occasion du deuxième rapport de ce même groupe, publié en décembre 2008. Vos rapporteurs ont aussi souhaité procéder à un recensement des 58 fichiers de police, actuellement utilisés ou en cours de création, qu'il a été possible de dénombrer. Le tableau figurant en annexe 1 détaille un certain nombre de caractéristiques de ces derniers, en retenant pour critère principal de classement la nature juridique du texte qui en est à l'origine. Les fichiers à usage de police ont également été retenus dans cet inventaire. Il s'agit de fichiers dont le but premier n'est pas la réalisation d'un travail d'investigation policière, mais pour lesquels des services de police disposent d'un droit d'accès permanent. En pratique, certains d'entre eux sont massivement utilisés, comme le fichier national des immatriculations. L'article 9 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 aéroportuaires a d'ailleurs étendu les possibilités de consultations de ce type de fichiers par les agents des services de police et de la gendarmerie chargés de la prévention et de la répression des actes de terrorisme ⁽¹⁾.

(1) Sous réserve d'une habilitation spéciale, leur sont accessibles, ainsi qu'aux agents des services de renseignement du ministère de la Défense, le fichier national des immatriculations, le système national de gestion des permis de conduire, le système de gestion des cartes d'identité, le système de gestion des passeports, le système de gestion informatisé des dossiers des ressortissants étrangers en France, ainsi que le « fichier des non admis ».

Si l'on s'attache aux **finalités des fichiers de police, plusieurs « familles » principales** peuvent être identifiées.

De nombreux fichiers de police ont un **caractère administratif** et sont destinés à enregistrer des données administratives sur des personnes, des objets ou des moyens de transport. Peuvent être cités par exemple le fichier national des immatriculations (FNI) ou le fichier des propriétaires ou possesseurs d'armes (AGRIPPA). Les fichiers d'identification administrative sont proches de cette catégorie et recensent des populations (fichier relatif à la carte d'identité, fichier relatif aux passeports, fichier de suivi des titres de circulation délivrés aux personnes sans domicile ni résidence fixe, etc.).

La deuxième famille de fichiers de police correspond davantage au « cœur du métier » policier ; il s'agit des **fichiers judiciaires** au sens large. Parmi ceux-ci peuvent être distinguées plusieurs sous catégories :

— les **fichiers à vocation judiciaire** ont pour objet la collecte et la centralisation de renseignements destinés à lutter contre des infractions bien déterminées. Y figurent notamment le fichier des véhicules volés (FVV), le fichier national du faux monnayage (FNFM) ou le fichier des brigades spécialisées (FBS), lequel constitue un outil de travail des offices centraux de police judiciaire ;

— les **fichiers d'antécédents judiciaires** visent à collecter certaines informations extraites des procédures de police judiciaire, avec pour finalité de faciliter la constatation des infractions pénales, le rassemblement des preuves des infractions et la recherche de leurs auteurs. Cette catégorie est constituée par le système de traitement des infractions constatées (STIC), mis en œuvre par la police nationale, et par le système judiciaire de documentation et d'exploitation (JUDEX) de la gendarmerie nationale ;

— les **fichiers d'identification judiciaire**, dont l'objet est l'identification d'un auteur d'infraction ou d'une personne disparue. Ces fichiers ont considérablement bénéficié des avancées scientifiques et informatiques. Leur montée en puissance correspond au développement de la police technique et scientifique afin d'améliorer l'élucidation des crimes et délits. Les exemples les plus connus sont constitués par le fichier automatisé des empreintes digitales (FAED) et par le fichier national des empreintes génétiques (FNAEG).

Les **fichiers de renseignement** forment une catégorie très particulière, puisque ces derniers comprennent par nature des informations sensibles, par exemple lorsqu'ils contribuent à la prévention d'actes de terrorisme, mais aussi parce que certaines des données collectées sont avant tout d'ordre « qualitatif ». De ce fait, les règles relatives à la conservation des données y sont différentes des autres fichiers, le principe retenu étant celui de leur conservation « *pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées* », selon les termes de l'article 6 de la loi n° 78-16 du

6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Ces fichiers existent depuis fort longtemps et relèvent pleinement de la notion de « fichiers de souveraineté ». Certains sont assez peu connus du grand public, comme le fichier alphabétique de renseignement (FAR), tenu sous la forme de fiches papiers par les brigades de gendarmerie. D'autres ont récemment acquis une certaine notoriété, comme EDVIGE (exploitation documentaire et valorisation de l'information générale), qui était destinée à succéder à une partie du fichier des renseignements généraux (FRG). On peut d'ailleurs relever qu'à bien des égards les débats suscités par le décret relatif au fichier EDVIGE ont porté très exactement sur les mêmes points que ceux apparus plus de quinze ans auparavant lors de la publication initiale d'un premier décret portant création du FRG, en 1990, d'ailleurs rapidement retiré pour être réécrit.

Enfin, les progrès de l'informatique autorisent également une meilleure exploitation des informations disponibles par le biais de **rapprochements**. Les systèmes de traitement du renseignement semblent de ce fait appelés à de nouveaux développements. Jusqu'à présent, ils ont été cantonnés à l'identification de crimes ou de délits sériels graves. La gendarmerie a été pionnière en la matière au travers de son logiciel d'analyse criminelle (ANACRIM), qui fonctionne à partir de fichiers temporaires d'investigation criminelle élaborés exclusivement dans le cadre de procédures judiciaires. La police nationale a, pour sa part, conçu le système d'analyse et de liens de la violence associés au crime (SALVAC), mis en œuvre par l'office central de répression des violences aux personnes. Toutefois, l'application de doses plus ou moins prononcées d'intelligence artificielle est également prometteuse pour procéder à des recoupements dans les domaines de la petite et la moyenne délinquance. Des traitements adaptés peuvent contribuer à l'amélioration de la qualité de l'information mise à la disposition des enquêteurs et, partant, du taux d'élucidation. Plusieurs initiatives issues du terrain sont récemment apparues, notamment au sein de la préfecture de police de Paris avec CORAIL (logiciel mis en œuvre par la cellule de rapprochement et d'analyse des infractions liées) et LUPIN (logiciel d'uniformisation des procédures d'identification). Au vu des résultats très encourageants que ces expérimentations permettent d'espérer en termes d'élucidation, un débat sur une adaptation du cadre législatif des fichiers dits sériels est souhaitable.

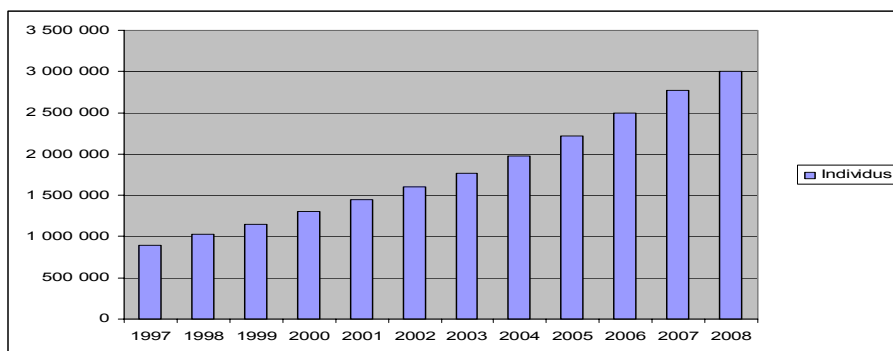
Ce très rapide panorama souligne la grande diversité des fichiers de police. Si une conclusion inquiète en est généralement tirée, une analyse différente est possible. Les fichiers de police peuvent **d'une certaine manière être d'autant plus nombreux qu'ils répondent à des besoins précis et ciblés** et que leurs finalités distinctes sont très encadrées. De fait, leur multitude et leur segmentation mêmes témoignent de l'inexistence d'une forme de « méta fichier » tentaculaire. Le refus d'un fichage de police massif et généralisé ou d'une interconnexion des fichiers suppose nécessairement l'existence d'un certain nombre de fichiers aux finalités spécifiquement définies.

Néanmoins, le sentiment de crainte plus ou moins diffuse d'une partie de l'opinion publique s'appuie aussi sur **l'idée d'une massification du fichage et**

d'une croissance irrépissible du nombre d'individus fichés. De ce point de vue, il est exact que les évolutions récentes se sont traduites par une augmentation sensible du volume de certains fichiers. C'est le cas tout particulièrement du STIC. 3,96 millions de personnes physiques mises en cause y figuraient en 2001. Ce nombre est passé à 5,58 millions au début de 2009, soit une progression du « stock » de près de 41 %. Il convient d'y ajouter 28,33 millions de personnes physiques victimes qui sont également inscrites dans le STIC. La croissance récente des fichiers d'identification judiciaire est également significative. En 1997, 889 755 individus étaient enregistrés dans le FAED ; ils étaient presque trois millions à la fin de 2008. Quant au FNAEG, créé *ex nihilo* par la loi du 17 juin 1998 relative à la répression des infractions sexuelles, il est passé de 2 635 individus inscrits en 2002 à 806 356 à la fin de 2008. L'augmentation du volume de cette base de données, au fonctionnement à vrai dire longtemps chaotique en raison d'un défaut d'anticipation lors de l'extension de son objet, est particulièrement rapide à partir de 2006, année à la fin de laquelle le FNAEG ne comprenait encore que 331 348 profils génétiques d'individus. Sa croissance s'établit donc à 143 % au cours des trois dernières années. Selon un responsable policier auditionné, ce fichier pourrait comprendre trois millions de personnes dans cinq ou six ans. Les graphiques suivants illustrent la croissance du volume des trois fichiers précités⁽¹⁾.

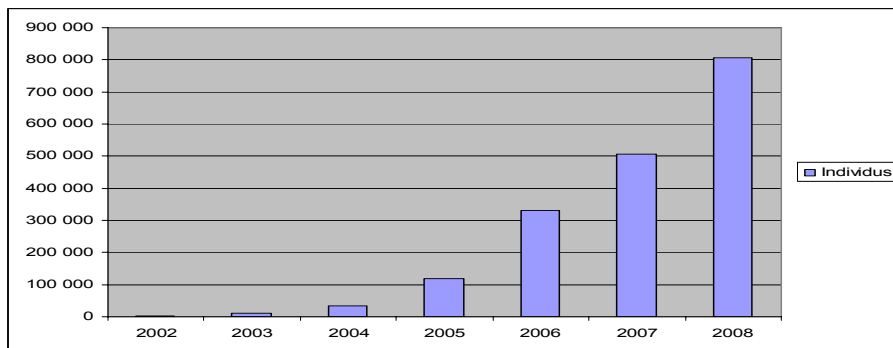
ÉVOLUTION DU VOLUME DES PRINCIPAUX FICHIERS DE POLICE

FICHER AUTOMATISÉ DES EMPREINTES DIGITALES

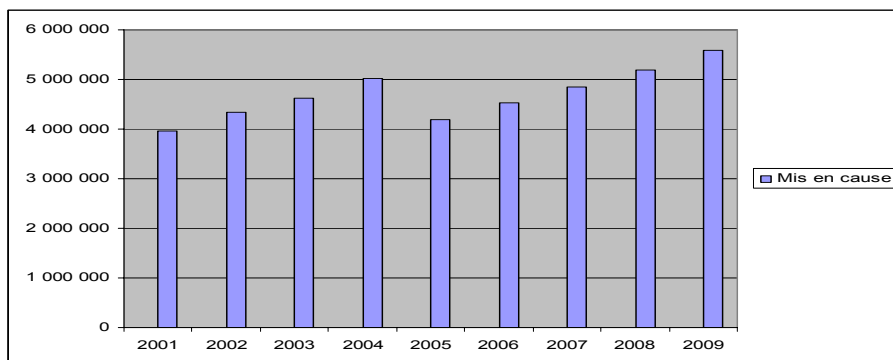


⁽¹⁾ Des données statistiques plus détaillées sur les évolutions quantitatives de ces trois grands fichiers figurent en annexe 2. On se référera tout particulièrement aux précisions méthodologiques relatives au STIC : en effet, les statistiques disponibles ne permettent pas de connaître le nombre d'individus mis en cause chaque année et les chiffres présentés correspondent à la volumétrie globale des mis en cause arrêtée à un instant donné, en l'espèce le 1^{er} janvier de chaque année.

FICHER NATIONAL DES EMPREINTES GÉNÉTIQUES



SYSTÈME DE TRAITEMENT DES INFRACTIONS CONSTATÉES



L'augmentation du nombre de personnes fichées est **un phénomène d'autant moins anodin que l'usage de certains fichiers n'est pas seulement limité à des fins policières**. Les fichiers ont été utilisés dans le passé, de façon peu encadrée, afin de réaliser des « enquêtes de moralité », notamment pour l'accès à certaines professions sensibles, à des emplois publics, à la nationalité française ou pour l'obtention d'habilitations permettant de connaître d'informations classifiées. La loi du 15 novembre 2001 relative à la sécurité quotidienne a explicitement prévu la possibilité d'une consultation des traitements automatisés de données personnelles gérés par les services de police judiciaire ou de gendarmerie dans le cadre de **certaines enquêtes administratives**. La liste de ces dernières a été considérablement allongée par la loi du 18 mars 2003 relative à la sécurité intérieure. La CNIL estime qu'au total ce sont **près d'un million d'emplois qui sont soumis à ce type d'enquête**⁽¹⁾. Sont notamment concernées

⁽¹⁾ Les fichiers d'antécédents judiciaires sont en effet utilisables à des fins d'enquêtes administratives dans les cas suivants : affectations et agréments concernant les emplois publics participant à l'exercice des missions de souveraineté de l'État ; emplois publics ou privés relevant du domaine de la sécurité et de la défense ; emplois privés ou activités privées réglementées relevant des domaines des jeux, paris et courses ; missions

les professions relevant du domaine de la sécurité privée. Or, il s'agit d'un secteur en pleine expansion. La sécurité privée emploie en France 150 000 personnes, à comparer aux 125 000 policiers actifs et aux effectifs de la gendarmerie nationale, soit un peu moins de 100 000 militaires. Des évaluations prospectives estiment, par ailleurs, que dans dix ans les effectifs de la sécurité privée auront doublé et s'établiront à 300 000 emplois ; ils dépasseront alors ceux de la police et de la gendarmerie, qui seront demeurés stables. De fait, **les fichiers d'antécédents judiciaires, et tout particulièrement le STIC, ont fait irruption dans la vie de nombre de nos concitoyens** sous la forme lapidaire d'un courrier administratif de refus d'agrément, expliquant que les mentions dans un traitement automatisé géré par les autorités de police emportent incapacité d'exercer l'emploi désiré. Or, dans bien des cas les faits reprochés ne sont pas forcément si importants qu'ils s'opposent à l'agrément, voire sont erronés ou n'auraient même pas dû figurer dans le fichier si les règles de conservation des données avaient été bien appliquées. Quoi qu'il en soit, la **lourdeur des diverses voies de recours et leur lenteur** font que, pour l'intéressé, la possibilité d'obtenir un emploi est définitivement perdue. L'exigence de bonne tenue des fichiers ne concerne donc plus seulement l'enquêteur, en droit d'attendre une information exacte ; elle est devenue la condition nécessaire d'un égal accès à l'emploi.

L'une des questions désormais posées est donc celle des **limites à ce phénomène de massification du volume des fichiers, notamment s'agissant de ceux destinés à l'identification**. Malgré le champ très large des possibilités de signalement des empreintes digitales ou génétiques, il est probable qu'un « plateau » finira par être atteint dans un délai assez rapproché. Toutefois, les exemples fournis par des États étrangers qui constituent de grandes et anciennes démocraties ne sont pas sans inquiéter sur la tentation d'une extension inconsidérée des bases informatiques d'identification des individus.

*

**

De ce point de vue, **le cas du fichier des empreintes génétiques mis en place au Royaume-Uni** est particulièrement intéressant, non seulement parce qu'il **illustre une politique très différente de celle choisie en France**, mais aussi parce qu'il est souvent présenté comme une préfiguration des évolutions à venir ⁽¹⁾.

Créée par une loi de 1994, la *National DNA Database* a atteint les 4 millions de profils d'individus enregistrés à la fin de 2006, et elle croît d'environ 30 000 profils par mois. La NDNAD constitue ainsi la plus importante base de

concernant les zones protégées en raison des activités qui s'y exercent et missions concernant les matériels, produits ou activités présentant un danger pour la sécurité publique.

⁽¹⁾ Afin de disposer d'éléments de comparaison, vos rapporteurs ont souhaité interroger certains postes diplomatiques sur les politiques menées en matière de fichiers de police. Les réponses apportées par les ambassades de France au Royaume-Uni et aux Pays-Bas, très denses et intéressantes, sont reproduites in extenso en annexe 3 et 4.

donnée d'empreintes génétiques au monde, tant en valeur absolue que rapportée à la population : ce taux atteint désormais **7,4 % de la population britannique, contre 1,25 % en France**⁽¹⁾. On relèvera que cette disproportion se manifeste également, quoique de façon moins connue, s'agissant des empreintes digitales : le *National Automated Fingerprint Information System* (NAFIS) comprenait 7,1 millions d'individus en 2007, soit près de 12 % de la population du royaume (4,7 % en France). **Le choix britannique a été de recueillir de manière aussi large que possible les empreintes génétiques.** Le *Criminal Justice Act* de 2003 a ainsi donné des pouvoirs supplémentaires à la police en vue de la collecte de prélèvements biologiques sans le consentement des personnes, lesquels sont désormais possibles sur tous les individus arrêtés pour une infraction susceptible de faire l'objet d'un enregistrement dans un fichier de police (*recordable offence*), quelles que soient les suites judiciaires données à l'affaire. Le champ couvert par ces infractions est ainsi particulièrement large. On peut, en outre, rappeler que **les garanties d'exactitude des données sont bien moins exigeantes** dans le cas de la NDNAD que dans celui du FNAEG. Les données figurant dans le fichier français font systématiquement l'objet d'une double saisie (contre un quart de double saisie des analyses, réalisées de manière aléatoire, au Royaume-Uni) et les prélèvements biologiques eux-mêmes sont conservés. Quant à la durée de conservation des données, elle peut s'étendre au Royaume-Uni jusqu'au centième anniversaire de la personne ayant fait l'objet d'un prélèvement biologique. On notera enfin que **la taille du NDNAD n'est pas sans incidence sur son coût**, le contribuable britannique ayant dépensé à ce titre près de 300 millions de livres au cours des cinq dernières années.

La **collecte de données sensibles** fait certes l'objet de perceptions très différentes en France et au Royaume-Uni. En témoigne notamment le degré pour le moins étonnant de détails exigés s'agissant des caractéristiques ethno-raciales, de la religion ou de l'orientation sexuelle, à l'occasion d'une simple candidature à un emploi dans la police. Une copie du formulaire à remplir à cet effet figure en annexe 5. Malgré tout, **face à l'extension considérable des pouvoirs confiés à la police, les mentalités évoluent au Royaume-Uni et des craintes commencent à contrebalancer sérieusement les bénéfices supposés d'un fichage très étendu.** À l'occasion de la présentation d'un projet de mise en place d'une nouvelle base de donnée informatisée du *National Health Service*, le ministre de la santé publique a indiqué que le but poursuivi à long terme était d'y inscrire les profils génétiques de l'ensemble de la population. Le coût estimé du projet, dont le déploiement est prévu à partir de 2012, représenterait 12 milliards de livres. La concomitance de cette annonce avec la discussion d'un projet de loi (*Coroners and Justice Bill*) comprenant des modifications de la loi sur la protection des données et permettant un élargissement très sensible des possibilités d'échanges d'informations a fait craindre à certaines organisations de défense des libertés la

(¹) La base de données génétique CODIS gérée par le FBI représente seulement 0,5 % de la population des États-Unis.

mise en place d'une sorte de fichier d'identification généralisé accessible aux forces de police ⁽¹⁾.

Un récent rapport de la Chambre des Lords, intitulé *Surveillance : les citoyens et l'État* ⁽²⁾, a estimé que l'accroissement des pratiques de surveillance, tant publiques que privées, « représente l'un des changements les plus significatifs dans la vie de la nation depuis la fin de Deuxième Guerre mondiale ». Il y est ainsi relevé que la généralisation de la surveillance, devenue massive et routinière, exerce une influence puissante sur la nature des relations entre l'État et les citoyens.

Parmi les 44 propositions du rapport figure la modification du cadre législatif du NDNAD, de manière à limiter les inscriptions dans ce fichier aux cas pour lesquels cela est vraiment justifié. Il s'agit notamment de tenir compte à cette occasion de **l'arrêt de la Cour européenne des droits de l'homme du 4 décembre 2008** (affaire *S. et Marper c. Royaume-Uni*), condamnant le royaume pour violation de l'article 8 de la Convention européenne des droits de l'Homme ⁽³⁾. La Cour a en effet observé que « la protection offerte par l'article 8 de la Convention serait affaiblie de manière inacceptable si l'usage des techniques scientifiques modernes dans le système de la justice pénale était autorisé à n'importe quel prix et sans une mise en balance attentive des avantages pouvant résulter d'un large recours à ces techniques, d'une part, et des intérêts essentiels s'attachant à la protection de la vie privée, d'autre part ». Les circonstances des affaires en question méritent d'être rappelées. Le premier requérant avait été arrêté en 2001, à l'âge de onze ans, pour une tentative de vol avec violence. Il fut par la suite acquitté. Le second, arrêté et inculpé de harcèlement à l'égard de sa compagne, bénéficia par la suite d'un classement sans suite pour retrait de plainte (il s'était entre-temps réconcilié avec l'intéressée). Dans les deux cas, leurs demandes de retrait de leurs empreintes digitales et biologiques des fichiers furent refusées. La Cour a considéré « que le caractère général et indifférencié du pouvoir de conservation des empreintes digitales, échantillons biologiques et profils ADN des personnes soupçonnées d'avoir commis des infractions mais non condamnées, tel qu'il a été appliqué aux requérants en l'espèce, ne traduit pas un juste équilibre entre les intérêts publics et privés concurrents en jeu, et que l'État défendeur a outrepassé toute marge d'appréciation acceptable en la matière. Dès lors, la conservation litigieuse s'analyse en une atteinte disproportionnée au droit des requérants au respect de leur vie privée et ne peut passer pour nécessaire dans une société démocratique. » Après que le Gouvernement britannique eut déclaré être « déçu » par la décision de la Cour, le 16 décembre 2008 le ministre de l'Intérieur a indiqué que le

⁽¹⁾ Data Bill « will wipe out privacy at a stroke », *The Independent*, 27 janvier 2009; Data-sharing Bill will build national DNA database in NHS, *GeneWatch press release*, janvier 2009.

⁽²⁾ Surveillance : Citizens and the State, *Select Committee on the Constitution*, 6 février 2009.

⁽³⁾ « 1. Toute personne a droit au respect de sa vie privée (...)

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire (...) à la défense de l'ordre et à la prévention des infractions pénales (...). »

Gouvernement entamait les travaux sur un Livre blanc sur les preuves médico-légales, qui traiterait notamment de la question des délais de conservation des données collectées dans le NDNAD.

*

* *

L'ampleur prise par les activités policières de surveillance et de fichage au **Royaume-Uni est parfois perçue comme un « modèle », positif ou négatif selon les opinions**, mais dont la transposition en France serait en tout état de cause inéluctable. Jusqu'à présent, cette crainte paraît injustifiée ; encore faut-il qu'un choix soit pleinement explicité pour l'avenir. Force est de constater, sur un plan pratique, que c'est précisément **l'antériorité de l'expérience britannique** en matière d'empreintes génétiques qui **a permis à la France d'éviter un certain nombre de dérives**, en mettant en place un dispositif à la fois plus proportionné aux finalités poursuivies et plus sûr s'agissant de l'exactitude des informations collectées. Il faut toutefois **rester attentif** à des évolutions qui peuvent parfois présenter de grandes similarités. La question de la finalité du traitement automatisé centralisé destiné à archiver les empreintes digitales relevées pour l'établissement la future carte d'identité « biométrique » méritera à cet égard un débat des plus approfondis à l'occasion de l'examen du futur projet de loi relatif à la protection de l'identité. Un tel traitement pourrait en effet contenir des données relatives à la presque totalité de la population, ce qui pose naturellement la question de son utilisation éventuelle pour d'autres usages que la simple authentification des documents d'identité.

Plus largement, la conception de la protection des libertés publiques et individuelles diffère entre les deux nations. L'histoire des fichiers de police et de leur contrôle est marquée en France par une très grande méfiance vis-à-vis de l'État. On sait combien la loi de 1978, relative à l'informatique, aux fichiers et aux libertés, doit au trouble engendré par la révélation en 1974 de l'existence d'un projet dit SAFARI (système automatisé pour les fichiers administratifs et le répertoire des individus) ⁽¹⁾. De cette idée d'une identification individuelle des 52 millions de Français d'alors, il est paradoxalement résulté l'instauration d'un système de contrôle des données personnelles à l'époque très en avance sur le reste de l'Europe, et qui a largement fait école. L'actualité plus récente liée au fichier EDVIGE montre que cette vigilance n'a pas diminué, loin s'en faut.

Mais, l'honnêteté commande également de relever qu'il existe aussi **une véritable différence de conception du rôle du fichier entre les policiers français et leurs homologues anglo-saxons**. On ne peut véritablement parler d'une « doctrine française » en la matière, dans la mesure où elle n'a malheureusement pas été exprimée jusqu'ici avec la clarté et la publicité nécessaires, mais c'est tout de même bien de cela dont il s'agit au fond. Jusqu'à

(1) Safari ou la chasse aux Français, *Philippe Boucher*, Le Monde, 21 mars 1974.

présent, un certain empirisme a occupé une place déterminante dans la mise en service de fichiers de police en France ; la création d'un fichier ayant toujours procédé d'un besoin concret, il serait illusoire de penser que toute forme d'empirisme pourrait disparaître dans ce domaine à l'avenir, tant au regard de l'évolution de la délinquance que des technologies. En revanche, notre pays aurait tout à gagner à la formalisation d'une doctrine française en matière de fichiers de police, s'appuyant tant sur des principes clairs s'agissant de protection des libertés que sur une certaine conception du savoir faire policier, où l'utilité et la nécessité du fichier informatique sont assumées avec la claire conviction que la machine ne remplacera jamais l'enquêteur. L'affirmation d'un tel choix stratégique permettrait certainement de rassurer les citoyens, et ainsi de sortir d'une situation où les craintes sont d'autant plus fortes qu'il y a un déficit de transparence, le plus souvent faute de débat démocratique. L'absence d'une telle clarification s'avère finalement nuisible pour la performance des outils dont disposent les policiers et les gendarmes, ainsi que pour la confiance que doivent avoir les citoyens dans leurs forces de sécurité.

Pour reprendre l'expression d'un responsable d'un service de renseignement entendu par les rapporteurs, dans bien des domaines « *les États-Unis font du chalut, et nous du harpon* ». Cette observation s'applique de manière assez générale au rôle assigné aux fichiers de police dans le monde anglo-saxon, où des outils très performants de connaissance approfondie du milieu criminel et de ses évolutions sont mis en œuvre, notamment à des fins statistiques et d'analyse stratégique. Mais les moyens considérables, financiers comme humains, qui sont consacrés dans ce pays à ce genre d'instruments ne constituent pas pour autant la garantie d'un meilleur taux d'élucidation. La *Serious Organized Crime Agency* (SOCA) britannique dispose ainsi, semble-t-il, d'une vision d'une très grande qualité s'agissant de l'organisation et des caractéristiques des trafics de drogues ; cela n'empêche pas la situation du Royaume-Uni dans ce domaine d'être sensiblement plus dégradée que celle de la France, tout particulièrement en ce qui concerne l'héroïne et les drogues de synthèses.

De la même façon qu'en matière de renseignement la France a misé sur la qualité du renseignement humain, en matière de fichiers de police **l'approche française** se traduit dans l'ensemble par la volonté de **disposer d'outils aussi opérationnels que possible et offrant une véritable plus-value pour l'enquêteur**. L'émergence de nouveaux fichiers de rapprochement, conçus le plus souvent par les utilisateurs eux-mêmes, confirme largement cette tendance profonde. De fait, la prise en compte des besoins conduit à limiter le champ des informations retenues et utilisées à celles véritablement utiles, et permet de s'orienter vers des instruments ciblés, respectant une proportionnalité avec les fins poursuivies. C'est ce caractère essentiel qu'il convient de souligner et d'utiliser comme critère de sélection des fichiers à créer : l'enquêteur doit toujours avoir la maîtrise de l'outil, ce dernier étant à son service, et l'ordinateur n'a pas vocation à remplacer le policier. De ce point de vue, la masse des informations collectées importe autant, si ce n'est moins, que leur nature, la taille d'une base de données ne pouvant être en soi un critère d'efficacité.

Ces fins ne doivent pas être perdues de vue dans les débats sur les fichiers de police : il s'agit en effet de la capacité des forces de sécurité républicaines à faire face efficacement à la délinquance et à la criminalité, ainsi qu'à leurs évolutions. Aussi vos rapporteurs partagent-ils la conviction manifestée par l'ensemble des policiers et gendarmes rencontrés : **« nous avons besoin de fichiers efficaces. »** De fait, le débat sur les fichiers de police est lié à celui sur les moyens dont sont dotées les forces de sécurité intérieure.

*

* *

De ce point de vue, **les principes posés par la loi de 1978 n'ont pas vieilli.** Les données collectées dans les traitements automatisés doivent l'être *« pour des finalités déterminées, explicites et légitimes »* ; elles doivent être *« adéquates, pertinentes et non excessives »* au regard de ces finalités, tout en étant *« exactes complètes et, si nécessaire, mises à jour »* ; enfin, elles doivent être conservées *« pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées »*.

C'est à l'aune de ces principes que vos rapporteurs ont souhaité **examiner comment « vivent » très concrètement les fichiers de police, de leur naissance à leur éventuelle disparition.** En effectuant ce travail, ils ont acquis la conviction profonde que la fiabilité et la performance des outils dont disposent les policiers et les gendarmes sont indissociables de la meilleure protection des données personnelles et des libertés des citoyens. Ces deux aspects d'un même problème vont de pair, contrairement à certaines idées reçues. Vos rapporteurs ont également attaché une importance toute particulière aux déplacements au sein des services mettant en œuvre ou contrôlant ces fichiers, afin de rencontrer dans leur activité quotidienne les personnels chargés de ces tâches. Cette démarche pragmatique leur a permis de mieux appréhender des situations qui peuvent au premier abord sembler fort prosaïques, mais dont la connaissance permet en fait de ne pas s'enfermer dans un débat par trop théorique, au risque de simplifier exagérément une réalité très complexe. Vos rapporteurs ont délibérément choisi de ne pas adopter une approche descriptive et exhaustive de l'ensemble des fichiers de police ou à usage de police, certains de ces derniers, notamment en matière de politique d'immigration, nécessitant sans doute un travail spécifique à eux seuls ; au contraire, ils ont préféré retenir les exemples les plus révélateurs du fonctionnement ou des dysfonctionnements de tel ou tel fichier, ou type de fichiers, pour faire ressortir des questions saillantes et apporter des **propositions adaptées et pragmatiques d'amélioration des outils et des garanties.**

Au terme de cette mission d'information de six mois, vos rapporteurs considèrent que la République a de nombreux défis à relever s'agissant des fichiers de police. Certes, ils ont pu s'assurer que, pour l'essentiel, dans leurs principes constitutifs, ces fichiers respectent les libertés fondamentales. Mais, en pratique, la situation actuelle est loin d'être satisfaisante. La défaillance,

l'inexactitude, les dysfonctionnements dans la gestion de certains fichiers ont une incidence réelle et préjudiciable pour certains citoyens. Les garanties de contrôles, prévues par les textes, sont en réalité faibles et ne sont pas à la hauteur de ce que l'on est en droit d'attendre d'une grande démocratie. De plus, les fichiers et outils informatiques les plus utilisés quotidiennement par les policiers et gendarmes ne sont pas toujours performants et reposent parfois sur des technologies obsolètes. C'est pourquoi vos rapporteurs appellent de leurs vœux une refonte du cadre juridique régissant la création et le fonctionnement des fichiers de police, ainsi qu'un effort soutenu de modernisation technique.

I. CLARIFIER LE CADRE JURIDIQUE

La protection des données à caractère personnel fait partie intégrante des libertés et droits fondamentaux reconnus à chaque citoyen. À cet égard, si la répression et la poursuite des infractions pénales ainsi que le maintien de l'ordre public sont des objectifs légitimes, justifiant l'existence des fichiers de police et d'un régime juridique dérogatoire emportant restrictions et limites au droit commun des fichiers, ils ne peuvent cependant pas permettre d'écarter tout encadrement juridique réel de ces fichiers.

En effet, l'obligation de respecter le principe de proportionnalité s'applique à toute mesure restreignant le droit au respect de la vie privée, tel qu'il est protégé par l'article 8⁽¹⁾ de la Convention de sauvegarde des Droits de l'Homme et des libertés fondamentales. Cette exigence implique une législation, qui, d'une part, soit suffisamment claire dans la définition des circonstances, de l'étendue et des modalités d'exercice des mesures limitant les droits fondamentaux, et qui, d'autre part, n'apporte que les restrictions strictement nécessaires à l'exercice de ces droits.

C'est pourquoi la France a adopté, dès la fin des années 1970, une loi fondatrice⁽²⁾, pierre angulaire de la protection des citoyens face aux traitements de données à caractère personnel. Or, ce cadre juridique national a devancé la mise en place de règles au niveau international. En effet, il faudra attendre les années 1980 pour que, par crainte que les législations nationales n'entravent la libre circulation des données, se dessinent les contours d'une législation européenne voire internationale en la matière. Aujourd'hui, ce cadre juridique européen et international a enrichi le droit interne de la protection des données, l'obligeant notamment à se conformer aux divers accords internationaux.

A. LES GRANDS PRINCIPES PRÉSIDENT À LA CRÉATION DES FICHIERS DE POLICE

Les conditions de création et de fonctionnement des fichiers de police s'inscrivent aujourd'hui dans un **cadre juridique complet qui, défini au niveau international et européen, prend tout son sens au niveau national**, où il trouve, dans la loi du 6 janvier 1978, ses prolongements naturels.

⁽¹⁾ **Article 8 : Droit au respect de la vie privée et familiale**

1- Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2- Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

⁽²⁾ Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

1. Le cadre juridique international et européen

Nombreux sont les textes internationaux, qui prévoient des dispositions spécifiques aux fichiers de police. L'article 55 de la Constitution du 4 octobre 1958 consacrant la primauté des traités et accords internationaux sur le droit national, **les textes internationaux définissant le cadre juridique des fichiers de police s'imposent en droit interne.**

a) Les textes de protection de l'Union européenne

• **Directive européenne 95/46/CE du 24 octobre 1995 sur la protection des données à caractère personnel et à la libre circulation de ces données**

Si l'échange d'informations est au cœur de la coopération policière européenne, le cadre juridique européen s'est longtemps désintéressé de cette question. En effet, la directive européenne du 24 octobre 1995 définit les règles applicables en matière de protection des données à caractère personnel **uniquement pour les bases de données relevant du premier pilier** ⁽¹⁾. Ainsi, l'article 3 de la dite directive dispose que la présente directive ne s'applique pas aux données personnelles échangées dans le cadre du 3^e pilier : « *La présente directive ne s'applique pas au traitement de données à caractère personnel mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal.* »

• **Traité de Prüm du 27 mai 1995**

Le Traité de Prüm a été signé le 27 mai 2005 entre sept états membres ⁽²⁾ de l'Union Européenne. Il renforce la coopération entre États, afin de lutter contre le terrorisme, la criminalité transfrontalière et l'immigration illégale. Établi à l'origine en dehors du cadre des Traités de l'Union Européenne, ce traité prévoit **l'échange de données génétiques, d'empreintes digitales et de données à caractère personnel.**

Le Traité de Prüm a constitué une nouvelle étape dans la coopération judiciaire et policière en facilitant, dans un but répressif, la consultation des bases de données de profils ADN de chaque État partie au Traité. En outre, dans un but préventif et répressif, il permet la consultation des bases de données

⁽¹⁾ Le pilier communautaire correspond aux trois communautés : la Communauté européenne, la Communauté européenne de l'énergie atomique (EURATOM) et l'ancienne Communauté européenne du charbon et de l'acier (CECA) (premier pilier). Le second pilier est consacré à la politique étrangère et de sécurité commune, couverte par le titre V du traité sur l'Union européenne, alors que le troisième pilier est consacré à la coopération policière et judiciaire en matière pénale, qui est couverte par le titre VI du traité sur l'Union européenne.

⁽²⁾ La Belgique, l'Allemagne, l'Espagne, la France, le Luxembourg, les Pays-Bas et l'Autriche.

dactyloscopiques (empreintes digitales), ainsi que de données figurant dans les registres d'immatriculation des véhicules de chaque État signataire.

L'approfondissement de la coopération policière et judiciaire en matière pénale va de pair avec le respect des droits fondamentaux, en particulier le droit au respect de la vie privée et le droit à la protection des données à caractère personnel. C'est pourquoi, l'intensification des échanges de données rendue possible par le Traité de Prüm s'accompagne de la **définition de règles relatives à la protection des données personnelles des individus**. Il convient toutefois de souligner qu'il n'est procédé à aucun transfert direct de données entre les pays signataires. Seule une procédure de consultation des données est mise en place. Cet échange d'informations repose sur un système de concordance / non-concordance (plus communément appelé « *hit – no hit* »), permettant dans un premier temps de comparer des profils anonymisés ⁽¹⁾.

En tout état de cause, ce traité impose aux États signataires de **garantir un niveau minimal de protection avant de mettre en œuvre les échanges de données**. L'article 34 se réfère précisément à la Convention du Conseil de l'Europe du 28 janvier 1981, à son protocole additionnel du 8 novembre 2001 et à la Recommandation n° R (87) 15 du Comité des ministres du Conseil de l'Europe aux États membres relative à l'utilisation de données à caractère personnel dans le domaine policier. Les dispositions du Traité de Prüm rappellent les principes fondamentaux en matière de protection des données, à savoir : la finalité du traitement des données, l'exactitude des données, la mise à jour des données, la mise en place de sécurités informatiques, la traçabilité des consultations.

• **Décision-cadre relative à la protection des données personnelles du 27 novembre 2008**

La décision-cadre relative à la protection des données personnelles du 27 novembre 2008 est venue définir, à l'échelle européenne, les **règles juridiques relatives aux fichiers de police et aux échanges d'informations dans le cadre du troisième pilier**, à savoir la coopération policière et judiciaire en matière pénale. Le cadre juridique ainsi établi reste cependant minimaliste dans la mesure où cette décision-cadre ne porte que sur les données à caractère personnel qui « *sont ou ont été transmises ou mises à disposition entre les États membres* » (article premier), ou entre systèmes d'informations européens et États membres. Sont expressément exclus les « *intérêts essentiels en matière de sécurité nationale et des activités de renseignement spécifiques dans le domaine de la sécurité nationale* ».

• **Charte européenne des droits fondamentaux du 7 décembre 2000**

Adoptée à l'occasion du traité de Nice, la **Charte européenne des droits fondamentaux a consacré le droit à la protection des données à caractère**

(1) Pour une présentation plus détaillée du fonctionnement des échanges de données dans le cadre du Traité de Prüm, se reporter à la page 172.

personnel comme valeur fondamentale de l'Union Européenne. Son article 7 précise, en effet, que : « *Toute personne a droit à la protection des données à caractère personnel la concernant. Les données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. Le respect de ces règles est soumis au contrôle d'une autorité indépendante* ». La Charte n'est pour le moment pas contraignante, bien qu'elle soit régulièrement citée en référence par les institutions de l'Union européenne. Si le Traité de Lisbonne venait à être ratifié par l'ensemble des États membres de l'Union européenne, la Charte européenne des droits fondamentaux aurait alors une valeur juridique contraignante pour les États.

• Les accords de Schengen

Les accords de Schengen du 14 juin 1985⁽¹⁾ et du 19 juin 1990⁽²⁾ ont pour objet la suppression des contrôles de personne aux frontières communes entre ces États et le renforcement de la coopération policière, douanière et judiciaire, ce qui entraîne le report des contrôles aux frontières extérieures, avec définition des conditions de leur franchissement, harmonisation des conditions d'entrée et de visas pour les courts séjours et surveillance de l'immigration clandestine.

L'échange d'informations étant à la base du renforcement de la coopération policière, douanière et judiciaire, **la « clef de voûte » de ces accords a été la création du Système d'Information Schengen (SIS), fichier de police comportant des signalements, notamment d'étrangers.** L'importance du SIS se reflète, en outre, dans la place qu'il occupe dans la convention d'application de l'accord Schengen⁽³⁾.

Le chapitre III du titre consacré au SIS fixe les **règles relatives à la protection des données à caractère personnel** applicables à ce système. Les États sont en effet tenus par un certain nombre d'obligations : respecter la finalité du fichier et ne pas utiliser les données à des fins administratives (article 102), assurer la sécurité des données en empêchant l'accès au système de personnes non autorisées. Il convient de noter que, contrairement à l'interdiction posée dans la Convention de Schengen, l'accès aux données Schengen est désormais effectif pour Europol⁽⁴⁾ et Eurojust⁽¹⁾. Les données doivent être exactes et actuelles. Leur

⁽¹⁾ Accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique Bénélux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes.

⁽²⁾ Convention d'application de l'accord Schengen signée le 19 juin 1990. La Convention est entrée en application le 26 mars 1995 entre sept États parties (les cinq pays fondateurs ainsi que l'Espagne et le Portugal).

⁽³⁾ Son titre IV lui est consacré ; il se compose de 28 articles sur un total de 142.

⁽⁴⁾ Europol est un organe de coopération entre les services policiers et douaniers des États membres. Le projet d'un Office européen de police a été évoqué dès le Conseil européen de Luxembourg (juin 1991). Prévu par le traité de Maastricht, l'Office a démarré ses activités en janvier 1994 sous le nom de « Unité Drogues Europol ».

intégration dans le fichier doit être licite, sous peine d'engager la responsabilité de l'État signalant (article 105).

Les données introduites par un État signalant ne peuvent être modifiées, complétées, rectifiées ou effacées que par lui. Mais l'État non signalant doit, s'il constate une erreur, en informer sans délai l'État signalant. En application de l'article 114 de la Convention de Schengen, **chaque État doit désigner une autorité de contrôle chargée d'exercer un contrôle indépendant du SIS pour sa partie nationale**. Cette autorité de contrôle s'assure notamment que les données intégrées sur la partie nationale du SIS ne sont pas attentatoires aux droits de la personne concernée.

La convention de Schengen a également prévu la création d'une autorité de contrôle commune (ACC), aux différents États membres, composée de deux représentants de chaque autorité nationale. Depuis une décision du Conseil du 10 juillet 1999, l'autorité de contrôle commune a été rattachée au secrétariat général du Conseil de l'Union européenne. Son rôle reste aussi difficile que restreint. Le 18 décembre 2007, M. Georges de la Loyère, commissaire de la CNIL, a été élu président de l'ACC Schengen pour deux ans.

• La Convention Europol du 26 juillet 1995

Europol a été créé par un acte du Conseil en date du 26 juillet 1995 portant établissement de la convention portant création d'un Office européen de police, dite « *convention Europol* ». Le champ de compétence d'Europol, déterminé par sa convention, a été considérablement étendu depuis sa création par trois protocoles et couvre désormais l'ensemble de la criminalité transnationale organisée.

L'intervention d'Europol est soumise à deux conditions : que deux États membres au moins soient affectés et qu'une organisation criminelle soit impliquée. Son rôle est essentiellement un rôle d'assemblage et d'analyse d'informations, raison pour laquelle a été créé **un système d'information Europol accessible aux agents des États habilités, ainsi qu'aux officiers de liaison et agents d'Europol**.

Une **autorité de contrôle indépendante**, composée de représentants de chacune des autorités de contrôle nationales chargées de la protection des données personnelles, s'assure du respect par Europol des dispositions de la Convention sur la protection des données.

L'autorité de contrôle commune d'Europol est chargée d'examiner les instructions de création de fichiers, les dispositions relatives à l'établissement de rapports sur les demandes concernant des données à caractère personnel, les règles

(¹) *Institué par une décision du Conseil en 2002, Eurojust est l'organe chargé de renforcer la lutte contre les formes graves de criminalité par le biais d'une coopération judiciaire plus étroite au sein de l'Union européenne.*

générales pour la transmission par Europol de données à caractère personnel à des États et instances tiers.

Pouvant être saisie par toute personne, elle doit également surveiller **l'exercice du droit d'information** prévu à l'article 24, paragraphe 3 de la Convention Europol, et examiner, à la demande de toute personne concernée, si les éventuels collecte, stockage, traitement et utilisation de données à caractère personnel la concernant ont été effectués au sein d'Europol de façon licite et correcte.

Le titre IV de la Convention Europol, intitulé « *Dispositions communes relatives au traitement de l'information* » fixe les **règles relatives à la protection des données à caractère personnel** applicables au système d'information Europol. Les États sont en effet tenus de respecter un certain nombre d'obligations. L'article 14 dispose que les États membres doivent assurer en droit interne **un niveau de protection des données** à caractère personnel « *correspondant au moins à celui qui résulte de l'application des principes de la Convention du Conseil de l'Europe du 28 janvier 1981 et tient compte de cet égard de la recommandation R (87) 15 du Comité des ministres du Conseil de l'Europe, du 17 septembre 1987, sur l'utilisation des données à caractère personnel par la police* ». À l'instar du niveau de protection des données exigé des États membres, Europol doit, lors de la collecte, du traitement et de l'utilisation de données à caractère personnel, respecter « *les principes de la convention du Conseil de l'Europe du 28 janvier 1981, et de la recommandation R (87) 15 du Comité des ministres du Conseil de l'Europe du 17 septembre 1987* ».

L'article 15 établit un régime dual de responsabilité en matière de protection des données, qui couvre « *le caractère licite de la collecte, de la transmission à Europol et de l'introduction ainsi que l'exactitude, l'actualité des données et le contrôle des délais de conservation* ». Alors que les États membres sont responsables des données qu'ils ont introduites ou transmis, Europol est responsable des données qui lui ont été transmises par des tiers ou qui résultent des travaux d'analyse d'Europol. Aux termes de l'article 21 de la Convention, les données ne doivent être conservées que le temps nécessaire pour permettre à Europol de remplir ses fonctions. La nécessité de continuer à conserver les données doit être examinée au plus tard trois ans après leur introduction.

Aux termes de l'article 17 de la Convention, les États ont également **une obligation de respecter la finalité du système d'information d'Europol**. Ainsi, les données à caractère personnel ne peuvent être utilisées ou transmises « *que par les services compétents des États membres pour prévenir et lutter contre la criminalité relevant de la compétence d'Europol et contre les autres formes graves de criminalité* ».

b) Les autres instruments internationaux

• Les textes du Conseil de l'Europe

Le Conseil de l'Europe s'est doté d'un ensemble de textes en matière de protection des personnes à l'égard des fichiers automatisés.

La Convention STE 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ⁽¹⁾ a constitué, à l'échelle européenne, **le premier instrument international contraignant**, ayant pour double objectif d'une part de protéger les personnes contre l'usage abusif du traitement automatisé des données à caractère personnel et, d'autre part, de réglementer les flux transfrontaliers des données. Cette Convention prévoit plusieurs garanties en matière de traitement des données à caractère personnel. D'une part, **elle proscrie le traitement des données « sensibles »** relatives à l'origine raciale, aux opinions politiques, à la santé, à la religion, à la vie sexuelle et aux condamnations pénales en l'absence de garanties offertes en droit interne. La Convention garantit d'autre part **le droit des personnes concernées de connaître les informations stockées à leur sujet** et d'exiger le cas échéant des rectifications, sauf lorsque les intérêts majeurs de l'État (sécurité publique, défense, etc.) sont en jeu. La Convention impose enfin des restrictions aux flux transfrontaliers de données dans les États où n'existe aucune protection équivalente.

Adoptée en application de la Convention n° 108, **la Recommandation R. (87) 15 du Comité des ministres du Conseil de l'Europe** ⁽²⁾ fait partie intégrante des règles encadrant l'exploitation des fichiers de police que la France s'est engagée à respecter dans le cadre des accords internationaux la liant à ses partenaires de l'Union Européenne. Aux termes de ce texte, **la création, l'organisation et les conditions de fonctionnement des fichiers de police relèvent de la loi**, qui doit définir avec précision l'étendue et les modalités d'exercice du pouvoir des services de police. La Cour européenne des droits de l'homme a rappelé dans un arrêt en date du 16 février 2000 (*Amman contre Suisse*) que les **dispositions législatives** doivent être **suffisamment claires et détaillées** pour assurer une protection adéquate contre les ingérences des autorités dans le droit du citoyen à sa vie privée. Ainsi, non seulement les fichiers doivent être encadrés par des textes, mais en outre ces textes doivent présenter une certaine qualité que la CEDH se réserve la possibilité de contrôler.

Par ailleurs, **le principe de respect des finalités des fichiers est un principe fondamental**, y compris pour des fichiers de police. L'article 5.2.i de la Recommandation précise que l'utilisation d'un fichier de police à des fins autres que la prévention et la répression des infractions pénales et le maintien de l'ordre public ne devrait être possible que dans des cas déterminés et sous certaines

⁽¹⁾ Entrée en vigueur le 1^{er} octobre 1985.

⁽²⁾ Recommandation R. (87) 15 du 17 septembre 1987 du Comité des ministres du Conseil de l'Europe concernant l'utilisation des données à caractère personnel dans le secteur de la police.

conditions. La CNIL s'était d'ailleurs, dans un premier temps ⁽¹⁾, opposée à toute consultation d'un fichier de police judiciaire à l'occasion des enquêtes dites de moralité. En outre, les données ne peuvent être communiquées à d'autres services de police, que s'il existe un intérêt légitime à cette communication (article 5.1 de la Recommandation). Ce principe exclut le croisement sans conditions et sans réserves des différents fichiers de police.

Si la Recommandation dispose qu'il doit être veillé à **l'exactitude et à la fiabilité des données** (articles 5.5.ii et 7.2 de la Recommandation), les données doivent également être différenciées en fonction de leur degré d'exactitude ou de fiabilité. Les données fondées sur des faits doivent ainsi être différenciées de celles fondées sur des opinions ou appréciations personnelles. En outre, **les données collectées à des fins administratives doivent faire l'objet d'un enregistrement distinct dans un fichier séparé** et les États doivent prendre toutes les mesures nécessaires pour que les données administratives ne soient pas soumises aux règles applicables aux fichiers de police.

S'agissant de la **communication des données**, celle-ci ne peut s'effectuer qu'après vérification de la qualité des données et l'indication au destinataire du degré de fiabilité et d'exactitude des données. Enfin, l'ingérence de la police dans les droits de l'individu doit pouvoir être **contrôlée par une autorité indépendante** (articles 6.1, 6.6 et 7.2. de la Recommandation) et en dernier recours par le pouvoir judiciaire.

La Recommandation R. (87) 15 constitue donc le prisme au travers duquel la Cour européenne des droits de l'homme examine les dispositions législatives nationales en matière de fichiers de police, notamment lorsqu'elle est saisie de recours relatifs à l'examen du respect du principe de proportionnalité entre l'atteinte portée aux principes essentiels en matière de protection des données et le but légitime poursuivi.

Cette Recommandation a été ratifiée par la France le 24 mars 1983 et a fait l'objet d'une publication par décret le 15 novembre 1985. Elle est donc aujourd'hui partie intégrante du droit positif français. En effet, les Traités ont, aux termes de l'article 55 de la Constitution du 4 octobre 1958, « *une autorité supérieure à celle de la loi* ». La Convention a cependant laissé le soin au législateur interne d'adopter les mesures nécessaires à son application ⁽²⁾, ce qui ne lui donne pas d'effet direct en droit interne. Pour pallier cette difficulté, **la CNIL n'a cessé de prendre en compte les dispositions de la Convention dans de nombreux domaines**. Ainsi, la CNIL a toujours interprété la notion de données à caractère personnel de manière large, conformément à « *la loi française, les lignes directrices de l'OCDE, la convention 108 et la directive européenne 95/46* » ⁽³⁾.

⁽¹⁾ 19^{ème} rapport d'activité, 1998, p. 63 et 21^{ème} rapport d'activité, 2000, p. 77.

⁽²⁾ Article 4 : « Chaque partie prend, dans son droit interne, les mesures nécessaires pour donner effet aux principes de base pour la protection des données énoncées dans le présent chapitre ».

⁽³⁾ 26^{ème} rapport d'activité, 2005, p.84.

- **Lignes directrices de l'OCDE**

Elles figurent dans la recommandation du 23 septembre 1980, qui fixe « *les lignes directrices régissant la protection de la vie privée et le flux transfrontalier de données à caractère personnel* ». Cette recommandation n'a **pas de valeur obligatoire**, mais incite les États à veiller au bon équilibre dans ce domaine.

Les États doivent répondre à deux types d'obligations : une **obligation de protection de la vie privée et des libertés individuelles** et une **obligation d'assurer la libre circulation des données**.

Sur l'obligation de protection de la vie privée et des libertés individuelles, les États doivent veiller à la collecte et à la qualité des données ainsi que le **respect des principes de finalité, de sécurité et de transparence**. Les États doivent, en outre, assurer le droit d'accès et de contestation et organiser la responsabilité du gestionnaire du fichier.

Sur l'obligation d'assurer la libre circulation des données, les États doivent s'efforcer de vérifier les conséquences sur les autres pays membres, **assurer la sécurité du flux transfrontalier des données** et prendre toutes mesures appropriées. Ils devront notamment adopter des lois adaptées, favoriser et soutenir les systèmes d'autoréglementation, faciliter la mise en œuvre du droit des personnes physiques, prévoir les sanctions et les recours et veiller à l'absence de discrimination.

Enfin, il existe une obligation d'information et d'assistance mutuelle entre les pays membres.

- **Réflexion menée par les Nations Unies**

Elle se distingue de celle de l'OCDE en ce qu'elle est plus précise. Cette réflexion est retranscrite dans des lignes directrices, adoptées par l'assemblée générale en 1990 ⁽¹⁾.

Le droit des personnes est au cœur du dispositif ainsi que l'autorité de contrôle dont la mise en place est conseillée. Elles concernent indifféremment les fichiers privés ou publics. Les garanties, notamment en ce qui concerne les données sensibles, y sont plus détaillées. Ce sont les données susceptibles de donner lieu à des discriminations illicites ou arbitraires, incluant les informations sur les origines raciales ou ethniques, la couleur, la vie sexuelle, les opinions politiques, philosophiques ou autres, comme l'appartenance à une association ou à un syndicat. En revanche, les données relatives à la santé ne sont pas mentionnées.

Des exceptions existent cependant : elles concernent la protection de la sécurité nationale, de l'ordre public, de la santé et de la moralité publique ainsi

(¹) Nations Unies, résolution n°45-95, 14 décembre 1990.

que des droits et libertés des personnes, en particulier de celles qui sont persécutées sous réserve des garanties appropriées et du respect des conventions internationales relatives aux droits de l'homme.

2. Le cadre juridique national

La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés demeure aujourd'hui **une loi fondatrice** en matière de protection des données à caractère personnel. En effet, elle a su poser les bases juridiques régissant la création et le fonctionnement des fichiers de police. Soumis à un régime d'autorisation ainsi qu'à d'autres dispositions spécifiques, ces fichiers sont placés sous la surveillance d'une autorité de contrôle, qui veille à l'exercice de ses prérogatives : la commission nationale informatique et libertés (CNIL).

a) Protection des données et des personnes : la genèse de la loi du 6 janvier 1978

Les fichiers de police sont inséparables du contexte plus général de protection des données personnelles. En effet, comme l'indiquaient deux juristes en 1978, MM. Jean Frayssinet et Pierre Kayser, dans les années soixante et soixante-dix, le développement de l'informatique, « a suscité, en même temps que l'espérance d'une société mieux informée, plus prospère et plus libre, des appréhensions très sérieuses. Appréhension, tout d'abord, pour le respect de la vie privée [...]. Appréhension ensuite, d'atteintes aux libertés publiques par la rupture de l'équilibre entre gouvernants et gouvernés, la multiplication des informations à la disposition des gouvernants leur conférant un pouvoir accru sur les gouvernés. On s'est enfin demandé si le développement de l'informatique n'était pas susceptible de **rompre l'équilibre des pouvoirs, au sein de l'État, au profit du pouvoir informé, c'est-à-dire du Gouvernement, à l'égard du Parlement** et même d'avoir des incidences sur le fonctionnement des institutions démocratiques ».

La plupart des États ont alors choisi d'apaiser ces craintes par une solution législative : la Suède en 1973, les États-Unis en 1974 ou encore la République fédérale d'Allemagne en 1977. Quant à la France, **le Parlement a adopté la loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978**, dont l'article 1^{er} dispose : « *L'informatique doit être au service de chaque citoyen. (...) Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.* »

Cette loi fondatrice a été adoptée à la suite de la **vive émotion suscitée en 1974 par la révélation au public du projet de fichier SAFARI** (« *système automatisé pour les fichiers administratifs et le répertoire des individus* »). Ce système prévoyait l'institution d'un identifiant unique (en l'occurrence le numéro de sécurité sociale) afin d'interconnecter les fichiers de l'administration, dont ceux des renseignements généraux, de la direction de la sécurité du territoire et de la police judiciaire. Devant l'indignation suscitée par ce projet, le projet fut retiré et

une commission, présidée par M. Bernard Chenot ⁽¹⁾, fut créée afin de proposer des mesures permettant de concilier le développement de l'informatique avec le respect de la vie privée et des libertés publiques. **Le rapport de cette commission**, rédigé par MM. Bernard Tricot et Pierre Catala et remis en juin 1975, **a très fortement inspiré la loi du 6 janvier 1978.**

Cette loi fondatrice en matière de protection des données n'a pas pu surprendre, à la fin des années 1970, la police française. En effet, celle-ci réfléchissait déjà à cette question, comme en témoignent les propos prémonitoires tenus en 1969 par M. Jacques Gandouin, alors directeur de la Direction des écoles et techniques, chargée d'assurer l'unité de la formation et l'homogénéité des méthodes et des techniques de police :

*« Il est par ailleurs une autre considération beaucoup plus importante encore à nos yeux, c'est le **souci de la liberté individuelle, du respect de l'homme et du citoyen.** (...) La mise en mémoire d'un certain nombre de données n'est-elle pas attentatoire à la liberté et même à la dignité de l'homme ? (...) Est-ce possible d'éviter une sorte de mise en carte de tous les citoyens et comment faire pour qu'une telle mesure ne risque pas de nuire à notre liberté ? (...) Je suis pour ma part convaincu que **seuls les délinquants pourront craindre les effets de l'exploitation électronique de la documentation criminelle.** (...) D'abord, il faut que l'utilité sociale des répertoires où son nom figurera soit incontestable, qu'elle s'inscrive dans les principes généraux de notre droit. Il faut encore que les accès aux répertoires soient strictement prévus par les lois et les règlements, que soient imaginées des protections, des garanties contre une éventuelle manœuvre illégitime. (...) Il faut donc que domine dans tous les travaux informatiques, plus que la moralité, plus que l'honnêteté, plus que la discrétion, un véritable, sincère, profond respect de la personne humaine. Alors les bons citoyens connaîtront peut-être d'immenses facilités de vie pendant que la délinquance sera plus efficacement poursuivie. »*

b) Régime de déclaration versus régime d'autorisation : la nécessaire publicité des actes créant des fichiers

La protection des données, quelle que soit la forme qu'elle revêt et quel que soit le type de fichier impliqué, repose sur un **principe cardinal** : celui qui veut créer un traitement de données doit donner une certaine publicité à cette création. **La publicité de la création de fichiers** présente un double avantage. En premier lieu, elle permet aux citoyens de prendre connaissance de l'existence de fichiers qui peuvent contenir des informations les concernant. En second lieu, la publicité permet à la CNIL d'exercer son contrôle sur l'ensemble des fichiers. Les fichiers de police présentent cette particularité d'obéir à des règles exceptionnelles en matière de création. Alors que le régime qui s'applique à tous les traitements de données, qu'ils soient du secteur public ou privé, est celui de la déclaration, les fichiers de police sont soumis à un régime spécifique, celui de l'autorisation.

(1) Vice-président du Conseil d'État de 1971 à 1978.

• Le régime de la déclaration

De manière générale, c'est le régime de la déclaration qui s'applique à **tous les traitements de données personnelles, qu'ils relèvent indifféremment du secteur public ou privé**. L'article 22 de la loi du 6 janvier 1978 dispose à ce titre « *qu'à l'exception de ceux qui relèvent des dispositions prévues aux articles 25 [données à caractère politique, philosophique, santé et vie sexuelle, données génétiques, infractions, exclusion d'un droit, interconnexions, biométrie], 26 [traitements intéressant la sécurité publique, la sûreté de l'État, la défense, les infractions pénales] et 27 [traitements publics NIR ⁽¹⁾, biométrie pour le compte de l'État, recensement, téléservices] ou qui sont visés au deuxième alinéa de l'article 36, les traitements automatisés de données à caractère personnel font l'objet d'une déclaration auprès de la Commission nationale de l'informatique et des libertés* ».

La déclaration peut être effectuée **par voie électronique**, à la suite de quoi la CNIL délivre un récépissé par la même voie (article 23). La CNIL publie des « *normes* » pour les catégories les plus courantes de traitements de données à caractère personnel « *dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés* » (article 24). Ces normes sont destinées à simplifier l'obligation de déclaration, dans la mesure où « *les traitements qui correspondent à l'une de ces normes font l'objet d'une déclaration simplifiée de conformité envoyée à la commission* ».

• Le régime spécifique d'autorisation : un contrôle *a priori* de la CNIL

La section II de la loi du 6 janvier 1978 prévoit des **exceptions au régime de la déclaration**. En effet, les traitements de données visés aux articles 25, 26 et 27 de la loi du 6 janvier 1978 sont soumis à un **régime d'autorisation**.

Tel n'était pas le cas à l'origine : la loi française faisait une **distinction fondamentale entre les fichiers du secteur privé et ceux du secteur public**. Alors que ceux du secteur privé devaient simplement être déclarés auprès de la CNIL, tous les fichiers émanant de la sphère publique relevaient d'un véritable régime d'autorisation. **En 2004, le législateur ⁽²⁾ a fait le choix d'abandonner cette distinction** entre fichiers du secteur privé (régime de déclaration) et ceux du secteur public (régime d'autorisation) pour faire de la déclaration le régime de droit commun, **recentrant ainsi la procédure d'autorisation sur certains types de fichiers bien ciblés** : les fichiers de police (article 26), les traitements publics portant sur des données relatives au numéro d'inscription des personnes au répertoire national d'identification des personnes physiques, à la biométrie, au recensement ainsi qu'aux téléservices (article 27) ainsi que les traitements portant

⁽¹⁾ Numéro d'inscription au répertoire (NIR) national d'identification des personnes physiques.

⁽²⁾ Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

sur des données génétiques ou sur des données à caractère politique et philosophique, à la santé et à la vie sexuelle (article 25). Grâce à ce régime d'autorisation ciblé sur certains types de fichiers bien identifiés, **la CNIL estime qu'elle a pu recentrer son activité sur les traitements à risque**, en fonction d'un critère matériel : le caractère sensible du traitement « *du fait de la finalité poursuivie ou de la nature des informations traitées* »⁽¹⁾.

S'agissant des **fichiers de police**, c'est la finalité du traitement qui rend nécessaire l'autorisation, par voie réglementaire, du fichier. Ainsi, aux termes de l'article 26, les traitements « *qui intéressent la sûreté de l'État, la défense ou la sécurité publique ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté* », à savoir les fichiers de police, sont autorisés par arrêté du ministre compétent, après avis motivé et publié de la CNIL. Lorsque les fichiers de police portent sur des données sensibles, au sens de l'article 8 de la loi du 6 janvier 1978⁽²⁾, ils sont autorisés par décret en Conseil d'État pris après avis motivé et publié de la CNIL.

Il convient de souligner que l'article 26 de la loi du 6 janvier 1978, prévoyant un régime d'autorisation soumis à décret en Conseil d'État, permet à de tels décrets de ne pas suivre l'avis de la CNIL, la loi imposant seulement leur publication. En effet, **le législateur a fait le choix en 2004 de modifier la nature de l'avis de la CNIL**. Alors qu'auparavant, les avis de la CNIL liaient les pouvoirs publics, qui ne pouvaient alors passer outre que par un décret pris sur avis conforme du Conseil d'État⁽³⁾, **ils sont désormais simplement rendus publics et sont dépourvus de toute force obligatoire** à l'égard du Gouvernement. La motivation ayant initialement présidé à cette réforme était que **la publicité de l'avis serait suffisamment dissuasive** pour obliger les pouvoirs publics à suivre les recommandations faites par la CNIL. Cinq ans après cette réforme, **le bilan est contrasté**. Si la Ligue des droits de l'homme considère que le caractère non contraignant de la CNIL est une « *catastrophe* », le président de la CNIL, M. Alex Türk, estime que la publicité de l'acte est une force de dissuasion suffisante. Or, ce n'est pas toujours le cas. Ainsi, s'agissant du fichier relatif aux passeports biométriques, dénommé DELPHINE, la CNIL avait considéré, dans sa délibération n° 2007-368 du 11 décembre 2007, que, « *si légitimes soient-elles, les finalités invoquées ne justifient pas la conservation, au plan national, de données biométriques telles que les empreintes digitales et que les traitements ainsi mis en œuvre seraient de nature à porter une atteinte excessive à la liberté individuelle* ». Cependant, le Gouvernement n'a pas tenu compte des réserves émises par la CNIL dans son avis et a autorisé, par le décret n° 2008-426 du 30 avril 2008, le

⁽¹⁾ Rapport d'activité de la CNIL 2004, page 24.

⁽²⁾ Les données sensibles au sens de l'article 8 de la loi du 6 janvier 1978 comprennent les opinions politiques, philosophiques, religieuses ou syndicales, les données relatives à la santé et à la vie sexuelle ainsi que les données relatives aux origines raciales ou ethniques.

⁽³⁾ L'alinéa 2 de l'article 15 de la loi du 6 janvier 1978 disposait dans sa version initiale que si l'avis de la Commission est défavorable, il ne peut être passé outre que par un décret pris sur avis conforme du Conseil d'État.

traitement automatisé des données, notamment biométriques, contenues dans les passeports.

- **Les dispositions spécifiques aux fichiers de police**

La loi du 6 janvier 1978 a prévu deux dispositions spécifiques pour les fichiers de police. En premier lieu, les demandes d'avis auprès de la CNIL pour la création de ces fichiers peuvent, dans certains cas, ne pas comporter certaines des mentions obligatoires pour les autres traitements de données. En second lieu, de manière exceptionnelle, certains actes réglementaires portant création de fichiers de police peuvent ne pas être publiés.

— D'une part, **certaines demandes d'avis concernant les fichiers de police peuvent ne pas comporter certaines des informations, qui sont cependant requises pour tout autre traitement de données.**

Aux termes des articles 29 et 30 de la loi du 6 janvier 1978, les demandes d'avis adressées à la CNIL concernant les fichiers de police doivent préciser l'identité et l'adresse du responsable du traitement, les caractéristiques, la finalité et la dénomination du traitement ainsi que la description générale de ses fonctions, le service chargé de sa mise en œuvre, le service auprès duquel s'exerce le droit d'accès, les catégories de personnes qui peuvent avoir accès aux informations enregistrées, les informations nominatives traitées, leur origine et leur durée de conservation ainsi que leur destinataire, les rapprochements et interconnexions, les dispositions de sécurité prises, et si le traitement est destiné à l'expédition d'informations nominatives à l'étranger.

Cependant, l'article 30 de la loi du 6 janvier 1978 dispose que « *les demandes d'avis portant sur les traitements intéressant la sûreté de l'État, la défense ou la sécurité publique peuvent ne pas comporter tous les éléments d'information énumérés ci-dessus* », notamment **les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement** ainsi que la durée de conservation des informations.

Le décret en Conseil d'État du 15 mai 2007 ⁽¹⁾, pris après avis de la CNIL, fixe la liste de ces traitements, qui peuvent ne pas comporter tous les éléments d'information généralement requis. Relèvent ainsi de la dérogation prévue à l'article 30 de la loi du 6 janvier 1978 :

— le décret portant création au profit de la direction centrale du renseignement intérieur d'un traitement automatisé de données à caractère personnel dénommé CRISTINA ;

⁽¹⁾ Décret n°2007-914 du 15 mai 2007 pris pour l'application du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

— le décret portant application des dispositions de l'article 31 de la loi n° 78-17 du 6 janvier 1978 aux fichiers d'informations nominatives mis en œuvre par la direction générale de la sécurité extérieure ;

— le décret portant application des dispositions de l'article 31 de la loi n° 78-17 du 6 janvier 1978 aux fichiers de la direction de la protection et de la sécurité de la défense ;

— le décret portant application des dispositions de l'article 31 de la loi n° 78-17 du 6 janvier 1978 au fichier d'informations nominatives mis en œuvre par la direction du renseignement militaire ;

— l'arrêté relatif au traitement automatisé d'informations nominatives mis en œuvre par la direction de la protection et de la sécurité de la défense ;

— l'arrêté relatif au traitement automatisé d'informations nominatives « *fichier de la DGSE* » mis en œuvre par la direction générale de la sécurité extérieure ;

— l'arrêté relatif au traitement automatisé d'informations nominatives « *fichier du personnel de la DGSE* » mis en œuvre par la direction générale de la sécurité extérieure ;

— l'arrêté relatif au traitement automatisé d'informations nominatives de personnes étrangères mis en œuvre par la direction du renseignement militaire.

L'article 16 du décret en Conseil d'État du 20 octobre 2005 ⁽¹⁾ a cependant précisé **les mentions que doivent « au minimum » comporter les actes autorisant ces traitements** : l'identité et l'adresse du responsable du traitement, la finalité et la dénomination du traitement ainsi que le service chargé de la mise en œuvre, le service auprès duquel s'exerce le droit d'accès indirect, les catégories de personnes qui ont accès aux informations enregistrées, les destinataires des informations, les rapprochements et interconnexions.

En définitive, **la dérogation prévue pour certains fichiers de renseignement limitativement énumérés reste substantielle** au regard de ce qui est exigé pour l'ensemble des fichiers intéressant la sûreté de l'État, la défense ou la sécurité publique, dans la mesure où la dérogation concerne les données à caractère personnel traitées, leur origine et les catégories de personnes concernées ainsi que leur durée de conservation.

— D'autre part, **l'acte réglementaire portant création du fichier peut, dans certains cas, ne pas être publié**. En effet, le III de l'article 26 de la loi du 6 janvier 1978 prévoit que « *certaines traitements mentionnés au I et au II peuvent être dispensés, par décret en Conseil d'État, de la publication de l'acte réglementaire qui les autorise ; pour ces traitements, est publié, en même temps*

⁽¹⁾ Décret n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

que le décret autorisant la dispense de publication de l'acte, le sens de l'avis émis par la commission ». Sont dispensés de publication, en vertu de l'article 1 du décret du 15 mai 2007 pris pour l'application du I de l'article 30 de la loi du 6 janvier 1978, les mêmes actes réglementaires que ceux qui peuvent ne pas comporter l'ensemble des éléments d'information, qui sont généralement requis.

L'article 83 du décret du 20 octobre 2005 pris pour l'application de la loi du 6 janvier 1978 prévoit que lorsque des traitements sont dispensés de la publication de l'acte réglementaire qui les autorise, le sens de l'avis émis par la CNIL ne peut porter que la mention « favorable », « favorable avec réserve » ou « défavorable ». Dans tous les cas, « **la commission ne peut mettre à la disposition du public que le sens de son avis** ».

Au regard des traitements de données, dont l'acte réglementaire d'autorisation est effectivement dispensé de publication, il apparaît très clairement que le III de l'article 26 a connu, dans la pratique, **une application restrictive**, dans la mesure où **il n'a été appliqué qu'à ce qu'on appelle communément les « services de renseignement »**. Alors que la dispense de publication de l'acte réglementaire d'autorisation, permise par l'article 26, visait potentiellement l'ensemble des fichiers « intéressant la sûreté de l'État, la défense et la sécurité publique », les gouvernements successifs ont fait le choix de ne l'appliquer en pratique qu'à certains des fichiers mis en œuvre par les services de renseignement, qui relèvent incontestablement des deux premières finalités, que sont la sûreté de l'État et la défense, mais qui n'épuisent pas la troisième, à savoir la sécurité publique. La loi a donc été appliquée en pratique comme si elle ne prévoyait une exception que pour les seuls fichiers mis en œuvre par les services de renseignement, les actes réglementaires créant tout autre fichier de police faisant l'objet d'une publicité de droit commun.

En définitive, les obligations de publication des actes réglementaires d'autorisation définies par la loi du 6 janvier 1978 se révèlent d'autant plus importantes et contraignantes pour le pouvoir exécutif que **les quelques aménagements prévus par la loi du 6 janvier 1978 n'ont été appliqués dans la pratique qu'à certains des fichiers mis en œuvre par les services de renseignement et non à l'ensemble des fichiers de police**.

c) La Commission nationale de l'informatique et des libertés (CNIL) : une autorité de contrôle veillant au respect des libertés publiques

Créée par la loi du 6 janvier 1978, la CNIL est une **autorité administrative indépendante**, rattachée budgétairement aux services du Premier ministre ⁽¹⁾, ce qui n'est pas sans poser des problèmes de gestion budgétaire. Elle dispose de **pouvoirs de décision, de contrôle et de sanction**. En effet, bien que n'étant pas une juridiction, elle peut appliquer des sanctions pécuniaires. Cependant, réitérant une jurisprudence qu'il avait déjà appliquée au Conseil

(1) Programme « Protection des droits et libertés » de la mission « Direction de l'action du Gouvernement ».

supérieur de l'audiovisuel, le Conseil d'État a reconnu à la CNIL, dans un arrêt ⁽¹⁾ en date du 19 février 2008, le **statut de juridiction au sens de l'article 6 § 1 de la Convention européenne des droits de l'homme** relatif aux règles du procès équitable.

- **Composition de la CNIL**

La loi du 6 août 2004 ⁽²⁾ a **maintenu le nombre des membres de la CNIL à 17**, modifiant toutefois celui des personnalités qualifiées pour l'informatique en le portant à cinq.

Ainsi, aux termes de l'article 13 de la loi du 6 janvier 1978, **sont membres de la commission** : deux députés et deux sénateurs, désignés respectivement par l'Assemblée nationale et le Sénat ; deux membres du Conseil économique et social, élus par cette assemblée ; deux membres ou anciens membres du Conseil d'État, élus par l'assemblée générale de ce dernier ; deux membres ou anciens membres de la Cour de Cassation, élus par son assemblée générale ; deux membres ou anciens membres de la Cour des comptes, élus par l'assemblée générale de celle-ci ; trois personnalités qualifiées pour leur connaissance de l'informatique ou des questions touchant aux libertés individuelles, nommées par décret ; deux personnalités qualifiées pour leur connaissance de l'informatique, désignées par le président de l'Assemblée nationale et par le président du Sénat. Un commissaire du Gouvernement, désigné par le Premier ministre, siège auprès de la commission, et assiste à toutes les délibérations.

Au regard de l'importance que revêt l'action de la CNIL dans le domaine de la protection des données à caractère personnel, **vos rapporteurs estiment nécessaire que, parmi les parlementaires membres de l'autorité de contrôle, soit représentée l'opposition.**

Proposition n° 1

Modifier l'article 13 de la loi du 6 janvier 1978 relatif à la composition de la CNIL, afin que les deux députés et les deux sénateurs, membres de l'autorité de contrôle, soient désignés respectivement par l'Assemblée nationale et par le Sénat, *« de manière à assurer une représentation pluraliste ».*

- **Les missions de la CNIL**

La loi du 6 août 2004 a détaillé les missions de la CNIL à son article 11. Outre sa mission d'information auprès du public et auprès des responsables de traitements de leurs droits et obligations, elle doit **veiller à ce que les traitements**

⁽¹⁾ CE, réf., 19 février 2008, n° 311974, Sté Profil France.

⁽²⁾ Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

de données à caractère personnel soient mis en œuvre conformément aux dispositions de la loi.

Elle a un **rôle de conseil**, notamment auprès des pouvoirs publics et, le cas échéant, des juridictions, ainsi que des personnes et organismes qui mettent en œuvre ou envisagent de mettre en œuvre des traitements automatisés de données à caractère personnel, joue un rôle auprès d'organisations professionnelles ou d'institutions regroupant des responsables de traitements, puisque, outre ce rôle de conseil, elle délivre un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel.

La CNIL doit se tenir informée de l'évolution des technologies de l'information et rendre publique, le cas échéant, son appréciation des conséquences qui en résultent pour l'exercice des droits et libertés. **Son rôle consultatif a été largement accru par la loi du 6 août 2004**, puisque, outre l'obligation de sa consultation sur tout projet de loi ou de décret relatif à la protection des personnes à l'égard des traitements automatisés, elle propose au gouvernement les mesures législatives ou réglementaires d'adaptation de la protection des libertés à l'évolution des procédés et techniques informatiques.

À la demande du Premier ministre, **elle peut**, d'une part, **être associée à la préparation et à la définition de la position française dans les négociations internationales** dans le domaine de la protection des données à caractère personnel, et, d'autre part, participer à la représentation française dans les organisations internationales et communautaires compétentes en ce domaine.

B. LA CRÉATION DES FICHIERS : EN FINIR AVEC L'AMBIGUÏTÉ DU CADRE JURIDIQUE ACTUEL

La tendance actuelle est à la **multiplication des fichiers de police** : alors que le groupe de travail présidé par M. Alain Bauer recensait 34 fichiers en 2006, il en a recensé près de 45 en 2008, une douzaine de fichiers étant, de plus, « *en cours de préparation* ». Vos rapporteurs ont complété la liste établie par le groupe de travail précité, en y ajoutant les fichiers « *à usage de police* », portant le total des fichiers de police ou à usage de police à 58 ⁽¹⁾.

Cette augmentation du nombre de fichiers s'explique en premier lieu par le fait que certains **traitements de données sont créés en dehors de tout cadre juridique** et sans aucune base normative. En second lieu, lorsque le gouvernement entend donner une base juridique aux fichiers, dont il envisage la création, il peut recourir à **un large éventail d'instruments normatifs** (lois, décrets, arrêtés, etc.).

Ainsi, l'ambiguïté du cadre juridique actuel tient à l'absence de base juridique dans certains cas et à la diversité de bases normatives dans les

⁽¹⁾ Cf. Tableau des fichiers de police ou ayant un usage de police figurant en annexe 1.

autres, soulignant par là même la nécessité de clarifier les conditions de création des fichiers de police.

1. Deux régimes juridiques coexistent actuellement pour créer les fichiers de police

En l'état actuel du droit applicable, le gouvernement dispose, sur le plan juridique, de **deux possibilités distinctes pour créer des fichiers de police**.

En premier lieu, sur le fondement de **l'article 26 de la loi du 6 janvier 1978**, relative à l'informatique, aux fichiers et aux libertés, **peut être créé par arrêté ou décret en Conseil d'État, pris après avis motivé et publié de la CNIL, tout fichier de police**, à savoir les traitements de données « *qui intéressent la sûreté de l'État, la défense ou la sécurité publique ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté* ». Le décret en Conseil d'État est nécessaire pour les fichiers de police qui portent sur des données sensibles (origines raciales ou ethniques, opinions politiques, philosophiques ou religieuses, appartenance syndicale des personnes, santé et vie sexuelle). Certains juristes ont pu considérer que, par là même, le législateur avait défini le **régime juridique général régissant la création des fichiers de police** et avait ainsi conféré au pouvoir réglementaire compétent **une habilitation générale** lui permettant de créer les fichiers de police par voie réglementaire.

En second lieu, **le gouvernement peut être autorisé par le législateur à créer tel ou tel fichier de police, lorsque des lois spécifiques l'y autorisent**. Il s'agit dans ce cas d'**habilitations législatives ponctuelles**, qui s'inscrivent en marge du régime général défini par l'article 26 de la loi du 6 janvier 1978. Ces habilitations législatives **ne sont pas rares et tendent même, ces dernières années, à augmenter** de manière sensible, marginalisant quelque peu le régime général défini par la loi « *Informatique et libertés* ». À titre d'exemple, l'article 7 de la loi du 23 janvier 2006 relative à la lutte contre le terrorisme autorise le ministère de l'Intérieur à créer le fichier des passagers aériens et son article 8 le traitement automatisé de contrôle des données signalétiques des véhicules. Le fichier national des immatriculations a été créé par la loi n° 90-1131 du 19 décembre 1990, alors que le fichier national automatisé des empreintes génétiques a été autorisé par la loi n° 98-468 du 17 juin 1998. De la même manière, c'est la loi du 12 décembre 2005 relative au traitement de la récidive des infractions pénales qui a créé les fichiers SALVAC et ANACRIM, soit un an seulement après la création du fichier judiciaire national automatisé des auteurs d'infractions sexuelles (FIJAIS) par la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.

Or, **l'articulation entre le régime général régissant la création des fichiers de police et les habilitations législatives ponctuelles** ne va pas sans poser **certaines difficultés**. Ainsi, lorsqu'une loi spéciale crée un fichier de police spécifique, le cadre juridique actuel reste flou sur le point de savoir si cela interdit

en retour au gouvernement de créer d'autres fichiers du même type, par voie réglementaire, sur le fondement du régime général prévu à l'article 26 de la loi « *Informatiques et libertés* ».

Certaines personnes, rencontrées par vos rapporteurs lors de leurs auditions, considèrent que « *le cadre législatif réduit le débat avec la CNIL* ». Pour eux, l'habilitation ponctuelle conférée par la loi spéciale irait jusqu'à réduire le débat entre les services de police et la CNIL, car **les finalités du fichier sont d'emblée définies par le législateur**. Cette remarque, formulée, entre autres, par la direction des libertés publiques et des affaires juridiques du ministère de l'Intérieur, paraît en grande partie infondée. D'une part, rien ne fait obstacle, tant sur le plan juridique que pratique, à ce que le gouvernement consulte la CNIL lors de l'élaboration d'un projet de loi créant un fichier de police. D'autre part, **les finalités**, dans l'hypothèse où elles n'auraient pas été débattues entre les services opérationnels et la CNIL, **sont néanmoins discutées et définies dans un débat public au Parlement**. En outre, lorsqu'un fichier de police a été créé par la loi et non par voie réglementaire, **le législateur s'est appuyé sur l'expertise de la CNIL ainsi que sur les attentes des services du ministère de l'Intérieur**. Ainsi, lors des travaux préparatoires de la loi du 23 janvier 2006 relative à la lutte contre le terrorisme, le rapporteur, M. Alain Marsaud, a reçu en audition aussi bien les différents services intéressés du ministère de l'Intérieur que la CNIL. En outre, la CNIL avait rendu un avis sur le projet de loi relatif à la lutte contre le terrorisme ⁽¹⁾.

2. Entre diversité et absence de base juridique : l'augmentation du nombre de fichiers de police

Actuellement, cette double habilitation conduit, en pratique, à recourir à une grande diversité de bases juridiques pour créer les fichiers de police. En outre, les habilitations existantes ne font pas obstacle, dans la pratique, à ce que certains fichiers soient mis en œuvre en dehors de tout cadre juridique. Ainsi le sentiment de confusion qui entoure la création de certains fichiers de police vient de ce que, **soit les fichiers de police sont mis en œuvre sans aucune base juridique, soit ils sont créés par une grande diversité d'instruments normatifs** (loi, décret, arrêté, circulaire, etc.).

En premier lieu, il apparaît qu'**un quart des fichiers de police n'ont aucune base juridique**. Ainsi en est-il, par exemple, du fichier des personnes nées à l'étranger, qui a été créé en 1975 sans texte de référence, du fichier des objets signalés de la gendarmerie nationale ou bien encore du système de traitement des images des véhicules volés, qui est également exploité par la gendarmerie nationale. Le fichier des brigades spécialisées de la police nationale est lui aussi dépourvu de base juridique.

⁽¹⁾ Délibération n° 2005-208 du 10 octobre 2005 portant avis sur le projet de loi relatif à la lutte contre le terrorisme.

En second lieu, **seulement 17 % des fichiers de police, soit moins d'un sur cinq, ont été créés par le législateur.** Ainsi, malgré une intensification du recours à la loi ces dernières années, la proportion de fichiers ayant été créés par la loi et ayant donné lieu à un débat public sur les finalités envisagées reste particulièrement faible. Il convient cependant de reconnaître que **la moitié des fichiers de police ayant une base législative ont été créés ces cinq dernières années.**

Enfin, la coexistence de deux sources d'habilitation en matière de création de fichiers de police a pu conduire à des **errements juridiques** portant préjudice tant au contrôle effectif du Parlement sur l'action du gouvernement que sur la clarté et la lisibilité du cadre juridique des fichiers de police. Ainsi, **il n'est pas rare de voir un fichier de police créé par décret en Conseil d'État recevoir une base législative quelques années plus tard**, alors même que le respect de la hiérarchie des normes voudrait que l'acte réglementaire vienne compléter la loi et non la précéder.

Ainsi, le STIC (Système de Traitement des Infractions Constatées) a tout d'abord fait l'objet du décret n° 2001-583 du 5 juillet 2001 et s'est ensuite vu conférer une base législative par l'article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure I. Le fichier national transfrontière (FNT) constitue un autre exemple éclairant des ambiguïtés juridiques présidant à la création des fichiers de police. Ce traitement a en effet fait l'objet d'un arrêté en date du 29 août 1991, avant de recevoir une base législative par l'article 7 de la loi n° 2006-1964 du 23 janvier 2006 relative à la lutte contre le terrorisme. C'est également le cas du fichier national des permis de conduire (FNPC).

Ce phénomène est symptomatique de **l'empirisme qui préside à la création des fichiers de police.** Les services de police et de gendarmerie conçoivent et mettent en œuvre les outils dont ils ont besoin. Une fois les fichiers pleinement opérationnels, les services s'attachent alors à les sortir d'une forme de « clandestinité » et à leur donner une base juridique conforme aux lois et règlements. **L'acte juridique autorisant ledit traitement ne fait alors que reprendre et constater un simple état de fait.**

Classement des fichiers de police suivant leur base juridique

Base juridique	Nombre de fichiers	En %
<i>Convention internationale</i>	1	2 %
<i>Règlement européen</i>	1	2 %
<i>Loi</i>	10	17 %
<i>Décret</i>	10	17 %
<i>Arrêté</i>	12	20 %
<i>Aucun texte</i>	14	25 %
<i>En préparation</i>	10	17 %
<i>Total</i>	58	100 %

La diversité des bases juridiques utilisées pour la création de fichiers de police explique en partie le développement des traitements automatisés de données à des fins policières. En effet, l'absence de base juridique pour certains fichiers et la coexistence de deux régimes juridiques pour créer des fichiers ne va pas sans **accentuer l'opacité du cadre juridique actuel** et *in fine* **faciliter l'augmentation du nombre de fichiers de police**. La confusion actuelle ne peut que renforcer le **sentiment que s'organise une collecte d'informations généralisée**, alors que la réalité est tout autre.

Lors de son audition par vos rapporteurs, le président de la CNIL, M. Alex Türk, a estimé qu'on assistait actuellement « à une *floraison de textes législatifs et réglementaires* ». Or, plus les fichiers se multiplient, plus les finalités se rapprochent et plus les risques, supposés ou réels, de dérive sont grands. Le cas du STIC est éclairant, car celui-ci est parfois dévoyé de sa finalité initiale pour devenir une forme de casier judiciaire clandestin. Vos rapporteurs estiment donc **indispensable de clarifier les conditions de création des fichiers de police**.

3. Pour un débat public éclairé : les fichiers de police doivent être créés par la loi

Le cadre juridique actuel, qui définit les modalités de mise en œuvre des fichiers de police, voit coexister **deux régimes juridiques distincts** pour créer de tels fichiers, ce qui nuit en retour à la clarté et à la publicité du débat en la matière.

En effet, l'exécutif, lorsqu'il entend donner une base juridique au fichier de police qu'il crée, peut toujours recourir soit à **la voie réglementaire sur le fondement de l'article 26 de la loi du 6 janvier 1978**, soit à **la voie législative**. En dépit du recours accru à la loi observé ces dernières années, rien n'interdit au gouvernement de créer un nouveau fichier de police par décret ou arrêté et *de facto* de soustraire ces traitements de données au contrôle du Parlement. C'est ce que les événements récents ont mis en exergue : alors que la loi a créé des fichiers

aussi importants que le FNAEG ⁽¹⁾ en 1998, le FIJAIS ⁽²⁾ en 2004, SALVAC et ANACRIM ⁽³⁾ en 2005 et le fichier des passagers aériens ⁽⁴⁾ en 2006, le gouvernement, dans la continuité des solutions retenues par ses prédécesseurs, a créé par voie réglementaire le fichier de renseignement EDVIGE ⁽⁵⁾, ou bien encore le fichier DELPHINE relatif aux passeports biométriques ⁽⁶⁾.

Or la vive émotion et la forte polémique suscitées par la création du fichier EDVIGE s'expliquent en partie par **l'absence de débat public sur les missions des services de renseignement**. Le manque d'information des citoyens et l'absence de réflexion sur la finalité de ce nouveau fichier de renseignement n'ont pu que redoubler les inquiétudes des citoyens. En effet, l'équilibre fragile, qu'il convient de trouver entre les besoins opérationnels des services de police pour l'exercice de leurs missions et la protection des libertés individuelles de tout citoyen, **nécessite l'intervention et le contrôle du Parlement**.

Ainsi, le législateur, pour chaque fichier de police dont la création est prévue, doit pouvoir débattre tant de la finalité que de la proportionnalité du traitement de données envisagé. Une telle évolution implique que l'article 26 de la loi du 6 janvier 1978 soit modifié pour **prévoir explicitement que tout fichier de police soit autorisé par la loi**.

Proposition n° 2

Seule la loi doit pouvoir autoriser la création d'un fichier de police.

En conséquence, modifier l'article 26 de la loi du 6 janvier 1978, afin que les fichiers ou toute catégorie de fichiers intéressant la sécurité publique et ceux qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ne soient autorisés que par la loi.

Afin que **l'autorisation conférée par le législateur aux services de police et de gendarmerie de créer un fichier de police** prenne tout son sens, vos rapporteurs proposent que chaque loi autorisant la création d'un tel fichier précise l'identité du responsable du traitement, **la finalité et la dénomination du traitement** ainsi que la description générale de ses fonctions, le service chargé de la mise en œuvre, le service auprès duquel s'exerce le droit d'accès (direct ou indirect), les catégories de données à caractère personnel enregistrées, leur origine

⁽¹⁾ Loi n° 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs.

⁽²⁾ Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.

⁽³⁾ Loi n° 2005-1549 du 12 décembre 2005 relative au traitement de la récidive des infractions pénales.

⁽⁴⁾ 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 frontaliers.

⁽⁵⁾ Décret n° 2008-632 du 27 juin 2008 portant création d'un traitement automatisé de données à caractère personnel dénommé « EDVIGE ».

⁽⁶⁾ Décret n° 2005-1726 du 30 décembre 2005 relatif aux passeports électroniques, modifié par le décret n° 2008-426 du 30 avril 2008.

et les catégories de personnes concernées par le traitement, **les catégories de personnes qui ont accès aux informations enregistrées**, les destinataires des informations, les rapprochements et interconnexions, **la durée de conservation des données**.

Proposition n° 3

Toute loi autorisant la création d'un fichier de police devra au minimum préciser l'identité du responsable du traitement, la finalité et la dénomination du traitement ainsi que la description générale de ses fonctions, le service chargé de la mise en œuvre, le service auprès duquel s'exerce le droit d'accès (direct ou indirect), les catégories de données à caractère personnel enregistrées, leur origine et les catégories de personnes concernées par le traitement, les catégories de personnes qui ont accès aux informations enregistrées, les destinataires des informations, les rapprochements et interconnexions, la durée de conservation des données.

Mais, si le recours exclusif à la loi est susceptible de clarifier les conditions de création des fichiers de police, **encore convient-il que le Parlement soit utilement éclairé sur ces questions**. Ainsi, **l'avis consultatif de la CNIL** sur tout projet de loi autorisant la création de fichiers de police doit être **rendu public et transmis au Parlement simultanément au dépôt du projet de loi** sur le bureau de l'Assemblée nationale ou du Sénat. Ainsi, le législateur sera informé en temps utile des éventuelles observations de la CNIL et sera en mesure de se prononcer en pleine connaissance de cause. Cette proposition implique que le gouvernement associe davantage en amont la CNIL à ses travaux de prospective en matière de création de fichiers de police.

Proposition n° 4

L'avis de la CNIL sur tout projet de loi autorisant la création de fichiers de police est rendu public et transmis au Parlement simultanément au dépôt, sur le bureau de l'Assemblée nationale ou du Sénat, du projet de loi autorisant la création d'un fichier de police.

La clarification des conditions de création des fichiers de police passe également par **la nécessité de mettre en œuvre des études d'impact préalables à la création de nouveaux fichiers de police**. Ces études auraient pour double objectif d'apprécier *ex ante* le volume du fichier et sa finalité, au regard notamment des fichiers existants. En effet, face à un problème déterminé, les autorités publiques ont trop souvent tendance à créer un nouveau fichier, alors présenté comme la réponse nécessaire et suffisante au problème posé. La mise en place d'études d'impact préalables sérieuses vise ainsi à prévenir la création systématique d'un fichier, dès lors qu'un problème nouveau apparaît. **La CNIL pourrait utilement être associée à la réalisation de ces études d'impact**.

Proposition n° 5

Les projets ou propositions de loi autorisant la création de fichiers de police doivent être accompagnés d'une étude d'impact appréciant le volume du fichier considéré ainsi que sa finalité, au regard de l'ensemble des fichiers d'ores et déjà existants. La CNIL sera associée à la réalisation de ces études d'impact préalables.

Enfin, en contrepartie des études d'impact *ab initio*, les projets de loi créant tout fichier de police devraient **prévoir une évaluation à moyen et long terme du traitement de données ainsi créé**. Cette évaluation ferait de surcroît l'objet d'un débat au Parlement afin d'apprécier si la finalité initialement conférée au fichier est toujours d'actualité et si l'utilité de ce traitement de données est toujours justifiée.

Proposition n° 6

Les projets de loi autorisant la création de fichiers de police doivent prévoir une clause de rendez-vous dans le temps, afin que le Parlement opère à moyen et long terme une évaluation du fichier considéré. Au terme de cette évaluation, qui doit faire l'objet d'un débat en séance publique, le Parlement peut décider de mettre fin, par la loi, au fichier concerné, si la finalité qui avait initialement présidé à sa création n'est plus démontrée.

C. SORTIR DES RELATIONS CONFLICTUELLES ENTRE LA CNIL ET LE MINISTÈRE DE L'INTÉRIEUR

La naissance d'un fichier de police est une étape majeure, car elle associe les services de police, qui conçoivent un outil répondant à leurs besoins opérationnels, et la CNIL, qui doit s'assurer que le traitement envisagé est conforme aux principes qui encadrent la protection des données personnelles.

Alors même que **la création des fichiers de police** doit permettre de trouver le point d'équilibre entre des intérêts convergents, à savoir la garantie des libertés individuelles et la réponse adéquate aux besoins opérationnels des policiers, elle **crystallise aujourd'hui les désaccords et les tensions entre la CNIL et le ministère de l'Intérieur**.

1. Un dialogue de sourds entre la CNIL et le ministère de l'Intérieur

Au cours des différentes auditions réalisées par vos rapporteurs, il est apparu que les relations nouées entre la CNIL et les services du ministère de l'Intérieur étaient empreintes d'**une forte incompréhension**. Ainsi, le directeur général de la police nationale, M. Frédéric Péchenard, a regretté « **le climat de suspicion et de mépris** » qu'entretient la CNIL à l'égard de la police nationale.

Cette dernière estime que la CNIL, lorsqu'elle rend ses avis ou dans ses activités de contrôle, ne tient pas suffisamment compte des besoins opérationnels des services de police. En outre, **le manque de confiance entre les deux parties** est patent, ce qui constitue un obstacle indéniable à une véritable collaboration ainsi qu'à un traitement efficace et rapide des dossiers : « **le partage en amont suppose la confiance** ». Ainsi, certains responsables de la police nationale estiment qu'elle ne pourrait réellement collaborer avec la CNIL que lorsque celle-ci la considérera comme un partenaire et non comme un adversaire. Enfin, sont critiquées par les services de police « **les campagnes de dénigrement et de parti pris systématique de la CNIL** » à leur égard. En sens inverse, la CNIL, par la voix de son président, M. Alex Türk, regrette **l'aisance des autorités publiques à créer des fichiers** de police sans associer en amont les services de la CNIL.

ARDOISE : EXEMPLE D'UN DIALOGUE DE SOURDS ENTRE LA CNIL ET LES SERVICES DE POLICE

Le logiciel dénommé ARDOISE, qui remplacera, à terme, l'actuel Logiciel de Rédaction des Procédures (LRP), est une application informatique de la police nationale ayant vocation à **rédigier les procédures** et à **alimenter le futur fichier ARIANE**.

La mise en œuvre de l'application ARDOISE est **symptomatique des mauvaises relations** qui existent entre les services de police et l'autorité de contrôle, à savoir la CNIL. En effet, **la liste des données personnelles susceptibles d'être enregistrées** dans ARDOISE, jugées discriminatoires par certaines associations, comme SOS Racisme ou le collectif contre l'homophobie, a suscité, au printemps 2008, de **vives critiques**. Afin de désamorcer la polémique, le ministère de l'Intérieur avait alors souligné que **la liste de ces données sensibles avait déjà été validée par la CNIL**, non pas lors de l'examen du dossier ARDOISE, mais **en décembre 2000** lors de la remise par l'autorité de contrôle **de son avis sur le STIC**.

La CNIL ayant validé ces données lors de l'examen du décret créant le STIC, le ministère de l'Intérieur avait considéré comme acquis l'accord à venir de la CNIL sur la liste des données sensibles collectées et conservées dans ARDOISE. Or **le président de la CNIL a demandé** au ministère de l'Intérieur **des « précisions » et des « éclaircissements »** sur la future application ARDOISE. La CNIL en a également profité pour rappeler publiquement qu'il revenait à l'autorité de contrôle d'émettre un avis préalablement à la mise en place de cette application, **regrettant par là même que l'application soit déjà en phase de test, alors même que le projet de décret n'avait pas été soumis à son avis**. Face à cette levée de boucliers, la ministre de l'Intérieur, Mme Michèle Alliot-Marie, a décidé de suspendre l'expérimentation du logiciel ARDOISE le 22 avril 2008. Le projet de décret créant l'application ARDOISE ainsi que le dossier de demande d'avis ont, depuis lors, été soumis à la CNIL et s'est engagé un dialogue difficile entre l'autorité de contrôle et le ministère de l'Intérieur. En effet, la police nationale estime que **le retard pris dans le déploiement de cette nouvelle application incomberait principalement à la CNIL, qui n'a pas rendu son avis dans le délai légal**. En effet, **l'article 28⁽¹⁾ de la loi « Informatique et libertés »** fait obligation à la CNIL de se prononcer dans un délai de deux mois, renouvelable une fois, sur la demande d'avis. L'absence d'avis dans ce délai de quatre mois vaut avis favorable.

⁽¹⁾ Article 28 de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (modifié par Loi n°2004-801 du 6 août 2004).

I. - La Commission nationale de l'informatique et des libertés, saisie dans le cadre des articles 26 ou 27, se prononce dans un délai de deux mois à compter de la réception de la demande. Toutefois, ce délai peut être renouvelé une fois sur décision motivée du président.

II. - L'avis demandé à la commission sur un traitement, qui n'est pas rendu à l'expiration du délai prévu au I, est réputé favorable.

Ainsi, s'agissant de l'application ARDOISE, si le dossier de demande d'avis a été déposé par le ministère de l'Intérieur à la CNIL le 30 mai 2008, celle-ci n'a pas rendu son avis dans le délai de quatre mois prévus par la loi. Or, la CNIL a bénéficié, dans le même temps, de deux présentations en séance plénière de l'application ARDOISE et a ainsi pu en délibérer le 23 octobre 2008. En définitive, elle a rendu son avis le 6 novembre 2008. **Ces dépassements de délais par la CNIL expliqueraient le sentiment de retardement systématique qu'éprouve la direction générale de la police nationale** à l'égard de la CNIL. Alors que l'application ARDOISE a nécessité le remplacement de 80 000 ordinateurs ainsi que la formation de 80 000 policiers, la lenteur, avec laquelle la CNIL a rendu son avis, conduit d'une part, à **une mise en exploitation tardive de l'application**, devenue largement obsolète au regard de l'état actuel des technologies et, d'autre part, à **la réitération du programme de formation des policiers**. Au final, les délais de réponse de la CNIL, jugés excessifs, ne manquent pas, en retour, d'alimenter une certaine forme d'incompréhension réciproque.

De son côté, la CNIL, par l'intermédiaire de son président, souligne qu'**une meilleure tenue des fichiers de police permettrait une amélioration notable des relations de travail** avec les services de police. Or, cette exigence est triple et implique non seulement la définition d'un cadre juridique précis, mais également le respect de la durée de conservation des données ainsi que la définition d'une finalité claire. Cette volonté forte de la CNIL de voir les fichiers de police bien entretenus repose sur la conviction qu'**il existe un intérêt commun aux services de police et à la CNIL**, autour duquel tous peuvent se retrouver. En effet, des fichiers exacts impliquent un taux d'élucidation plus élevé, une performance accrue des services de police et une meilleure garantie du respect des droits des citoyens.

En dépit de ces mauvaises relations dommageables à tout point de vue, vos rapporteurs ont constaté que **les échanges entre la CNIL et les services opérationnels de police ne sont pas inexistants**. En effet, ces derniers sont amenés à échanger régulièrement *via* le courrier électronique et les auditions communes, réunissant la CNIL, son rapporteur ainsi que les services opérationnels de police. Cependant, c'est bien un « *dialogue de sourds* » qui semble s'être instauré entre les services de police et ceux de la CNIL, les premiers exigeant une plus grande reconnaissance de leurs préoccupations de la part de la CNIL et les seconds rappelant la nécessité d'une bonne tenue des fichiers de police. Ainsi, une des conséquences directes de ce dialogue de sourds lors de la création des fichiers de police est la tendance des services de police à mettre en œuvre *a priori* une application et à la régulariser *a posteriori* : « *l'usage des services, c'est de mettre en œuvre d'abord et de régulariser ensuite* ».

Afin de mettre fin à ces mauvaises relations, vos rapporteurs souhaitent que soient **formalisées les procédures pour un dialogue apaisé et constructif** entre l'autorité de contrôle et les services opérationnels de police et de gendarmerie. C'est là l'ambition des propositions qui suivent.

Proposition n° 7

Améliorer les relations de travail entre la CNIL et le ministère de l'Intérieur grâce à la transmission systématique de l'avant-projet de rapport annuel de la CNIL au Ministère de l'Intérieur, afin qu'il puisse formuler toutes les réponses nécessaires aux différentes observations de la CNIL le concernant. L'objectif est de créer, sur le modèle de la Cour des Comptes, une procédure contradictoire entre l'autorité de contrôle et les services de police et de gendarmerie, où la première, avant la publication de son rapport définitif, recueille les réponses des seconds aux observations qui leur sont adressées.

Eu égard aux bénéfices attendus d'une telle procédure contradictoire, calquée sur le modèle de la Cour des comptes, vos rapporteurs estiment qu'elle ne doit pas être limitée aux seules relations entre la CNIL et le ministère de l'Intérieur. Aussi proposent-ils de l'étendre à **l'ensemble des fichiers et des traitements de données à caractère personnel mis en œuvre pour le compte de l'État**. Cette proposition vise à formaliser les procédures d'un dialogue nourri et suivi entre l'autorité de contrôle et l'ensemble des services de l'État.

Proposition n° 8

Étendre la procédure écrite et contradictoire, entre la CNIL et le ministère de l'Intérieur, à l'ensemble des traitements de données à caractère personnel mis en œuvre pour le compte de l'État.

Dans ce dialogue de sourds entre la CNIL et le ministère de l'Intérieur, **la direction des libertés publiques et des affaires juridiques (DLPAJ) du ministère de l'Intérieur occupe une place délicate**, dans la mesure où les services n'ayant pas d'accès direct avec la CNIL, l'ensemble de la procédure transite par elle. Ainsi, lors de la déclaration d'un fichier de police, c'est le directeur des libertés publiques et des affaires juridiques qui est le correspondant de la CNIL pour le ministère de l'Intérieur.

La direction doit jouer **un rôle d'interface entre les services opérationnels chargés des traitements et la CNIL**. Elle est saisie des projets de fichiers, qu'elle remet en forme sur le plan juridique, préalablement à la saisie de la CNIL. La procédure d'élaboration des décrets avant saisie de la CNIL prévoit à ce titre que chaque service saisisse la DLPAJ d'un projet de texte, obligeant ainsi les services responsables à rédiger un texte et *in fine* à évaluer leurs besoins. M. Laurent Touvet, directeur des libertés publiques et des affaires juridiques, lors de son audition par vos rapporteurs, a estimé qu'un dialogue juridique s'était instauré entre la CNIL et la direction des libertés publiques et des affaires juridiques.

Mais, **si la DLPAJ se voit comme une interface entre la CNIL et les services de police, d'autres la perçoivent davantage comme un écran**, qui fait

obstacle à une prise en compte directe des besoins opérationnels des services de police. En effet, lorsqu'un fichier de police est élaboré, **il est essentiel de partir des attentes concrètes des services de police et de gendarmerie**. Or, ces derniers n'ont pas d'accès direct à la CNIL, qui, en retour, a davantage d'échanges avec la DLP AJ qu'avec les services opérationnels. **Certains policiers regrettent ainsi que les échanges opérationnels en amont soient le plus souvent indirects**, *via* l'intermédiaire du cabinet du ministre de l'Intérieur, la DLP AJ et le cabinet du directeur général de la police nationale. En outre, lors de l'élaboration des fichiers de police, les services opérationnels, qui font remonter leurs demandes, doivent pouvoir être entendus par la DLP AJ, afin de mieux prendre en compte leurs besoins. Or, selon certains policiers rencontrés lors des auditions par vos rapporteurs, il ne semble pas que cela soit réellement ou suffisamment le cas aujourd'hui. De manière générale, vos rapporteurs ont pu constater que **nombre des malentendus** et des difficultés entourant la création des fichiers proviennent du fait que **la conception de l'outil ne prend pas en compte les besoins des policiers et des gendarmes tels qu'ils les expriment sur le terrain**.

En dépit de son rôle délicat et fragile entre les services de police et la CNIL, la DLP AJ partage le constat suivant lequel les relations entre les services de police et la CNIL sont empreintes d'une « *incompréhension qui dure et où les positions s'écartent* ». **La CNIL constitue, selon M. Laurent Touvet, « un partenaire difficile et un censeur vigilant »**, qui suggère voire impose des précisions dans les décrets, souvent mal vécues par la direction générale de la police nationale. À titre d'exemple, **la CNIL demande systématiquement que la durée de conservation des données soit explicitement mentionnée** dans le texte portant création de tel ou tel fichier de police. Cette mention est nécessaire pour permettre l'exercice du droit d'accès indirect et de rectification. Il revient alors à la direction des libertés publiques et des affaires juridiques de les expliquer et de faciliter la compréhension réciproque.

Par ailleurs, l'attitude parfois adoptée, au moment de la création des fichiers, par la direction générale de la police nationale ou par la direction générale de la gendarmerie nationale est révélatrice des **mauvaises relations qui se sont instaurées avec l'autorité de contrôle**. En effet, la direction générale de la police nationale ou celle de la gendarmerie nationale, dans la crainte de voir leur projet initial fortement diminué par la CNIL, ont tendance à présenter à la CNIL un projet très ambitieux et plus large que les besoins initiaux, suivant la logique « *Demander beaucoup pour obtenir peu* ». En effet, selon un responsable du ministère de l'Intérieur, « *la direction générale de la police nationale ou celle de la gendarmerie nationale part avec un projet ambitieux très large car elle sait que la CNIL va le censurer. Elle demande beaucoup pour gagner peu* ».

2. L'introduction d'une procédure de mise en application par étapes des fichiers de police sous le contrôle de la CNIL

Vos rapporteurs ont proposé qu'à l'avenir, **seule la loi puisse autoriser la création d'un fichier de police**. Ainsi, en premier ressort, seul le législateur

pourrait, d'une part, autoriser les services de police ou de gendarmerie à créer un fichier de police spécifique et, d'autre part, fixer les grands principes régissant ce fichier. Or **l'autorisation législative de créer un fichier de police doit ensuite se traduire par l'élaboration d'un outil informatique**, donnant vie, sur le plan technique, aux grands principes fixés par le législateur. Cette mise en application technique du fichier de police relève de la **responsabilité du pouvoir réglementaire** sous le contrôle de la CNIL.

Or, en matière de création de fichiers de police, il convient de partir d'un constat partagé par de nombreux intervenants, notamment, par la direction des libertés publiques et des affaires juridiques : **les services de police ont quelques réticences culturelles à l'encontre de la logique d'avis** présidant à la mise en exploitation d'un fichier de police. Or, ces réticences ne sont pas entièrement infondées dans la mesure où **il existe un véritable problème consubstantiel à la loi de 1978** : les annexes techniques aux dossiers de déclaration sont d'une extrême précision, ce qui implique en pratique **d'avoir développé un système opérationnel pleinement abouti au moment de la déclaration auprès de la CNIL**.

Or, les fichiers de police nécessitent une architecture informatique complexe, faisant l'objet de tests techniques importants lors des différentes phases de validation. Actuellement cette phase de validation n'est pas prévue par la loi : **les services doivent avoir conçu de manière théorique leur système, faire une demande d'avis de la CNIL et ensuite seulement le mettre en exploitation**. Lors de la mise en exploitation du traitement, certains dysfonctionnements peuvent apparaître, nécessitant quelques modifications.

En l'état actuel du droit, **les services doivent demander auprès de la CNIL de nouveaux avis pour chaque nouvelle version du système**. L'introduction d'une procédure de mise en application par étapes permettrait d'apporter plus de souplesse et de fluidité dans l'élaboration technique du fichier considéré. Il s'agit là d'une demande très forte du ministère de l'Intérieur, dans la mesure où **les demandes de modifications successives du système**, qui n'interviennent qu'une fois celui-ci développé, **conduisent à une hausse des coûts ainsi qu'à des difficultés techniques importantes**. Ainsi en a-t-il été récemment lors de la mise en place de l'interopérabilité du FAED au sein de la plate-forme du traité de Prüm : les délais de réponse trop longs de la CNIL ont obligé l'État à verser des pénalités au profit de la société contractante.

Afin de remédier à ces difficultés, vos rapporteurs proposent de **consacrer dans la loi de 1978 une procédure de mise en application par étapes, sous le contrôle de la CNIL**. Cette procédure repose sur l'idée que le dialogue entre la CNIL et les services de police doit s'instaurer, non pas une fois que le projet est conçu et achevé, mais tout au long du processus d'élaboration technique et, notamment, à chaque étape clé (définition des grandes propriétés techniques du système, conception de l'architecture informatique de l'application, réalisation des différents tests techniques, première mise en production, etc.).

Ce dispositif de mise en application par étapes, qui comporterait des clauses de rendez-vous obligatoires entre l'autorité de contrôle et le ministère de l'Intérieur, **serait l'occasion d'échanges réguliers et nourris entre la CNIL et les services de police** tout au long de l'évolution du projet, afin de mieux prendre en compte les observations de la CNIL et les besoins opérationnels des services. Toutefois, **ce schéma ne peut fonctionner que sous certaines conditions** : émergence d'une doctrine partagée et précise selon le type de données traitées (au regard de la sensibilité des données, de l'étendue des personnes ayant accès aux fichiers, etc.) ; stabilité de cette doctrine évitant les changements d'interprétation au cours de la procédure de mise en application par étapes ; clauses de confidentialité réciproque évitant toute fuite dans les médias.

Proposition n° 9

Créer une procédure de mise en application par étapes des fichiers de police sous le contrôle de la CNIL.

En conséquence, introduire dans la loi du 6 janvier 1978 une disposition nouvelle prévoyant que les fichiers relevant de l'article 26 (ceux intéressant la sécurité publique et ceux ayant pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté), une fois autorisés par le législateur et en amont de la publication du décret d'application de la loi, font l'objet, sur le plan technique, d'une procédure de mise en application par étapes, afin qu'ils puissent, à chaque étape clé de leur élaboration et lors de rendez-vous obligatoires, faire l'objet d'une validation conjointe entre la CNIL et le ministère de l'Intérieur.

II. MIEUX PROTÉGER LES DONNÉES SENSIBLES

Lorsqu'est créé un fichier de police, se pose avec acuité la question de la nature des données qui doivent être collectées, au regard, notamment, des finalités poursuivies par le traitement. Apparaît alors **une double exigence de proportionnalité et de nécessité**. En effet, les données qui sont collectées et conservées doivent être utiles à la poursuite de la finalité du fichier et se limiter aux données strictement nécessaires aux services de police pour accomplir leurs missions.

Cette double exigence de proportionnalité et de nécessité, venant encadrer le contenu des fichiers de police, repose sur le principe simple, mais fondamental, d'adéquation : **les données doivent être pertinentes et non excessives au regard des finalités pour lesquelles elles ont été collectées**. Ainsi, la Convention 108 du Conseil de l'Europe dispose-t-elle à son article 5 *c) et d)*, que les données doivent être « *adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles ont été enregistrées* », suivie en cela par l'article 6 de la loi du 6 janvier 1978 qui prévoit, pour sa part, que les données sont « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs* ».

Aussi convient-il de définir très précisément les conditions exceptionnelles dans lesquelles les données sensibles, au sens de l'article 8 de la loi du 6 janvier 1978, les données relatives aux mineurs et celles relatives au signalement peuvent être collectées de manière pertinente et adéquate au regard des finalités initialement imparties. Il convient cependant avant toutes choses de définir ce que recouvre **la notion de « données sensibles »**. Au sens strict, les données sensibles sont celles limitativement énumérées à l'article 8 précité, relative à l'informatique, aux fichiers et aux libertés : les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale ainsi que les données relatives à la santé et à la vie sexuelle. Dans leur acception plus large, les données sensibles comprennent, outre celles qui viennent d'être énumérées, les données relatives aux mineurs ainsi que les signes physiques particuliers, objectifs et permanents, collectés à des fins de signalement des personnes recherchées.

A. LES DONNÉES SENSIBLES DANS LES FICHIERS DE RENSEIGNEMENT

L'article 8 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés pose **une interdiction de principe** de « *collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celle-ci.* » Mais cette interdiction de principe connaît **quelques exceptions**. En effet, l'article 8 prévoit à son quatrième paragraphe que les fichiers de police peuvent comporter de telles données, dites « *sensibles* », dès lors qu'elles sont justifiées par l'intérêt public et

autorisées par décret en Conseil d'État, après avis motivé et publié de la CNIL. Or, si la loi du 6 janvier 1978 pose une interdiction de principe, la dérogation autorisant à titre exceptionnel la collecte de ces données sensibles a connu une application extensive pour les fichiers de renseignement.

1. Le fichier des renseignements généraux : un cadre juridique progressivement clarifié

a) Les renseignements généraux : rôle et actions

Apparus pour la première fois en 1911 sous cette appellation, les renseignements généraux ont rempli, jusqu'à la réforme des services de renseignements intervenue en juillet 2008, **une fonction régaliennne d'information de l'État et du gouvernement** reconnue par tous les régimes qui se sont succédé en France depuis la fin du XVIII^e siècle.

Confrontée à de virulentes oppositions politiques, notamment royalistes, bonapartistes, boulangistes ou encore anarchistes, la III^e République développa cette institution dans les années 1890. En 1911, parallèlement à la création du contrôle général des services de recherches judiciaires et des « *brigades du Tigre* », le directeur de la sûreté générale, Célestin Hennion, nommé par Georges Clemenceau, créa **une « brigade des Renseignements généraux »**, première apparition du terme dans un organigramme policier. Après la première guerre mondiale, la pénétration des idéologies portées par les régimes totalitaires donna lieu à la création en 1937 d'une « *direction des services de renseignements généraux et de la police administrative* », à laquelle succède, en 1938, une « *Inspection générale des services de renseignements généraux et de la police administrative* ». Bien qu'elles aient échoué, faute de moyens budgétaires, ces nouvelles tentatives de centralisation attestent la continuité des efforts entrepris sous la III^e République pour structurer les renseignements généraux.

À la Libération ⁽¹⁾, les RG, rattachés à la sûreté nationale, conservèrent leurs compétences en matière de suivi de la vie politique, économique et sociale, et de surveillance des hippodromes et établissements de jeux. **Le champ de leur activité s'élargit rapidement les années suivantes**, dans un contexte politique marqué par l'agitation sociale, le début de la guerre froide et les conflits coloniaux. Sous la V^e République, l'évolution de la guerre d'Algérie (création de l'OAS en 1961) conduisit les RG à adapter leurs services pour lutter efficacement contre les actes de violence et de terrorisme, en créant notamment des groupes régionaux. Jusqu'à la réforme des services de renseignement intervenue en juillet 2008, **les RG ont poursuivi leur effort d'adaptation à l'évolution des menaces qui pèsent sur l'État**. Le développement du terrorisme a conduit la direction à renforcer sensiblement ses moyens de recherche opérationnelle. Dans les années 1990, les policiers des RG ont joué leur **rôle d'alerte en se penchant**

⁽¹⁾ Pour les aspects historiques concernant les Renseignements généraux sous le régime de Vichy, se reporter au mémoire de Mlle Isabelle JEURGEN, « L'affaire des fichiers des renseignements généraux », 1994.

sur les phénomènes de violences urbaines, les dérives sectaires, le « hooliganisme » ou les diverses formes de contestation sociale. Un rapport d'audit⁽¹⁾, réalisé du 3 novembre au 22 décembre 1988, notait ainsi que « **les Renseignements généraux représentent une force unique dans l'administration, qui accepte de se déplacer et de tirer des sonnettes en toutes circonstances et à des propos divers. Pour autant qu'une question leur est posée, ils développent l'ingéniosité nécessaire pour apporter une réponse de qualité dans des délais très brefs** ».

Le décret du 16 janvier 1995⁽²⁾ a fixé **les missions de la direction centrale des renseignements généraux**, au nombre desquelles on compte : « la recherche et la centralisation des renseignements destinés à informer le Gouvernement » ; « la défense des intérêts fondamentaux de l'État » ; la participation « à la mission générale de sécurité intérieure ».

A contrario, certaines activités, autrefois assurées par les RG, ont officiellement disparu. En effet, la réputation des renseignements généraux a été souvent ternie par certaines révélations sur **le rôle qu'ils ont pu jouer dans la collecte d'informations concernant les partis politiques, voire la vie privée de personnalités politiques**. L'existence de ces activités de renseignement politique a d'ailleurs été confirmée par un ex-directeur central des renseignements généraux et plusieurs anciens ministres de l'Intérieur. Sous l'effet de ces révélations, **les RG ont dû abandonner progressivement leurs « missions politiques »**. Ainsi, il a été mis fin en 1995 au suivi des partis politiques. L'évolution des RG s'est poursuivie en 1997 puis en 2002 avec la suppression des « notes blanches », suppression confirmée en 2004, date à laquelle il a également été officiellement mis fin aux activités de prévisions électorales. Toutefois, les RG, dans le cadre de leurs missions d'information générale, sont demeurés **une source non négligeable d'information des Préfets** pour tout ce qui a trait à la vie politique et sociale du département.

En 2004, le ministre de l'Intérieur avait assigné **aux services des renseignements généraux trois priorités**, à savoir la lutte contre le terrorisme, la lutte contre les violences urbaines et l'économie souterraine ainsi que l'anticipation et la gestion des crises. Jusqu'au 1^{er} juillet 2008, ces services exerçaient leurs missions sur l'ensemble du territoire national, sous la double autorité des préfets et de la direction générale de la police nationale.

(¹) *Audit des services des Renseignements généraux, réalisé, à la demande de M. Pierre Joxe, ministre de l'Intérieur, du 3 novembre au 22 décembre 1988 grâce à des entretiens avec 385 fonctionnaires des RG, cité par Francis Zanponi dans « Les RG à l'écoute de la France », La Découverte, 1998.*

(²) *Décret n° 95-44 du 16 janvier 1995 portant création à la direction générale de la police nationale de la direction de l'administration de la police nationale et de la direction centrale des renseignements généraux et modifiant le décret n° 85-1057 du 2 octobre 1985 relatif à l'organisation de l'administration centrale du ministère de l'Intérieur.*

b) Le fichier des renseignements généraux : un outil au service des missions assignées aux RG

Les nombreuses missions confiées aux RG, telles que la surveillance des groupes à risque, la centralisation du renseignement sur les dérives urbaines, l'analyse de la menace et l'anticipation, le suivi de l'opinion publique et des conflits sociaux, **impliquent que les services soient dotés d'outils de travail suffisamment performants** pour leur permettre de rassembler, d'exploiter et d'analyser en temps utile l'ensemble des renseignements nécessaires à l'accomplissement de leurs missions d'information du Gouvernement. Pour ce faire, **ils se sont très vite dotés de fichiers spécifiques, dits de renseignement**, qu'il convient de ne pas confondre avec les fichiers d'antécédents judiciaires.

Alors que les fichiers d'antécédents judiciaires permettent de collecter des informations extraites des procédures de police judiciaire, afin de faciliter la constatation des infractions pénales, **les fichiers de renseignement** forment une catégorie toute différente. En effet, comme l'a souligné le syndicat des commissaires de la police nationale lors de son audition, les fichiers de renseignement ne sont pas « *un outil de soupçon, mais un instrument de mesure de la menace délinquante et des tensions urbaines* ». Au nombre de ces fichiers de renseignement, qui existent depuis fort longtemps et qui relèvent pleinement de la notion de « *fichiers de souveraineté* », il y a, entre autres, **le fichier des renseignements généraux (FRG)**.

S'il existait bien avant bien avant la loi du 6 janvier 1978 « *Informatique et libertés* », ce fichier n'avait, jusqu'au 14 octobre 1991, aucune base juridique. À partir de 1982, le décret relatif au fichier des renseignements généraux a fait l'objet de négociations difficiles entre le ministère de l'Intérieur, le Conseil d'État et la CNIL. Cette dernière avait finalement rendu un avis conforme le 6 septembre 1988. Afin de régulariser la situation du FRG et de clarifier son cadre juridique, **deux décrets⁽¹⁾ ont été publiés le 27 février 1990**. Le premier autorisait les renseignements généraux à collecter et conserver des informations nominatives concernant « *les opinions politiques, philosophiques, religieuses ou l'appartenance syndicale* » ainsi que « *l'origine ethnique en tant qu'élément de signalement* » de deux catégories de personnes expressément visées dans le décret :

— les personnes susceptibles de « *porter atteinte à la sûreté de l'État ou la sécurité publique, par le recours ou le soutien actif apporté à la violence* », soit directement, soit parce qu'elles ont entretenu des relations avec des individus susceptibles de menacer ainsi la sûreté de l'État ;

(¹) Décret n° 90-184 du 27 février 1990 portant application aux fichiers automatisés, manuels ou mécanographiques gérés par les services des renseignements généraux des dispositions de l'article 31, alinéa 3, de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et décret n° 90-185 du 27 février 1990 relatif au fichier informatisé du terrorisme mis en oeuvre par les services des renseignements généraux du ministère de l'Intérieur.

— les personnes ayant accès à des « **informations protégées** » susceptibles de porter atteinte à la sûreté de l'État ou à la sécurité publique.

Le deuxième décret autorisait la direction centrale des renseignements généraux à mettre en œuvre un « **fichier informatisé du terrorisme** » pour « **l'accomplissement exclusif de sa mission de lutte contre le terrorisme et les troubles à l'ordre public** ». Il était expressément prévu que ce fichier comporterait notamment des renseignements sur l'« *origine ethnique* » des personnes aux fins de signalement. Or la publication de ces deux décrets, autorisant la collecte de données sensibles, a suscité dans la classe politique, comme dans le monde associatif, une vive polémique, conduisant le Premier ministre à retirer ces deux décrets le 3 mars 1990, soit quelques jours seulement après leur publication.

C'est à la suite d'une large concertation, que seront publiés, **le 14 octobre 1991, deux décrets** ⁽¹⁾ pour que le cadre juridique des fichiers des renseignements généraux soit pleinement clarifié. Désormais, la collecte et le traitement des données sensibles dans le FRG étaient encadrés. Ce fichier se voyait en outre assigner **trois finalités** et concernait à ce titre :

— 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 ayant entretenu des liens avec elle) ;

— les personnes soumises à une enquête administrative d'habilitation pour accéder à des **informations protégées** ;

— les personnes qui ont sollicité, exercé ou exercent **un mandat politique, syndical ou économique** ou qui jouent un rôle politique, économique, social ou religieux significatif.

En pratique, le FRG était **un fichier informatique d'indexation** d'une part des personnes morales, d'autre part des personnes physiques, comportant les informations sur l'état civil, l'adresse et la profession de la personne, complétées, le cas échéant, par des éléments d'identification ou relatifs à ses activités, et **renvoyant à un numéro de dossier ou de note « papier » archivés par les différents services départementaux des RG**. Ce système d'indexation permettait de savoir dans quelle direction départementale des renseignements généraux se trouvait une note consacrée à une personne inscrite dans le FRG et, le cas échéant, de contacter, après accord de l'autorité hiérarchique compétente, le service détenteur de la note afin d'en prendre connaissance. Selon la CNIL, ce sont près de **2,5 millions de personnes** qui étaient **inscrites au FRG**. À titre d'exemple, lors de leur déplacement au service départemental d'information

(1) Décret n° 91-1051 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 et décret n° 91-1052 du 14 octobre 1991 relatif au fichier informatisé du terrorisme mis en œuvre par les services des renseignements généraux du ministère de l'Intérieur.

générale du Val-de-Marne, il a été indiqué à vos rapporteurs que le FRG de ce département comportait 40 000 références et recensait 28 000 personnes.

c) Le fichier des renseignements généraux posait une interdiction de principe de collecter des données sensibles

Le décret du 14 octobre 1991 ⁽¹⁾ relatif au fichier des renseignements généraux posait à l'article premier **une interdiction de principe** de collecter et conserver « *des données nominatives qui font apparaître, directement ou indirectement, les origines raciales ou les opinions politiques, philosophiques ou religieuses ainsi que les appartenances syndicales des personnes.* »

À côté de cette interdiction de principe, le décret prévoyait **deux dérogations**.

D'une part, pouvaient être collectées et conservées **les données relatives aux « signes physiques particuliers, objectifs et inaltérables, comme éléments de signalement »** uniquement lorsque ces informations concernaient la première finalité du FRG, à savoir 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, ces données relatives au signalement ne pouvaient en aucun cas faire l'objet d'un traitement dans le cadre des deux autres finalités imparties au fichier des renseignements généraux, à savoir les enquêtes administratives et les informations nécessaires au Gouvernement concernant les personnes physiques ou morales qui ont sollicité, exercé ou exercent un mandat politique, syndical ou économique ou qui jouent un rôle politique, économique, social ou religieux significatif. Par ailleurs, les données relatives aux origines raciales et ethniques ne pouvaient être collectées.

D'autre part, **les données relatives aux « activités politiques, philosophiques, religieuses ou syndicales »** pouvaient également être collectées et conservées et ce, dans le cadre des trois finalités assignées au fichier des renseignements généraux.

Au final, l'interdiction de principe, posée en 1991, de collecter des données sensibles connaissait **des dérogations globalement limitées et encadrées**, notamment pour les données relatives au signalement, ces dernières étant exclusivement traitées pour le motif de « *sûreté de l'État* » ou de « *sécurité publique* ».

⁽¹⁾ Décret n°91-1051 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.

	Décret du 27 février 1990	Décret du 14 octobre 1991
Données relatives au signalement (signes physiques, photographie)	Ne sont pas mentionnées dans les données sensibles pouvant être collectées.	Exclusivement pour le motif « sûreté de l'État » ou « sécurité publique »
Données relatives à la santé et à la vie sexuelle	Ne sont pas mentionnées dans les données sensibles pouvant être collectées.	Expressément interdites depuis 2004.
Données relatives aux origines raciales ou ethniques	Pouvaient être collectées les données relatives à l'origine ethnique « <i>en tant qu'élément de signalement</i> ».	Ne pouvaient être collectées (la CNIL, délibération n° 82-205 du 7 décembre 1982, acceptait cependant une collecte d'informations de ce type comme élément de signalisation des personnes ⁽¹⁾).
Activités politiques, philosophiques, religieuses ou syndicales	L'ensemble des « <i>opinions</i> » politiques, philosophiques ou religieuses ou l'appartenance syndicale, mais seulement pour les personnes relevant de la sphère politique, sociale et économique.	Seulement les « <i>activités</i> » politiques, philosophiques, religieuses ou syndicales pour toutes les personnes référencées dans le traitement.

2. Le fichier EDVIGE a opéré une extension notable des données sensibles susceptibles d'être collectées

a) La création du fichier EDVIGE est liée à la nouvelle architecture du renseignement intérieur

En effet, une réforme de grande ampleur du renseignement intérieur est intervenue à compter du 1^{er} juillet 2008. En premier lieu, une direction centrale du renseignement intérieur (DCRI) a été créée ⁽²⁾. Elle exerce les attributions antérieurement dévolues à la direction de la surveillance du territoire (DST), ainsi que celle de la direction centrale des renseignements généraux

⁽¹⁾ La CNIL avait estimé, dans sa délibération n° 82-205 du 7 décembre 1982 portant avis conforme sur le projet de décret pris en application des dispositions de l'article 31 alinéa 3 de la loi du 6 janvier 1978 aux traitements automatisés d'informations nominatives mis en œuvre par les renseignements généraux, que le recueil d'informations sur le « type racial » est d'intérêt public, dès lors que ces informations constituent des éléments de signalement des personnes.

⁽²⁾ Article 1 du décret n° 2008-609 du 27 juin 2008 relatif aux missions et à l'organisation de la direction centrale du renseignement intérieur :

« La direction centrale du renseignement intérieur a compétence pour lutter, sur le territoire de la République, contre toutes les activités susceptibles de constituer une atteinte aux intérêts fondamentaux de la nation.

À ce titre :

- a) Elle est chargée de prévenir les activités inspirées, engagées ou soutenues par des puissances ou des organisations étrangères et de nature à menacer la sécurité du pays, et concourt à leur répression ;
- b) Elle participe à la prévention et à la répression des actes terroristes ou visant à porter atteinte à l'autorité de l'État, au secret de la défense nationale ou au patrimoine économique du pays ;
- c) Elle contribue à la surveillance des communications électroniques et radioélectriques susceptibles de porter atteinte à la sûreté de l'État ainsi qu'à la lutte, en ce domaine, contre la criminalité liée aux technologies de l'information et de la communication ;
- d) Elle participe également à la surveillance des individus, groupes, organisations et à l'analyse des phénomènes de société, susceptibles, par leur caractère radical, leur inspiration ou leurs modes d'action, de porter atteinte à la sécurité nationale. »

(DCRG) relevant de sa mission de renseignement *stricto sensu* (lutte contre le terrorisme, contre les atteintes à la sûreté de l'État...).

En second lieu, les autres missions des RG ne relevant pas du renseignement (information générale sur l'activité politique, économique et sociale, surveillance des violences urbaines...) sont dorénavant attribuées à la direction centrale de la sécurité publique (DCSP)⁽¹⁾. Afin de réaliser cette mission, une nouvelle sous-direction a été créée en son sein : **la sous-direction de l'information générale (SDIG)**, ainsi que des services départementaux d'information générale au sein des directions départementales de la sécurité publique⁽²⁾.

Dans le domaine des fichiers, cette réorganisation entraîne la **disparition de deux types de traitements automatisés** : ceux gérés par la DST et ceux gérés par la DCRG, qui doivent donc être **remplacés par de nouveaux traitements** :

— **un traitement géré par la DCRI** qui reprend les données des anciens fichiers de la DST ainsi que les données des fichiers gérés par les Renseignements généraux qui concernaient des personnes susceptibles de porter atteinte à la sûreté de l'État, notamment le FRG et le fichier informatisé du terrorisme. Ce nouveau traitement, créé par décret, a été baptisé **CRISTINA** (centralisation du renseignement intérieur pour la sécurité du territoire et les intérêts nationaux) ;

— **un traitement géré par la DCSP** qui collecte les données jusque-là traitées par les renseignements généraux dans le cadre de leurs activités

⁽¹⁾ **Article 12 du décret n° 85-1057 du 2 octobre 1985 modifié relatif à l'organisation de l'administration centrale du ministère de l'Intérieur et de la décentralisation :**

« La direction centrale de la sécurité publique est une direction active de la direction générale de la police nationale.

Dans le cadre de sa mission d'information générale, la direction centrale de la sécurité publique est chargée, sur l'ensemble du territoire national à l'exception de Paris, de la recherche, de la centralisation et de l'analyse des renseignements destinés à informer le Gouvernement et les représentants de l'État dans les collectivités territoriales de la République dans les domaines institutionnel, économique et social, ainsi que dans tous les domaines susceptibles d'intéresser l'ordre public, notamment les phénomènes de violence. Cette mission s'exerce sur l'ensemble du territoire des départements et collectivités. La direction centrale de la sécurité publique concourt, à ce titre, à l'exercice des missions de renseignement et d'information confiées aux forces de sécurité intérieure ».

⁽²⁾ **Article 4 du décret n° 2008-633 du 27 juin 2008 relatif à l'organisation déconcentrée de la direction centrale de la sécurité publique :**

« Pour l'information du représentant de l'État et du Gouvernement dans les conditions définies à l'article 12 du décret du 2 octobre 1985 susvisé, il est créé dans chaque direction départementale de la sécurité publique un service départemental d'information générale.

Dans chaque chef-lieu de région, ce service est également chargé de la centralisation et de la synthèse des renseignements fournis par les services départementaux d'information générale des directions départementales de la sécurité publique de la région. Dans chaque chef-lieu de zone de défense, ce service assure en outre la centralisation et la synthèse des renseignements destinés à informer le préfet de zone et le Gouvernement. À ce titre, sous l'autorité du préfet de zone, le directeur départemental de la sécurité publique du chef-lieu de la zone de défense coordonne l'activité des services départementaux d'information générale des directions départementales de la sécurité publique de la zone. En Île-de-France, le préfet de police, préfet de la zone de défense de Paris, désigne le service de la préfecture de police chargé, sous son autorité, des missions de niveaux régional et zonal définies aux deuxième et troisième alinéas du présent article ».

d'information générale. Ce traitement dénommé **EDVIGE** a été créé par le décret n° 2008-632 du 27 juin 2008, publié au *Journal Officiel* du 1^{er} juillet 2008.

Le traitement de données **EDVIGE** s'est alors vu assigner **trois finalités**, plus larges que celles conférées au FRG, et visait à ce titre :

— les individus, groupes, organisations et personnes morales qui, en raison de leur activité individuelle ou collective, **sont susceptibles de porter atteinte à l'ordre public** (et personnes ayant entretenu des liens avec elles) ;

— les personnes soumises à une enquête administrative **pour déterminer si le comportement des personnes physiques ou morales intéressées est compatible avec l'exercice des fonctions ou des missions envisagées** (et personnes ayant entretenu des liens avec elles) ;

— les personnes physiques ou morales ayant sollicité, exercé ou exerçant **un mandat politique, syndical ou économique** ou qui jouent un rôle institutionnel, économique, social ou religieux significatif (et personnes ayant entretenu des liens avec elles).

En pratique, **la création du fichier EDVIGE**, liée à la réforme des services de renseignement, **ne s'est pas traduite par la mise en place d'un nouveau système de traitement informatique**. En effet, la réflexion concernant le futur outil informatique EDVIGE était à peine initiée lorsqu'est intervenue la réforme du renseignement intérieur, sa conception et sa réalisation étant envisagées dans un délai de deux ans. C'est pourquoi, au 1^{er} juillet 2008, la sous-direction de l'information générale a procédé à une copie du FRG figé au 30 juin. EDVIGE consistait alors à alimenter cette copie « *en mode FRG* », c'est-à-dire avec le même système d'indexation, en tenant compte du nouveau cadre juridique.

À l'avenir, **l'architecture technique de cette future application informatique devra faire l'objet d'une attention toute particulière** s'agissant des choix à opérer entre, d'une part, le maintien d'un système d'indexation nationale renvoyant à des dossiers informatiques consultables uniquement au niveau du service départemental détenteur et, d'autre part, la possibilité de consulter nationalement l'ensemble des données de ce fichier de renseignement.

b) Le décret créant le fichier EDVIGE opère une extension du champ des données sensibles recueillies

Sur la base des trois finalités qui lui ont assigné, le fichier EDVIGE ⁽¹⁾, allant au-delà d'un simple toilettage de l'ancien fichier des renseignements généraux, a opéré une **extension importante des données sensibles susceptibles d'être collectées**, suscitant ainsi plusieurs interrogations, voire des inquiétudes.

⁽¹⁾ Décret n° 2008-632 du 27 juin 2008 portant création d'un traitement automatisé de données à caractère personnel dénommé « EDVIGE ».

S'agissant des données relatives au signalement, à savoir les « *signes physiques, particuliers et objectifs, photographies et comportement* », elles pouvaient être collectées et conservées **pour toutes les personnes référencées dans le traitement, quelle que soit la finalité visée** (enquête administrative, personnes relevant de la sphère politique, économique, sociale et religieuse, personnes susceptibles de porter atteinte à l'ordre public). **Dans le cadre du FRG**, au contraire, la conservation et le traitement des données relatives au signalement n'étaient autorisés **que pour le seul motif d'atteinte à la « sûreté de l'État ou à la sécurité publique, par le recours ou le soutien actif apporté à la violence »**. En outre, le décret créant le traitement EDVIGE ne précisait pas ce que recouvrent les éléments de signalement, qui, dans le cadre du FRG, étaient définis comme des « *signes physiques particuliers, objectifs et inaltérables* », conformément à l'article 2 du décret du 14 octobre 1991.

S'agissant des **données sensibles au sens de l'article 8 de la loi du 6 janvier 1978** ⁽¹⁾, leur collecte dans le fichier EDVIGE était beaucoup plus large que dans le cadre du FRG. En premier lieu, alors que **les données relatives à la santé et à la vie sexuelle** étaient expressément interdites depuis 2004 dans le cadre du FRG, le décret portant création d'EDVIGE prévoyait qu'elles pouvaient être collectées ⁽²⁾ **au titre des trois finalités, mais seulement « à titre exceptionnel » pour les personnes « ayant sollicité, exercé ou exerçant un mandat politique, syndical ou économique ou qui jouent un rôle institutionnel, économique, social ou religieux significatif »** sans que les critères permettant d'apprécier le caractère exceptionnel ne soient précisés. Il convient de relever que, face à la polémique soulevée par la possibilité de collecter des **données relatives à la santé et à la vie sexuelle**, le ministère de l'Intérieur avait argué du fait que ces données pouvaient d'ores et déjà être collectées par les renseignements généraux dans le cadre du FRG, puisqu'elles ne faisaient pas partie à l'origine des données sensibles au sens de l'article 31 de la loi de 1978. Toutefois, ces données relatives à la santé et à la vie sexuelle ont été incluses par la loi du 6 août 2004 dans la catégorie des données sensibles.

En second lieu, alors que **les données relatives aux « origines raciales ou ethniques »** ne pouvaient être collectées dans le FRG, même si la CNIL acceptait la collecte d'informations de ce type comme élément de signalisation des personnes ⁽³⁾, le décret portant création du traitement automatisé de données EDVIGE prévoyait qu'elles puissent être collectées **au titre des trois finalités, mais seulement « à titre exceptionnel » pour les personnes relevant de la sphère politique, économique, sociale et religieuse**. Enfin, le fichier EDVIGE autorisait la collecte de données relatives aux « *opinions politiques,*

⁽¹⁾ Les données sensibles au sens de l'article 8 de la loi du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, sont les suivantes : les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale ainsi que les données relatives à la santé et à la vie sexuelle.

⁽²⁾ Toutefois, il restait interdit de sélectionner une catégorie particulière de personnes à partir de ces informations.

⁽³⁾ Délibération n° 82-205 du 7 décembre 1982 de la CNIL.

philosophiques, religieuses ou syndicales » pour toutes les personnes référencées dans le traitement, là où le FRG ne permettait la collecte que des seules données relatives aux « *activités politiques, philosophiques religieuses ou syndicales* » pour toutes les personnes figurant dans le fichier.

Par ailleurs, comme l'a souligné la CNIL dans sa délibération ⁽¹⁾ du 16 juin 2008 sur le projet de décret portant création du traitement EDVIGE, le décret ne définissait pas la nature des données sensibles, au sens de l'article 8, qui étaient susceptibles d'être enregistrées au titre de chacune des finalités. Ainsi, **ce sont les mêmes données sensibles qui pouvaient être indifféremment collectées et conservées et ce, quelle que soit la finalité visée.**

	Fichier des RG	Fichier Edvige
Données relatives au signalement (signes physiques, photographie)	Exclusivement pour le motif « sûreté de l'État » ou « sécurité publique »	Pour toutes les personnes référencées dans le traitement. Mais dispositif de reconnaissance faciale à partir de la photographie interdit.
Données relatives à la santé et à la vie sexuelle	Expressément interdites depuis 2004.	Pouvaient être collectées au titre des trois finalités, mais seulement « à titre exceptionnel » pour les personnes relevant de la sphère politique, économique, sociale et religieuse.
Données relatives aux origines raciales ou ethniques	Ne pouvaient être collectées (la CNIL, délibération n° 82-205 du 7 décembre 1982, acceptait cependant une collecte d'informations de ce type comme élément de signalisation des personnes).	Pouvaient être collectées au titre des trois finalités, mais seulement « à titre exceptionnel » pour les personnes relevant de la sphère politique, économique, sociale et religieuse.
Activités politiques, philosophiques, religieuses ou syndicales	Seulement les « activités » politiques, philosophiques, religieuses ou syndicales pour toutes les personnes référencées dans le traitement.	L'ensemble des « opinions » politiques, philosophiques, religieuses ou syndicales pour toutes les personnes référencées dans le traitement.

Au regard de la vive émotion suscitée par la possibilité ouverte par le fichier EDVIGE de collecter et de conserver des données sensibles au sens de l'article 8 de la loi du 6 janvier 1978, vos rapporteurs proposent qu'**il ne puisse être dérogé à l'interdiction** édictée par cet article **de collecter et de conserver des données sensibles que sur autorisation expresse du législateur**. De cette manière, la protection juridique des données sensibles en serait améliorée. En effet, pour déroger à l'interdiction de principe de collecter de telles données, **il faudrait une loi, là où le droit en vigueur n'exige actuellement qu'un simple décret en Conseil d'État après avis de la CNIL**. Ainsi, un fichier de police ne pourrait être créé que par une loi (cf. proposition n° 2), qui, dans le même temps, préciserait systématiquement si la collecte, le traitement et la conservation de

⁽¹⁾ Délibération n° 2008-174 du 16 juin 2008 de la Commission nationale de l'informatique et des libertés (CNIL) portant avis sur un projet de décret en Conseil d'État portant création au profit de la direction centrale de la sécurité publique d'un traitement automatisé de données à caractère personnel dénommé « EDVIGE ».

données sensibles sont autorisés dans la stricte mesure où les finalités du fichier l'exigent.

Proposition n° 10

Seule la loi peut autoriser un fichier de police à déroger à l'interdiction de principe, posée par l'article 8 de la loi du 6 janvier 1978, de contenir des données sensibles (origines raciales ou ethniques, opinions politiques, philosophiques ou religieuses, appartenance syndicale et données relatives à la santé et à la vie sexuelle) et ce dans la stricte mesure où les finalités du fichier l'exigent. Modifier en conséquence le IV de l'article 8 de la loi du 6 janvier 1978.

3. EDVIRSP : des données collectées et conservées quelle que soit la finalité visée.

En raison de la décision de retrait du traitement automatisé de données EDVIGE, prise en octobre 2008 par le ministre de l'Intérieur et définitivement actée par le décret du 19 novembre 2008 ⁽¹⁾, les services du ministère de l'Intérieur travaillent actuellement sur un projet de décret visant à doter la sous-direction de l'information générale d'un nouveau cadre juridique, en remplacement d'EDVIGE. Le projet de décret, actuellement en cours d'examen par le Conseil d'État, portant création d'une nouvelle application relative à l'exploitation documentaire et la valorisation de l'information relative à la sécurité publique (EDVIRSP), apporte **quelques évolutions notables** en matière de collecte et de traitement des données sensibles, **sans toutefois lever toutes les ambiguïtés**. Afin de parvenir à un texte abouti, éclairé par le débat public, **vos rapporteurs proposent que le futur fichier EDVIRSP soit créé par la loi**. Aussi, les propositions qui suivent visent à détailler quels seraient les apports de cette loi par rapport au projet de décret actuellement en cours d'examen.

Proposition n° 11

Le futur fichier EDVIRSP devra être créé par la loi.

Dans l'attente de la discussion et de l'adoption de la loi autorisant la création d'EDVIRSP, que vos rapporteurs espèrent rapides, il convient de ne pas laisser s'installer plus longtemps une situation de paralysie des services de la sous-direction de l'information générale. Tel est le sens de la proposition n° 53 formulée dans le VI de ce rapport.

⁽¹⁾ Le décret n° 2008-1199 du 19 novembre 2008 portant retrait du décret n° 2008-632 du 27 juin 2008 portant création d'un traitement automatisé de données à caractère personnel dénommé « EDVIGE ».

a) La réaffirmation de l'interdiction de principe de collecter des données sensibles au sens de l'article 8 de la loi du 6 janvier 1978

Le projet de décret portant création du futur traitement EDVIRSP semble revenir à la solution retenue en 1991 dans le cadre du fichier des renseignements généraux. Ainsi, **l'article 1^{er} réaffirme l'interdiction de principe**, pour les services de la direction centrale de la sécurité publique, dans le cadre de leurs missions de renseignement et d'information générale, de « *collecter ou traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci* ».

Seules **deux dérogations** seraient autorisées en la matière. Pourraient ainsi être collectées et conservées les données sensibles faisant apparaître « *l'origine géographique ainsi que les signes physiques particuliers et objectifs* » ainsi que « *les activités politiques, philosophiques, religieuses ou syndicales* ». Alors que le traitement EDVIGE opérait une extension importante des données sensibles susceptibles d'être collectées, le futur fichier EDVIRSP semble opérer un recentrage des données sensibles qui pourront être traitées, **sans toutefois lever toutes les ambiguïtés**. En effet, le projet de décret ne différencie pas les données sensibles qui sont susceptibles d'être enregistrées au titre de chacune des finalités. En outre, il n'est pas précisé, dans le projet de décret dont vos rapporteurs ont eu connaissance, si les données sensibles susceptibles d'être collectées au titre de chacune des deux finalités concernent, outre les personnes physiques, les personnes morales. Un effort de précision dans la rédaction est nécessaire afin de lever toute ambiguïté juridique.

	Fichier Edvige	Fichier Edvirsp
Données relatives au signalement (signes physiques, photographie)	Pour toutes les personnes référencées dans le traitement. Mais dispositif de reconnaissance faciale à partir de la photographie interdit.	Pour toutes les personnes référencées dans le traitement. Mais dispositif de reconnaissance faciale à partir de la photographie interdit.
Données relatives à la santé et à la vie sexuelle	Pouvaient être collectées au titre des trois finalités, mais seulement « à titre exceptionnel » pour les personnes relevant de la sphère politique, économique, sociale et religieuse.	Ne pourront être collectées.
Données relatives aux origines raciales ou ethniques	Pouvaient être collectées au titre des trois finalités, mais seulement « à titre exceptionnel » pour les personnes relevant de la sphère politique, économique, sociale et religieuse.	Ne pourront être collectées, mais risque d'une collecte détournée les données relatives à « l'origine géographique » pouvant être référencées.

	Fichier Edvige	Fichier Edvirsp
Activités politiques, philosophiques, religieuses ou syndicales	L'ensemble des « <i>opinions</i> » politiques, philosophiques, religieuses ou syndicales pour toutes les personnes référencées dans le traitement.	Seulement les « <i>activités</i> » politiques, philosophiques, religieuses ou syndicales pour toutes les personnes référencées dans le traitement.

b) Des données collectées et traitées quelle que soit la finalité visée

Le projet de décret actuellement en cours d'examen prévoit que le futur fichier EDVIRSP se verrait assigner **deux finalités** et concernerait, d'une part, les personnes « *dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique* » et, d'autre part, les personnes « *faisant l'objet d'enquêtes administratives* ».

Or, la première finalité assignée à EDVIRSP est beaucoup plus large que celle assignée au FRG par le décret du 14 octobre 1991, qui avait retenu une formulation plus restrictive, à savoir : « *les personnes qui peuvent, en raison de leur activité individuelle ou collective, porter atteinte à la sûreté de l'État ou 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* ». **La finalité étant plus étendue, les données sensibles susceptibles d'être collectées concernent de facto un public plus important.** Vos rapporteurs estiment donc nécessaire que la définition de cette finalité soit plus précise, en s'inspirant notamment de celle retenue en 1991, et ce après une large concertation.

À la suite des auditions qu'elle avait réalisées **sur le fichier EDVIGE, la commission des Lois a formulé neuf recommandations**, dont la première vise à définir de manière plus rigoureuse la finalité relative aux atteintes à l'ordre public. Ainsi, la commission avait recommandé qu'EDVIGE concerne « *les individus, groupes, organisations et personnes morales qui, en raison de leur activité individuelle ou collective, peuvent porter atteinte à la sécurité des personnes et des biens et les personnes ayant entretenu un lien avec eux* ». Vos rapporteurs ont simplement souhaité compléter cette recommandation en y ajoutant, d'une part, la notion de lien « *direct et non fortuit* » et, d'autre part, la notion de « *recours ou soutien actif apporté à la violence* », reprenant sur ces deux points la rédaction du décret de 1991 sur le FRG.

En outre, à la suite des auditions et des déplacements qu'ils ont pu réaliser, **vos rapporteurs recommandent que les différentes finalités assignées à EDVIRSP ne soient plus regroupées dans un fichier unique** géré par la sous-direction de l'information générale. Aussi vos rapporteurs proposent-ils que chaque finalité fasse l'objet d'un traitement spécifique. En ce qui concerne les enquêtes administratives, certains SDIG conservent exclusivement celles qui se sont conclues par un refus. Vos rapporteurs proposent de généraliser cette pratique.

Proposition n° 12

D'une part, le fichier EDVIRSP ne concernera que « *les personnes, groupes, organisations et personnes morales qui, en raison de leur activité individuelle ou collective, peuvent porter atteinte à la sécurité des personnes et des biens, par le recours ou le soutien actif apporté à la violence, ainsi que les personnes entretenant ou ayant entretenu un lien direct et non fortuit avec celles-ci* ».

D'autre part, un fichier distinct, relatif aux personnes « *faisant l'objet d'enquêtes administratives* » sera créé. Ce traitement de données ne recensera que les personnes ayant fait l'objet d'une décision administrative défavorable.

En l'état actuel du projet de décret, **les données susceptibles d'être collectées et traitées sont les mêmes et ce, quelle que soit la finalité visée.** Ainsi, les données sensibles, relatives à « *l'origine géographique* », aux « *signes physiques particuliers et objectifs* » ou bien aux « *activités politiques, philosophiques, religieuses ou syndicales* » pourront, semble-t-il, être collectées aussi bien pour des personnes faisant l'objet d'une simple enquête administrative que pour celles pouvant porter atteinte à la sécurité publique. Aussi vos rapporteurs recommandent-ils que la collecte et la conservation de données sensibles, dont celles enregistrées dans la catégorie « *signalement* », soient strictement interdites dans le fichier relatif aux enquêtes administratives défavorables.

Proposition n° 13

Prévoir que la collecte et la conservation de données sensibles, dont celles enregistrées dans la catégorie « *signalement* », soient strictement interdites dans le fichier relatif aux enquêtes administratives défavorables.

Parmi les données susceptibles d'être collectées et conservées dans EDVIRSP au titre du signalement, **la notion d'« origine géographique » fait débat.**

Votre rapporteur considère que les données relatives à l'origine géographique peuvent être recueillies, dès lors qu'elles constituent des éléments de signalement des personnes. En effet, les services de police doivent pouvoir identifier de manière rapide et efficace les personnes recherchées. Aussi, votre rapporteur estime-t-il qu'une classification géographique constitue un élément objectif et adapté aux attentes concrètes des agents de terrain.

En revanche, **votre rapporteure estime que la notion d'« origine géographique » n'est pas acceptable.** En effet, le projet de décret, dans sa rédaction actuelle, ne définit pas explicitement les éléments qui peuvent être collectés au titre de l'« *origine géographique* ». Le lieu de naissance des

personnes pouvant figurer dans le fichier au titre de l'état civil, il apparaît improbable que, dans l'esprit des rédacteurs du projet de décret, « *l'origine géographique* » recouvre cette seule signification. L'utilisation de cette notion permettrait alors d'inscrire dans le fichier EDVIRSP qu'un citoyen français a pour origine géographique un autre pays, quand bien même il n'y serait pas né et qu'il n'y aurait pas vécu. Votre rapporteure considère qu'il s'agit là d'un artifice juridique pour le moins maladroit, très certainement destiné à contourner l'interdiction de principe, posée par l'article 8 de la loi du 6 janvier 1978, de collecter, directement ou indirectement, des données relatives aux « *origines raciales et ethniques* ». Aussi votre rapporteure propose-t-elle d'**abandonner la notion d'origine géographique au profit des seuls « *signes physiques particuliers, objectifs et inaltérables* », comme éléments de signalement des personnes.**

Proposition n° 14 de votre rapporteur

Conserver, au titre des données sensibles susceptibles d'être collectées et conservées dans EDVIRSP, la notion d'« *origine géographique* » comme élément de signalement des personnes.

Proposition n° 14 bis de votre rapporteure

Limiter les données sensibles collectées et conservées dans EDVIRSP au titre du signalement aux seuls « *signes physiques particuliers, objectifs et inaltérables* ».

4. Le « *fichier des personnalités* »

Parmi les activités des services des renseignements généraux, a longtemps figuré en bonne place le fichage nominatif des « *personnes physiques ou morales ayant sollicité, exercé ou exerçant un mandat politique, syndical ou économique ou qui jouent un rôle institutionnel, économique, social ou religieux significatif* ».

Le décret du 27 juin 2008 portant création d'EDVIGE a repris cette finalité, celle-ci plus connue sous l'appellation de fait inappropriée de « **fichiers des personnalités** », ne serait *a priori* pas reprise dans le futur traitement de données EDVIRSP. L'éventuelle utilité pour le Gouvernement de collecter et de conserver des données sur les personnes relevant de la sphère politique, économique et sociale paraît en effet discutable.

En premier lieu, les différentes finalités assignées par le décret de 1991 au FRG aboutissaient à un certain mélange des genres. Figuraient ainsi dans un même fichier de renseignement, d'une part, des personnes qui exerçaient les droits et libertés constitutionnellement garantis et, d'autre part, des personnes qui pouvaient porter atteinte à la sécurité publique. Ce mélange des genres semble relever d'un autre âge. En effet, le fichage nominatif des personnes au titre de

leurs activités politiques, associatives ou syndicales, de leur rôle institutionnel, économique, social ou religieux, ne paraît ni opportun, ni même indispensable à l'information du Gouvernement.

En second lieu, vos rapporteurs ont été informés, lors de leur déplacement à **la direction du renseignement de la préfecture de police (DRPP)**, le 15 janvier 2009, du fait que, depuis la fin des années 1990, les préfets de police successifs ont décidé de recentrer l'activité des renseignements généraux parisiens sur les violences urbaines, l'ordre public et la lutte contre l'extrémisme violent. Ainsi, **la décision a été prise en 2001**, lors de l'informatisation des fichiers des renseignements généraux de la préfecture de police, **de mettre fin à l'activité traditionnelle de fichage nominatif des personnes en fonction de leurs activités politiques, économiques, sociales ou religieuses** et donc de ne plus alimenter le fichier manuel et mécanographique dénommé « *archives centrales* »⁽¹⁾. Les seuls fichiers « *vivants* » et informatisés de la direction du renseignement de la préfecture de police sont depuis lors constitués par GEVI (gestion des violences urbaines) et GESTEREXT (gestion du terrorisme et des extrémismes à potentialité violente).

Or, les interlocuteurs rencontrés par vos rapporteurs ont tenu à souligner que le choix de ne plus fiché nominativement les personnes relevant de la sphère politique, économique, sociale et religieuse **n'altère pas la capacité opérationnelle de renseignement de la préfecture de police**. En effet, le recensement sur des fiches individuelles des activités politiques ou syndicales légales « *ne sert à rien* » en pratique. Ainsi, lorsque des personnalités politiques ou syndicales participent à des manifestations, le préfet est informé en temps réel par le biais de « *messages flash* », mais il n'y a pas consignation et archivage de cette participation dans des fiches individuelles.

L'abandon du « *fichier des personnalités* » n'empêche pas un suivi précis des mouvements politiques et sociaux : ces derniers sont désormais étudiés sous un angle thématique, afin de fournir aux autorités des prévisions et des renseignements ciblés et pertinents, permettant d'anticiper les éventuelles menaces à l'ordre public et d'offrir une aide à la décision. Ainsi, si les notes d'analyse sur des mouvements politiques ou sociaux peuvent comporter des données nominatives, elles ne sont plus classées sur une telle base.

En revanche, si des éléments se rapportant à des mouvements extrémistes ou à des actes de violence urbaine se manifestent, les services de la direction du renseignement de la préfecture de police procèdent à une indexation nominative dans le cadre des deux fichiers informatisés précités, à savoir GEVI et GESTEREXT. Les critères de partage entre activité politique ou syndicale légale n'emportant pas fichage individuel et activité du même type permettant

(¹) Si, depuis 2001, la DRPP n'alimentait plus le fichier manuel et mécanographique, dénommé « *archives centrales* », au titre de ses missions « *fichiers des personnalités* », elle pouvait en revanche le consulter.

l'inscription dans GESTEREXT et GEVI sont le respect de la loi républicaine et l'appel ou le recours à la violence.

Proposition n° 15

Abandonner définitivement l'inscription dans tout fichier, quelles que soient sa nature et sa portée, des personnes physiques ayant sollicité, exercé ou exerçant un mandat politique, syndical ou économique ou qui jouent un rôle institutionnel, économique, social ou religieux significatif.

LES DONNÉES SENSIBLES DANS LES FICHIERS D'ANTÉCÉDENTS JUDICIAIRES

Les fichiers d'antécédents judiciaires, à l'instar des fichiers de renseignement, peuvent, sous certaines conditions, contenir des **données sensibles, au sens de l'article 8 de la loi du 6 janvier 1978.**

Ainsi, aux termes de l'article 1 du décret du 5 juillet 2001 portant création du STIC et du décret du 20 novembre 2006 portant création de JUDEX, les fichiers d'antécédents judiciaires peuvent contenir des données relatives aux « *origines raciales ou ethniques, aux opinions politiques, philosophiques ou religieuses, à l'appartenance syndicale des personnes ou à la santé ou à la vie sexuelle de celles-ci* », **uniquement lorsque « ces données résultent de la nature ou des circonstances de l'infraction ».**

Les données sensibles sont enregistrées uniquement si elles ont un lien direct et nécessaire avec l'infraction considérée : elles doivent permettre de caractériser les faits. À partir du moment où l'agression est liée à certaines caractéristiques (culte, orientation sexuelle), il convient de le spécifier dans le fichier, par le biais de la « *qualification des faits* ». En effet, **si l'infraction est liée à la nature même de la victime** (agression à caractère racial ou sexuel), **il faut que le fichier conserve la mémoire de la nature de l'infraction**, afin de permettre les recoupements et rapprochements indispensables à la résolution des affaires similaires.

B. LA DÉLICATE QUESTION DU FICHAGE DES MINEURS

Compte tenu des mutations affectant la délinquance juvénile et des missions dévolues à la direction centrale de la sécurité publique dans la lutte contre les phénomènes dits de « *violences urbaines* », le ministre de l'Intérieur avait autorisé, lors de la création du traitement EDVIGE, **l'inscription des mineurs dans un fichier de renseignement**, dans une **logique d'analyse et d'anticipation** de possibles atteintes à l'ordre public, alors que **l'inscription des mineurs dans un fichier d'antécédents judiciaires résulte de la commission d'une infraction pénale.**

1. Les mineurs dans les fichiers de renseignement

Alors que les mineurs ne sont recensés dans les fichiers d'antécédents judiciaires qu'à la seule condition qu'il existe à leur encontre « *des indices graves ou concordants rendant vraisemblable qu'ils aient pu participer, comme auteurs*

ou complices » à la commission d'une infraction pénale, la logique à l'œuvre dans les fichiers de renseignement est différente : il s'agit alors d'analyser, de mesurer et d'anticiper une menace.

a) Le projet EDVIGE : répertorier les mineurs « susceptibles de porter atteinte à l'ordre public »

Alors que le décret du 14 octobre 1991 ⁽¹⁾ ne prévoyait pas la possibilité d'inclure des mineurs dans le fichier des renseignements généraux, le décret du 27 juin 2008 ⁽²⁾ portant création d'EDVIGE disposait, pour sa part, que **les mineurs « susceptibles de porter atteinte à l'ordre public » pouvaient être répertoriés et ce, dès l'âge de 13 ans**. En outre, les mineurs pouvaient également être répertoriés dès l'âge de 16 ans, dès lors qu'ils étaient soumis à une enquête administrative, qu'ils sollicitaient ou exerçaient un mandat politique, syndical ou économique ou bien qu'ils jouaient un rôle institutionnel, économique, social ou religieux significatif.

Cette évolution par rapport au cadre juridique défini en 1991 a été justifiée par **les évolutions de la délinquance et notamment de la participation accrue des mineurs aux violences urbaines**. Le ministère de l'Intérieur a également fait valoir que l'âge de treize ans correspond à l'âge à partir duquel les mineurs sont reconnus pénalement responsables.

Toutefois, l'évolution relative au traitement des mineurs contenue dans EDVIGE entérine un état de fait dans la mesure où, **depuis 1991, les fichiers des renseignements généraux répertoriaient déjà, de manière illégale, des mineurs**. Ainsi, le nombre de mineurs inscrits au fichier des renseignements généraux était évalué à **environ 3 000**, dont près de 600 pour la seule finalité « *sécurité du territoire* ». M. Alex Türk, président de la CNIL, lors de son audition le mercredi 17 septembre 2008 par la commission des Lois de l'Assemblée nationale, a ainsi rappelé : « *Je confirme que le fichier actuel des renseignements généraux comportait déjà certaines informations concernant des mineurs. C'est d'ailleurs une des raisons pour lesquelles nous avons toujours été favorables à ce qu'un texte vienne encadrer juridiquement ce qui se faisait depuis des années. Voilà pourquoi en tant que CNIL, nous considérons qu'il fallait faire le texte. Mais ce texte, à nos yeux, pose certains problèmes* ». Il avait en outre rappelé devant les membres de la commission des Lois que la CNIL avait considéré, lors de l'examen du projet de décret portant création d'EDVIGE, que le traitement aurait dû se limiter aux mineurs de plus de seize ans ⁽³⁾.

⁽¹⁾ Décret n° 91-1051 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.

⁽²⁾ Décret n° 2008-632 du 27 juin 2008 portant création d'un traitement automatisé de données à caractère personnel dénommé « EDVIGE ».

⁽³⁾ Dans sa délibération n° 2008-174 du 16 juin 2008 portant avis sur le projet de décret portant création d'EDVIGE, la CNIL considérait « que la majorité pénale, d'ailleurs relative, des mineurs âgés de treize ans ne saurait servir de référence en la matière, dès lors que le traitement EDVIGE ne revêt aucune finalité de police judiciaire et vise, pour l'essentiel, comme son nom l'indique, à l'information générale du Gouvernement et de ses représentants dans les départements et collectivités ».

b) La nécessité d'encadrer et de définir les conditions précises de fichage des mineurs

Un des principaux enjeux est d'examiner **les critères, qui déterminent les conditions d'inscription** d'un mineur dans un fichier de renseignement. À cet égard, il convient de noter que les mineurs de plus de treize ans pouvaient être inscrits dans EDVIGE dès lors qu'ils **« sont susceptibles de porter atteinte à l'ordre public »**.

Cette formulation reste **une notion aux contours relativement vagues**. La définition que le droit administratif donne à l'ordre public a en outre évolué dans le temps : alors que l'ordre public renvoyait essentiellement à l'absence de troubles matériels au XIX^e siècle, ses buts se sont depuis lors diversifiés. Ainsi, selon la définition traditionnelle donnée par Maurice Hauriou, reprise en partie à l'article L. 131-2 du code des communes et à l'article L. 2212-2 du code général des collectivités territoriales, l'ordre public comporte trois composantes, à savoir la tranquillité, la salubrité et la sécurité publique. **Au final, le critère de l'ordre public semble être un critère suffisamment vaste pour concerner un trop grand nombre de mineurs**. Lors des auditions réalisées par la commission des Lois de l'Assemblée nationale, le mercredi 17 septembre 2008, sur le fichier EDVIGE, certains observateurs ont souligné que la notion d'ordre public était **insuffisamment précise pour constituer un critère pertinent d'inscription des mineurs dans un fichier de renseignement**. Ainsi, M. Jean-Pierre Dubois, président de la Ligue des droits de l'homme, avait souligné que *« non seulement [le fichage] devient possible pour les mineurs à partir de 13 ans, mais il répond désormais à des critères extrêmement flous. Il n'y a pas en France un juriste capable de définir avec précision « l'ordre public », et donc une personne « susceptible de le troubler, alors que la sécurité publique et la sûreté de l'État sont des notions beaucoup plus rigoureuses. Le fichage dépendra du soupçon d'un policier ou d'un gendarme, sans contrôle judiciaire et sur des critères particulièrement flous, ce qui nous paraît grave. »* Mme Hélène Franco, secrétaire générale du syndicat de la magistrature avait exprimé la même idée en affirmant que le syndicat qu'elle représentait avait **« une hostilité totale au fichage des mineurs sur la base d'une notion aussi vague que celle d'ordre public. »**

Or, la définition de critères précis d'inscription ne va pas sans poser quelques difficultés. En effet, certaines personnes auditionnées, comme M. Éric Le Douaron, directeur central de la sécurité publique au ministère de l'Intérieur, ont souligné la difficulté de définir avec précision des critères exacts d'inscription : **« il est difficile d'avoir des critères exacts. Par exemple, pour des individus gravitant autour d'une bande... »** L'approche de travail retenue par les services départementaux d'information générale repose sur une *« phase latente de première observation »*, qui, si elle ne débouche pas sur une procédure judiciaire, reste cependant, aux dires de certains policiers rencontrés, intéressante pour le travail d'analyse, de surveillance et d'évaluation de la menace délinquante et des tensions urbaines. Ainsi, toujours selon certains fonctionnaires de la sous-direction de l'information générale, les mineurs qu'il conviendrait de pouvoir inscrire dans

le fichier seraient ceux qui ne présentent pas nécessairement de lien direct avec la délinquance, ces derniers étant déjà recensés dans le STIC, mais ceux qui y concourent d'une manière ou d'une autre. Aussi estiment-ils qu'il est difficile de définir clairement des critères précis et rigoureux de fichage des mineurs, dans la mesure où **le choix de recenser tel mineur plutôt qu'un autre se fait « suivant la seule expérience des agents en charge des dossiers. »**

Or, au regard des principes à valeur constitutionnelle de protection des mineurs ⁽¹⁾ et face à l'aléa qui peut présider à l'inscription d'un mineur dans un fichier de renseignement, il convient de **définir des critères précis et rigoureux**, venant encadrer strictement les conditions dans lesquelles un mineur peut être recensé dans un tel fichier. La définition de ces critères fait débat.

Votre rapporteure recommande que **deux critères cumulatifs** soient expressément mentionnés dans la future loi autorisant la création de l'application concernant l'exploitation documentaire et la valorisation de l'information relative à la sécurité publique, à la seule fin de les inscrire dans l'application « Gestion des violences urbaines » (GEVI)

En premier lieu, **la définition de la première finalité proposée par vos rapporteurs** constitue un critère plus précis et rigoureux que celui retenu par le décret EDVIRSP actuellement en cours de préparation. À cet égard, la Défenseure des enfants, dans son avis du 2 octobre 2008 sur le fichier EDVIRSP, a estimé que « *le motif d'entrée dans le fichier EDVIRSP, qui est devenu un « risque d'atteinte à la sécurité publique », apparaît contenir des risques d'appréciation très subjective et nécessiterait d'être clairement précisé par une définition des éléments susceptibles de porter atteinte à la sécurité publique* ». Votre rapporteure propose que les mineurs de plus de treize ans puissent être inscrits seulement lorsque, « *en raison de leur activité individuelle et collective* », ils peuvent « *porter atteinte à la sécurité des personnes et des biens, par le recours ou le soutien actif apporté à la violence* ». La mission assignée à la sous-direction de l'information générale de lutter contre les violences urbaines est ainsi clairement identifiée et la collecte de données concernant des personnes mineures est strictement liée à cet objectif.

En second lieu, ce premier critère doit être complété par une deuxième condition. En effet, l'inscription de mineurs dans un fichier de renseignement ne peut être fondée uniquement sur des éléments d'appréciation subjectifs et, par nature, aléatoires, qui reviendraient dans les faits à faire peser sur l'ensemble des mineurs une « *présomption* » de délinquance. La rédaction de la future loi autorisant la création d'EDVIRSP devra prévoir que **seuls puissent être référencés les mineurs qui sont déjà inscrits dans un fichier d'antécédents**

(¹) *Décision du Conseil Constitutionnel DC 2002-461 du 29 août 2002 sur la loi d'orientation et de programmation pour la justice* : « l'atténuation de la responsabilité pénale des mineurs en fonction de l'âge, comme la nécessité de rechercher le relèvement éducatif et moral des enfants délinquants par des mesures adaptées à leur âge et à leur personnalité, prononcées par une juridiction spécialisée ou selon des procédures appropriées, ont été constamment reconnues par les lois de la République ».

judiciaires, comme le STIC ou JUDEX. Ceux-ci sont en effet déjà mis en cause pour une infraction pénale. Ainsi, l'inscription au STIC ou au JUDEX constituerait un critère nécessaire, mais non suffisant, pour l'inscription initiale dans un fichier de renseignement, qui a, quant à lui, une finalité toute différente. Votre rapporteure rappelle, à ce titre, que la mission des services départementaux de l'information générale n'est pas de faire du « *pré-judiciaire* », mais bien de réaliser un travail d'information, de renseignement et d'analyse. Par ailleurs, en matière de violences urbaines, les besoins opérationnels des SDIG concernent, dans la très grande majorité des cas, des mineurs déjà largement connus des services de police. C'est pourquoi, votre rapporteure considère qu'il ne convient pas d'étendre la possibilité d'inscrire des mineurs dans un fichier de renseignement au-delà de ceux qui ont des antécédents judiciaires. Ces derniers sont au demeurant déjà trop nombreux puisque le nombre de mineurs mis en cause chaque année a augmenté de 12,9 % entre 2002 et 2007 ⁽¹⁾.

En revanche, votre rapporteur estime qu'il n'est pas nécessaire d'ajouter un critère supplémentaire au premier. En effet, si l'inscription dans un fichier d'antécédents judiciaires (STIC ou JUDEX) devient nécessaire pour figurer dans EDVIRSP, apparaît le risque de répertorier dans deux fichiers différents les mêmes mineurs. Aussi votre rapporteur considère-t-il que le recours à un double critère se heurte à deux difficultés. D'une part, il conduirait à l'exploitation de deux fichiers en partie redondants. D'autre part, il constituerait une réponse inadaptée aux besoins des services de renseignement qui, afin de prévenir les menaces à la sécurité des biens et des personnes ainsi que les tensions urbaines, ont parfois besoin de répertorier des personnes qui n'ont pas encore forcément commis d'infraction.

Proposition n° 16 de votre rapporteur

Pourront être collectées et conservées dans le futur fichier EDVIRSP les données relatives aux mineurs de plus de treize ans lorsqu'« *en raison de leur activité individuelle ou collective, ils peuvent porter atteinte à la sécurité des personnes et des biens* ».

Proposition n° 16 bis de votre rapporteure

Ne pourront être collectées et conservées dans le futur fichier EDVIRSP et à la seule fin de les inscrire dans l'application « Gestion des violences urbaines » (GEVI), que les données relatives aux mineurs de plus de treize ans qui, d'une part, sont référencés dans un fichier d'antécédents judiciaires (STIC ou JUDEX) et, d'autre part, peuvent, « *en raison de leur activité individuelle et collective, porter atteinte à la sécurité des personnes et des biens, par le recours ou le soutien actif apporté à la violence, ainsi que les personnes entretenant ou ayant entretenu un lien direct et non fortuit avec ceux-ci* ».

(¹) Observatoire national de la délinquance, rapport annuel 2008.

c) Sur la base de critères objectifs clairement définis pour le fichage des mineurs, étendre l'application « Gestion des violences urbaines » (GEVI) sur l'ensemble du territoire

La proposition de vos rapporteurs, visant à préciser, dans la rédaction de la future loi autorisant la création d'EDVIRSP, les critères d'inscription des mineurs de plus de treize ans dans un fichier de renseignement, poursuit un double objectif :

— d'une part, **élargir l'application « Gestion des violences urbaines »**, développée et gérée par la préfecture de police, **aux mineurs, sur la base des critères proposés par vos rapporteurs** ;

— d'autre part, **doter chaque service départemental d'information générale d'un fichier GEVI** à vocation exclusivement départementale.

En effet, alors que le fichier GEVI, actuellement utilisé par la direction du renseignement de la préfecture de police de Paris, est une **application moderne et performante**, répondant aux besoins des services de renseignement en matière de violences urbaines, vos rapporteurs ont pu constater, à leur grande surprise, que **la sous-direction de l'information générale ne connaissait pas l'existence de ce fichier**. En outre, lors du déplacement réalisé à la direction départementale de la sécurité du Val-de-Marne, certains agents rencontrés ont confirmé ne pas connaître cette application, alors même que, dans le même temps, ils ont **besoin d'un outil de travail performant et efficace en matière de violences urbaines**.

L'APPLICATION GEVI DE LA DIRECTION DU RENSEIGNEMENT DE LA PRÉFECTURE DE POLICE

Conçue en 1996 en interne par la direction de la logistique de la préfecture de police, l'application dénommée « *gestion des violences urbaines* » (GEVI) a pour fondement juridique le décret n° 91-1051 du 14 octobre 1991 relatif aux fichiers gérés par les services des renseignements généraux ⁽¹⁾. Il s'agit à ce titre d'un fichier de renseignement et non d'antécédents judiciaires.

Il constituera l'un des fichiers autorisés par la loi autorisant la création de l'application concernant l'exploitation documentaire et la valorisation de l'information relative à la sécurité publique (EDVIRSP).

Le fichier GEVI constitue un traitement automatisé comprenant **des données sur des individus majeurs ou des personnes morales susceptibles d'être impliqués dans des actions de violences urbaines** ou de violences sur les terrains de sport pouvant porter atteinte à l'ordre public et aux institutions. Il contient actuellement 7 300 fiches ⁽²⁾.

Son mode d'exploitation permet, à partir de recherches élémentaires (un ou plusieurs champs), d'**effectuer des rapprochements et d'établir des liens entre des individus, des groupes, des bandes, des événements et des faits**. GEVI permet, à partir du renseignement collecté, un véritable travail d'analyse (réalisation de sociogrammes...).

⁽¹⁾ Sa conformité avec ce texte a été reconnue par la CNIL le 19 novembre 1996.

⁽²⁾ Le fichier GEVI n'est plus alimenté depuis la décision de retrait du nouveau fichier de renseignement EDVIGE, prise en octobre 2008 par la ministre de l'Intérieur et définitivement actée par le décret du n° 2008-1199 du 19 novembre 2008 (cf. page 180 et suivantes).

Conformément au décret du 14 octobre 1991, **aucun mineur n'était jusqu'ici enregistré dans le fichier** ce qui constitue, selon la préfecture de police de Paris, un « *lourd handicap pour l'efficacité de l'outil* », un grand nombre d'acteurs de violences urbaines ne pouvant ainsi pas être pris en compte.

Ce traitement informatisé est **géré par le pôle « phénomènes urbains violents » de la DRPP**. Le fichier, qui n'est interconnecté avec aucune autre application, est exclusivement alimenté par les fonctionnaires chargés du suivi des phénomènes urbains violents et spécialement habilités par le préfet de police. Ils sont d'ailleurs les seuls à pouvoir le consulter. À l'avenir, les fonctionnaires spécialement habilités des services départementaux d'information générale de la région d'Île-de-France pourraient éventuellement contribuer à l'alimentation et consulter l'application au titre des missions d'animation et de coordination de la DRPP dans ce domaine.

GEVI étant un fichier de renseignement, à l'heure actuelle, aucune durée de conservation fixe n'est prévue. Les données ne sont conservées qu'en fonction des finalités (très strictement délimitées) du fichier et donc, pour l'essentiel, de l'intérêt qu'elles présentent au regard des phénomènes urbains violents.

De manière générale, GEVI est jugée comme étant **une application « moderne et bien faite »**, dont les utilisateurs sont entièrement satisfaits en raison du **caractère « très opérationnel » du logiciel**. De surcroît, les rapporteurs ont pu constater que GEVI constituait une application fonctionnelle et souple d'utilisation.

Dans la mesure où la future loi autorisant la création de l'application concernant l'exploitation documentaire et la valorisation de l'information relative à la sécurité publique (EDVIRSP) constituera la base juridique autorisant le fichier GEVI et où le cadre juridique, qu'elle déterminera, s'imposera pleinement à cette application de la préfecture de police, la rédaction proposée par votre rapporteure permettra qu'à l'avenir, **seuls puissent être recensés dans le fichier GEVI les mineurs, qui sont, d'une part, référencés dans un fichier d'antécédents judiciaires (STIC ou JUDEX) et qui, d'autre part, peuvent « en raison de leur activité individuelle et collective, porter atteinte à la sécurité des personnes et des biens, par le recours ou le soutien actif apporté à la violence »**.

En revanche votre rapporteur propose, pour sa part, que puissent être recensés dans le fichier GEVI les mineurs de plus de treize ans, qui, « *en raison de leur activité individuelle ou collective, peuvent porter atteinte à la sécurité des personnes et des biens* ».

Proposition n° 17 de votre rapporteur

Élargir l'application GEVI, actuellement développée et gérée par la préfecture de police, aux mineurs de plus de treize ans qui, « *en raison de leur activité individuelle ou collective, peuvent porter atteinte à la sécurité des personnes et des biens* ».

Proposition n° 17 bis de votre rapporteure :

Élargir l'application GEVI, actuellement développée et gérée par la préfecture de police, aux mineurs de plus de treize ans, qui, d'une part, sont référencés dans un fichier d'antécédents judiciaires (STIC ou JUDEX) et qui, d'autre part, peuvent, *« en raison de leur activité individuelle et collective, porter atteinte à la sécurité des personnes et des biens, par le recours ou le soutien actif apporté à la violence, ainsi que les personnes entretenant ou ayant entretenu un lien direct et non fortuit avec ceux-ci »*.

Au regard du caractère performant et très opérationnel, vos rapporteurs proposent également que l'application GEVI soit diffusée sur l'ensemble du territoire. Ainsi, **chaque service départemental d'information générale se verrait doter d'un fichier GEVI**, qui aurait une vocation exclusivement départementale, afin de conserver le caractère opérationnel de cette application. En outre, l'application GEVI de la préfecture de police ne couvrant actuellement que le département de Paris, **vos rapporteurs proposent que le fichier GEVI ait en Île-de-France une vocation régionale** et qu'il puisse, à ce titre, être alimenté et consulté par les fonctionnaires spécialement habilités des services départementaux d'information générale de la région d'Île-de-France.

Proposition n° 18

Doter les services départementaux d'information générale (SDIG), situés dans des départements particulièrement confrontés à la gestion des violences urbaines, d'un fichier GEVI à vocation départementale.

Proposition n° 19

Dans le cas plus spécifique de l'Île-de-France, mettre en place un fichier GEVI à vocation régionale, en permettant l'alimentation et la consultation du fichier GEVI par les fonctionnaires spécialement habilités des services départementaux d'information générale de la région d'Île-de-France.

d) Le droit à l'oubli : pierre angulaire de la protection des mineurs

S'agissant des mineurs de plus de treize ans, qui pourraient figurer dans un fichier de renseignement, vos rapporteurs proposent en tout état de cause que soit introduit un **droit à l'oubli**. Si l'utilité pour la police de disposer d'informations sur certains mineurs, dans le cadre de la lutte contre les violences urbaines, peut être avérée, le mineur ne doit pas être pénalisé tout au long de sa vie par la conservation de données sur des comportements qui, pendant quelque temps, ont conduit à le fichier.

Dans sa décision n° 2003-467 DC du 13 mars 2003 sur la loi pour la sécurité intérieure, le Conseil constitutionnel, à propos des dispositions relatives aux fichiers d'antécédents judiciaires et aux enquêtes administratives inscrites aux

articles 21 et 25 de la loi précitée, a rappelé que **la durée de conservation des données concernant les mineurs « doit concilier, d'une part, la nécessité de rechercher les auteurs d'infractions et, d'autre part, celle d'assurer le relèvement éducatif et moral des mineurs délinquants »**. Ces principes, définis par le juge constitutionnel pour les fichiers d'antécédents judiciaires, doivent par extension s'appliquer aux fichiers de renseignement.

Le droit à l'oubli, pierre angulaire de la protection des mineurs, fait par ailleurs largement **consensus**. Ainsi, M^e Christian Charrière-Bournazel, bâtonnier de l'ordre des avocats à la Cour de Paris, avait souligné devant la commission des Lois le mercredi 17 septembre 2008 qu' « *il est logique que, lorsque des mineurs sont fichés pour des actes qui ne donnent pas lieu à procédure, ou à une procédure qui n'aboutit pas, ils puissent bénéficier d'un droit à l'oubli.* »

Proposition n° 20

Introduire, dans les fichiers de renseignement, un droit à l'oubli pour les mineurs de plus de treize ans avec effacement de l'élément enregistré le jour du troisième anniversaire de son enregistrement, à défaut de nouvel événement.

Mais **ce droit à l'oubli**, pour être protecteur et effectif, **doit bénéficier du contrôle de l'autorité judiciaire**. En effet, la réticence à la collecte de données sur les mineurs dans un fichier de renseignement s'explique en partie par l'exclusion du contrôle du juge. Ainsi, **vos rapporteurs proposent qu'un magistrat référent soit nommé sur le plan national pour contrôler la bonne application du droit à l'oubli**.

Ce magistrat sera automatiquement saisi à la date du troisième anniversaire de l'intégration du mineur dans le fichier. Deux hypothèses seront alors envisageables. En l'absence de nouvel événement justifiant la conservation des données concernant le mineur, il s'assurera que celles-ci sont effectivement effacées. Si, au regard d'un nouvel événement, les services gestionnaires demandent le maintien des informations le concernant, ils devront alors présenter au magistrat l'ensemble des raisons justifiant le maintien dans le fichier.

En cas de maintien des données **au-delà du troisième anniversaire de leur enregistrement, une clause de rendez-vous annuel** entre les services gestionnaires et le magistrat référent sera prévue afin que, chaque année, les premiers viennent expliquer au second les raisons justifiant la poursuite du fichage du mineur. Si les explications sont insuffisamment fondées, le magistrat aura la possibilité d'ordonner l'effacement des données.

Proposition n° 21

Nommer un magistrat référent au plan national, chargé de veiller au respect du droit à l'oubli pour les mineurs à la date du troisième anniversaire de l'inscription dans le fichier. En l'absence de nouvel événement justifiant la conservation des données concernant le mineur, le magistrat s'assure que celles-ci sont effectivement effacées. Si, au regard de tout nouvel événement, les services gestionnaires souhaitent le maintien des informations concernant le mineur, ils doivent alors présenter au magistrat l'ensemble des raisons le justifiant.

Dans le cas où un tel maintien des données au-delà du troisième anniversaire est autorisé par le magistrat, les services gestionnaires et le magistrat référent doivent se réunir tous les ans, afin d'étudier de nouveau les raisons justifiant le maintien dans le fichier. S'il estime que la demande de maintien est insuffisamment motivée, le magistrat peut ordonner l'effacement des données.

2. Les mineurs dans les fichiers d'antécédents judiciaires

L'article 21 de la loi du 18 mars 2003 pour la sécurité intérieure, qui constitue la base législative des fichiers d'antécédents judiciaires, dispose que ces derniers « *peuvent contenir des informations sur les personnes, sans limitation d'âge, à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer, comme auteurs ou complices, à la commission des infractions mentionnées au premier alinéa du I.* » Les infractions concernées sont les crimes, les délits ainsi que les contraventions de cinquième classe « *sanctionnant un trouble à la sécurité ou à la tranquillité publiques ou une atteinte aux personnes.* »

Si la loi dispose que les mineurs peuvent être inscrits au STIC « *sans limitation d'âge* », la circulaire⁽¹⁾ du ministère de l'Intérieur relative aux modalités de mise en œuvre du STIC prévoit que « *les informations relatives aux mineurs de moins de 10 ans ne sont pas enregistrées, sauf pour des faits particulièrement graves ou en raison de la personnalité des mineurs* ». Elle offre donc un pouvoir d'appréciation aux services régionaux de documentation criminelle.

Ainsi, les mineurs mis en cause peuvent être inscrits au STIC ou dans JUDEX. **Les informations les concernant sont alors conservées cinq ans.** Par dérogation, le délai de conservation est ramené à :

— **dix ans** lorsque la personne est mise en cause pour l'une des infractions suivantes⁽²⁾ : infractions contre les personnes, exploitation de la mendicité

⁽¹⁾ Circulaire NOR/INT/C0700059C du 9 mai 2007.

⁽²⁾ La liste des infractions est détaillée à l'article ANNEXE II du décret n° 2006-1411 du 20 novembre 2006 portant création de JUDEX et à l'article ANNEXE II du décret n° 2001-583 du 5 juillet 2001 portant création du STIC.

aggravée ou en bande organisée, vol avec violences, violences volontaires aggravées, trafic de stupéfiants autre que le trafic international, trafic d'êtres humains, exhibition sexuelle, infractions contre les biens, atteintes à la paix publique, recel de malfaiteurs, etc. ;

— **vingt ans** lorsque la personne est mise en cause pour l'une des infractions suivantes⁽¹⁾ : enlèvement, séquestration, prise d'otage, génocide et autres crimes contre l'humanité, homicide volontaire, tortures et actes de barbarie, agressions sexuelles, proxénétisme, viol, vol en bande organisée, vol à main armée, atteintes à la paix publique, actes de terrorisme, association de malfaiteurs et atteintes aux intérêts fondamentaux de la nation, etc.

En cas de mise en cause dans une ou plusieurs infractions avant que les délais de conservation des données initiales ne soient arrivés à expiration, les articles 7 des décrets portant respectivement création des fichiers STIC et JUDEX disposent que « **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** ». Au regard de ces délais de conservation relativement importants, une définition plus stricte d'un régime spécifique pour les durées de conservation des données relatives aux mineurs dans les fichiers d'antécédents judiciaires paraît nécessaire.

LES AUTRES FICHIERS DE POLICE CONTENANT DES DONNÉES RELATIVES AUX MINEURS

Les fichiers d'antécédents judiciaires ne sont pas les seuls à contenir des données relatives aux mineurs : **le FIJAIS concerne également les mineurs de plus de 10 ans et le FNAEG les mineurs de plus de 13 ans.**

On notera que la **circulaire du ministère de la Justice du 9 juillet 2008 relative au FNAEG** indique qu'« *il convient de faire preuve de prudence en matière de prélèvements des mineurs en qualité de suspects dans un souci de conciliation entre la finalité du FNAEG, d'une part, et les dispositions de l'ordonnance du 2 février 1945 relative à l'enfance délinquante, d'autre part* ». **Ainsi, ne sauraient être prélevés les mineurs de moins de 13 ans**, ceux-ci ne pouvant faire l'objet que de mesures ou sanctions éducatives, mais pas de condamnations pénales. S'agissant des mineurs âgés de plus de 13 ans, « *l'opportunité du prélèvement doit être appréciée avec rigueur, à l'issue d'un dialogue entre l'officier de police judiciaire et le parquet.* »

C. LE SIGNALEMENT DES PERSONNES : À LA RECHERCHE DES « SIGNES PHYSIQUES PARTICULIERS, OBJECTIFS ET PERMANENTS »

Les fichiers d'antécédents judiciaires, que sont STIC et JUDEX, peuvent contenir des données sensibles, au sens de l'article 8 de la loi du 6 janvier 1978, « **dans les seuls cas où ces données [...] se rapportent à des signes physiques particuliers, objectifs et permanents, en tant qu'éléments de signalement des**

⁽¹⁾ La liste des infractions est détaillée à l'article ANNEXE III du décret n° 2006-1411 du 20 novembre 2006 portant création de JUDEX et à l'article ANNEXE III du décret n° 2001-583 du 5 juillet 2001 portant création du STIC.

personnes, dès lors que ces éléments sont nécessaires à la recherche et à l'identification des auteurs d'infractions. »⁽¹⁾

Il n'est cependant pas facile de définir précisément la manière de caractériser une personne, à partir de ses « signes physiques particuliers, objectifs et permanents. » Lorsqu'une infraction est commise, les services de police et de gendarmerie ont besoin d'informations aussi précises que possible leur permettant d'identifier rapidement les auteurs de ces infractions ou d'engager des recherches à partir des éléments de description du suspect tels qu'ils sont donnés par la victime ou les témoins. Si cette nécessité opérationnelle n'est contestée par personne, les modalités de cette identification et de son enregistrement dans les fichiers prêtent davantage à discussion. Faut-il **recourir à une typologie ethno- raciale**, comme celle actuellement utilisée dans le STIC-Canonge et dans son équivalent JUDEX, ou bien faut-il **considérer la couleur de peau comme un « signe physique objectif », au même titre que la couleur des yeux ou des cheveux ?** Si, sur le plan des principes, nombreuses sont les voix qui s'élèvent pour dénoncer la situation qui prévaut actuellement dans le STIC-Canonge, encore faut-il proposer une solution alternative capable de répondre aux besoins des enquêteurs.

1. Le STIC-Canonge et son équivalent JUDEX : une identification des personnes recherchées basée sur une typologie ethno- raciale

Créé en 1950 par l'inspecteur principal René Canonge de la sûreté urbaine de Marseille, il s'agissait, à l'origine, d'un **fichier signalétique manuel avec photographie**. Développé dans le cadre du système de traitement des infractions constatées (STIC) et **informatisé en juin 1992**, le logiciel Canonge permet d'identifier un auteur d'infraction à partir du signalement donné par une victime ou un témoin. L'identification se fait au moyen d'une base documentaire (textes et photographie) constituée de notices individuelles pour chaque personne déjà mise en cause dans une procédure judiciaire. On estime que grâce aux deux millions de personnes recensées, **il permet chaque année d'identifier plus de 30 000 personnes.**

Chaque notice individuelle comprend la photographie, l'identité complète ainsi que l'adresse de la personne mise en cause, les infractions pour lesquelles le mis en cause a été signalé, les références des procédures, les complices éventuels ainsi que les **éléments du signalement du mis en cause**. Parmi ces derniers, on trouve le sexe, le type, l'âge apparent, la taille, la corpulence, les cheveux, la couleur des cheveux, la couleur des yeux, l'accent et les signes particuliers.

Dans la partie « *signalement* », **un filtre sur le « type » distingue 12 types différents** : blanc (caucasien) ; méditerranéen ; gitan ; moyen-oriental ; nord-

⁽¹⁾ Article 1 du décret n° 2001-583 du 5 juillet 2001 portant création du système de traitement des infractions constatées et article 1 du décret n° 2006-1411 du 20 novembre 2006 portant création du système judiciaire de documentation et d'exploitation dénommé « JUDEX ».

africain maghrébin ; asiatique eurasiens ; amérindien ; indien (Inde) ; métis mulâtre ; polynésien ; mélanésien canaque. De nombreux observateurs, comme SOS Racisme, émettent de fortes réserves à l'égard du fichier STIC-Canonge, dans la mesure où il opère **une classification sur la base d'une nomenclature fondée en partie sur les appartenances « ethno-raciales »** supposées. De surcroît, cette classification ne figure dans aucun texte et semble contraire aux principes figurant dans le Préambule de la Constitution, qui postule l'unicité du peuple français à son article 1^{er}. Enfin, les catégories, qui sont actuellement utilisées dans le cadre de la typologie STIC-Canonge, méconnaissant le « *métissage* » de la population.

2. Les nouvelles classifications proposées par le groupe de travail d'Alain Bauer en 2006 : des amendements à la marge de la typologie Canonge

Dans le cadre de ses travaux sur l'évolution du fichier STIC-Canonge, et notamment des types mentionnés en vue de l'identification puis de l'interpellation des individus recherchés, le groupe de travail, présidé par M. Alain Bauer, avait proposé **en 2006 une nouvelle déclinaison**, reposant sur la suppression du type « *gitan* » et la redéfinition des autres types, à savoir : européen (avec trois subdivisions : nordique, caucasien, méditerranéen) ; africain/antillais ; métis ; maghrébin ; moyen-oriental ; asiatique ; indo-pakistanaï ; latino-américain ; polynésien ; mélanésien.

À ce jour, et au regard des auditions réalisées par vos rapporteurs, **les services de la police nationale, contrairement à ceux de la gendarmerie, n'ont pas mis en œuvre cette nouvelle typologie**, pour des raisons techniques liées à la difficulté de requalifier le stock des données au regard de la nouvelle classification. Bien que les propositions faites en 2006 n'aient pas été mises en œuvre, le groupe de travail sur les fichiers de police a recommandé **en 2008 de nouvelles modifications de la classification Canonge** : le type « européen » disparaît au profit du type « *caucasien* » et « *méditerranéen* », alors que le type « *asiatique* » devient le type « *asiatique/eurasiens* ». De la même manière, le type « *latino-américain* » disparaît au profit du type « *amérindien* ». Le groupe de travail a également rappelé sa volonté de voir disparaître le type « *gitan* », tout en recommandant la requalification du stock existant.

Or, **ces différentes propositions** d'amendement à la marge de la typologie Canonge **ne semblent pas faire l'unanimité** au sein même du groupe de travail présidé par M. Alain Bauer. En effet, M. Jean-Marc Leclerc, journaliste au *Figaro*, a fait observer que « *concernant le fichage Canonge des personnes, et son équivalent dans le fichier JUDEX de la gendarmerie, il importe de constater que les forces de l'ordre ne sont pas demandeuses d'une réforme. Ces professionnels sont le mieux à même d'exprimer, dans un souci de pragmatisme, quelle typologie représente le moyen le plus efficace d'identifier un auteur d'infraction quand débute une enquête.* » Par ailleurs, M. Christian Lothion, directeur central de la police judiciaire, a souligné lors de son audition par vos rapporteurs que les

recommandations successives faites par le groupe de travail présidé par M. Alain Bauer n'ont pas été prises en compte pour des raisons essentiellement techniques : « **le problème, c'est de répartir différemment une catégorie en plusieurs catégories** ». Ainsi, le groupe de travail proposait-il en 2006 que la catégorie « *blanc caucasien* » soit subdivisée en trois sous-catégories (nordique, caucasien, méditerranéen). Or, cette nouvelle typologie impliquait d'isoler les « *blancs caucasiens* » des deux millions de personnes recensées dans le Canonge (soit plus de 500 000) et de passer en revue manuellement l'ensemble des fiches afin de les répartir dans les sous-catégories adéquates. Aux dires des services, il s'agit là d'**un vrai problème technique, qui aurait nécessité la mobilisation de nombreux agents, sans que l'utilité de cette nouvelle typologie soit avérée**. Aussi a-t-il émis des doutes sur la pertinence de la requalification de la catégorie « *amérindien* », qui deviendrait « *latino-américain* ». De la même manière, dans sa contribution au deuxième rapport du groupe de travail sur les fichiers de police, **la Haute autorité de lutte contre les discriminations (HALDE)** rappelle qu'elle ne peut considérer que « *la classification proposée institue un outil fondé sur des critères objectifs* », insistant sur le fait que « **la typologie ainsi proposée, comme celle qui existe déjà, fait davantage référence à l'origine dite « ethnique » des personnes qu'à leurs caractéristiques physiques objectives** »⁽¹⁾.

3. Identification des personnes recherchées : typologie ethno-raciale versus portrait-robot

Les **principales critiques** résident dans le fait que la typologie, ainsi proposée, comme celle qui existe déjà, fait davantage référence à l'origine dite « *ethnique* » des personnes qu'à leurs caractéristiques physiques objectives.

Afin d'appuyer l'avis défavorable qu'elle a émis à l'encontre de la typologie proposée, la HALDE a tenu à souligner dans sa contribution au rapport sur les fichiers de police remis en 2008 au ministre de l'Intérieur que « *la reprise du terme « latino-américain » utilisé aux États-Unis et en Grande-Bretagne pour définir une catégorie ethno-raciale semble particulièrement éloquente à ce sujet, tout comme le type « africain/antillais » qui s'apparente plus à l'origine réelle ou supposée des intéressés qu'à leur description physique* ». L'autre **risque mis en avant** par des autorités, comme la HALDE et la Commission nationale consultative des droits de l'homme, ou des associations, comme SOS Racisme, est celui de la mise en place de **statistiques ethniques, à partir des données collectées et des informations présentes dans le STIC ou dans JUDEX**, tendant à générer du racisme en établissant, par exemple, que l'appartenance à tel type ethno-racial est surreprésentée parmi certains auteurs de crimes ou délits.

Dans ses recommandations du 16 mai 2007 sur la mesure de la diversité et la protection des données, **la CNIL** avait, de manière plus générale, émis de **fortes réserves sur la création d'une nomenclature nationale de catégories « ethno-**

⁽¹⁾ Rapport « Mieux contrôler la mise en œuvre des dispositifs pour mieux protéger les libertés » remis au ministre de l'Intérieur (décembre 2008), page 116.

raciales » et avait estimé que la décision de principe de créer une telle nomenclature, si elle devait être utilisée de façon obligatoire, relèverait du législateur, sous le contrôle du Conseil constitutionnel.

C'est pourquoi, comme le souligne SOS Racisme, dans sa contribution au rapport Bauer sur les fichiers de police⁽¹⁾ (2008), il serait plus judicieux pour le STIC-Canonge de **faire référence « à la couleur de peau telle que perçue par les témoins »**. Ainsi, le signalement de la personne mise en cause se ferait à partir de sa couleur de peau, au même titre que la couleur de ses cheveux ou de ses yeux. La couleur de peau constituerait, pour M. Alain Bauer, un « **critère objectif stable** », davantage adapté au métissage à l'œuvre dans la société française.

Ainsi, vos rapporteurs considèrent qu'il est nécessaire de **mettre un terme définitif à la typologie actuellement utilisée pour le STIC-Canonge** au profit d'une identification des personnes recherchées fondée sur les éléments constitutifs du portrait-robot, dont la couleur de peau, telle que perçue par les témoins ou la victime, fait partie.

Proposition n° 22

Remplacer la typologie ethno-raciale du STIC-Canonge et de son équivalent JUDEX par les éléments du portrait-robot, dont la couleur de peau est une composante au même titre que la couleur des yeux et des cheveux, par exemple.

⁽¹⁾ « Mieux contrôler la mise en œuvre des dispositifs pour mieux protéger les libertés » - Rapport du groupe de contrôle des fichiers de police et de gendarmerie remis au ministre de l'Intérieur en décembre 2008 – page 126.

III. GARANTIR L'EXACTITUDE DES FICHIERS

Aux termes de l'article 6 de la loi n° 78-17, la licéité des traitements de données à caractère personnel suppose notamment que celles-ci « *sont exactes, complètes et, si nécessaire, mises à jour* » ; en outre, « *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* ». Par-delà le peu d'intérêt d'outils incomplets ou approximatifs pour les services de police eux-mêmes, il convient de souligner combien l'exactitude des données figurant dans les fichiers conditionne très largement leur légitimité aux yeux des citoyens. En pratique, la question de l'exactitude des fichiers de police se pose toutefois en des termes sensiblement différents selon qu'il s'agit de fichiers d'identification ou de fichiers d'antécédents judiciaires. Les premiers ont fait l'objet de précautions particulières dans la définition de leur architecture et de leurs caractéristiques techniques, ce qui s'explique naturellement par le rôle décisif qu'ils peuvent jouer en matière de preuve, à charge ou à décharge. Ils n'en connaissent pas moins des problèmes sérieux, liés non pas à l'inexactitude des informations saisies, mais aux délais observés pour faire face aux flux croissants de signalements en provenance des services enquêteurs. S'agissant des fichiers d'antécédents, et singulièrement du STIC, la situation est complètement différente : c'est au niveau des données saisies elles-mêmes et de l'ensemble du processus de contrôle de la qualité que se situent les difficultés. Celles-ci sont telles qu'il est malheureusement illusoire de compter sur les dispositifs actuels de mise à jour par les autorités judiciaires ou, en dernier ressort, par la CNIL, pour espérer pouvoir remédier au volume considérable des erreurs de toutes sortes, de portée inégale, mais parfois très sérieuses.

A. DES FICHIERS D'IDENTIFICATION QUI ONT DU MAL À INTÉGRER ET À EXPLOITER LE FLUX DES DONNÉES

1. Une modernisation nécessaire du fichier automatisé des empreintes digitales

• Créé par le décret n° 87-249 du 8 avril 1987 (modifié par le décret n° 2005-585 du 27 mai 2005), le **fichier automatisé des empreintes digitales** (FAED) est un fichier commun à la police et à la gendarmerie nationales. Il permet, d'une part, **d'identifier les traces digitales et palmaires** relevées sur les scènes d'infraction, afin de **rechercher et d'identifier les auteurs** de crimes ou de délits, et, d'autre part, de **détecter les usurpations d'identité et les identités multiples**. À cet effet sont enregistrées dans le FAED : les traces relevées au cours des enquêtes judiciaires ou sur ordre de recherches délivré par une autorité judiciaire ; celles relevées à l'occasion d'une enquête ou d'une instruction pour recherche des causes d'une disparition inquiétante ou suspecte ; les empreintes relevées, dans le cadre des enquêtes pour crimes ou délits, sur les personnes à l'encontre desquelles il existe des indices graves ou concordants ; enfin, les

empreintes relevées dans les établissements pénitentiaires afin de s'assurer de l'identité de la personne détenue et d'établir les cas de récidive.

La **durée de conservation** des données est de 25 ans au maximum pour les empreintes (ou jusqu'aux 70 ans de la personne) et fonction du délai de prescription de l'action publique pour les traces (3 ans pour les délits et 10 ans pour les crimes).

• Alors qu'auparavant les fiches papiers étaient toutes envoyées par courrier aux divers centres d'alimentation du FAED pour saisie manuelle, ce qui représentait un énorme travail, ce fichier est désormais pour partie alimenté par les commissariats grâce des **terminaux de signalisation**, dans 58 % des cas. Leur équipement au moyen de **deux types de bornes** autorise une transmission en temps réel des empreintes digitales. Il s'agit des bornes T1, présentes dans 52 sites traitant un haut volume de signalisation et d'une valeur unitaire de 75 000 euros. Ce type de terminal permet la capture sans encrage sur un bloc optique et la numérisation immédiate des relevés dactyloscopiques. Les bornes T4, au nombre de 251 et d'une valeur unitaire de 15 000 euros, offrent seulement une faculté de numérisation des fiches papiers. Par ailleurs, en cas d'urgence nécessitant une réponse rapide, les empreintes relevées peuvent être envoyées par télécopie.

Cette modernisation des modalités de transmission permet également aux services enquêteurs de **bénéficier d'un retour d'information beaucoup plus rapide**. Un résultat en matière d'identification et de rapprochement peut ainsi être obtenu dans un délai de cinq à six heures par l'intermédiaire des bornes. Dans tous les cas, le FAED établit une simple liste de rapprochements potentiels, auxquels sont associés des seuils de correspondance. Une validation humaine est toujours requise au terme du processus par un travail de dactyloscopie ⁽¹⁾.

Au 1^{er} octobre 2008, le FAED comptait **2 998 523 individus enregistrés** et 171 801 traces non identifiées. Environ **4,7 % de la population** française y figurent. La France reste parmi les pays européens dont la base de données dactylaires est assez peu volumineuse rapportée à la population, puisque ce taux représente 11,8 % au Royaume-Uni et 7 % en Italie. La position relative de la France se rapproche davantage de celles de l'Espagne (4,8 %) et de la Belgique (4,7 %), tandis que la proportion de personnes dont les empreintes digitales ont été relevées représente 4 % en Allemagne.

Entre le 1^{er} janvier et le 1^{er} octobre 2008, le FAED a **permis d'identifier 11 697 traces** (plus de 13 000 sur l'ensemble de l'année 2007) et de détecter 61 273 usurpations d'identités ou identités multiples.

• Le FAED doit cependant faire face à **deux grandes difficultés** : une **alimentation inégale** en quantité et en qualité, d'une part, et une **technologie dépassée**, d'autre part.

⁽¹⁾ Pour réaliser une identification, les normes internationales exigent 12 points caractéristiques homologues et sans différences.

De fait, ce n'est qu'à partir de 2003 que le rythme annuel des saisies de fiches décadaclaires s'est accéléré. Ainsi, alors que le fichier est passé d'un à deux millions d'individus entre 1998 et le début de 2005, il est ensuite passé de deux à trois millions d'individus en trois ans. Cette accélération significative au cours des cinq dernières années s'explique par l'augmentation constante du nombre de gardes à vue, mais aussi par le déploiement des terminaux de signalisation et par le développement de la police technique permettant une augmentation des signalisations des mis en cause. Toutefois, en moyenne, que ce soit pour la police ou la gendarmerie, seulement 80 % des gardes à vue pour lesquelles la signalisation est possible donnent lieu à un relevé d'empreintes digitales. La **contribution de la gendarmerie nationale à l'alimentation du FAED reste insuffisante, faute de moyens adaptés**. La part de la gendarmerie dans le total des fiches enregistrées n'a cessé de baisser entre 2004 et 2007, passant de 22,3 % à 14,8 %. Celle-ci n'est en effet pas dotée de bornes, ce qui se traduit par des délais importants pour la remontée à l'échelon de la région des relevés décadaclaires effectués par les brigades territoriales, même si les réseaux Rubis et Saphir sont utilisés à titre de palliatif. En outre, la plate-forme FAED du service technique de recherches judiciaires et de documentation (STRJD) connaît des difficultés importantes d'enregistrement des fiches qui lui sont transmises en raison d'une insuffisance de personnels. Tous ces éléments pèsent de manière dommageable sur l'efficacité générale du fichier, et sont à l'origine d'une certaine démotivation des personnels.

Par ailleurs, des **progrès doivent être réalisés en matière de qualité des relevés** effectués. Celle-ci reste en effet inégale, avec près de 7 % de cas où elle est tellement insuffisante qu'il ne peut être procédé à l'enregistrement. Avec le système actuel, il n'est malheureusement pas possible d'identifier la provenance géographique des relevés d'empreintes dont la qualité est la moins satisfaisante ; avec le nouveau moteur du fichier, il sera possible d'identifier les régions ou les unités « défaillantes » et d'adapter en conséquence la politique de formation des personnels si le taux d'erreur dépasse un certain seuil.

Le moteur actuel du FAED est constitué par la version 3.1 du système MORPHO, qui **date de 1999** et permet seulement des rapprochements d'empreinte à empreinte ou des rapprochements d'empreinte à trace. Compte tenu du volume atteint par le fichier et du nombre accru de demandes de comparaisons, ce système apparaît désormais **sous dimensionné et a atteint ses limites**. Une **nouvelle version** du moteur sera **opérationnelle à la fin de l'année 2009 ou au début de l'année 2010** : le système **MetaMorpho**, développé par la SAGEM. Adaptée aux bornes T1 et T4, cette version offrira des algorithmes de calcul plus performants, permettant de faire des **rapprochements de trace à trace**. L'exploitation des **empreintes palmaires**, dont la collecte a déjà commencé, va augmenter le nombre de rapprochements⁽¹⁾. Il est donc probable que dès les

(1) 300 000 empreintes palmaires ont été collectées depuis la mise en service des terminaux T1 et T4. La préfecture de police a, pour sa part, conservé 20 000 paires d'empreintes palmaires, notamment en raison d'une vieille tradition locale d'enregistrement pour les « beaux voyous ».

premiers mois de sa mise en place, MetaMorpho va permettre de résoudre de nombreuses affaires ou donner de nouvelles pistes d'enquêtes. Selon les mots d'un des responsables auditionnés, « *cela va 'hiter'* ». On rappellera à cet égard que le FAED comprend 171 000 traces non résolues.

Par-delà les progrès technologiques, il faudra veiller à ce que la politique menée en matière de ressources humaines permette de disposer des personnels nécessaires pour exploiter pleinement l'outil modernisé. Un soin tout particulier doit ainsi être apporté à **la formation et à l'entretien du « vivier »** des dactylotechniciens (dits « **traceurs** ») ; la transmission de ces compétences très pointues est en effet essentielle pour l'efficacité du fichier.

Proposition n° 23

Afin de garantir une meilleure alimentation du fichier automatisé des empreintes digitales, déployer de bornes de signalisation T1 et T4 dans les unités de la gendarmerie nationale, aussi bien dans les 100 brigades départementales de renseignements et d'investigations judiciaires que dans les unités territoriales les plus chargées.

2. Des garanties très sérieuses d'exactitude des données en matière d'empreintes génétiques

a) Un processus d'alimentation du FNAEG très encadré, afin de garantir l'exactitude des informations

• Comme a pu le relever un magistrat entendu par vos rapporteurs, le FNAEG est un outil qui fonctionne selon un cahier des charges précis et respecté. À la différence du STIC, **il s'agit d'un fichier très normé et cloisonné**. Lors de la mise en place du FNAEG, il a été décidé de ne pas « lésiner » sur les garanties d'exactitude, et celles-ci sont sans comparaison avec celles offertes par son homologue britannique. Ces **garanties** s'expriment à plusieurs niveaux.

Tout d'abord, la France est le **seul pays en Europe** à avoir mis en place un **système de conservation des prélèvements biologiques**, aussi bien s'agissant de kits FTA de prélèvement que de pièces à conviction (certaines étant préservées par cryogénie). Ces éléments sont conservés au sein du service central de préservation des prélèvements biologiques (SCPPB), situé à Pontoise. L'ensemble des prélèvements biologiques est archivé **pour une durée de quarante ans**, ou jusqu'aux 80 ans de l'individu ayant fait l'objet d'un prélèvement.

Dès réception du dossier par la sous-direction de la police scientifique et technologique, située à Écully, **une cellule dite « contentieux juridique »** en examine avec soin tous les éléments avant intégration dans le fichier, pour **vérifier que les dispositions législatives et réglementaires ont bien été respectées** à tous les stades de la procédure (nature de l'affaire, réquisition d'un OPJ, etc.). Au total,

cette cellule identifie et traite entre 2 000 et 3 000 dossiers par an comprenant des anomalies administratives diverses.

Un **système de saisie en double aveugle** est destiné à limiter les risques d'erreurs au stade de l'alimentation. Lorsque le résultat d'analyse en provenance d'un laboratoire parvient à Écully⁽¹⁾, les opérateurs saisissent manuellement la totalité du profil génétique. Pour chaque profil, ils renseignent également les données nominatives (état civil, filiation, etc.) ainsi que les données relatives à l'infraction (date de jugement, tribunal, requérant, etc.) et au kit utilisé (numéro de code barre, nom de la personne ayant effectué les tests en laboratoire). L'ensemble de ces données fait ensuite l'objet d'une seconde saisie, afin d'en garantir la cohérence et l'exactitude. Toutes ces précautions présentent un coût, mais offrent assurément des **garanties infiniment supérieures au système adopté au Royaume-Uni**, où seulement 25 % des profils sont traités en double analyse, sur la base d'un choix aléatoire.

Enfin, les **comparaisons** réalisées par le système informatique sont **validées par un expert**. Le moteur du fichier offre un certain nombre de propositions de rapprochements, qu'il appartient à un opérateur de vérifier. Il revient ensuite à un biologiste, ayant le statut d'expert agréé auprès d'une cour d'appel, de se prononcer sur le résultat définitif du rapprochement.

Le taux d'erreur de saisie apparaît en conséquence très faible. Sur les six premiers mois de 2008, 11 profils n'ont pas pu être validés en raison d'incohérences, les erreurs affectant de manière égale la police et la gendarmerie nationales, ainsi que les laboratoires privés et publics. Il convient de souligner que ces incohérences ont pu être identifiées par l'application des différentes procédures de contrôle de la qualité, les fiches incomplètes étant renvoyées aux responsables initiaux des erreurs.

• Toujours au titre des garanties, on relèvera que l'article R. 53-16 du code de procédure pénale dispose que **le FNAEG est placé sous le contrôle d'un magistrat du parquet hors hiérarchie**, nommé pour trois ans, et assisté par un comité de trois personnes. Cette équipe est formée actuellement par un magistrat du parquet, un informaticien (directeur à l'INSERM) et un biologiste. Le magistrat référent est également en charge du suivi du fonctionnement du SCPPB.

Le rôle du magistrat référent porte avant tout sur **le contrôle de la définition des processus et de leur mise en œuvre**, ainsi que sur la validation des éventuelles modifications qui pourraient apparaître nécessaires. En trois ans, l'actuel titulaire n'a été saisi d'aucune requête individuelle à des fins de rectification. En pratique, ce magistrat effectue plusieurs visites par an sur place

⁽¹⁾ Si dans la plupart des cas les résultats d'analyse sont transmis par courrier sous forme papier, certains laboratoires transmettent d'ores et déjà les résultats des prélèvements par CD-Rom. Ce dernier mode de transmission simplifie la procédure d'alimentation du FNAEG, mais ralentit toutefois le rythme d'intégration, les supports numériques étant envoyés seulement lorsqu'ils comportent un nombre suffisant de profils.

pour contrôler le fichier. Il est destinataire de l'ensemble des rapports de service du SCPPB et du FNAEG. Il joue également un **rôle de conseil**, les services de police technique et scientifique chargés de l'administration du fichier le sollicitant sur des points juridiques délicats.

b) Vers la fin de la crise de croissance du FNAEG ?

Le FNAEG a énormément changé depuis sa création ⁽¹⁾. Il est passé d'un fichier où n'étaient recensés que les condamnés pour certains crimes et délits, soit environ 10 000 personnes par an, à un fichier comprenant plusieurs centaines de milliers d'inscriptions d'individus supplémentaires chaque année, le signalement étant désormais opéré pour l'essentiel à l'initiative d'un OPJ ⁽²⁾. Or, comme l'a relevé un des magistrats auditionnés, en 2004, « nous étions encore dans le domaine de l'utopie, car le Parlement avait multiplié les exigences sans se soucier de la logistique ». La **grande affaire du FNAEG** ces dernières années a donc été **d'absorber l'augmentation considérable des flux de prélèvements**, conséquence directe de l'élargissement de l'objet du fichier. Aussi un double engorgement s'est-il manifesté, s'agissant non seulement de l'analyse des empreintes par les laboratoires, mais aussi au stade de l'insertion des résultats obtenus dans le fichier lui-même. De l'« artisanat », il a fallu passer à l'« industrialisation ».

• Le **premier point** qui avait été **mal anticipé** concerne les **capacités des chaînes de génotypage des laboratoires publics**. Un recours important à des laboratoires privés a permis pour partie de combler ces lacunes pendant la phase d'amélioration des capacités des laboratoires publics. La capacité de traitement est désormais répartie de la manière suivante : le site de l'Institut national de la police scientifique (INPS), à Lyon, peut traiter 120 000 empreintes par an ; l'Institut de recherches criminelles de la gendarmerie nationale est en mesure de traiter environ 80 000 profils ; enfin, les laboratoires privés CODGENE (Strasbourg) et IGNA ⁽³⁾ (Nantes) disposent à eux deux d'une capacité d'environ 300 000 analyses par an. Les capacités d'analyses des laboratoires publics devraient encore progresser en 2009. L'objectif fixé pour 2009 est de doubler la capacité automatisée de génotypage du laboratoire de Lyon, afin de passer de 10 000 à 20 000 profils par mois. À cet effet, 2,5 millions d'euros sont affectés à l'acquisition de matériels supplémentaires pour l'INPS et au recrutement de 10 techniciens biologistes supplémentaires. Cette mesure devrait permettre de faire face au flux de demandes nouvelles et de traiter progressivement le retard accumulé, soit plus de 80 000 profils à la fin de l'année 2008.

⁽¹⁾ L'origine de ce fichier remonte à l'adoption d'un amendement présenté par Mme Frédérique Bredin et M. Jacques Floch à l'occasion de l'examen du projet de loi relatif à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs. JO Débats Assemblée nationale, séance du 30 septembre 1997, pages 36 et 37.

⁽²⁾ Au 1er octobre 2008, la base de données contenait les empreintes génétiques de 38 184 traces non identifiées et de 806 356 individus. La montée en puissance du fichier est très récente et rapide, puisqu'en 2005 seulement 119 612 individus figuraient dans la base FNAEG.

⁽³⁾ Institut génétique Nantes Atlantique.

Les investissements consentis en faveur des laboratoires publics ont parfois été critiqués en raison du **ralentissement du flux annuel de profils à saisir pouvant être anticipé à terme**. Compte tenu du fait que de nombreux délinquants d'habitude n'ont pas vocation à être signalés de nouveau, le système finira par atteindre une forme de « plateau » s'agissant de l'intégration de nouveaux profils. Toutefois, l'existence d'une filière publique permettra d'éviter la reconstitution d'une position oligopolistique des laboratoires privés, qui n'a pas été sans influence sur les coûts lors de la mise en place du fichier. Dès 2005, une mission de l'IGPN sur la maîtrise des coûts en matière génétique a été créée, dont l'un des premiers effets a été une baisse significative des tarifs pratiqués par les laboratoires privés, de peur d'un tarissement des commandes publiques. **Le coût unitaire de la réalisation d'un profil est ainsi passé de 350 euros à 80 euros, avant d'être ramené au niveau actuel d'environ 50 euros**. Compte tenu d'un flux annuel d'environ 400 000 analyses actuellement, les coûts associés à l'alimentation du FNAEG restent encore importants.

• Le **deuxième goulet d'engorgement** du FNAEG se situe à l'étape de **l'intégration des données dans la base**. Outre le fait que les procédures sont particulièrement lourdes, **l'insuffisance de personnels** a eu un impact direct sur la vitesse de mise à jour du fichier en fonction de résultats d'analyses reçus. Compte tenu du retard dans la saisie, les délais observés ont pu atteindre jusqu'à un an, ce qui n'a pas été sans conséquences sur la perception de l'utilité du fichier au sein des services enquêteurs dans un premier temps.

En outre, lors du déplacement à Écully, les personnes rencontrées ont été unanimes pour considérer que le FNAEG était actuellement dans une « *phase techniquement difficile* ». Les **logiciels du traitement n'ont en effet pas été prévus pour traiter une telle masse d'information**. Actuellement, le FNAEG fonctionne avec **un moteur de recherche de secours**, le CODIS, développé par le FBI ; le moteur développé par les services informatiques du ministère de l'Intérieur n'a pas résisté à la montée en puissance du fichier et a accumulé des temps de réponse prohibitifs. Après des développements assez laborieux, un nouveau moteur devrait être déployé prochainement, avec pour objectif de ramener de huit minutes à 20 secondes le temps nécessaire pour effectuer une comparaison de profil.

Pour faire face à cette situation, dès 2006 des **vacataires** sont venus renforcer le service gestionnaire à plusieurs reprises, leur effectif atteignant jusqu'à trente personnes entre mars et novembre 2006. Environ 50 personnes sont affectées à la saisie des données sur le site d'Écully et, avec le recours aux vacataires en période de pointe, les effectifs peuvent être portés à 90. Le temps de réponse dans l'alimentation est désormais jugé satisfaisant et il n'y a plus de difficultés liées à la surcharge des profils à « rentrer ».

L'utilité du fichier est désormais bien perçue par l'ensemble des services enquêteurs s'agissant des affaires de criminalité ou de délinquance sérieuse. Il a **permis de rapprocher 17 190 affaires depuis sa création**.

EXEMPLE D'AFFAIRE RÉSOLUE GRÂCE AU FNAEG

Dans le cadre des constatations techniques effectuées sur la scène d'un nouveau fait de viol perpétré en 2007 à Grenoble, plusieurs traces papillaires latentes étaient mises en évidence dans l'appartement de la victime.

Deux traces papillaires, exploitées au FAED, identifiaient un individu connu pour actes d'exhibition sexuelle et violation de domicile en 1998.

À la suite d'un prélèvement biologique effectué sur l'individu, le FNAEG rapprochait le profil extrait de ce prélèvement avec les profils extraits de dix traces différentes, relevées dans dix affaires de viol et agressions sexuelles aggravées, toutes perpétrées à Grenoble.

L'histoire du FNAEG n'est malheureusement pas composée seulement de succès. Des dysfonctionnements se sont en effet manifestés, le plus célèbre étant celui de la non-inscription du profil de Bruno Cholet dans le fichier, alors qu'un prélèvement avait été opéré en 2005. Le dossier envoyé par un laboratoire privé étant incomplet, il n'avait pas été possible d'intégrer les résultats d'analyse. Il avait été adressé en retour au service de police ayant fait la demande, sans qu'un suivi soit assuré de son évolution. L'obligation pour les OPJ d'effectuer désormais leurs réquisitions par voie de message informatique, toutes les demandes sous forme papier étant refusées, devrait offrir une plus grande traçabilité. Néanmoins, l'engorgement du FNAEG a pu avoir des conséquences dommageables sur l'élucidation de certains crimes. Ainsi, alors qu'un prélèvement ADN sur l'auteur d'une agression sexuelle arrêté en flagrant délit en Seine-Saint-Denis en 2006 aurait pu permettre d'effectuer rapidement un rapprochement avec l'auteur présumé de trois viols commis entre 2004 et 2005, celui-ci n'a été élucidé qu'à l'automne 2007 car « *cette agression n'était pas considérée comme prioritaire. L'empreinte génétique de son auteur n'a été inscrite au fichier national qu'un an après* »⁽¹⁾, selon un enquêteur.

En outre, il conviendra d'être particulièrement vigilant sur les conditions pratiques d'alimentation du fichier compte tenu de **l'augmentation prévisible des analyses de traces** découlant de la généralisation des prélèvements sur des scènes d'infraction. Le plan triennal 2008-2010 pour une police technique et scientifique plus performante dans la lutte contre la délinquance de masse fixe en effet l'objectif de couvrir par l'investigation technique, dès lors que des traces peuvent être recueillies, 100 % des cambriolages, des véhicules signalés volés et découverts, ainsi que 100 % des autres délits de voie publique. La rapidité du retour d'information vers les enquêteurs apparaît comme l'une des conditions de l'efficacité de la politique de systématisation du recours à la police technique et scientifique.

(1) « Le violeur parisien trahit par son ADN », Le Parisien, samedi 13 octobre 2007.

c) Préciser davantage les circonstances dans lesquelles un prélèvement peut être effectué

Comme l'a indiqué un responsable du ministère de la Justice, « **la prise d'ADN en profil était un peu trop systématique** ».

• L'article 706-55 du code de procédure pénale fixe le champ des infractions pour lesquelles un prélèvement biologique est possible. Son extension a notamment été justifiée par une évolution qualitative de la délinquance : d'une part, les auteurs de crimes et de délits seraient de moins en moins spécialisés et de plus en plus « multicartes », d'autre part, il s'avère qu'ils laissent désormais peu d'empreintes digitales exploitables. Ces dernières tendent donc à être remplacées par les traces biologiques pour confondre les délinquants et criminels. Il convient de rappeler à cet égard que l'article 706-54 prévoit que « *les empreintes génétiques conservées dans ce fichier ne peuvent être réalisées qu'à partir de segments d'acide désoxyribonucléique **non codants**, à l'exception du segment correspondant au marqueur du sexe* », c'est-à-dire qu'ils ne permettent pas de déterminer les caractéristiques organiques, physiologiques ou morphologiques des personnes concernées.

Le dispositif législatif présente cependant encore plusieurs ambiguïtés qu'il convient de lever.

L'article 706-54 dudit code prévoit les **trois cas de figure** pour lesquels il est **possible d'effectuer un prélèvement biologique** sur une personne, tout refus pouvant être sanctionné au titre du II de l'article 706-56⁽¹⁾ :

- le premier alinéa prévoit le cas des **personnes condamnées** pour l'une des infractions entrant dans le champ du fichier ;

- le deuxième alinéa concerne les personnes à l'encontre desquelles il existe des **indices graves ou concordants** qu'elles aient commis l'une de ces infractions ;

- le troisième alinéa porte sur toute personne « *à l'encontre de laquelle il existe **une ou plusieurs raisons plausibles de soupçonner qu'elle a commis un crime ou un délit*** ». Dans ce cas, il s'agit **simplement d'un prélèvement à fin de comparaison**, et non pas pour enregistrer un profil supplémentaire dans le fichier. Cette faculté a notamment été utilisée dans des affaires criminelles pour vérifier si l'auteur des faits habitait dans le village où ils avaient été commis, comme dans le cas de l'assassinat de la famille Flactif au Grand-Bornand, en 2003.

Pour les condamnés et les suspects visés à l'alinéa 2, la possibilité de prélever est strictement limitée aux infractions mentionnées à l'article 706-55. Si cette liste ne comprenait que des infractions d'une particulière gravité aux termes

⁽¹⁾ « *Le fait de refuser de se soumettre au prélèvement biologique [...] est puni d'un an d'emprisonnement et de 15 000 € d'amende. Lorsque ces faits sont commis par une personne condamnée pour crime, la peine est de deux ans d'emprisonnement et de 30 000 € d'amende.* ».

de la loi n° 2001-1062 du 15 novembre 2001 ⁽¹⁾, elle a été très largement étendue par la loi du 18 mars 2003 pour la sécurité intérieure. Demeurent toutefois hors de cette liste d'infractions les délits routiers ou les infractions à la législation sur les étrangers. Au cours des auditions, il a dans l'ensemble été indiqué à vos rapporteurs que dans les cas couverts par le deuxième alinéa, les services enquêteurs avaient plutôt fait preuve de prudence en matière de signalement au FNAEG des mis en cause, préférant s'abstenir en cas de doute. En témoigne le fait qu'en moyenne, aussi bien pour la police que pour la gendarmerie nationales, 50 % des cas de gardes à vue pour lesquelles un prélèvement est juridiquement possible aux termes du deuxième alinéa de l'article 706-54 précité donnent effectivement lieu à une telle opération.

• Toutefois, selon un responsable du ministère de la Justice, « *la prise d'ADN en profil était un peu trop systématique* » et **plusieurs juridictions** de première instance ou d'appel saisies de d'infractions de refus de prélèvement ont rendu des **décisions de relaxe**, au motif qu'elles n'étaient pas en mesure d'apprécier la régularité de la décision des OPJ. Comme le relève une **circulaire du ministère de la Justice du 9 juillet 2008** ⁽²⁾ : « *Dans ces affaires, qui ont jusqu'à présent toutes concerné des « suspects » et non pas des condamnés, les magistrats ont estimé ne pas disposer des éléments suffisants pour apprécier s'il existait réellement des indices graves ou concordants, ou une ou plusieurs raisons plausibles, de soupçonner que l'individu prélevé avait commis un crime ou un délit figurant à l'article 706-55 du code de procédure pénale. Plusieurs juridictions ont ainsi considéré que la simple information selon laquelle l'intéressé faisait l'objet d'une garde à vue ne suffisait pas à caractériser en quoi il était suspect au sens de l'alinéa 3 de l'article 706-54 du code de procédure pénale.* »

S'agissant de prélèvements opérés dans le cadre de l'alinéa 2, la circulaire précitée précise que leur régularité « *suppose donc, soit l'existence de plusieurs indices, même légers dès lors qu'ils sont concordants, soit l'existence d'un seul indice, à condition qu'il soit grave. Ainsi, une personne contre laquelle le seul indice de culpabilité résulte de sa mise en cause par la victime ou par un témoin, si cette mise en cause n'est ni circonstanciée ni corroborée par d'autres éléments de la procédure, ne peut être prélevée sur ce fondement car un tel indice ne peut être considéré comme grave à lui seul.* » De fait, ce texte constitue un rappel de la définition du mis en cause, qui ne saurait être confondue par les services enquêteurs avec le simple fait de mettre une personne en garde à vue.

Quant à la **rédaction du troisième alinéa traitant des « raisons plausibles »**, elle présente un certain flou, puisqu'elle ne renvoie pas expressément à la liste des infractions de l'article 706-55. La **circulaire du 9 juillet enjoint pourtant d'utiliser cette faculté de prélèvement en se limitant**

⁽¹⁾ *Infractions de nature sexuelle ; crimes d'atteinte volontaire à la vie de la personne, de torture et actes de barbarie et de violences volontaires ; crimes de vols, d'extorsions et de destructions, dégradations et détériorations dangereuses pour les personnes ; crimes constituant des actes de terrorisme.*

⁽²⁾ *Annexe 6.*

au champ des infractions pour enregistrement d'un profil au FNAEG. Elle précise très explicitement que même en l'état actuel de la rédaction de l'alinéa 3 « *il convient pourtant de considérer que le champ d'application de ce dernier alinéa est circonscrit aux infractions de l'article 706-55 du code précité. En effet, les débats parlementaires montrent que telle est la volonté du législateur, et une interprétation différente tendrait à détourner le texte de son esprit.* » Par ailleurs, il est indiqué qu'« *enfin, et compte tenu de la vocation initiale de ce traitement, une politique pénale de prélèvements systématiques de personnes mises en cause pour tout crime ou délit ne pourrait qu'alimenter les critiques portées sur le fichier et multiplier les comportements de refus de prélèvements, dont la poursuite et le jugement pourront se révéler problématiques compte tenu d'un fondement juridique fragile.* »

D'une certaine manière, cette circulaire tient compte de décisions judiciaires de relaxe en cas de refus de prélèvement biologique, notamment dans des affaires de « faucheurs volontaires » d'OGM, fondées sur la notion de disproportion ⁽¹⁾. La Cour d'appel de Montpellier a ainsi confirmé en octobre 2008 les relaxes prononcées en première instance par le tribunal correctionnel de Millau et a infirmé une condamnation du tribunal correctionnel de Montpellier, notamment au motif que « *le recueil de l'ADN du prévenu en vue de son identification et de sa recherche était inadéquat, non pertinent, inutile et excessif. Le prélèvement n'étant pas justifié au regard des dispositions de la loi de 1978 [...], il ne saurait être fait grief au prévenu de s'y refuser.* » Le ministère public s'est pourvu en cassation.

Afin de ne pas donner prise aux critiques sur la légitimité d'un fichier dont l'utilité est avérée pour lutter contre des crimes et délits graves, **il apparaît nécessaire de modifier le troisième alinéa de l'article 706-54 du code de procédure pénale.** Un renvoi explicite aux infractions énumérées par l'article 706-55 permettra en effet de mieux encadrer les cas de prélèvements biologiques et d'éviter un certain nombre de contentieux ultérieurs.

Proposition n° 24

Lorsqu'il est possible de réaliser un prélèvement biologique à des fins de comparaison sur une personne à l'encontre de laquelle il existe une « raison plausible » de soupçonner qu'elle a commis un crime ou un délit, la loi n'énumère pas actuellement les infractions concernées. Il est nécessaire de renvoyer explicitement à la liste des infractions pour lesquelles l'enregistrement d'un profil génétique est possible. En conséquence, modifier l'alinéa 3 de l'article 706-54 du code de procédure pénale.

(¹) Arrêts n° 1407 à 1409 du 21 octobre 2008, troisième chambre correctionnelle.

B. UNE CHAÎNE D'ALIMENTATION DU STIC COMPLÈTEMENT OBSOLETE

Comme l'a relevé un responsable de la sécurité publique, « *le STIC est un instrument précieux* ». Malheureusement, ce fichier souffre de nombreux défauts qui réduisent son efficacité opérationnelle et entraînent des conséquences très préjudiciables pour les personnes qui y figurent indûment.

Dans son rapport sur le STIC présenté le 20 janvier 2009 ⁽¹⁾, la CNIL a relevé que « *sur le nombre d'investigations effectuées dans le cadre du droit d'accès indirect à la demande de particuliers [...] entre le 1^{er} janvier et le 31 octobre 2008, il s'avère que seules 17 % des fiches de personnes mises en cause étaient exactes ; 66 % ont fait l'objet d'une modification de portée variable (changement dans la durée de conservation, de qualification pénale, etc.) ; 17 % ont été purement et simplement supprimées du fichier.* » Comme le note la CNIL elle-même, il s'agit d'erreurs relevées dans le cadre d'un droit d'accès indirect et donc sur des fiches qui faisaient, d'une certaine manière, l'objet d'une suspicion d'erreur. On ne peut donc en extrapoler un taux d'erreur général.

Tout d'abord, l'utilisation de fichiers d'antécédents judiciaires dans le cadre d'enquêtes administratives confère une portée malheureusement très concrète aux erreurs de qualification, voire aux inscriptions infondées de personnes en tant que mis en cause, avec des conséquences sur l'accès à certains emplois et à la nationalité française. Ensuite, ce type de fichiers est devenu un outil de travail quotidiennement utilisé par les enquêteurs ; or, des policiers ont indiqué à vos rapporteurs combien ils considéraient avec prudence la valeur des informations figurant dans le STIC. La question posée est donc au moins autant celle du taux d'erreurs que celle de leur origine. Sur ce point, les réponses ont été dépourvues d'ambiguïtés : ce système est, aux dires mêmes de certains de ses utilisateurs, « *complètement dépassé et limité* », car la chaîne de traitement a été pensée à la fin des années 1980, avec une mise en place effective à la fin des années 1990. Elle correspond de ce fait à des moyens techniques datés, très redondants (avec entre trois et cinq niveaux de saisie manuelle des informations) et elle est très « gourmande » en personnels. En outre, il faut d'autant plus souligner l'importance d'un processus d'alimentation de qualité que les contrôles ultérieurs ne permettent pas de garantir une correction effective de l'ensemble des erreurs accumulées, qu'ils soient réalisés par les parquets, notamment dans le cadre de leur mission de mise à jour des fichiers d'antécédents en fonction des suites judiciaires, ou bien en dernier ressort par la CNIL.

De manière générale, le STIC souffre d'un défaut de contrôle interne, les contrôles externes ne permettant pas de remédier ultérieurement dans de bonnes conditions au volume des erreurs accumulées. La comparaison avec le FNAEG est de ce point de vue instructive. Ce dernier obéit à un fonctionnement très étroitement défini et encadré, un magistrat référent assurant en outre un contrôle de la qualité des procédures. Le STIC et JUDEX, pour leur part, n'ont jamais fait

⁽¹⁾ Conclusions du contrôle du système de traitement des infractions constatées, MM. Jean-Marie Cotteret et François Giquel, rapporteurs.

l'objet du moindre rapport de l'IGPN ou de le l'IGGN. S'agissant du STIC, une bonne part des problèmes rencontrés résulte précisément d'une insuffisance de contrôle de la qualité des processus et des pratiques, en partie parce que les gestionnaires considèrent que cela relève davantage des responsabilités de la CNIL. De fait, de l'ensemble des fichiers de police, le STIC apparaît de très loin comme celui connaissant le plus grand nombre de problèmes d'alimentation et de gestion.

1. Une alimentation initiale à la source de nombreuses erreurs

a) « Ce sont les personnels administratifs qui vérifient les procédures des actifs. »

Le **premier degré d'alimentation du STIC** se situe au niveau des commissariats. Il **ne relève pas directement des enquêteurs**. Ceux-ci réalisent des comptes rendus d'infraction (CRI, en cas de plainte contre X) et des comptes rendus d'enquête après identification (CREI, dans les cas où au moins un auteur a été identifié). Ces documents sont imprimés et soumis quotidiennement au chef de service (ou éventuellement au chef d'unité de police judiciaire). C'est donc à un commissaire, ou au moins à un OPJ, qu'il revient normalement de vérifier la qualification des faits et d'effectuer un premier contrôle de la qualité des procédures. Dans la pratique, la qualité de ce travail peut varier en fonction du niveau de formation et de spécialisation en droit pénal, mais aussi en fonction de la disponibilité effective au regard de l'urgence d'autres tâches.

L'ensemble des procédures papiers est ensuite adressé aux agents administratifs chargés du travail de saisie dans le STIC-FCE. Selon les mots d'un responsable d'un syndicat de policiers, ce système est « *une antiquité* », « *un système complètement dépassé qui n'utilise même pas de souris* ». Les personnels administratifs ne disposent pas d'une compétence particulière en droit pénal et de procédure pénale, ce qui ne va pas sans augmenter le risque d'erreur de qualification des faits. Il n'est pas toujours simple pour ces agents d'interpréter les procès-verbaux qui leur sont confiés, d'où des erreurs assez fréquentes. Des représentants syndicaux interrogés à ce sujet ont souligné combien la **formation juridique** de ces personnels est très **largement insuffisante**, avec un nombre trop faible de stages accordés au regard des demandes.

En outre, l'alimentation du STIC est une tâche particulièrement fastidieuse et répétitive. L'organisation du travail devrait en tenir davantage compte. Et ce d'autant plus que le faible attrait de ces postes entraîne un *turn over* important, phénomène aggravé par le fait que les personnels administratifs affectés à la gestion des fichiers de police jugent que leur travail n'est pas valorisé à sa juste mesure et qu'ils bénéficient de très peu de mesures d'avancement. Selon des responsables syndicaux, « *il y a eu une augmentation des gardes à vue, des mis en cause, mais les postes d'administratifs créés ont été affectés à des postes de secrétariat dans les commissariats, et pas à la gestion des fichiers. On fait revenir*

les personnels administratifs à 6 heures du matin pour les statistiques, mais pas pour mettre à jour les fichiers. »

Proposition n° 25

Mettre en place une politique de formation adaptée au profit des agents administratifs affectés à l'alimentation des fichiers.

b) L'enjeu du juste moment de l'inscription au STIC

L'article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure dispose que peuvent figurer dans les fichiers d'antécédents judiciaires des informations nominatives recueillies au cours des enquêtes préliminaires ou de flagrance, ou sur commission rogatoire, s'agissant des « *personnes, sans limitation d'âge, à l'encontre desquelles il existe 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^e classe.

Il convient tout d'abord de noter que, techniquement, l'inscription au STIC intervient dès que l'agent administratif procède à la saisie des procédures effectuées par les enquêteurs. Le système est toutefois différent s'agissant de la préfecture de police de Paris, qui utilise le STIC-Oméga à la place du STIC-FCE : l'inscription du mis en cause sur la base nationale n'intervient qu'à partir du traitement du dossier par la division de la statistique et de la documentation criminelle (DSDC). Pendant un délai de l'ordre de 6 à 7 mois, l'individu mis en cause dans le ressort de la préfecture de police de Paris n'apparaît de ce fait pas dans le STIC.

Mais, quel que soit le mode initial d'alimentation du STIC, local ou centralisé comme à Paris, **il apparaît malheureusement dans les faits que l'inscription dans ce fichier d'antécédents judiciaires est trop souvent pratiquement inéluctable dès qu'une personne est placée en garde à vue** et figure sur un compte rendu d'enquête. Il a été indiqué par des représentants syndicaux que même dans certains cas où les enquêteurs notent en rouge sur le procès-verbal « *ne pas faire figurer au STIC* », les personnels chargés de saisir les données passent outre en appliquant strictement les consignes, par crainte d'une manipulation éventuelle de la procédure. La systématisation de l'inscription au STIC des personnes placées en garde à vue n'est pas sans poser problème, même s'il faut noter que l'augmentation de 41 % des inscrits au STIC entre 2001 et 2009 est inférieure à celle de 71 % du nombre de mesures de garde à vue sur la même période. Il convient cependant de rappeler que, si une personne peut être suspecte au moment où l'officier de police judiciaire décide de son placement en garde à vue ⁽¹⁾, cette mesure nécessaire à la manifestation de la vérité peut permettre de

⁽¹⁾ *L'article 63 du code de procédure pénale dispose que « L'officier de police judiciaire peut, pour les nécessités de l'enquête, placer en garde à vue toute personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis ou tenté de commettre une infraction. »*

conclure que cette personne n'est en fait pas mise en cause. Dans ce cas, elle n'a pas à être enregistrée au STIC, aucune poursuite judiciaire n'étant engagée.

C'est pourquoi, dans certains cas, la hiérarchie policière a érigé en « *bonne pratique* » de différer l'inscription au STIC dans l'attente d'un premier retour du parquet, particulièrement sur des affaires simples et de faible gravité pour lesquelles les classements sans suite sont fréquents. Cette mesure a été mise en œuvre de manière ponctuelle et informelle dans le ressort de la cour d'appel de Montpellier. Elle mérite d'être généralisée tout simplement parce qu'elle respecte la lettre et l'esprit de la loi, mais aussi parce qu'elle répond à l'épineux problème de la prise en compte par les services de police des consignes reçues des parquets dans le cadre du traitement en temps réel (TTR).

Les services de police sont en effet particulièrement réticents à tirer toutes les conséquences des décisions de classement sans suite formulées par téléphone, aux motifs qu'il n'y a pas de trace écrite et que l'opinion du parquet sur les faits est susceptible d'évoluer après transmission de l'ensemble de la procédure. On peut légitimement considérer que **les conséquences de ce formalisme sont particulièrement absurdes**, puisque des dossiers pour lesquels un classement sans suite a été effectivement notifié suivent malgré tout la chaîne procédurale normale, avec inscription au fichier, transmission de la procédure au parquet et seulement ensuite mise à jour éventuelle du fichier sur instruction de ce dernier. Pourtant, les procès-verbaux rédigés par les policiers font expressément mention de la décision du parquet et l'article 3 du décret n° 2001-583 relatif au STIC dispose clairement que « *le responsable du traitement est tenu de modifier ou d'effacer les données enregistrées dès qu'il constate qu'elles sont inexactes, incomplètes ou périmées* ».

Une somme précieuse d'énergie est ainsi consacrée à la laborieuse saisie de dossiers dont on sait par avance qu'ils devront faire l'objet d'un effacement des données par la suite. Sans parler des **conséquences pour les personnes mises en cause à tort, qui peuvent demeurer longtemps au STIC** compte tenu des délais de rectification le plus souvent très long. Il ne s'agit pas d'exemples marginaux : un magistrat d'un des parquets visités a estimé la proportion de ce type d'affaires à environ trois quarts des classements pour insuffisance de charges. On peut enfin noter que dans ces cas d'enregistrement de personnes ne correspondant de fait plus à la notion de mis en cause, l'impact sur les statistiques du commissariat n'est pas négligeable s'agissant du taux d'élucidation, puisque l'enregistrement sur la base locale STIC-FCE apparaît dans la grille E (« élucidé »). Ce phénomène a été confirmé lors du déplacement auprès du SRDC de Versailles, selon un agent administratif, en raison des « *gardes à vue non MEC* » (c'est-à-dire des gardes à vue à l'issue desquelles la personne concernée n'est pas mise en cause), « *environ 10 % des procédures ne devraient pas être dans le STIC* ». En outre, à cette occasion, vos rapporteurs ont pu constater qu'un auteur de faits de violence avec arme entraînant une interruption temporaire de travail ne figurait pas en tant que mis en cause dans le STIC, la procédure n'ayant pas été enregistrée dans les faits constatés. Dans ce cas précis, le SRDC de Versailles a reçu l'avis de suite

judiciaire du parquet alors que la procédure n'était pas encore enregistrée au STIC...

Proposition n° 26

Enjoindre les services de police de tenir compte sans délai des décisions de classement sans suite formulées par les parquets dans le cadre du traitement en temps réel par le biais d'une circulaire du ministre de l'Intérieur rappelant les conditions d'inscription d'une personne mise en cause dans les fichiers d'antécédents.

En outre, afin d'automatiser les conséquences du traitement en temps réel, il conviendra d'examiner précisément, lors de la mise en service du nouveau logiciel de saisie des procédures ARDOISE, destiné à remplacer le LRP, le processus informatique de validation de la procédure par l'enquêteur qui entraînera la transmission des informations dans la base de données du fichier.

Compte tenu de la situation actuelle, il semble opportun de mettre fin à l'anomalie qui consiste en ce que les personnes susceptibles d'être ultérieurement inscrites au STIC parce qu'elles ont fait l'objet d'une procédure judiciaire à un moment donné ne soient pas informées de cette possibilité, ni des droits dont elles disposent pour accéder à ces données et, le cas échéant, les faire rectifier. À cet égard, vos rapporteurs proposent une mesure simple consistant à délivrer systématiquement un document imprimé.

Proposition n° 27

Remettre à toute personne placée en garde à vue un document d'information précisant que d'éventuelles poursuites judiciaires peuvent entraîner l'inscription dans un fichier d'antécédent judiciaire et récapitulant de manière pratique les différentes possibilités qui sont offertes aux citoyens en matière de droit d'accès, de demande de mise à jour et de rectification des données.

c) « Les chiffres seront très différents avec ARIANE »

ARIANE est le nom de la nouvelle base de données qui devra remplacer le STIC et JUDEX.

En 1995, lors de l'ouverture de la base STIC nationale et de la mise en place de la chaîne de traitement actuelle de la documentation criminelle, il a été décidé de ne pas développer un nouvel outil pour servir de premier maillon : les commissariats continueraient à utiliser l'outil existant STIC-FCE, qui permettait depuis 1985 de centraliser les statistiques sur les crimes et délits.

Les liens entre le STIC et les statistiques policières d'activité sont restés étroits. Des représentants syndicaux ont ainsi décrit **des pratiques locales**

d'alimentation du STIC destinées à influencer sur les résultats statistiques, comme par exemple le fait d'ordonner la cessation de l'alimentation du STIC dans un commissariat à partir du 20^e jour du mois dès lors que le taux d'élucidation des affaires a atteint un niveau jugé satisfaisant. Une autre pratique consiste à changer le code de référencement de l'infraction dans la base locale STIC-FCE. Ainsi certaines infractions qui sont soit des faits constatés (code « C »), soit des faits élucidés (code « E »), sont passées en code « Q » (pour « quelconque ») : cette opération permet de les faire disparaître des statistiques et de diminuer mécaniquement le volume des faits constatés. Ainsi, une dégradation de peu d'importance sur un véhicule peut être référencée par le code « Q », alors que cette infraction était auparavant décomptée comme un fait constaté (code « C »). De la même manière, lorsque dix véhicules sont brûlés, il est possible de ne saisir dans le STIC qu'un fait constaté, l'incendie du premier véhicule étant considéré comme à l'origine d'une propagation sur neuf autres.

Des responsables des services chargés de la documentation criminelle ont confirmé qu'il était **plus que probable que la mise en place du nouveau logiciel ARDOISE et de son système de communication automatique avec ARIANE conduise à des « surprises statistiques »**, de brutales progressions des faits constatés faisant apparaître au grand jour certaines pratiques locales d'« améliorations » des statistiques de la délinquance. En effet, dans ce nouveau système, le lien entre outil statistique et policier sera nettement moins important que dans le STIC : les rubriques seront beaucoup plus « verrouillées », tant en termes de possibilités de renseignement des champs que de liens avec les codes statistiques.

LE CAS DE JUDEX

Le fichier d'antécédents judiciaires de la gendarmerie nationale bénéficie de certains avantages par comparaison avec le STIC : réalisé beaucoup plus tardivement, il a profité des avancées des techniques informatiques, ce qui lui permet de ne pas s'appuyer sur un immense circuit de circulation de papier comme c'est le cas du STIC. De plus, l'architecture sensiblement différente de JUDEX permet un bien plus grand degré d'exactitude au stade de l'alimentation.

La saisie initiale de celles-ci est assurée directement par les responsables des enquêtes, ce qui limite les erreurs d'imputation d'infraction et de qualification des faits. Les messages d'information judiciaire (MIJ), qui sont des synthèses des procédures judiciaires, sont réalisés automatiquement par l'application ICARE lors de la rédaction des pièces de procédures. Ces messages sont adressés aux brigades départementales de renseignements et d'investigations judiciaires (BDRIJ), qui assurent un premier contrôle de cohérence avant de les intégrer aux bases départementales.

Le contrôle de la qualité est beaucoup plus centralisé et automatisé que dans le cas du STIC. La division des fichiers du service technique de recherches judiciaires et de documentation (STRJD), installé au fort de Rosny-sous-Bois, a pour mission principale d'assurer l'administration fonctionnelle des traitements de données et de centraliser l'information judiciaire au niveau national. Chaque nuit, 3 000 à 3 500 fiches « remontent » au STRJD. Un tiers d'entre elles présente des anomalies, lesquelles font alors l'objet d'un contrôle manuel. Les vérifications portent principalement sur l'auteur (notamment son état civil, le fichier JUDEX étant capable de détecter les doublons) et la codification exacte de l'infraction. Après traitement, les informations sont intégrées dans la base nationale.

À la différence du STIC, il n'y a pas de lien direct entre l'établissement de statistiques et l'inscription dans JUDEX. Les statistiques de la délinquance, collectées à partir des messages d'information statistiques envoyés dès la prise de plainte, sont figées au niveau départemental en fin de mois.

Au demeurant, JUDEX n'est pas exempt de difficultés techniques. Il semble que dans certains cas la transmission des MIJ n'est pas correctement effectuée en raison de problèmes de réseau, ce qui se traduit par des « pertes en ligne », s'agissant surtout de petites affaires et de brigades situées en milieu rural. Selon des gendarmes rencontrés, « *Rosny a des problèmes techniques fréquents* ».

2. Des structures de contrôle de la qualité ne pouvant faire face aux flux de procédures

Lors des déplacements réalisés auprès du service régional de documentation criminelle de Versailles (SRDC) et de la DSDC de la préfecture de police de Paris, vos rapporteurs ont pu mieux appréhender la masse de travail requise par l'enrichissement et le contrôle de la qualité des informations transmises par les commissariats à l'échelon régional. Ces visites ont permis de prendre la mesure de **la réalité en quelque sorte physique du STIC**. Ainsi, la DSDC de **la préfecture de police de Paris reçoit cinq millions de feuillets chaque année**. Les couloirs du service et les pans de mur disponibles sont envahis de colonnes de procédures papiers, avec un flux qui ne se tarit jamais. Au SRDC de Versailles, les procédures en attente de traitement représentent deux millions et demi de feuilles A4 et occupent **des pièces entières, du sol au plafond**.

a) L'ampleur de la tâche d'enrichissement et de contrôle de la qualité

• En pratique, le chef de service procède à un **premier tri systématique** de l'ensemble des procédures transmises. Si la procédure semble renseignée correctement, elle est **orientée vers la saisie**. Chaque agent se voit assigner un quota hebdomadaire de 200 procédures à traiter. Il s'agit alors de vérifier l'état civil des personnes mises en cause (notamment la filiation), la qualification juridique des faits et la qualité de victime ou de mis en cause.

Les appréciations sur **l'évolution de la qualité des procédures reçues** sont variables. Dans l'un des services régionaux chargé de la documentation criminelle, il a été relevé qu'à la suite du plan national d'enrichissement mis en place en 2006 et de l'édition d'un livret guide, la qualité s'est améliorée. Les personnels administratifs affectés à l'alimentation du STIC dans les commissariats consultent désormais souvent l'échelon régional par téléphone afin de résoudre en amont des cas un peu complexes. En revanche, dans un autre service il a été souligné combien la forte progression du nombre de personnes mises en cause dans la région concernée (+ 6 % entre 2006 et 2007 et + 5 % entre 2007 et 2008) avait eu un effet sur la dégradation de la qualité des procédures reçues, ce qui implique un contrôle qualité plus poussé.

• **En cas de problème important** constaté lors du tri initial, les procédures sont **transmises aux agents chargés du contrôle qualité**. Dans le cas du SRDC de Versailles, l'intégralité de ce travail est confiée à un seul adjoint administratif. Vos rapporteurs ont pu à cette occasion constater combien était remarquable la connaissance du droit pénal et de la procédure pénale qui avait pu être acquise au cours d'années de pratique par cette fonctionnaire.

L'un des principaux défauts constatés est l'absence de prise en compte du classement sans suite pour absence d'infraction. Dans ce type de cas, des personnes innocentées en cours de garde à vue, et ne correspondant de fait plus à la notion policière de mis en cause, restent près de deux ans enregistrées au STIC. La cellule de contrôle qualité procède alors à la radiation de la fiche dans la base nationale ; il est procédé à un envoi groupé régulier récapitulant les différentes anomalies constatées aux commissariats concernés, avec consigne de procéder à l'effacement dans les bases locales et dans le fichier CANONGE. Il n'existe pas de statistiques exhaustives sur le taux de radiation, mais durant le mois de novembre 2008, sur environ 5 000 procédures traitées, 77 demandes de radiation ont été effectuées par le SRDC de Versailles (soit un taux de 1,5 %).

Compte tenu de l'**architecture régionalisée du STIC**, il peut se produire des cas où le travail d'enrichissement d'un SRDC peut être remis en question par un autre SRDC, notamment en ce qui concerne l'identité exacte des mis en cause. Cependant, ce phénomène reste rare dans la mesure où, en cas de doute, les services préfèrent laisser subsister deux fiches plutôt que d'opérer une fusion sans avoir toutes les garanties nécessaires.

• En outre, **lorsque les données sont transférées de la base locale vers la base nationale**, différents types d'erreurs peuvent se produire. Le **service central de documentation judiciaire** (SCDC) situé à Écully joue donc également un rôle dans le processus de contrôle de la qualité. Un programme informatique est chargé la nuit de faire le relevé de toutes les erreurs d'intégration intervenues au moment du transfert, qu'il s'agisse d'erreurs de procédure informatique, de grille ou de manipulation.

Le SCDC comprend également une section d'exploitation, dont les 16 agents sont chargés d'apporter toutes les rectifications nécessaires aux données contenues dans le STIC, suite à l'exercice du droit d'accès indirect. En moyenne, ce service opère 1 000 rectifications par an. Mais, ces modifications sont délicates sur le plan informatique, car le STIC est un « *vieux système* ». L'effacement de certaines données est très complexe, notamment lorsque celles-ci sont indissociables d'autres affaires. En effet, lorsque des procédures sont liées, les opérateurs sont parfois obligés de supprimer un dossier et de le recréer, afin de conserver le chaînage existant entre les différentes affaires. La version actuelle du STIC n'offrant aucune arborescence des dossiers liés, les opérateurs n'ont pas de vision d'ensemble et doivent se livrer à un véritable « *jeu de pistes* », basculant d'écran à écran pour reconstituer les différentes affaires et en assurer le chaînage.

b) « Nous sommes défaillants depuis des années et des années. La défaillance n'a été que croissante. »

• Les services concernés souffrent d'une **insuffisance patente de personnels** pour faire face à la masse de formulaires à ressaisir en partie et à compléter. Malgré la bonne volonté et le sens du service des agents à qui ce travail est confié, le retard de traitement des procédures est de fait considérable. Le SRDC de Versailles accuse un **retard de trente mois**, tandis que la DSDC de la préfecture de police de Paris met entre six et sept mois pour traiter les procédures qu'elle reçoit. Le retard est **particulièrement préoccupant s'agissant des délits routiers**. En effet, l'intégration de ce type de délits dans le fichier relève entièrement des SRDC, et tant que ce travail n'a pas été fait, le mis en cause reste inconnu au STIC.

Les responsables de ces services souhaitent un « *gros coup de main* », nécessaire pour « *digérer le stock de papier* » avant l'arrivée d'ARIANE. La mise en place de cette application à l'horizon du deuxième semestre 2010 devrait théoriquement permettre de résoudre une partie du problème à la source, en limitant la masse du travail de ressaisie. Toutefois, elle ne permettra pas de répondre à la **question du stock accumulé**. Le recours temporaire à des vacataires doit donc être envisagé dans l'ensemble des SRDC, comme cela a été décidé pour combler le retard du FNAEG. Selon les responsables du SRDC de Versailles, l'embauche de six personnes vacataires à temps plein pendant un an permettrait de résorber une partie du retard, pour le ramener à un an et demi de stock à traiter. Le retard étant variable selon les SRDC, en fonction notamment de l'importance de la délinquance, on peut considérer que le besoin pour traiter l'ensemble du stock accumulé s'élève en moyenne à dix contractuels à temps plein pour chacun des 20 services régionaux de documentation métropolitains. Le coût annuel d'une telle mesure peut être évalué à un peu plus de 3,8 millions d'euros.

• La **masse du travail** à réaliser a, en outre, conduit à **faire des choix**. S'agissant des plaintes contre X (CRI), le travail d'enrichissement doit normalement permettre de les rendre « exploitables » dans le cadre du STIC, notamment pour rendre possibles des rapprochements ultérieurs par les enquêteurs. Ces procédures sont alors complétées par des informations sur des objets volés identifiables, notamment par un numéro de série, et par une description des modes opératoires. Faute de personnel en nombre suffisant, le SRDC de Versailles n'est plus en mesure de faire ce travail d'exploitation des plaintes depuis 2001, soit 400 000 procédures par an pour les départements de la « grande couronne ». Si la **carence dans la saisie des modes opératoires** n'est pas vraiment problématique s'agissant d'affaires mineures de sécurité publique, elle l'est certainement pour les affaires plus importantes traitées notamment par les sûretés départementales. Les **insuffisances de renseignements sur les objets volés** empêchent pour leur part, lors de la découverte éventuelle d'objets d'origine douteuse chez un receleur, de pouvoir identifier le propriétaire victime du vol. Surtout, la France se trouve dans **l'incapacité de respecter ses engagements**

internationaux, les **accords de Schengen** imposant de saisir dans le cadre du SIS les numéros des armes, des billets de banque et des pièces d'identité volés.

Compte tenu des moyens disponibles, toute l'activité d'enrichissement du SRDC de Versailles a été concentrée sur les affaires pour lesquelles un auteur au moins a été identifié (CREI), dont il faut souligner qu'elles sont passées de 10 000 procédures par an avant 2001 à 80 000 par an actuellement. Ce choix a été fait eu égard aux conséquences importantes pour les personnes mises en cause de l'inscription au STIC.

Proposition n° 28

Recruter des contractuels en nombre suffisant pour permettre aux services régionaux de documentation criminelle de résorber le stock de procédures en attente de traitement s'agissant du STIC.

Proposition n° 29

Mettre en place une politique de revalorisation, d'intéressement et de validation des acquis de l'expérience en direction des personnels administratifs chargés de l'alimentation et du contrôle de la qualité des fichiers d'antécédents.

3. Prendre dès à présent les décisions nécessaires pour qu'ARIANE soit effectivement un progrès

a) Le déploiement laborieux de la nouvelle application commune à la police et à la gendarmerie

La mise en place d'ARIANE enregistre actuellement **18 mois de retard** par rapport au calendrier initial. Ce délai s'explique pour partie par la « **marche** » **technologique** à passer, s'agissant d'un système dont l'architecture technique est entièrement nouvelle et ambitieuse. ARIANE a en effet été **conçue pour fonctionner quinze ans** ; le système repose sur l'utilisation de « briques » technologiques et de logiciels dont le fonctionnement est dans la plupart des cas individuellement éprouvé, mais pour lesquels l'intégration au sein d'un ensemble plus vaste s'est révélée de fait difficile.

Même s'il s'agit d'une critique souvent entendue, on ne peut pas véritablement considérer qu'entre la décision de lancer le programme et son déploiement sur le terrain, le système est devenu obsolète. En fait c'est plutôt l'inverse dans le cas d'ARIANE : sachant qu'il s'agit de se doter d'un fichier pour une longue durée d'usage, c'est une **architecture évolutive** qui a été retenue, associée parfois à des technologies avancées ; certaines ne sont d'ailleurs pour l'instant pas complètement arrivées à maturité, comme pour les moteurs de recherche du système, ce qui explique également une partie des difficultés de développement rencontrées.

La seconde raison du retard observé tient à **l’affichage dès le départ d’un calendrier techniquement difficile à tenir**. La société LOGICA, attributaire du marché, subit d’ailleurs les conséquences financières du retard, avec des pénalités et la nécessité de faire travailler ses équipes plus longtemps que prévu. Alors que le temps de travail pour ce projet était initialement estimé à neuf mois, il en représentera au bout du compte au moins 36. En outre, cette société a dû faire face à un renouvellement constant de ses équipes techniques.

La phase de recette de l’ultime version a débuté la mi-janvier 2009 et devrait durer trois mois ; si elle est concluante, la phase de déploiement pourra débuter ; elle prendra entre 12 et 18 mois.

b) Définir des procédures adaptées de contrôle de la qualité des informations saisies

• Outre le fait qu’elle sera consultable à la fois par les agents habilités de la police nationale et par ceux de la gendarmerie nationale, **ARIANE apportera un progrès décisif** sur deux points.

Tout d’abord, **il appartiendra à l’enquêteur d’assurer directement la saisie** d’un beaucoup plus grand nombre d’informations. Son degré de formation devrait normalement limiter le nombre d’erreurs de qualification juridique des faits. De surcroît, cette application sera alimentée de façon beaucoup moins libre que ne l’est actuellement le STIC par le biais du logiciel de rédaction des procédures. L’utilisation d’un thésaurus fermé sécurisera davantage la qualité de mis en cause ou de victime ainsi que la qualification juridique des faits. Les erreurs d’identité seront en outre évitées au maximum, car l’enquêteur pourra, aux divers stades de la saisie, rappeler automatiquement l’identité à partir d’un menu déroulant. Ensuite, ce nouveau système **limitera considérablement le travail de ressaisie manuelle à diverses étapes**, celui-ci constituant le défaut majeur du STIC.

Le **problème de l’organisation du contrôle qualité reste cependant posé**. L’ensemble des personnes entendues a souligné la nécessité de maintenir un tel contrôle, et ce d’autant plus qu’une bonne partie des tâches précédemment confiées à l’échelon régional pourrait revenir à l’échelon local. Il conviendra de continuer à vérifier les procès-verbaux ⁽¹⁾, tandis que la question des pièces jointes aux procédures, comme par exemple les certificats médicaux, n’est pas encore tranchée. Cela reviendra soit directement à l’enquêteur, qui en assurera la numérisation, soit aux personnels administratifs des commissariats, soit aux SRDC. En fonction de la nouvelle répartition du travail de contrôle de la qualité et d’enrichissement des procédures, il est possible que les gains de productivité,

⁽¹⁾ Dans un premier temps, ARIANE ne permettra pas l’accès direct aux procédures numérisées et les enquêteurs devront continuer à en effectuer la transmission aux SRDC. Ceux-ci disposeront d’une visibilité sur l’ensemble des champs saisis localement sous ARDOISE. Toutefois, une évolution ultérieure du système est déjà prévue pour un accès direct à l’ensemble des procédures dans le cadre de la base de données ANADOC.

censés permettre d'employer à d'autres tâches une partie des personnels administratifs actuellement affectés à l'alimentation du STIC, soient en fin de compte moins importants que prévu.

En outre, la mise en place d'ARIANE ne tranche pas le débat sur l'architecture la plus adaptée aux besoins, centralisée comme dans le cas de la gendarmerie, ou régionalisée comme dans le cas de la police. Il sera cependant nécessaire à terme d'évaluer avec précision les avantages et inconvénients de chacune de ces solutions, notamment au regard de l'organisation du contrôle de la qualité.

En tout état de cause, compte tenu des besoins criants des SRDC, il apparaît nécessaire de renforcer ceux-ci en priorité en y affectant autant que possible les personnels libérés des tâches de saisie initiale au niveau des commissariats. Ces agents ont en effet acquis une précieuse expérience de la gestion des fichiers qui mérite d'être mise à profit dans le cadre d'une refonte des missions des SRDC. L'organisation du travail au sein de ces services repose actuellement sur une grande spécialisation des tâches et elle devra être revue en profondeur pour répondre aux besoins issus de l'installation de nouveaux outils informatiques, y compris en matière de rapprochement d'informations.

Proposition n° 30

Définir un processus de contrôle qualité et d'enrichissement des données dans le cadre du déploiement d'ARIANE.

- Si ARIANE constitue un véritable progrès technique, on ne peut sembler-il pas en dire autant de son outil d'alimentation **ARDOISE**, qualifié par un responsable des technologies de « *vieux truc en langage C* », qui **deviendra assez rapidement obsolète**. Ce logiciel en est actuellement à sa troisième version et ses premiers développements remontent à 1995.

Certains représentants syndicaux ont déploré le fait de ne pas avoir été consultés en amont sur le sujet. Ils ont également indiqué qu'au cours de formations sur ARDOISE, dispensées alors que le système était officiellement encore en cours de test, les utilisateurs sont « *tombés des nues* » en découvrant une application « *moyenâgeuse* », inadaptée à la procédure pénale et encore moins fiable que le pourtant bien peu performant logiciel de rédaction des procédures.

Si l'on souhaite que le déploiement d'ARIANE se traduise par un **véritable progrès**, tant pour les utilisateurs que pour les usagers **en termes de service rendu**, notamment par un gain de temps lors de l'enregistrement des plaintes, il convient de déployer un outil initial d'information à la hauteur des attentes.

Proposition n° 31

Prévoir un remplacement rapide du logiciel ARDOISE, en tenant compte en amont des réalités du travail des utilisateurs.

c) Garantir l'exactitude du stock d'informations anciennes qui seront transférées vers ARIANE

La nouvelle application **ARIANE** sera alimentée dès le début par **l'ensemble des données figurant actuellement dans le STIC et dans JUDEX**. L'une des causes du retard accumulé est d'ailleurs la complexité de la reprise technique des fiches, qui implique une vigilance particulière afin de sécuriser l'information. Il faut en effet reprendre et convertir dans un format informatique compatible avec ARIANE l'ensemble des données figurant dans les fichiers d'antécédents de la police et de la gendarmerie. On rappellera que JUDEX comprend 9,8 millions de fiches « affaires » et 2,15 millions de personnes mises en cause, tandis que figurent au STIC 5,49 millions d'individus mis en cause, 36 millions de dossiers de procédures et 28,33 millions de personnes physiques victimes.

Nombre de ces dossiers comportent des inexactitudes en ce qui concerne notamment la qualification des faits (et partant la durée de conservation des données) et la prise en compte des suites judiciaires. Si l'opération de tri réalisée actuellement se limite à une reprise technique au nouveau format informatique, **ARIANE risque dès le départ d'être un fichier inexact**, avec les mêmes conséquences sur sa légitimité et sur son utilisation pratique que pour le STIC. **Le passage au nouveau système** est certes l'occasion de la mise en place de procédures assurant un flux à venir d'informations plus exactes, mais il doit être **mis à profit pour purger l'ensemble du stock de ses erreurs**. À l'évidence, il s'agit d'une décision lourde de conséquences en raison du travail considérable que cela implique. Mais il s'agit aussi d'une nécessité pour rendre aux fichiers d'antécédents une **véritable légitimité**, fondée sur l'exigence légale d'exactitude. De surcroît, l'investissement consenti pour la mise en place du nouveau système est certes déjà très important, mais ne perd-il pas tout son sens si, pour encore dix années voire plus, l'outil n'apporte pas véritablement de garanties supplémentaires pour le citoyen ?

Dans un premier temps, la **définition des procédures à suivre, de l'organisation générale et du calendrier des travaux** pourrait être confiée à une **commission associant l'ensemble des acteurs concernés**. **Sous la direction d'un procureur général**, elle associerait des représentants des **inspections générales** de la police nationale et de la gendarmerie nationale, ainsi que de la **CNIL**. Il convient en effet d'associer davantage celle-ci à la réflexion sur les processus de gestion des fichiers d'antécédents. Il est possible de compléter par la suite la tâche de cette commission en lui confiant la **direction des opérations** engagées sur la base de ses propositions.

Proposition n° 32

Confier à une commission, présidée par un procureur général et associant l'IGPN, l'IGGN et la CNIL, le soin de définir les modalités de reprise de l'ensemble des données figurant dans le STIC et dans JUDEX, de telle sorte qu'ARIANE n'hérite pas du stock d'erreurs accumulées dans les traitements actuellement en service. Consacrer les moyens et le temps nécessaires à la réalisation effective de ce chantier considérable.

IV. RENDRE LES CONTRÔLES PLUS EFFICACES

Un contrôle indépendant est indispensable pour assurer le respect de l'exigence d'exactitude des données, celui-ci ne pouvant reposer sur les seuls processus internes de contrôle des différentes administrations gestionnaires des fichiers. Or, force est de constater que, compte tenu de l'ampleur de la tâche et de moyens trop limités, il est malheureusement illusoire de compter sur les dispositifs actuels de mise à jour par les autorités judiciaires ou, en dernier ressort, par la CNIL, pour pouvoir remédier au volume considérable des erreurs de toutes sortes. C'est d'autant plus regrettable que la question du contrôle externe des fichiers va bien au-delà du simple aspect de la bonne gestion des fichiers. Elle est au cœur de la relation de confiance entre les citoyens et les forces de sécurité. C'est précisément cette nécessaire confiance qui est entamée lorsque les procédures sont exagérément longues, au point que leur efficacité pratique peut être légitimement mise en cause.

A. LES INSUFFISANCES DU CONTRÔLE DES FICHIERS D'ANTÉCÉDENTS JUDICIAIRES PAR LES PARQUETS

Lors des auditions, l'ensemble des acteurs concernés a unanimement identifié le **défaut de mise à jour systématique** des fichiers d'antécédents **au vu des suites judiciaires** données aux affaires comme la source principale de la persistance de nombreuses erreurs dans les fiches individuelles de mis en cause. De ce point de vue, la responsabilité des parquets ne fait guère de doute. Surchargés d'autres tâches, ils ont trop longtemps négligé le travail de transmission systématique des décisions judiciaires aux gestionnaires des fichiers STIC et JUDEX, ce travail s'effectuant de surcroît dans des conditions pratiques qui témoignent, selon les mots de l'un des magistrats entendus, d'« *un archaïsme assez remarquable* ».

Un examen plus détaillé et les déplacements ont cependant permis à vos rapporteurs de mesurer combien **les responsabilités sont partagées** en la matière. Les services de police chargés de l'administration du STIC ont procédé à une interprétation des dispositions relatives au rôle du parquet et aux conditions d'effacement des mis en cause qui traduit une forme de sentiment de propriété exclusive de l'outil que constitue ce fichier. De fait, **son contrôle par les parquets a été vidé de sa substance**, alors qu'il est prévu en termes dépourvus d'ambiguïtés par le législateur. On assiste même parfois à une forme d'inversion des rôles, laquelle a pu faire dire à l'un des magistrats du parquet entendu que non seulement « *le contrôle des parquets sur les fichiers est virtuel* », mais qu'en outre « *c'est nous qui sommes contrôlés par la police* ».

1. Un cadre juridique clairement établi

• S'agissant des fichiers d'antécédents mis en œuvre par la police nationale et la gendarmerie nationale, le III de l'article 21 de la loi n° 2003-239 du

18 mars 2003 pour la sécurité intérieure dispose que « *le traitement des informations nominatives est opéré sous le contrôle du procureur de la République compétent qui peut demander qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire.* »⁽¹⁾

L'intervention du parquet à des fins de mise à jour peut avoir lieu à trois occasions.

Tout d'abord, l'exercice de **requalification** des infractions doit normalement intervenir **dès la réception des procédures** envoyées par les services de police et de gendarmerie.

Ensuite, la **mise à jour des données** à caractère personnel peut être effectuée **à deux stades différents**.

Premièrement, l'article 3 des décrets n° 2001-583 du 5 juillet 2001 modifié portant création du STIC, et du décret n° 2006-1411 du 20 novembre 2006 relatif à JUDEX couvre **deux cas principaux** : la **transmission spontanée des suites judiciaires par le procureur de la République** au gestionnaire du traitement, lequel est « *tenu de modifier ou d'effacer les données enregistrées dès lors qu'il constate qu'elles sont inexactes, incomplètes ou périmées* » ; la transmission de ces mêmes suites par le procureur **à la demande d'une personne enregistrée comme mis en cause**. L'article 3 précité précise que ce type de demande peut être adressé soit directement au procureur de la République territorialement compétent, soit, par l'intermédiaire de la CNIL, au responsable du traitement qui les soumet au procureur de la République territorialement compétent.

Deuxièmement, la mise à jour par le parquet peut intervenir **dans le cadre de l'exercice d'un droit d'accès indirect auprès de la CNIL**, prévu par l'article 8 des deux décrets précités. Dans le cas où la personne figure dans les fichiers, le gestionnaire sollicite le ou les parquets compétents pour qu'ils exercent leur rôle de mise à jour des mentions au vu des suites judiciaires, d'une part, et pour recueillir l'accord de l'autorité judiciaire sur la communication des informations aux personnes dans le cas où la procédure n'est pas close, d'autre part. La circulaire du ministre de la justice du 26 décembre 2006 souligne sur ce point le « *rôle crucial* » que joue le procureur de la République dans le cadre de l'exercice du droit d'accès indirect. Il lui appartient en effet d'intervenir avec la diligence nécessaire de manière à ce que le délai strict de quatre mois prévu pour la réponse au requérant par l'article 87 du décret du 20 octobre 2005⁽²⁾ puisse être respecté. Cette circulaire souligne que « *l'intervention rapide et rigoureuse du parquet saisi d'une demande de droit d'accès indirect constitue en effet une*

(¹) Ces dispositions reprennent sans modifications substantielles l'économie générale du contrôle du STIC par le procureur de la République telle qu'elle était prévue par le décret n° 2001-583 portant création de ce traitement.

(²) Décret n° 2005-1309 pris pour l'application de la loi n° 78-17 du 6 février 1978 relative à l'informatique, aux fichiers et aux libertés.

occasion supplémentaire de mise à jour des données enregistrées dans des fichiers dont la consultation peut avoir, notamment dans le cadre d'enquêtes administratives, des conséquences importantes. »

• **Les motifs de mise à jour** sont **très limitativement définis** par l'article 21 de la loi du 18 mars 2003 : *« 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, auquel cas elle fait l'objet d'une mention. Les décisions de non-lieu et, lorsqu'elles sont motivées par une insuffisance de charges, de classement sans suite font l'objet d'une mention sauf si le procureur de la République ordonne l'effacement des données personnelles. »*⁽¹⁾

Deux cas sont donc distingués, celui de la relaxe ou de l'acquiescement, d'une part, et celui de la décision de non-lieu ou de classement sans suite motivée par une insuffisance de charges, d'autre part.

Une **décision de relaxe ou d'acquiescement**, quel qu'en soit le fondement, **entraîne en principe la suppression** par le gestionnaire du fichier des données personnelles relatives au mis en cause qui a bénéficié d'une telle décision définitive. **Toutefois**, la loi prévoit que **le procureur peut prescrire le maintien** au fichier et la circulaire précitée précise que cette possibilité s'explique *« pour des raisons liées à la finalité du fichier considéré ; ainsi en sera-t-il par exemple lorsque le mis en cause est un multirécidiviste. Dans le cas d'une telle prescription, le gestionnaire du fichier STIC ou JUDEX n'effacera donc pas les données à caractère personnel relatives à la personne mise en cause ayant fait l'objet de la décision de relaxe ou d'acquiescement, mais inscrira une mention faisant état de cette décision. »*

S'agissant d'une **décision de non-lieu ou de classement sans suite motivée pour une insuffisance de charge**, elles font **l'objet d'une mention dans le fichier, sauf si le procureur ordonne expressément l'effacement des données**. Le champ des décisions de classement concernées est précisément défini et correspond en pratique aux **motifs numéros 11 et 21** dans la nomenclature de la Chancellerie (absence d'infraction et infraction insuffisamment caractérisée). Le classement sans suite prononcé pour un autre motif que l'insuffisance de charges, tel que le classement pour un motif juridique, en opportunité ou en raison du recours à une procédure alternative aux poursuites, ne permet donc pas de compléter les mentions enregistrées au STIC ou dans JUDEX. Quant à l'effacement des données personnelles, la circulaire du 26 décembre 2006 indique qu'*« il apparaît qu'il devrait être ordonné dès lors que la personne a été totalement mise hors de cause et que le maintien des informations la concernant*

⁽¹⁾ On rappellera que dans sa version initiale, l'article 3 du décret de 2001 relatif au STIC prévoyait l'effacement obligatoire des fiches des mis en cause pour des faits couverts par une amnistie. Ce motif de mise à jour n'a pas été conservé par la loi de 2003.

au STIC ou au JUDEX n'est plus justifié au regard des finalités du fichier considéré. »

L'application effective des textes témoigne malheureusement d'une grande distance avec ce bel ordonnancement.

2. Des mises à jour très insuffisantes en pratique

a) Une trop faible utilisation de la faculté de requalification lors de la réception des procédures

La situation en la matière est assez bien résumée par un procureur de la République : « *pour les requalifications, il y a un gros problème. Nous n'avons que deux fonctionnaires au bureau d'ordre qui sont débordés* ».

La circulaire du 26 décembre 2006 décrit de manière circonstanciée l'importance du rôle du procureur lors de la réception des procédures établies par les services d'enquêtes. S'agissant de la qualification des faits, il est noté qu'il appartient au procureur de la République « *de vérifier cette qualification juridique et, le cas échéant, de lui substituer la qualification appropriée, voire de solliciter l'effacement de la mention dans le cas où la qualification finalement retenue ne permettrait pas d'inscription au STIC ou au JUDEX en vertu de l'article 2 des décrets correspondants* ».

Lors de déplacements auprès des parquets de deux tribunaux de grande instance de la région parisienne, vos rapporteurs ont reçu des réponses très franches sur la manière dont cette mission était remplie. Il apparaît **qu'en pratique il n'est pas procédé à des demandes de rectification du fichier à la réception des procédures afin de tenir compte d'une requalification**⁽¹⁾. La raison en est d'abord et principalement d'ordre pratique et réside dans la masse considérable des tâches assignées au parquet au regard des moyens humains et matériels dont il dispose. Une autre raison est, pour ainsi dire, culturelle. Dans les cas où les justiciables ont, par exemple, fait l'objet d'une mesure de correctionnalisation s'inscrivant avant tout dans une démarche de gestion des flux procéduraux vers les juridictions de jugement, des réticences se manifestent envers l'idée d'une requalification. Comme l'a indiqué l'un des magistrats entendus : « *Il n'apparaît pas opportun de mettre en place une procédure systématique lourde, alors que l'on a déjà été indulgent envers le mis en cause.* » En revanche, comme on le verra plus loin, la question de la requalification des faits est davantage prise en compte lorsque le procureur est saisi directement d'une demande de rectification par un mis en cause. Dans son rapport précité sur le STIC, la CNIL a relevé que les juridictions sollicitées dans le cadre de son contrôle n'ont pas été en mesure de transmettre des éléments d'information, notamment chiffrés, sur le nombre de requalifications opérées.

⁽¹⁾ En revanche ce travail de requalification est réalisé de manière systématique lors de l'édition de fiches de mises à jour en cas de classement 11 ou 21.

Cette situation est d'autant plus regrettable que le choix de la qualification initiale par les services enquêteurs est lourd de conséquences s'agissant de la durée de conservation des données, laquelle varie entre cinq ans et quarante ans pour les majeurs selon le type d'infraction. Les responsables des parquets rencontrés ont confirmé l'analyse de la CNIL figurant dans le rapport précité : les qualifications choisies par les services enquêteurs sont souvent plus lourdes que celles finalement retenues par la justice au cours des stades ultérieurs de traitement de la procédure. Ce phénomène conduit d'ailleurs à des disparités entre les statistiques d'infractions des parquets et celles des services de police dans un même secteur géographique.

Toutefois, compte tenu de la réalité du travail des parquets, il apparaît quelque peu illusoire de demander de nouveau par le biais d'une circulaire de mieux répondre à l'exigence de réexamen de la qualification des faits figurant dans les fichiers d'antécédents dès le stade de la réception des procédures. Cette situation ne pourra probablement être améliorée que dans le cadre plus général d'une automatisation des modalités de mise à jour des données au regard des suites judiciaires et en garantissant l'accès direct des parquets aux fichiers concernés.

L'UTILISATION DES FICHIERS D'ANTÉCÉDENTS PAR LE MINISTÈRE PUBLIC AU COURS DU PROCÈS PÉNAL

Les avocats entendus par vos rapporteurs ont indiqué que l'utilisation des fichiers de police par le ministère public au cours du procès pénal n'est pas sans conséquences sur l'équilibre entre défense et accusation.

À la différence du FNAEG, dont les éléments sont versés au dossier et peuvent faire l'objet d'une demande d'expertise contradictoire par la défense, les fichiers d'antécédents judiciaires sont souvent utilisés par l'accusation de manière orale, sans que la défense puisse y avoir accès. La mention des affaires dans lesquelles une personne a été mise en cause précédemment peut jouer un rôle non négligeable dans l'opinion que se forme le juge, tout particulièrement en cas de comparution immédiate.

Aussi faut-il encadrer davantage cet usage et appliquer la règle du contradictoire. Le versement systématique au dossier d'un procès-verbal circonstancié des services de police récapitulant les principaux éléments figurant dans les fichiers d'antécédents pourrait permettre à la défense d'en avoir une meilleure connaissance, et éventuellement de pouvoir les contester de manière plus circonstanciée.

Proposition n° 33

L'utilisation des fichiers d'antécédents judiciaires dans le cadre d'un procès pénal doit respecter la règle du contradictoire. Dans le cas où le ministère public mentionne les affaires pour lesquelles un prévenu ou un mis en examen a été mis en cause, la fiche correspondante doit être versée au dossier.

b) La prise en compte inégale et tardive des suites judiciaires

• Un **système de fiches navettes** a été prévu pour permettre aux parquets d'adresser leurs demandes de mise à jour des mentions aux gestionnaires des fichiers STIC et JUDEX. Des modèles d'imprimés figurent à cet effet en annexe des circulaires d'application des décrets de 2001 et de 2006 précités portant création de ces deux fichiers. Ces fiches doivent être jointes aux comptes rendus d'enquête après identification envoyés par les services de police et des messages d'information judiciaire de la gendarmerie nationale lorsque l'auteur de l'infraction a été identifié. Si la circulaire du 26 décembre 2006 pousse le souci du détail jusqu'à préciser qu'il conviendra de s'assurer que *« les fiches-navettes annexées restent jointes au dossier de manière visible mais mobile, par exemple dans une sous-chemise agrafée en début de dossier »*, **dans les faits c'est l'exigence même de transmission de fiches navettes qui n'a parfois été respectée que très tardivement**, avec un impact évident sur le travail de mise à jour.

Ainsi, les MIJ envoyés par les services de la gendarmerie nationale n'ont pas comporté de fiche navette longtemps après la parution de la circulaire de la direction générale de la gendarmerie nationale du 10 août 2007 relative à l'emploi du système JUDEX. Celle-ci prévoyait expressément l'utilisation d'une telle fiche, afin que les parquets puissent transmettre leurs consignes aux brigades départementales de renseignements et d'investigations judiciaires (BDRIJ), mais son application effective semble avoir été particulièrement lente. En témoigne un échange de courriers datés respectivement du 21 juillet et du 25 septembre 2008 entre un commandant de groupement de gendarmerie et un procureur de la République, soit un an après la parution de la circulaire⁽¹⁾. De fait, selon un magistrat entendu par vos rapporteurs sur cette question, *« les erreurs sont désormais plus fréquentes dans JUDEX que dans le STIC, car la prise en compte des retours des parquets y est plus récente, depuis environ six mois »*. Au 1^{er} janvier 2008, le STRJD n'a d'ailleurs procédé qu'à 2 068 effacements du fichier JUDEX à la demande des parquets et a été informé de seulement 298 relaxes, soit des flux très limités au regard du nombre d'affaires transmises par la gendarmerie.

En outre, ce dispositif de transmission est apparu peu efficace pour les utilisateurs. Lors de leur déplacement auprès de la division de la statistique et de la documentation criminelle (DSDC) de la préfecture de police de Paris, vos rapporteurs ont pu constater que les formulaires renvoyés aux fins de mise à jour par les parquets des tribunaux de Paris et des trois départements de la petite couronne ne reprennent pas systématiquement le modèle type. De fait, la recherche des fiches navettes dans chaque dossier prend beaucoup trop de temps. Une modification du logiciel de la nouvelle chaîne pénale (NCP) en région parisienne permet depuis un peu plus de deux ans l'édition automatique d'une note récapitulant les suites judiciaires à destination des services gestionnaires des

(1) Reproduits en annexe 7.

fichiers. En tout état de cause, selon un magistrat du parquet d'un TGI de la région parisienne « *l'expérience enseigne que tout ce qui ne s'intègre pas dans notre chaîne informatisée ne fonctionne pas* ».

Dans les cas où le travail de mise à jour est effectivement réalisé, il prend encore un temps important. Ainsi, à Évry, il faut compter en moyenne trois semaines à un mois pour procéder à l'enregistrement de la procédure rédigée par les services de police ou de gendarmerie à compter de son arrivée au tribunal, tandis que le délai de traitement du dossier par un magistrat peut prendre ensuite d'un à trois mois. Dans certains cas, un retard bien plus important a été enregistré : les atteintes aux biens comportaient jusqu'à récemment des délais de traitement de 15 à 18 mois ; un effort d'ensemble a été réalisé pour y remédier. Pour l'essentiel, les retards observés résultent d'un manque de personnels disponibles dans des greffes surchargés ⁽¹⁾.

• S'agissant des **flux de demandes de mises à jour** en fonction des suites judiciaires adressées par les parquets, la situation apparaît très contrastée. Le rapport précité de la CNIL souligne combien sont insuffisantes en 2007 les transmissions des décisions de classement sans suite (21,5 %), de non-lieu (0,47 %), d'acquiescement (6,88 %) et de relaxe (31,17 %) ⁽²⁾. Il faut cependant noter qu'à l'exception du cas des décisions de non-lieu, des progrès non négligeables ont été réalisés, les pourcentages mentionnés ayant très significativement augmenté depuis 2005.

Compte tenu des consignes données par la Chancellerie et des recommandations de la CNIL, le rythme d'envoi des demandes de mises à jour s'est considérablement accéléré en ce qui concerne le STIC. Lors de leur déplacement auprès de la DSDC de la préfecture de police, il a été indiqué à vos rapporteurs que les suites judiciaires étaient transmises « *naturellement* » par les tribunaux parisiens. Quant aux TGI des départements de la petite couronne, après un certain retard observé les années précédentes, les demandes de mises à jour arrivent désormais « *par tombereaux* ». Ainsi, ce sont plus de 32 000 demandes d'effacement et de rectification qui sont parvenues en 2008 au « groupe juridique » de la DSDC, chargé de la gestion de l'ensemble des demandes de mises à jour, qu'elles viennent spontanément des parquets ou fassent suite à des vérifications opérées à l'occasion d'une consultation administrative du fichier d'antécédents. Ce phénomène a été également confirmé lors du déplacement auprès du service régional de documentation judiciaire (SRDC) de Versailles, qui couvre les départements de la grande couronne. La chaîne de traitement des suites judiciaires favorables y a débuté en janvier 2002 et, jusqu'en 2006, le nombre de demandes émanant des parquets d'Île-de-France est resté très limité (50 par an tout au plus). Depuis 2007, une augmentation très nette des courriers a pu être

⁽¹⁾ Au parquet du TGI d'Évry, cette tâche de suivi était précédemment confiée au service de l'exécution des peines, malheureusement débordé par d'autres tâches. Aussi a-t-elle été par la suite confiée au service central, où elle occupe une personne, mais seulement pour le tiers de son temps de travail.

⁽²⁾ Ces ratios constituent une moyenne obtenue grâce aux réponses à un questionnaire de la CNIL fournies par 34 TGI, représentant la moitié de l'activité pénale.

constatée et le nombre de 1 000 demandes par mois est désormais atteint. Cet afflux a d'ailleurs provoqué un certain encombrement au sein de ce SRDC, dans la mesure où le suivi des procédures judiciaires est assuré par une seule personne. Aussi faut-il compter entre quatre et cinq mois entre la réception de la demande du parquet et sa traduction dans le fichier.

Les réalités d'un système de mise à jour quelque peu anarchique, fonctionnant au moyen de fiches navettes qui constituent seulement un pis aller, soulignent l'urgence de l'adoption de solutions techniques plus modernes.

• Comme l'a indiqué un responsable du ministère de la Justice, face à ces difficultés « *la solution c'est soit d'attendre CASSIOPÉE, soit d'injecter des moyens massifs* ». Si manifestement c'est la première solution qui a été retenue, les différents acteurs rencontrés ont malheureusement tous fait part d'un **grand scepticisme** sur les améliorations effectives susceptibles d'être apportées à cette question des mises à jour par la **mise en place de l'application CASSIOPÉE** au sein du ministère de la Justice, au moins dans un premier temps ⁽¹⁾.

Il convient tout d'abord de rappeler que le déploiement de cette application a pris un retard considérable par rapport au calendrier initial. Après une série de tests dans trois sites pilotes, elle est en cours de pré-généralisation pour une vingtaine de TGI de moyenne importance. La mise en exploitation à Bordeaux à partir de janvier 2009 constitue une étape importante, puisqu'il s'agira du premier tribunal ayant un fort volume d'activité dans lequel l'application sera testée. En cas de succès, la phase de déploiement doit débiter à partir de février ou de mars 2009, avec un déploiement en Île-de-France prévu pour 2010. Alors que CASSIOPÉE devait être pleinement opérationnelle en 2007-2008, sa mise en œuvre ne sera complète au mieux qu'en 2010.

Au départ, CASSIOPÉE sera simplement un outil de gestion de la chaîne pénale au sein du ministère de la Justice. Il est cependant prévu de mettre en place une interface entre cette application et le système de numérisation des procédures pénales (NPP) installé dans chaque juridiction, afin de pouvoir consulter les procédures judiciaires sous une forme numérisée depuis CASSIOPÉE. Cela suppose qu'une décision soit prise en ce sens par le comité des directeurs du projet et la réalisation effective pourrait intervenir dès 2010, une fois l'ensemble du déploiement de CASSIOPÉE achevé.

(1) *L'application CASSIOPÉE est destinée à améliorer le fonctionnement de la chaîne pénale en permettant le partage des données et en évitant des ressaisies d'informations. Il s'agit à ce stade d'un système de gestion des données, permettant aux différents acteurs judiciaires d'accéder aux informations préalablement saisies telles que l'identité de la personne poursuivie, celle de la partie civile, la qualification des faits poursuivis, les peines prononcées et l'état de l'exécution de ces peines. On rappellera que dans son rapport d'information sur l'exécution des décisions de justice pénale concernant les personnes majeures (n° 505), publié en décembre 2007, M. Etienne Blanc avait déjà souligné l'urgence d'une installation rapide de CASSIOPÉE, ainsi que la nécessité d'assurer la communication entre cette application et tous les acteurs de la chaîne pénale, dont notamment les fichiers STIC et JUDEX.*

S'agissant des relations entre les services d'enquête et CASSIOPÉE, cela concerne à la fois les « flux entrants », c'est-à-dire des procédures en provenance de la police (ARDOISE) et de la gendarmerie (ICARE) et les « flux sortants », pour la mise à jour automatique d'ARIANE, c'est-à-dire des instructions des parquets pour les suites judiciaires. Ces échanges n'étaient pas prévus initialement, mais ils font désormais l'objet de travaux assez avancés sous l'égide d'un groupe de travail tripartite, notamment sur le plan des spécifications techniques. Selon les informations transmises à vos rapporteurs, les échanges interapplicatifs pourraient intervenir dès 2010, sous réserve d'un respect du calendrier de déploiement des deux applications en cause. La mise en place de ce système d'alimentation croisée ne doit pas faire perdre de vue que chaque gestionnaire d'application gardera la maîtrise complète de l'outil qui lui est confié. Ainsi, les consignes de mise à jour des parquets envoyées sous forme électronique faciliteront certes la tâche, mais il appartiendra aux gestionnaires d'ARIANE de veiller à leur bonne intégration.

C'est désormais vers un système véritablement automatisé qu'il convient de s'orienter. À cet égard, le président de la CNIL a déclaré n'avoir aucune objection de principe à de telles transmissions sécurisées de données entre la police et la justice. La dématérialisation complète des procédures de la chaîne pénale est d'ailleurs un chantier d'une toute autre ampleur, posant notamment la question de l'authentification des signatures des différents acteurs (témoins et mis en cause, notamment) ainsi que celle du sort des annexes aux procédures (scellés, etc.). Malgré ces indéniables difficultés techniques et pratiques, ce dossier doit constituer une véritable priorité, dans un souci de simplification et d'efficacité du service public de la justice. Dans son rapport précité sur l'exécution des décisions de justice pénale, M. Étienne Blanc avait déjà souligné que « *les applications informatiques utilisées par les juridictions pénales sont aujourd'hui totalement obsolètes* » et que « *les heurts et les retards dans la chaîne pénale ne pourront être réduits que par la dématérialisation de cette chaîne et par la poursuite des efforts pour accélérer l'enregistrement des décisions par le casier judiciaire.* »

On relèvera, pour terminer, qu'en raison précisément de l'absence d'interconnexion entre les fichiers, il n'existe pas actuellement de procédure automatisée d'effacement du fichier Canonge ou du FNAEG dans les cas où la fiche d'un mis en cause dans le STIC a été effacée à la suite d'une décision de mise à jour prise par le procureur de la République. Selon un responsable de la sous-direction de la police technique et scientifique, dans ces cas, l'effacement du FNAEG s'effectue « *si on a l'information* ».

Proposition n° 34

Mettre en place au plus vite le dispositif d'échanges d'informations entre CASSIOPÉE et ARIANE, afin de tenir compte plus rapidement et plus efficacement des changements de qualification et des suites judiciaires.

Proposition n° 35

Garantir la transmission systématique des décisions judiciaires d'effacement des fichiers d'antécédents afin de procéder aux effacements correspondants dans le fichier CANONGE et dans le FNAEG.

c) Garantir un traitement rapide des demandes de mise à jour adressées directement aux parquets

• Vos rapporteurs ont procédé à des déplacements auprès des parquets de deux TGI de la région parisienne, Évry et Bobigny, où le volume des demandes de mise à jour est particulièrement important compte tenu de la présence de deux plates-formes aéroportuaires, employant de nombreuses personnes faisant l'objet d'enquêtes administratives pour la délivrance de cartes d'accès à ces zones. Si à Évry le flux de demandes de mises à jour adressées directement au parquet reste stable, avec un peu plus d'une centaine de requêtes par an (111 demandes effectuées en 2008, contre 120 environ en 2007), il est en augmentation à Bobigny (299 demandes en 2007, 340 en 2008).

Le III de l'article 21 de la loi n° 2003-239 pour la sécurité intérieure dispose qu'une personne figurant dans les fichiers d'antécédents judiciaires peut saisir directement le procureur de la République d'une demande de rectification des données la concernant. Le traitement des requêtes se déroule de la manière suivante :

— le parquet demande à la police et à la gendarmerie si la personne est connue dans le STIC ou dans JUDEX ; la réponse intervient désormais dans des délais rapides, contrastant avec des « *débuts plus chaotiques* » ;

— en fonction des réponses, le requérant est orienté vers les TGI territorialement compétents en raison de la localisation des faits ;

— l'ensemble des procédures mentionnées est recherché, ce qui n'est pas toujours facile pour les procédures anciennes. Dans le cas où aucune trace n'en est trouvée, il est demandé aux services de police ou de gendarmerie copie des procédures transmises au parquet, afin de pouvoir apprécier les circonstances de l'affaire (six cas sur les 111 requêtes enregistrées en 2008 au parquet du TGI d'Évry).

Au vu du contenu même des procédures, il faut ensuite schématiquement distinguer deux cas de figure : celui des affaires simples, avec un seul fait de faible gravité ; celui des délinquants d'habitude, pour lesquels le parquet demandera parfois l'effacement de certains faits, mais où, en tout état de cause, d'autres infractions resteront inscrites légitimement dans les fichiers. Les responsables des parquets rencontrés ont indiqué qu'ils avaient particulièrement conscience des enjeux en matière d'accès à l'emploi et qu'en conséquence les cas simples, pour lesquels l'effacement de la seule infraction mentionnée dans le fichier est

envisageable, sont traités avec une diligence particulière. Il s'agit cependant seulement d'une bonne pratique, récente, et les requérants ne se voient offrir aucune garantie que le traitement de leur demande sera effectué dans des délais raisonnables.

• D'un point de vue pratique, l'installation de terminaux de consultation du STIC et de JUDEX au sein des parquets permettrait de gagner du temps dans le traitement des dossiers (entre un et deux mois).

Par ailleurs, l'article 87-1 du décret du 20 octobre 2005 précité fixe un **délaï de trois mois** aux procureurs de la République **pour instruire les demandes de mises à jour**, que celles-ci leur aient été directement adressées par les requérants ou qu'elles leur aient été adressées par le responsable du traitement lui-même saisi par la CNIL⁽¹⁾. Il reste que même si la circulaire du ministre de la justice du 31 mai 2007 appelle l'attention sur la nécessité de veiller au respect de ce délai, celui-ci reste simplement indicatif.

Or, **une grande rapidité de décision est hautement souhaitable** afin de ne pas réduire à néant une **chance d'accès à un emploi**.

De manière générale, le délai de réponse aux demandes de rectification de données à caractère personnel figurant dans des fichiers d'antécédents judiciaires, dans les cas prévus par l'article 21 de la loi du 18 mars 2003 relative à la sécurité intérieure, devrait être ramené à un mois à compter du dépôt de la demande.

En outre, il convient **d'instituer un magistrat référent des fichiers d'antécédents et de le charger du traitement en temps réel des dossiers manifestement urgents**. Choisi parmi les magistrats du parquet, il sera à même de bien apprécier le bien fondé des demandes et de faire procéder aux modifications nécessaires en temps réel. Par analogie, on notera que l'article R. 53-17 du code de procédure pénale confie au magistrat référent du FNAEG des pouvoirs importants, puisqu'il peut ordonner l'effacement d'enregistrements illicites.

Proposition n° 36

Réduire à un mois le délai de traitement du dossier en cas de demande de mise à jour émanant d'une personne figurant dans un fichier d'antécédents judiciaires.

Proposition n° 37

Mettre en place une procédure de traitement en temps réel auprès d'un magistrat référent des fichiers d'antécédents afin de répondre aux demandes de mise à jour présentant un degré d'urgence particulièrement élevé.

⁽¹⁾ Dans la pratique, ces derniers cas semblent très rares.

• Comme l'a indiqué un des avocats auditionnés, normalement, « *la relaxe, c'est la relaxe !* ».

Or, la loi offre au procureur de la République de **maintenir dans un fichier d'antécédents** judiciaires les données personnelles concernant **un mis en cause ayant bénéficié d'une décision de relaxe ou d'acquiescement devenue définitive**.

On peut s'interroger sur l'utilité d'un tel dispositif dérogatoire, permettant de maintenir des données personnelles alors même que l'intéressé est reconnu innocent. En pratique, les témoignages obtenus par vos rapporteurs montrent une diversité certaine des points de vue. D'une part, un responsable du ministère de la Justice a relevé crûment que lorsqu'une personne a été relaxée ou acquittée malgré des charges qui semblaient lourdes au parquet, « *dans ces cas-là, on ne lâche pas l'affaire* ». En revanche, lors des déplacements de vos rapporteurs auprès des parquets de TGI d'Évry, de Niort et de Bobigny, les procureurs de la République ont indiqué ne jamais faire usage de cette faculté, dans un cas par opposition de principe à la possibilité de contredire une décision favorable d'une juridiction de jugement, dans deux autres, faute de temps et de moyens. Enfin, un autre magistrat du parquet a indiqué qu'« *en tant que procureur, je n'ai jamais prescrit le maintien au fichier* ».

On soulignera que les ministères de l'Intérieur et de la justice ont été interrogés par vos rapporteurs, afin de disposer de données statistiques précises sur cette question. Par un courrier du 18 mars 2009, la garde des Sceaux a indiqué que « *les décisions de maintien des données personnelles dans les fichiers de police judiciaire STIC et JUDEX prises par les procureurs de la République ne font pas l'objet de comptabilisation* ».

Sur ce point, vos rapporteurs ont exprimé des points de vue différents.

Votre rapporteur considère que dans certains cas bien particuliers, concernant pour l'essentiel des récidivistes, **la possibilité de maintenir des informations sur un mis en cause finalement innocenté peut être utile** s'il s'agit de pouvoir ultérieurement disposer d'éléments d'information sur le parcours d'un individu. C'est notamment le cas lorsqu'il s'agit d'affaires particulièrement graves d'atteinte aux personnes, et la prudence commande de maintenir un dispositif qui permet, sur décision d'un magistrat du parquet, de garder la trace de soupçons très étayés.

En revanche, **votre rapporteure estime cette disposition excessive, inutile et désuète**. Le fait que, dans le cas où le procureur de la République prend une telle décision, les données sont radiées du STIC « administratif », mais sont conservées dans le STIC « antécédents judiciaires » ne paraît pas une garantie suffisante. Il convient de souligner que la décision du procureur de la République n'est actuellement susceptible d'aucun recours. Lors des travaux menés dans le cadre du groupe de travail sur les fichiers de police, aussi bien en 2006 qu'en

2008, le ministère de la Justice s'est en effet opposé à l'instauration d'un tel recours au motif « *qu'il appartient au seul responsable du traitement [...] de prendre ou non la décision d'effacement ou de rectification dans le cadre du droit d'accès indirect [...] et ce même lorsqu'il est tenu de suivre la position prise par le procureur de la République* »... Quant à l'invocation de la finalité du traitement figurant dans l'article 21 de la loi du 18 mars 2003, elle apparaît peu convaincante. Dans les cas où le maintien est demandé notamment parce que la personne est un récidiviste notoire, les fichiers d'antécédents conservent trace de l'ensemble des autres affaires dans lesquelles il a été impliqué et permettent aux services enquêteurs de disposer de suffisamment d'informations pour, le cas échéant, orienter ultérieurement une enquête ou un interrogatoire en garde à vue.

Proposition n° 38 de votre rapporteur

Maintenir la faculté accordée au procureur de la République de prescrire le maintien dans un fichier d'antécédent judiciaire des données personnelles concernant les personnes mises en cause en cas de décision de relaxe ou d'acquiescement devenue définitive.

Proposition n° 38 bis de votre rapporteur

Supprimer la faculté accordée au procureur de la République de prescrire le maintien dans un fichier d'antécédent judiciaire des données personnelles concernant les personnes mises en cause en cas de décision de relaxe ou d'acquiescement devenue définitive (modification du III de l'article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure).

3. Le contrôle des fichiers d'antécédents judiciaires par les parquets est-il seulement « un concept » ?

Cette appréciation sur le contrôle du STIC par les parquets a été formulée par un policier à l'occasion d'un déplacement. Elle témoigne de manière abrupte de la façon dont les services de police envisagent parfois leurs relations avec le parquet. Il a été clairement indiqué à l'occasion du déplacement auprès du SRDC de Versailles qu'en ce qui concerne la mise à jour du fichier en fonction des suites judiciaires, « *les parquets prescrivent des mesures d'effacement, mais en tant que gestionnaires, nous ne sommes pas obligés d'en tenir compte* ». Le texte du III de l'article 21 de la loi du 18 mars 2003 déjà cité est pourtant explicite, puisque c'est bien « *le traitement des informations nominatives* » figurant dans les fichiers d'antécédents judiciaires qui est placé sous le contrôle du procureur de la République. En outre, la possibilité de « prescrire » une action s'applique seulement au cas où le procureur souhaite qu'une décision de relaxe ou d'acquiescement devenue définitive, qui emporte normalement effacement du fichier, fasse malgré tout l'objet d'une mention. Dans les cas de décisions de non-lieu et de classement sans suite motivé par une insuffisance de charges, si le

procureur souhaite effacer les données, il l'« ordonne » ; le terme est dépourvu d'ambiguïté.

• Aussi bien la DSDC de la préfecture de police de Paris que le SRDC de Versailles ont indiqué qu'en cas de demande d'effacement émanant du procureur de la République pour les cas de classement sans suite, la procédure initiale est minutieusement consultée afin de **vérifier si la décision est effectivement fondée sur un classement 11 ou 21**. Si ce n'est pas le cas, la demande d'effacement n'est pas prise en compte ⁽¹⁾.

Le caractère extrêmement restrictif des textes en matière d'effacement et la lecture qui en est faite ne sont pas sans **poser des problèmes très importants, parfois pour des faits mineurs**. L'un des exemples présentés à vos rapporteurs est celui d'un passager de la SNCF qui, risquant de rater son train et perdant son calme en raison de la lenteur du guichetier à lui délivrer un billet, a donné un coup de pied dans la porte vitrée et l'a endommagée. La personne a remboursé les travaux de remplacement et le parquet a, en conséquence, estimé les poursuites inopportunes. Toutefois, le mis en cause demeure dans le fichier d'antécédents et le service gestionnaire refuse de l'en effacer car le cas ne correspond pas strictement aux motifs d'effacement prévus. « *Petite cause, grands effets* ». Autre exemple : des jeunes quittent un café sans régler l'addition, sont rattrapés par le propriétaire de l'établissement et payent immédiatement, sous les yeux des policiers. Inscrits au STIC, ils y demeurent malgré les demandes du parquet, car les faits sont reconnus et l'infraction caractérisée.

• **Un autre type de cas apparaît particulièrement préoccupant**. Il s'agit des **personnes arrêtées et mises en garde à vue mais jamais déférées à la justice, et pour lesquelles il n'y a eu aucune décision de classement sans suite** par le parquet. L'exemple classique est le suivant : une trentaine de personnes sont arrêtées dans le cadre de violences urbaines et mises en garde à vue ; la plupart sont rapidement relâchées après consultation téléphonique du parquet, faute d'éléments permettant de vraiment soutenir une procédure de poursuite ; huit seulement sont poursuivies et six d'entre elles sont condamnées et deux relaxées. Si le parquet peut prescrire l'effacement des fichiers d'antécédents de ces deux dernières, il n'en est pas de même pour celles qui n'ont pas été déférées, car en l'absence de toute décision judiciaire, le gestionnaire du traitement refuse l'effacement. De fait et selon les magistrats du parquet rencontrés, par ce biais, « *on inscrit comme auteurs des victimes et des témoins* ».

Lorsque le parquet demande l'effacement à la suite d'une requête individuelle dans un cas semblable, il tente de la motiver par un classement 11 ou 21 ; mais le service gestionnaire fait valoir l'absence de mention d'un tel

(1) Vos rapporteurs ont en outre remarqué lors d'un de leurs déplacements dans un service chargé de la documentation criminelle qu'à la demande de la sous direction de la police technique et scientifique, une application locale a été créée afin de suivre le traitement des demandes de mises à jour (références du dossier, relevé des décisions du procureur de la République et liste des courriers éventuels). Il s'agit en quelque sorte d'un fichier local des « radiés ».

classement dans la procédure. Il s'appuie en outre le plus souvent dans ce type de cas sur le fait que certains éléments conduisent à ses yeux légitimement à une mise en cause, tout particulièrement le fait d'avoir été reconnu par un policier. Dans d'autres cas, plus rares, il peut également arguer du fait que « *les faits ont été reconnus par l'intéressé* » lors de sa garde à vue et donc que l'infraction est constituée, ce qui peut par exemple apparaître à l'occasion de bagarres, lorsque des coups ont été portés mais qu'ils bénéficient de l'excuse de provocation ou de légitime défense. Le **service gestionnaire refuse la suppression de la mention au fichier et en informe même par écrit le procureur**. La copie de tels échanges de **courriers, pour le moins surprenants**, figure en annexe 8 ⁽¹⁾. **Des personnes qui n'ont jamais été poursuivies demeurent donc dans les fichiers**. Dans un des parquets visités, ce type d'affaire représente **environ 10 % des requêtes individuelles chaque année**, et dans un peu moins de la moitié de ces mêmes cas les services de police refusent l'effacement.

On relèvera que ces observations s'appliquent avant tout aux services de la police nationale. Selon les magistrats entendus, la gendarmerie nationale semble appliquer sans restriction les décisions de mise à jour du fichier JUDEX formulées par le parquet.

• Même si le **procureur de la République** insiste auprès du service gestionnaire pour que soit mis fin à une telle anomalie, il **n'a in fine aucun moyen de vérifier que ses demandes ont été suivies d'effets**. Alors que le IV de l'article 21 de loi pour la sécurité intérieure prévoit que l'accès aux informations figurant dans les fichiers d'antécédents judiciaires est ouvert aux magistrats du parquet et que la circulaire du 6 juillet 2001 prévoit **l'installation** à cet effet **de terminaux dans les parquets**, cette mesure n'a connu **aucune application**. Selon l'un des magistrats entendus, c'est « *sans doute parce que la police n'a pas véritablement envie que nous ayons un regard plus précis sur ses fichiers* », tandis qu'un autre a noté que l'un des arguments qui avait été opposé par les gestionnaires de traitements à la mise en place d'un tel accès direct était l'insuffisant degré d'habilitation des personnels travaillant au parquet.

En définitive, le caractère extrêmement limité des cas d'effacement des fichiers en fonction de décision de classement sans suite débouche sur une situation pour le moins absurde. **Les fichiers d'antécédents tendent de plus en plus à jouer un rôle de casier judiciaire parallèle, et ce sans contrôle juridictionnel effectif**. Ainsi, alors que le juge peut décider de ne pas inscrire une condamnation sur le bulletin n° 2 du casier judiciaire, des mesures d'une portée similaire n'ont pas d'effet pour le STIC ou JUDEX. L'encadré ci-après récapitule pour mémoire les règles applicables au casier judiciaire.

⁽¹⁾ *Quatre courriers échangés au cours de l'année 2008 témoignent des difficultés rencontrées pour obtenir l'effacement au fichier dans une affaire de dégradations volontaires. Par ailleurs, trois courriers adressés au procureur de la République par le service gestionnaire du STIC illustrent l'importance accordée à la reconnaissance des faits par le mis en cause.*

LES RÈGLES RELATIVES À LA DISPENSE D'INSCRIPTION ET À L'EFFACEMENT DU CASIER JUDICIAIRE

• Les règles applicables en matière de **dispense d'inscription** sont différentes selon le bulletin concerné.

Pour le **bulletin n° 1**, qui ne peut être transmis qu'aux autorités judiciaires, l'article 768 du code de procédure pénale dispose qu'y sont inscrites notamment les condamnations pour crime, délit ou contravention de la cinquième classe, ainsi que les déclarations de culpabilité assorties d'une dispense de peine ou d'un ajournement du prononcé de la peine, sauf si la mention de ces décisions a été expressément exclue en application de l'article 132-59 du code pénal. Ce dernier permet au juge d'accorder une telle dispense *« lorsqu'il apparaît que le reclassement du coupable est acquis, que le dommage causé est réparé et que le trouble résultant de l'infraction a cessé »*.

S'agissant du **bulletin n° 2**, l'article 775-1 du code de procédure pénale prévoit que le tribunal qui prononce une condamnation peut exclure expressément sa mention au bulletin n° 2 soit dans le jugement de condamnation, soit par jugement rendu postérieurement sur la requête du condamné. L'article 777-1 du code de procédure pénale dispose que ces règles s'appliquent également à l'exclusion de la mention d'une condamnation du **bulletin n° 3**.

• Des **règles particulières** sont prévues **en faveur des mineurs** par l'article 770 du code de procédure pénale.

Lorsque, à la suite d'une décision prise à l'égard d'un mineur de dix-huit ans, la rééducation de ce mineur apparaît comme acquise, le tribunal pour enfants peut, après l'expiration d'un délai de trois ans à compter de ladite décision et même si le mineur a atteint sa majorité, décider, à sa requête, à celle du ministère public ou d'office, la suppression du casier judiciaire de la fiche concernant la décision dont il s'agit.

La suppression de la fiche relative à une condamnation prononcée pour des faits commis par une personne âgée de dix-huit à vingt et un ans peut également, si le reclassement du condamné paraît acquis, être prononcée à l'expiration d'un délai de trois ans à compter de la condamnation. Cette suppression ne peut cependant intervenir qu'après que les peines privatives de liberté ont été exécutées et que les amendes ont été payées et, si des peines complémentaires ont été prononcées pour une durée déterminée, après l'expiration de cette durée.

• L'article 769 du code de procédure pénale prévoit que sont **retirées** du casier judiciaire les fiches relatives à des condamnations effacées par une **amnistie**. Le sont également :

- les condamnations prononcées depuis plus de **quarante ans** et qui n'ont pas été suivies d'une nouvelle condamnation à une **peine criminelle ou correctionnelle** ;

- les **dispenses de peines et les condamnations pour contravention**, à l'expiration d'un délai de **trois ans** à compter du jour où elles sont devenues définitives ;

- les mentions relatives à la **composition pénale**, à l'expiration d'un délai de **trois ans** à compter du jour où l'exécution de la mesure a été constatée, si la personne n'a pas, pendant ce délai, soit subi de condamnation à une peine criminelle ou correctionnelle, soit exécuté une nouvelle composition pénale.

Or, l'utilisation des fichiers d'antécédents à des fins administratives leur confère une influence considérable sur certains destins individuels. **Il est donc nécessaire de modifier la loi de 2003 afin d'élargir le champ des motifs emportant l'effacement des fichiers d'antécédents à certains motifs d'inopportunité des poursuites**, tout particulièrement les classements pour

désistement du plaignant (classement 42), dus au comportement de la victime (classement 45) et pour régularisation d'office (classement 47). De plus, il faut envisager de mieux prendre en compte certaines procédures alternatives mises en œuvre par les parquets, comme la réparation (classement 51), la médiation (classement 52) et le rappel à la loi ou l'avertissement (classement 56)⁽¹⁾. En effet, de manière assez paradoxale le système actuel faisant de la reconnaissance des faits un motif de maintien dans les fichiers constitue pour les mis en cause une incitation à nier et à ne pas s'engager dans la voie de procédures alternatives.

Par ailleurs, l'installation de terminaux STIC et JUDEX au sein des parquets apparaît comme une nécessité au regard de l'exigence d'un contrôle effectif des fichiers d'antécédents.

Proposition n° 39

Élargir le nombre de cas dans lesquels le procureur de la République peut ordonner l'effacement des données personnelles en modifiant le III de l'article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure.

Proposition n° 40

Installer au plus vite dans les parquets des TGI des terminaux permettant l'accès direct aux données figurant dans les traitements STIC et JUDEX, afin d'assurer un véritable contrôle par le procureur de la République et d'accélérer le traitement des mises à jour en fonction des suites judiciaires.

D. L'ULTIME RECOURS DU DROIT D'ACCÈS INDIRECT

L'article 41 de la loi du 6 janvier 1978, modifiée par la loi du 6 août 2004, dispose que, « *Par dérogation aux articles 39 [droit d'accès] et 40 [droit de rectification], 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.* » Le droit d'accès à ces fichiers s'effectue donc de manière indirecte. Toute personne souhaitant l'exercer 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 toutes investigations utiles. Ce commissaire exerce, en lieu et place du requérant, le droit d'accès et le droit de rectification ou d'effacement des données soit inexactes, soit collectées ou conservées en contradiction avec la loi.

Dans la pratique, l'exercice de ce droit est rendu plus difficile par des délais de réponse très longs. En outre, l'encadrement de la communication des

(¹) Si l'on se réfère à l'activité d'un des parquets visités, celui du TGI d'Evry, on peut noter que les motifs de classement sans suite pouvant actuellement emporter effacement du fichier représentent 7051 affaires en 2008, soit 21 % du nombre d'affaires classées sans suite. L'élargissement proposé de la faculté d'effacement porterait cette proportion à 47,7 % (27,3 % si l'on ne prend pas en considération le classement 56 rappel à la loi/avertissement).

données au requérant est significativement différent selon qu'il s'agit de fichiers d'antécédents judiciaires ou de fichiers de renseignement.

1. Les difficultés rencontrées pour faire face à la croissance des demandes

a) Un volume croissant de demandes adressées à la CNIL et des délais très longs

- Les **flux de demandes d'accès indirect aux fichiers de police**, et plus particulièrement au fichier des renseignements généraux (FRG) ont connu une **augmentation considérable depuis 2002**, puisqu'ils sont **passés d'environ 1 000 demandes par an à cette date à 2 660 en 2007** (dont 1 607 visant exclusivement le FRG). De 2006 à 2007, la progression des demandes s'établit à 67 %. De fait, cette augmentation est corrélée à la communication accrue sur les possibilités de recours à la suite d'« affaires » particulièrement médiatisées, comme celle de la fiche RG de Bruno Rebelle durant la campagne pour les élections présidentielles, ou comme la polémique sur le fichier EDVIGE. À la suite de ces derniers débats, un grand nombre de requêtes a été enregistré (709 entre le 1^{er} juillet et le mois d'octobre), ce qui laisse présager qu'un nouveau record sera établi en 2008.

- Face à cette explosion de la demande, les **complexes procédures d'instruction** des dossiers restent assurées par **un nombre limité de personnels**. En ce qui concerne le STIC, c'est à la division des études, des liaisons et de la formation (DELFI) du service central de documentation criminelle, situé à Écully, que revient la charge de collecter les informations et d'instruire le dossier en vue de son examen par la CNIL. Cette division est composée d'une dizaine d'agents, dont six sont occupés à temps plein par le droit d'accès indirect. En ce qui concerne le FRG, l'essentiel des personnels affectés à l'instruction des dossiers appartient à la sous-direction de l'information générale (sept personnes à temps plein), tandis que deux personnes sont chargées du droit d'accès indirect à la direction du renseignement de la préfecture de police de Paris, sans qu'il s'agisse pour autant d'une tâche à temps plein.

Surtout, **au sein de la CNIL**, si l'on fait abstraction des **sept commissaires** auxquels est confiée par roulement la mission d'exercice du droit d'accès indirect, la **cellule administrative « droit d'accès indirect » se limite à sa responsable, épaulée par une assistante**. Or, la tâche d'instruction et de suivi des dossiers s'avère de plus en plus lourde.

En témoignent des **délais de réponse** particulièrement longs. S'agissant des demandes d'accès au **STIC**, il faut compter entre **douze et dix-huit mois** si le requérant est inscrit dans le fichier. **Pour le FRG, le délai est encore plus long** : lors du déplacement effectué par vos rapporteurs en décembre 2008, la CNIL traitait les demandes déposées au cours du premier semestre 2007, soit un retard de près de deux ans.

L'augmentation des moyens de la CNIL apparaît donc éminemment nécessaire pour **garantir des conditions réelles d'exercice du droit d'accès indirect à la hauteur de l'enjeu** en termes de libertés publiques.

Proposition n° 41

Prévoir l'engagement de personnels contractuels ponctuellement nécessaires à la CNIL pour traiter le stock des recours accumulé et garantir ainsi des délais convenables d'exercice du droit d'accès indirect.

b) Une procédure complexe : l'exemple du droit d'accès indirect pour les fichiers d'antécédents judiciaires

• Le requérant adresse sa demande par écrit à la CNIL. Si cette demande ne doit pas être nécessairement motivée, elle doit toutefois être accompagnée des justificatifs d'identité, de la copie des éventuels refus d'agrément ou de refus de visa, ainsi que de tout document prouvant une suite judiciaire favorable. Dès la réception de la demande de droit d'accès indirect, la CNIL adresse systématiquement un courrier au requérant pour l'informer des modalités de la procédure. Le ou les commissaires chargés de procéder aux vérifications sont désignés par un ordre de mission signé par le président de la CNIL.

Lorsque la demande est transmise par la CNIL aux gestionnaires des fichiers pour lesquels l'accès indirect a été demandé par le requérant, **trois cas de figure** peuvent se présenter.

Si **la personne est inconnue dans les fichiers**, après accord des gestionnaires concernés mentionnés sur la fiche remise lors de l'examen du dossier, le président de la CNIL informe le requérant de l'absence de signalement.

Dans le cas où le requérant est **connu comme victime**, les services gestionnaires des fichiers éditent sa fiche STIC ou JUDEX et saisissent le ou les procureurs de la République compétents, afin que ceux-ci puissent donner leur accord à la communication des informations.

Enfin, quand la personne est **connue comme mis en cause**, il est également procédé à l'édition de sa fiche mais sont aussi collectés les divers éléments de procédure référencés. Les parquets compétents sont également saisis afin d'actualiser le dossier au vu des suites judiciaires.

• Dans ces deux derniers cas, **il appartient ensuite au magistrat de la CNIL saisi de la requête de vérifier l'ensemble des documents collectés**. Les services gestionnaires des fichiers lui présentent également les demandes de mises à jour ou de suppressions transmises par l'autorité judiciaire, ainsi que son accord ou son refus de communication. Dans le cas d'une demande de suppression ou de mise à jour formulée par le procureur de la République, le gestionnaire du fichier

fournit au commissaire de la CNIL l'ancienne version et la nouvelle version de la fiche concernée.

À la suite de la séance d'examen, si les informations s'avèrent inexactes, incomplètes ou périmées, ou si l'enregistrement n'est pas conforme aux conditions de fonctionnement du fichier fixées par les textes les instituant, le président de la CNIL, sur proposition du commissaire, **peut demander la suppression ou la mise à jour des informations**.

Une lettre de notification est ensuite adressée au requérant lui indiquant la fin des vérifications. À cette occasion, sous réserve de l'accord du procureur de la République, une fiche récapitulative des informations enregistrées dans les fichiers d'antécédents lui est transmise, tandis que sont indiquées les suppressions éventuelles survenues à la suite des démarches de la CNIL.

Afin de mieux comprendre les réalités des contrôles effectués, l'encadré ci-après fournit quelques informations sur des cas pratiques assez représentatifs qui ont pu être portés à la connaissance de vos rapporteurs à l'occasion de leur participation à une séance d'examen du STIC par un commissaire de la CNIL, à Écully.

EXEMPLES DE DOSSIERS EXAMINÉS DANS LE CADRE DE L'EXERCICE DU DROIT D'ACCÈS INDIRECT

Le dossier n° 1 concernait une personne mise en cause en avril 2004 pour trafic de stupéfiants. Or, le parquet concerné a requalifié l'infraction en « détention pour usage personnel ». Ainsi le délai de conservation des données dans le STIC passe de 20 à 5 ans. Ce délai de 5 ans étant expiré à la date d'examen du dossier, il a été décidé l'effacement des données. La fiche d'investigation, signée par le magistrat de la CNIL récapitule l'ensemble des décisions prises lors de l'examen de ce dossier : requalification de l'infraction et effacement des données périmées. La demande de droit d'accès indirect avait été formulée en décembre 2007 et n'a été instruite qu'en novembre 2008, soit un délai d'instruction de près d'un an.

Le dossier n° 2 concernait une personne mise en cause en octobre 2002 pour violence sur agent de la force publique. Au regard des documents rassemblés, le magistrat de la CNIL a jugé que l'enquête n'a pas permis de mettre en cause totalement la personne visée, le dossier ne comportant qu'une simple garde à vue. Aussi a-t-il été décidé l'effacement des données, la personne impliquée ne répondant pas à la définition de mis en cause. Elle avait adressé à la CNIL sa demande de droit d'accès indirect en octobre 2007, à la suite d'un refus d'agrément pour la profession d'agent de sécurité.

Le dossier n° 3 concernait une personne mise en cause dans deux affaires : l'une d'atteinte aux personnes, l'autre d'escroquerie. Compte tenu de la nature de ces infractions, le délai de conservation des données est de 40 ans. Le procureur de la République compétent, saisi afin de transmettre les suites judiciaires, avait indiqué que le dossier avait fait l'objet d'un classement sans suite après régularisation à la demande du parquet (motif numéro 55 dans la nomenclature du ministère de la Justice). Ce motif ne pouvant donner lieu à effacement du STIC, le magistrat de la CNIL a décidé que les données concernant la personne mise en cause seraient conservées.

L'application de la même lourde procédure d'accès indirect aux victimes comme aux mis en cause n'apparaît pas justifiée. Un droit d'accès direct des

victimes à leur fiche doit donc être mis en place afin qu'elles puissent beaucoup plus rapidement faire valoir leurs éventuelles demandes de rectification. Cette mesure permettrait de « désengorger » en partie les flux de demandes adressés à la CNIL, accélérant d'autant le traitement des demandes des personnes mises en cause ; elle est en outre d'autant plus souhaitable que les victimes sont désormais mieux informées du fait qu'elles figurent dans les fichiers d'antécédents à l'occasion du dépôt de plainte.

Proposition n° 42

Instituer un droit d'accès direct des victimes aux fichiers d'antécédents judiciaires.

c) Des moyens insuffisants pour des défis toujours plus nombreux : la difficile équation de la CNIL

Dans son avant-propos au rapport d'activité 2006 de la CNIL, intitulé « *Orages sur la CNIL !* »⁽¹⁾, le président Alex Türk a mis en exergue la difficile équation que la CNIL doit résoudre : « *Avec 570 % d'augmentation de son activité en trois ans (2003 à 2006), plus de 70 000 fichiers déclarés chaque année, la CNIL connaît une croissance spectaculaire.* »

Or, de manière générale, la CNIL reste la plus pauvre des autorités de protection des données européennes, notamment en termes d'effectifs. Alors que l'équivalent britannique de la Commission dispose de 270 postes budgétaires, la CNIL n'était dotée en 2008 que de 120 postes budgétaires. En matière de fonctionnement aussi, les comparaisons internationales sont souvent défavorables à la CNIL. À titre d'exemple, l'autorité anglaise dispose d'un budget de communication 30 fois supérieur à celui de la CNIL, soit environ 3 millions d'euros (10 % du budget total) contre 100 000 euros (0,9 % du budget total) pour la CNIL. Si son budget a augmenté de 75,4 % au cours des quatre dernières années (2004-2008), cette hausse est sept fois moins importante que celle enregistrée par l'activité de la CNIL sur la même période.

(1) 27^{ème} rapport d'activité 2006 de la CNIL, pages 7 et 8.

Évolution des moyens de la CNIL (lois de finances initiales)

	2004	2005	2006	2007	2008	Évolution (en nombre) 2004-2008	Évolution (en %)
Postes	80	85	95	105	120	40	50,0
Crédits (en M€)	6,5	7,2	9,0	9,9	11,4	4,9	75,4
<i>Personnels</i>	4,2	4,7	5,3	6,1	7,2	3,0	71,4
<i>Fonctionnement</i>	2,3	2,5	3,7	3,8	4,2	1,9	82,6

Source : 28^{ème} rapport d'activité 2007 de la CNIL, p. 96.

Pour 2009, la CNIL sera dotée de 12 954 000 euros en autorisations d'engagement et en crédits de paiement, soit une hausse de 13,2 % par rapport à 2008. Lors de son audition le jeudi 9 octobre 2008 par vos rapporteurs, M. Alex Türk a souligné que l'insuffisance des moyens, dont dispose la CNIL, compromet gravement la reconnaissance accrue des droits fondamentaux des citoyens, garantis, d'une part, par le droit d'accès indirect et, d'autre part, par les contrôles généraux opérés par la CNIL. Ainsi, saisie de 2 000 à 3 000 demandes d'accès indirect par an, la CNIL s'estime incapable de répondre au requérant dans un délai raisonnable. En outre, rapportés à la population française, ses effectifs font également de la CNIL la « dernière du peloton » des autorités de protection des données de l'Union européenne. Ainsi, alors qu'on compte 10 agents de protection des données par million d'habitants en République tchèque et 5 en Suède ainsi qu'aux Pays-Bas, ils ne sont qu'à peine deux pour un million de citoyens en France.

Effectifs des autorités de protection des données en Europe

Autorités de protection des données	Nombre d'employés	Population totale (en millions)	Nombre d'employés / population totale
<i>République Tchèque</i>	100	10	10
<i>Irlande</i>	22	4	5,5
<i>Pays-Bas</i>	75	16	4,7
<i>Suède</i>	42	9	4,7
<i>Royaume-Uni</i>	260	60	4,3
<i>Espagne</i>	154	45	3,4
<i>Allemagne Fédérale et Länder</i>	177	82,4	2,15
<i>France</i>	120	62	1,94
<i>Italie</i>	106	59	1,8

Au-delà de la seule question des moyens, la CNIL reste une institution, à bien des égards, « *trop parisienne* », qui ne s'est pas véritablement déployée sur l'ensemble du territoire. Selon son président, une meilleure garantie des droits des citoyens répertoriés dans les fichiers de police passe par un rapprochement avec l'autorité de contrôle chargée de les protéger des pratiques abusives. La création d'antennes interrégionales de la commission pourrait apporter une réponse à cette préoccupation.

Quoi qu'il en soit, le déploiement de la CNIL ne saurait être envisageable sans l'allocation de moyens correspondants. Dans cette perspective, il est possible de s'interroger sur l'opportunité de doter la CNIL d'une ressource propre, capable de garantir son autonomie et sa pérennité financières. Une des évolutions possibles, défendue par le président de la CNIL, est de passer à un financement à l'anglaise, c'est-à-dire non plus fondé sur l'impôt, mais sur une redevance acquittée par les acteurs de l'informatique (collectivités territoriales ou entreprises d'une certaine taille).

Cette redevance pourrait représenter entre 30 et 40 euros par acteur, des exemptions étant toutefois possibles pour les plus petites des entreprises et des collectivités locales. Le but poursuivi par une telle réforme est certes d'augmenter le budget de la CNIL, mais également de conforter son indépendance. Selon les premières estimations, l'instauration d'une telle redevance permettrait de doubler le budget de la CNIL en 7 à 10 ans. Un groupe de travail commun entre la CNIL et les services du Premier ministre étudie actuellement la faisabilité de cette réforme.

Proposition n° 43

Engager une réflexion sur la création au profit de la CNIL d'une redevance modeste, acquittée par les utilisateurs de l'informatique, en vue d'adapter les moyens de l'autorité de contrôle à la croissance continue des recours.

2. L'accès aux données figurant dans les fichiers de renseignement

a) Les modalités particulières de communication prévues pour le fichier des renseignements généraux

Dans le cas de demande d'accès indirect au fichier des renseignements généraux, l'architecture générale de la procédure est proche de celle observée pour le STIC, avec cependant des particularités en matière de travail d'instruction, de décision sur la communication des données et d'information du requérant. La procédure suivie a été détaillée au sein d'un protocole entre la CNIL et le ministère de l'Intérieur de février 1992.

• À la différence des fichiers d'antécédents judiciaires, qui constituent des dossiers automatisés, **le FRG est organisé sur une base départementale et seule**

l'indexation des dossiers est informatisée. Les dossiers eux-mêmes sont conservés sous forme papier. La **phase d'instruction** constitue donc un **travail particulièrement long**. Il s'agit tout d'abord de vérifier si le requérant figure bien dans le fichier. En cas de réponse positive du ministère, des demandes sont adressées aux SDIG du lieu de naissance, des lieux de résidence et éventuellement des départements mentionnés par le requérant dans la saisine. La direction du renseignement de la préfecture de police de Paris (DRPP) est éventuellement saisie lorsqu'elle est territorialement compétente.

L'intégralité des dossiers doit être transmise à la cellule chargée du droit d'accès indirect. Pour cela, ils sont « **gelés à la date de la saisine** ». Cette démarche constitue une garantie, puisque les éventuelles informations dont la présence est interdite dans le FRG (comme des mentions de condamnations, par exemple) sont maintenues dans le dossier communiqué au requérant. Ce n'est qu'après cette communication que la CNIL fait usage de son pouvoir de rectification ou de suppression. En revanche, les requérants ne peuvent naturellement pas avoir connaissance des éléments susceptibles d'être collectés après la date de la saisine.

• **L'instruction du dossier** comprend une phase de discussion entre la CNIL et les services responsables des traitements. À cette occasion, il est statué sur la **communicabilité totale ou partielle** du dossier. L'article 7 du décret n° 91-1051 du 14 octobre 1991 ⁽¹⁾ dispose que le ministre de l'Intérieur « *peut s'opposer à la communication au requérant de tout ou partie des informations le concernant lorsque cette communication peut nuire à la sûreté de l'État, à la défense ou à la sécurité publique* ». Dans le cas où une telle décision est prise, il est indiqué par courrier au requérant qu'il figure effectivement dans le fichier, qu'il a été procédé à la vérification des éléments composant son dossier et quelles sont les voies de recours devant le juge administratif pour contester la décision de refus de communication ⁽²⁾.

Lors de l'instruction du dossier sont également prises les décisions relatives à l'occultation du nom des tiers (en pratique, ces informations sont « blanchies »).

• **La phase de communication** a lieu soit dans les locaux de la CNIL, pour les personnes résidant en région parisienne, soit en préfecture, dans les autres cas. Elle clôt une procédure particulièrement longue et dure en général peu de temps, au plus un quart d'heure, parfois seulement quelques minutes quand le dossier est particulièrement peu fourni. Lors de ces séances, le **dossier est présenté au requérant**, qui peut prendre des notes écrites ou recourir à un

⁽¹⁾ *Portant application aux fichiers informatisés, manuels ou mécanographiques gérés par les services de renseignements généraux des dispositions de l'article 31, alinéa 3, de la loi du 6 janvier 1978.*

⁽²⁾ *Dans l'arrêt Demaria du 21 novembre 2003, le Conseil d'État a annulé une décision de refus de communication d'un dossier pour laquelle « le ministre de l'Intérieur s'est fondé exclusivement sur l'appartenance [du requérant] à « l'église de scientologie » et sur la menace pour la sécurité publique que représente ce mouvement sectaire », sans qu'il soit apporté d'éléments démontrant que cette communication pourrait porter atteinte à la sécurité publique ou à la sécurité de l'État.*

dictaphone, mais aucune copie d'une pièce ne peut être effectuée. Il lui est possible de se faire assister par un avocat. Comme vos rapporteurs ont pu le constater en assistant à une telle réunion, il semble que les requérants sont souvent déçus par l'aspect squelettique de leur dossier FRG (« *C'est tout ce qu'il y a ? Je m'attendais à des choses plus piquantes compte tenu de mon parcours* »).

Le requérant peut ensuite adresser une **note d'observation** au président de la CNIL récapitulant les demandes de modification et de rectification. Celles-ci sont étudiées lors d'une nouvelle réunion entre la CNIL et les services de police pour déterminer quelles sont les suites qui sont apportées à cette note.

À l'issue de la séance de communication, le représentant de la CNIL et les services décident de la **suppression éventuelle de certaines pièces du dossier, soit en raison de mentions non conformes aux textes, soit, le plus souvent, du fait de l'ancienneté et de l'absence d'intérêt** des documents. Lors de la réunion précitée, un des dossiers ne contenait qu'un élément : une enquête de moralité réalisée en 1966, à la suite d'une inscription à un concours de la fonction publique ; il a été décidé de procéder à sa suppression. Dans ce cas, les documents en question sont collectés par les services de police, puis présentés par lots aux Archives nationales, lesquelles choisissent alors ceux qu'elles souhaitent conserver. Les fiches restantes sont définitivement détruites, avec procès-verbal de destruction.

b) Les fichiers de renseignement classés secret-défense

• À la suite de la réforme du renseignement, les textes instituant des fichiers classés secret-défense ont fait l'objet de modifications afin de les adapter à la nouvelle architecture des services. La mise en place de la direction centrale du renseignement intérieur (DCRI) a ainsi conduit à la création, par un décret du 27 juin 2008, d'un fichier de **centralisation du renseignement intérieur pour la sécurité du territoire et les intérêts nationaux (CRISTINA)**. Ce dernier a repris depuis le 1^{er} juillet 2008, les données figurant auparavant dans le fichier de la direction de la surveillance du territoire (DST), qui datait de 1986, ainsi que certaines données des fichiers gérés auparavant par la direction centrale des renseignements généraux, dont le fichier informatisé du terrorisme. Dans le même temps, l'application GESTEREXT est destinée à remplacer GESTER, créée en 1996, pour permettre à la direction du renseignement de la préfecture de police de Paris d'exercer sa mission de renseignement intérieur.

CRISTINA traite de la lutte anti-terroriste et du renseignement en milieu fermé. Comme le permet l'article 26 de la loi de 1978 et en raison du caractère éminemment sensible de l'objet du fichier, **le décret du 27 juin 2008 précité n'a pas été publié au Journal Officiel**⁽¹⁾. Parmi les raisons avancées pour justifier la non-parution du décret figurent la préservation du secret des modalités d'action de

(¹) *En vertu de l'article 83 du décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, ce décret a été soumis pour avis à la CNIL, laquelle a émis un « avis favorable avec réserves ».*

la DCRI ainsi que la nécessité de maintenir une classification secret-défense de ce fichier, afin de protéger la crédibilité et les relations de confiance bilatérales qui ont pu être nouées avec d'autres services de renseignement dans le cadre de coopérations internationales.

• Le **contrôle de ces fichiers** est prévu par l'article 41 de la loi de 1978 : au même titre que pour les autres fichiers de police, il s'effectue par le biais du **droit d'accès indirect**. Il présente cependant **quelques particularités**, dont notamment **l'absence de possibilité de contrôle sur place** par la CNIL. Par ailleurs, selon l'article 84 du décret n° 2005-1309, « *les agents de la commission et les personnes lui prêtant leur concours, appelés dans le cadre de l'exécution de leur mission, à prendre connaissance d'informations classifiées au titre de la protection du secret de la défense nationale, doivent y être habilités par le Premier ministre* ».

En pratique, le magistrat de la CNIL chargé du contrôle se rend au siège de la DCRI et se fait présenter les notes concernant les requérants. Comme il s'agit d'un fichier informatique centralisé, à la différence du FRG, la phase d'instruction est grandement facilitée. Le magistrat procède alors au contrôle des données figurant dans les dossiers. Il s'agit d'un fichier de renseignement et si aucune durée fixe de conservation des données n'est prévue, celles-ci ne doivent être conservées qu'en fonction des finalités du fichier.

Le troisième alinéa de l'article 41 de la loi de 1978 dispose que « *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.* » En pratique, il est rarissime que tel soit le cas. Il est **notifié au requérant par courrier qu'il a été procédé aux vérifications nécessaires**, sans préciser donc s'il figure dans le fichier ⁽¹⁾. Le contrôle de la CNIL sur les fichiers de renseignement couverts par le secret de la défense nationale existe bien et il est pratiqué dans les conditions précédemment décrites, qui sont différentes de celles du contrôle exercé sur des fichiers de renseignement moins sensibles, comme le FRG. Compte tenu du caractère secret des fichiers classifiés, vos rapporteurs ne sont cependant pas en mesure d'évaluer précisément la profondeur de ce contrôle.

• La **question de la légitimité** de ce type de fichiers se pose donc moins en termes de contrôle des données personnelles que de **contrôle démocratique sur les actes réglementaires portant création de tels outils**. Il est possible d'y répondre, au moins en partie, en prévoyant la transmission systématique à la délégation parlementaire au renseignement de l'ensemble des textes prévoyant la création de traitements automatisés de données personnelles au profit des services de renseignement. On rappellera à cet effet que la loi n° 2007-1443 du 9 octobre

(¹) Ces observations s'appliquent également aux autres fichiers de renseignement, qu'il s'agisse de ceux mis en oeuvre par la direction générale de la sécurité extérieure ou par la direction de la protection et de la sécurité de la défense.

2007 portant création de cette délégation lui fixe pour mission de « *suivre l'activité générale et les moyens des services spécialisés à cet effet placés sous l'autorité des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget* ».

Proposition n° 44

Assurer une transmission systématique à la délégation parlementaire au renseignement de l'ensemble des textes relatifs à la mise en place de traitements automatisés de données à caractère personnel par les services de renseignement, lorsque les textes portant création des fichiers intéressant la sûreté de l'État et la défense ne sont pas publiés au *Journal Officiel*.

V. RESPECTER LES FINALITÉS

Les différents fichiers de police sont devenus des outils de travail quotidiens et indispensables pour les forces de sécurité intérieure. Il ne s'agit cependant pas d'instruments banals et leurs usages doivent être très étroitement encadrés pour garantir le respect des finalités qui ont présidé à leur création. L'accès aux fichiers est de ce point de vue un enjeu de toute première importance. La traçabilité offerte par les systèmes informatiques permet certes d'identifier plus facilement les auteurs d'éventuelles consultations abusives, lesquelles existaient déjà du temps des fichiers papiers. Toutefois, les dispositifs techniques actuels destinés à traquer ces faits sont pour l'essentiel mis en œuvre *a posteriori*, et c'est assurément vers des possibilités d'alerte en temps réel qu'il convient de s'acheminer, afin de renforcer l'effet dissuasif.

Une autre pratique ancienne a été récemment transformée : celle de la consultation des fichiers de police à des fins administratives. Si elle est désormais autorisée et encadrée par les textes, elle n'en continue pas moins de poser des difficultés sérieuses, tout particulièrement en matière d'accès à l'emploi.

Enfin, l'usage des fichiers semble appelé à se développer sur deux plans. D'une part, les possibilités offertes par l'informatique en matière de rapprochements entre affaires sont considérables et la question désormais posée est celle de l'utilisation de tels instruments non plus seulement pour les crimes sériels, mais aussi pour améliorer le taux d'élucidation de la petite et moyenne délinquance. D'autre part, on peut relever un accroissement sensible de l'intérêt porté aux fichiers dans le cadre de la coopération policière internationale. Dans ces deux cas, le cadre juridique mérite d'être précisé pour atteindre un équilibre satisfaisant entre deux exigences, celle de poursuite des infractions et celle de protection des libertés individuelles.

A. ACCROÎTRE LA LUTTE CONTRE LES CONSULTATIONS ABUSIVES

Plusieurs affaires de ventes de données à caractère personnel par des fonctionnaires ayant accès aux fichiers de police ont été révélées ces derniers mois, celle concernant Olivier Besancenot ayant eu un retentissement certain. Cette pratique a malheureusement toujours existé et porte dans la police le nom évocateur de « tricoche ». Les affaires les plus récentes ont pour point commun la rapidité avec laquelle les auteurs de ces infractions graves ont été confondus. La traçabilité des consultations constitue à l'évidence une des avancées de l'informatisation des fichiers : l'utilisation de ces derniers peut être très précisément analysée et les preuves d'abus sont de ce fait plus faciles à réunir. Cette observation ne s'applique malheureusement pas encore à l'ensemble des fichiers en service, puisque certains continuent à fonctionner sous forme papier. Ainsi, à l'occasion d'un déplacement au sein d'une brigade de gendarmerie, vos rapporteurs ont pu constater que l'accès au fichier alphabétique de renseignement était particulièrement aisé et qu'aucun registre des consultations n'était tenu.

S'agissant des fichiers informatisés, selon les mots d'une des personnes auditionnées, d'une certaine manière la technologie « *sécète ses propres anticorps* ». Encore faut-il que les dispositifs techniques destinés à traquer les agents indéliçats soient suffisamment dissuasifs, afin de tarir autant que possible la source des fuites. Il s'agit d'une priorité d'autant plus grande que les pratiques de renseignement privé, sous des appellations diverses, semblent en augmentation et que l'encadrement de ce secteur « hétérogène » n'est par définition pas aisé.

1. Divers degrés d'abus, dans un contexte susceptible d'en accroître la fréquence

• Il convient de distinguer **plusieurs cas de figure d'utilisations détournées**, qui ne présentent **pas le même degré de gravité**.

Les fraudes peuvent être animées par la **curiosité**, sans qu'il y ait pour autant volonté de diffusion à des tiers. Il s'agit dans ces cas soit de vérifier si telle ou telle « célébrité » est connue dans les fichiers ⁽¹⁾, soit de s'informer sur des personnes avec lesquelles on est directement en relation. Dans ce dernier cas, la consultation peut prendre un tour plus grave si elle est animée par une volonté de régler un litige personnel.

Il peut également s'agir de « rendre service » à son entourage, par exemple en fournissant des informations sur un candidat à un emploi, le tout sans véritable contrepartie matérielle directe.

Enfin, il existe la « tricoche » proprement dite, qui consiste à **fournir des informations à un tiers en échange d'une contrepartie** (financière, matérielle ou d'échange de renseignements).

• L'une des **questions délicates** consiste à **évaluer s'il existe une véritable augmentation de la demande de renseignements par divers organismes privés**, susceptible d'induire davantage de tentations. Plusieurs affaires récentes tendent à montrer que tel est bien le cas et que la croissance générale du secteur de la sécurité privée se traduit également par un développement du marché privé du renseignement.

Les activités des **agences de recherche privées** sont régies par le titre II de la loi n° 83-629 du 12 juillet 1983 réglementant les activités privées de sécurité, modifiée par la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure. Ce texte encadre « *la profession libérale qui consiste, pour une personne, à recueillir, même sans faire état de sa qualité ni révéler l'objet de sa mission, des informations ou renseignements destinés à des tiers, en vue de la défense de leurs intérêts* ». L'exercice de ces activités est soumis à un agrément préfectoral, dans les conditions prévues par l'article 2 du décret n° 2005-1123 du 6 septembre 2005. Il convient de souligner en outre que l'article 21 de la loi précitée dispose que

(1) « *La policière aimait trop les "people"* », *Le Monde*, 5 février 2009.

« les fonctionnaires de police et les officiers et sous-officiers de la gendarmerie nationale ne peuvent exercer [cette activité] durant les cinq années suivant la date à laquelle ils ont cessé définitivement ou temporairement leurs fonctions que sous réserve d'avoir obtenu au préalable l'autorisation écrite, selon le cas, du ministre de l'Intérieur ou du ministre de la défense ». **Cette autorisation n'est cependant nécessaire que pour l'exercice à titre libéral**, le fait d'être employé pour participer à une telle activité étant soumis à déclaration préalable à l'embauche auprès du préfet, à enquête administrative et à une justification de l'aptitude professionnelle ⁽¹⁾.

Quant aux **entreprises relevant du secteur de l'intelligence économique**, elles ne font pas l'objet d'un tel encadrement. Il n'existe aucune définition législative ou réglementaire de cette activité. Selon le rapport d'Henri Martre, « l'intelligence économique peut être définie comme l'ensemble des actions coordonnées de recherche, de traitement et de distribution, en vue de son exploitation, de l'information utile aux acteurs économiques » ⁽²⁾. S'agissant d'un secteur neuf et émergent, plusieurs personnes auditionnées ont noté que parfois « la mauvaise monnaie chasse la bonne », notamment par le biais de l'utilisation de sous-traitants en cascade. Or, l'exercice de fonctions dans de telles entreprises par d'anciens policiers ou militaires de la gendarmerie est seulement soumis au droit commun du contrôle par la commission de déontologie instaurée par la loi n° 93-122 du 29 janvier 1993 relative à la prévention de la corruption et à la transparence de la vie économique et des procédures publiques ⁽³⁾.

La question d'un encadrement plus étroit de ces secteurs et de l'extension des règles limitant, pour une durée déterminée, la possibilité pour d'anciens fonctionnaires de police et de militaires de la gendarmerie d'y exercer dépasse naturellement le cadre du présent rapport. Il reste que la lutte contre l'utilisation abusive des fichiers de police doit s'inscrire dans une **perspective globale**, visant à éviter la constitution d'un « marché » et à s'attaquer tant à « l'offre » qu'à la « demande », afin de permettre une plus grande étanchéité entre deux mondes ⁽⁴⁾.

⁽¹⁾ L'article 10 du décret n° 2005-1123 du 6 septembre 2005 prévoit que « les fonctionnaires de la police nationale et les militaires de la gendarmerie nationale ayant la qualité d'officier de police judiciaire, d'agents de police judiciaire ou d'agent de police judiciaire adjoint [...] justifient en cette qualité de l'aptitude professionnelle à être salarié. ».

⁽²⁾ Intelligence économique et stratégie des entreprises, Henri Martre, Philippe Clerc et Christian Harbulot. Commissariat général au plan, La documentation française, 1994.

⁽³⁾ Selon le douzième rapport d'activité de cette commission, les fonctionnaires issus du ministère de l'Intérieur ont représenté 13,5 % des avis émis de 2000 à 2006 en moyenne. Ceux relevant du ministère de la Défense sont à l'origine de 7,9 % des avis, sans qu'il soit possible de distinguer la part de la gendarmerie nationale de celle des autres armes.

⁽⁴⁾ De ce point de vue, il convient de souligner combien sont profondes les différences entre la France et les États-Unis. Les sociétés d'intelligence économique américaines proposent en effet sur leurs sites Internet des services de « background screening » permettant aux sociétés privées désirant embaucher une personne de vérifier de manière très complète ses antécédents, professionnels mais aussi éventuellement judiciaires. De fait, ces sociétés réalisent un « environnement » du candidat.

2. La « tricoche » : un phénomène sévèrement sanctionné

- Le phénomène des consultations abusives **reste marginal**, selon la grande majorité des interlocuteurs rencontrés.

S'agissant de la **police nationale**, en 2008 il a été procédé à 211 réquisitions auprès des services informatiques en vue de l'analyse de consultations de fichiers, tant dans le cadre d'enquêtes administratives que judiciaires. Toutes n'ont pas conduit à mettre en cause les fonctionnaires concernés, certains pics de consultation anormaux s'expliquant dans de nombreux cas légitimement par les exigences particulières d'une enquête en cours. Au cours des **cinq dernières années**, une **centaine d'affaires d'abus véritables** a pu être détectée. Dans 80 % des cas, ces fraudes ne poursuivaient aucune fin mercantile, et environ la moitié de cette part s'expliquait par la seule curiosité des fonctionnaires mis en cause. Dans les **20 % des cas** restants, les informations fournies à des tiers ont fait l'objet d'une **contrepartie**, financière ou non. Comme le relève la CNIL dans son rapport de janvier 2009, ces chiffres doivent être rapportés aux 100 000 policiers habilités à consulter le STIC et aux 20 millions de consultations annuelles de ce fichier.

Selon les responsables de la **gendarmerie nationale** entendus, peu de cas de ventes d'informations à des tiers ont été signalés. **Une dizaine d'incidents** ont été recensés dans cette arme sur les **dix dernières années**, dont deux affaires significatives en 2004 ; des sanctions disciplinaires ont été prises à l'encontre des contrevenants (allant jusqu'à 40 jours d'arrêt et à la mutation d'office), mais il n'y a pas eu de suites judiciaires après transmission des affaires en question au procureur de la République. Dans la moitié des cas où l'inspection générale de la gendarmerie effectue une enquête à la suite d'un soupçon, les gendarmes sont finalement disculpés.

- L'ensemble des responsables administratifs et des représentants syndicaux entendus sur le sujet ont souligné combien les **sanctions disciplinaires** étaient **désormais sévères** en cas de consultation abusive ; **la communication interne sur ces sanctions** a également fait l'objet d'un soin particulier, afin de décourager autant que possible les tentations.

La gamme des sanctions encourues apparaît suffisamment large. Les consultations abusives constituent, quel que soit leur degré de gravité, une violation de l'article 7 du code de déontologie de la police nationale⁽¹⁾. Au demeurant, la police est une administration « bien sanctionnée » : elle représente 8 % de la fonction publique et 40 % des sanctions disciplinaires. Dans les cas où une révocation est prononcée, l'affaire connaît des suites sur le plan judiciaire.

(1) « Le fonctionnaire de la Police Nationale est loyal envers les institutions républicaines. Il est intègre et impartial ; il ne se départit de sa dignité en aucune circonstance. Placé au service du public, le fonctionnaire de police se comporte envers celui-ci d'une manière exemplaire. Il a le respect absolu des personnes, quelles que soient leur nationalité ou leur origine, leur condition sociale ou leurs convictions politiques, religieuses ou philosophiques. ».

Le fait de détourner des informations personnelles de leur finalité ou de les porter à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans de prison et de 300 000 euros d'amende ⁽¹⁾; il constitue en outre une atteinte au secret professionnel, punie d'un an d'emprisonnement et de 15 000 euros d'amende ⁽²⁾.

3. Améliorer le contrôle d'accès et mettre en place des dispositifs d'alerte précoce

• L'un des points clés de la lutte contre les consultations abusives est la **responsabilisation** de chaque agent disposant d'une habilitation à consulter les fichiers. De ce point de vue, il convient tout d'abord de relever qu'une trop forte restriction du nombre d'habilitations peut se révéler contre productive, l'un de ses effets pervers pouvant être le développement de la pratique du prêt de codes. En revanche, lorsque chacun a son propre code d'accès, dont il est responsable sous peine de sanctions sévères, une plus grande discipline peut être observée et une forme d'« autorégulation » efficace s'installe.

Les négligences fréquemment constatées dans le passé en matière d'utilisation des codes personnels, telle que leur affichage sur le micro-ordinateur au moyen d'un *post it*, ont semble-t-il fortement régressé, notamment en raison de la connaissance des sanctions encourues. Toutefois, des pratiques ponctuelles de communication de code ou de consultation pour le compte d'autrui peuvent persister. On peut également relever que la multiplication des codes d'accès personnels pour accéder aux différentes applications informatiques ainsi qu'aux différents fichiers, sensée être plus stricte en matière de contrôle d'accès, peut en pratique conduire les personnels à noter sur un pense-bête la liste de leurs codes.

L'une des voies possibles pour limiter la fréquence de ces comportements est l'**amélioration du contrôle d'accès**, soit par des moyens biométriques, soit par le biais de **cartes à puce**. La gendarmerie nationale est actuellement en train de travailler sur ce dernier type de solution ; à partir de 2009 une carte à puce, remplaçant la carte professionnelle de chaque gendarme, aura vocation à mieux assurer leur identification lorsqu'ils souhaitent accéder aux fichiers et, à terme, pourra servir également de vecteur de signature électronique dans le cadre d'une dématérialisation progressive des procédures.

• La deuxième marge de progression réside dans la **réalisation de liens avec l'annuaire des ressources humaines**, permettant d'associer la « vie administrative » de la personne avec son profil d'accédant aux fichiers.

De ce point de vue, la mise en place progressive de PASSAGE, successeur du réseau CHEOPS ⁽³⁾, constituera un véritable saut technologique. CHEOPS a été

⁽¹⁾ Articles 226-21 et 226-22 du code pénal.

⁽²⁾ Article 226-13 du code pénal.

⁽³⁾ CHEOPS (pour « circulation hiérarchisée des enregistrements opérationnels de police sécurisés ») est un portail d'accès et d'identification permettant l'accès aux applications de police du ministère de l'Intérieur.

conçu pour des technologies « *mainframe* » et n'est plus du tout adapté aux nouvelles technologies de type Web. En outre, il pose de très lourds problèmes d'interopérabilité avec des systèmes externes et est, de ce fait, inadapté au rapprochement avec la gendarmerie nationale. Dans le cadre du déploiement de PASSAGE, il sera possible de réutiliser certaines briques technologiques déjà utilisées par la gendarmerie nationale, par exemple en matière de contrôle d'accès et pour veiller à la traçabilité des connexions, tel que LemonLDAP-NG.

Il n'existe actuellement pas de système d'authentification unifié pour les agents du ministère de l'Intérieur, ce qui entraîne une grande complexité des procédures d'autorisation d'accès, réparties entre de nombreuses autorités, et peut conduire à des incohérences entre les comptes attribués et les personnels effectivement présents. Ainsi, en cas de mutation, voire de sortie des cadres, si l'ensemble des retraits d'habilitations qui en découle n'est pas traité de manière appropriée, des « comptes dormants » peuvent persister. La solution à ce problème passe par un couplage de la gestion du contrôle des habilitations avec celui du personnel (Geopole). Elle ne pourra être mise en place que de manière progressive. Lors de la première phase du déploiement de PASSAGE, le gestionnaire d'habilitations de CHEOPS (GEHA) continuera en effet à être utilisé ; la deuxième phase verra l'unification de la gestion des habilitations de l'ensemble des agents du ministère ; et c'est seulement au cours de la troisième étape que seront utilisées les solutions précitées de contrôle d'accès et de traçabilité déjà utilisées dans la gendarmerie. C'est également à partir de ce moment qu'il sera possible d'utiliser des techniques comme la carte à puce ou la biométrie, PASSAGE étant suffisamment évolutif pour accepter des solutions techniques très diverses en matière de contrôle d'accès.

Proposition n° 45

Remplacer par un contrôle d'accès sécurisé au moyen de cartes à puce la multitude de codes attribués aux policiers et gendarmes pour utiliser les différentes applications dont ils disposent.

- Enfin, les contrôles réalisés sur les utilisations des fichiers sont effectués *a posteriori*, la plupart du temps quand un soupçon de détournement se manifeste⁽¹⁾. Si ce contrôle est une des tâches incombant aux chefs de service, encore faut-il la rendre réalisable en pratique. En l'état actuel des technologies, un examen systématique des connexions par ces derniers apparaît *de facto* difficile en raison du volume des informations à traiter, mais aussi du nombre des autres tâches devant être assurées par ce responsable.

Aussi est-il nécessaire, pour améliorer la réactivité des investigations et de mieux détecter les comportements anormaux, de s'orienter vers la mise en place

⁽¹⁾ Il est parfois procédé à la pose de « sonnettes » sur des dossiers particulièrement sensibles du STIC, par exemple pour des enquêtes portant sur du grand banditisme, ce qui permet de réagir en temps réel à une consultation par un policier ne participant pas directement à l'enquête et qui pourrait paraître suspecte.

des systèmes d'alerte en temps réel fondés sur des « analyses comportementales » de l'utilisation des fichiers. De telles technologies existent d'ores et déjà dans d'autres domaines d'activité, notamment pour détecter les utilisations frauduleuses des cartes bancaires en identifiant les retraits d'espèces ou les paiements s'éloignant du profil d'utilisation habituel de leur propriétaire. Une fois l'alerte déclenchée, le chef de service aurait la charge de procéder aux vérifications nécessaires, en appréciant l'adéquation des consultations effectuées aux tâches et enquêtes confiées à l'agent soupçonné. Ce type d'évolution technologique deviendra réalisable avec la mise en service de PASSAGE.

Proposition n° 46

S'orienter vers la mise en place de systèmes d'alerte en temps réel fondés sur l'analyse du comportement de l'utilisateur et permettant de mieux réprimer les détournements de données personnelles figurant dans les fichiers de police.

B. L'UTILISATION DES FICHIERS D'ANTÉCÉDENTS JUDICIAIRES DANS LE CADRE D'ENQUÊTES ADMINISTRATIVES : D'UNE UTILISATION ANNEXE À UNE PRATIQUE MASSIVE

D'une certaine manière, la possibilité reconnue par la loi d'utiliser les fichiers d'antécédents judiciaires dans le cadre de certaines enquêtes administratives constitue un progrès par rapport aux pratiques antérieures. Les demandes des préfets sur la moralité de candidats à certains emplois sensibles recevaient auparavant des réponses laconiques et invérifiables du type « bien connu de nos services ». Le **meilleur encadrement de pratiques anciennes** opéré à partir de 2001 ne peut cependant masquer les **difficultés de l'exercice**. Si l'on peut considérer que les erreurs figurant dans les fichiers d'antécédents judiciaires restent « acceptables » tant que l'usage qui est fait de ces derniers est cantonné à des objectifs strictement policiers, il n'en est pas de même lorsque la consultation de ces bases de données **conditionne l'accès à l'emploi et à la nationalité française**. Or, comme vos rapporteurs ont pu le relever, l'ampleur des inexactitudes affectant les fichiers d'antécédents, et au premier chef le STIC, est des plus préoccupantes. De fait, **des décisions extrêmement lourdes de conséquences** pour nombre de citoyens relèvent en ultime analyse des capacités d'appréciation des situations individuelles manifestées par le préfet et par les services de police.

1. Des possibilités très larges de consultation à des fins administratives

• L'article 28 de la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne a prévu la possibilité d'une consultation des traitements automatisés de données personnelles gérés par les services de police judiciaire ou de gendarmerie « *dans la stricte mesure exigée par la protection des personnes et la défense des intérêts fondamentaux de la nation* ». Cette faculté n'était alors

ouverte que lorsqu'il s'agissait de « *décisions administratives d'affectation, d'autorisation, d'agrément ou d'habilitation, prévues par des dispositions législatives ou réglementaires, concernant soit l'exercice de missions de sécurité ou de défense, soit l'accès à des zones protégées en raison de l'activité qui s'y exerce, soit l'utilisation de matériels ou produits présentant un caractère dangereux, [qui] font l'objet d'enquêtes administratives destinées à vérifier que le comportement des candidats n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées* ».

L'article 25 de la loi n° 2003-239 du 18 mars 2003 a étendu de manière significative les possibilités de consultation à des fins administratives, qui comprennent désormais les enquêtes relatives :

— aux affectations et agréments concernant les emplois publics participant à l'exercice des missions de souveraineté ;

— aux emplois publics ou privés relevant du domaine de la sécurité ou de la défense ;

— aux emplois privés ou activités privées réglementées relevant des domaines de jeux, paris et courses ;

— aux missions concernant des zones protégées en raison des activités qui s'y exercent, aux missions concernant les matériels, produits ou activités pour la sécurité publique ;

— à 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 ;

— aux nominations et à la promotion dans les ordres nationaux ⁽¹⁾.

L'article 25 de la loi de 2003 a expressément autorisé les consultations des fichiers d'antécédents judiciaires mentionnés par l'article 21 de cette même loi, c'est-à-dire le STIC et JUDEX, dans le cadre d'enquêtes administratives.

Le décret n° 2005-1124 du 6 septembre 2005 fixant la liste des enquêtes administratives donnant lieu à la consultation de ces fichiers détaille de manière très précise les forts nombreux cas pour lesquels de telles consultations peuvent être réalisées. Au total, selon la CNIL, **plus d'un million d'emplois sont concernés**.

⁽¹⁾ *L'article 25 prévoit par ailleurs que « La consultation des traitements automatisés de données personnelles mentionnés à l'article 21 de la loi n° 2003-239 du 18 mars 2003 précitée peut également être effectuée, y compris pour des données portant sur des procédures judiciaires en cours, pour l'exercice de missions ou d'interventions lorsque la nature de celles-ci ou les circonstances particulières dans lesquelles elles doivent se dérouler comportent des risques d'atteinte à l'ordre public ou à la sécurité des personnes et des biens, ainsi qu'au titre des mesures de protection ou de défense prises dans les secteurs de sécurité des installations prioritaires de défense visés à l'article 17 de l'ordonnance n° 59-147 du 7 janvier 1959 portant organisation générale de la défense. ».*

• Une bonne partie des cas exigeant des agréments administratifs est constituée par les **professions relevant du domaine de la sécurité privée**, comme les « *personnes physiques exerçant à titre individuel une activité privée de surveillance et de gardiennage, de transport de fonds, de protection physique des personnes ou une activité de recherches privées ou dirigeant ou gérant une personne morale exerçant cette activité* », ou comme les agents de sûreté exerçant dans les zones aéroportuaires pour assurer la fouille des bagages à main ou les palpations de sécurité (article L. 282-8 du code de l'aviation civile).

Conformément à l'article 6 de la loi n° 83-629 du 12 juillet 1983 réglementant les activités privées de sécurité, toute personne employée pour participer à une telle activité doit faire l'objet d'une enquête administrative destinée à vérifier si son comportement et ses agissements sont compatibles avec l'exercice de ces fonctions. Les représentants des entreprises de ce secteur ont indiqué à vos rapporteurs que dans ce cadre, lorsque la personne recrutée est inconnue dans le STIC ou dans JUDEX, la réponse favorable parvient dans un délai de deux à trois semaines. En revanche, si la personne est connue dans les fichiers, les démarches d'enquête administrative peuvent prendre plus d'un an. Les entreprises se seraient en quelque sorte adaptées à cette situation : d'une part, « *la profession contourne la loi en pratique. Tant que la préfecture ne dit pas non, on considère que l'on peut embaucher* » ; d'autre part, les préfectures ayant la réputation d'avoir une conception plus souple des enquêtes administratives auraient vu affluer les demandes des entreprises.

L'article 75 de la loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance a substantiellement modifié l'économie générale du dispositif : en effet, la demande d'habilitation ne relève plus désormais de l'employeur mais du salarié ou du candidat à un emploi dans le secteur de la sécurité. Celui-ci doit désormais détenir une carte professionnelle, qui est délivrée pour une durée de cinq ans lorsque les conditions de moralité précitées sont remplies et en cas de succès à une formation professionnelle qualifiante (l'accès à cette formation est lui-même soumis à autorisation administrative). Un fichier national des personnes détentrices de ce document est en cours de mise en place, et il permettra aux employeurs de vérifier que les candidats peuvent effectivement être embauchés. Cette modification législative était demandée depuis longtemps par les employeurs du secteur de la sécurité, mais elle n'emporte pas de changements significatifs pour les personnes devant faire l'objet d'un agrément, qui restent soumises à une enquête administrative dont les conclusions dépendent, en grande partie, des informations figurant dans les fichiers d'antécédents judiciaires.

2. Une exigence particulière de discernement

Comme a pu le relever un procureur de la République entendu par vos rapporteurs, compte tenu de l'impossibilité pour les parquets de faire modifier les données figurant dans les fichiers d'antécédents en dehors des cas très limitativement prévus par la loi, « *en fin de compte, c'est le préfet qui devient*

l'arbitre de l'importance des faits » au travers des décisions d'habilitation prises à la suite d'enquêtes administratives. La manière dont sont effectivement réalisées ces enquêtes et prises les décisions d'agrément revêt donc une importance considérable. Au demeurant, les différents acteurs entendus à ce sujet ont tous souligné combien ils avaient conscience des enjeux pour les personnes dont l'emploi dépend d'une réponse de l'administration.

• **Certaines pratiques antérieures en la matière ont parfois été l'objet de critiques justifiées.** Des décisions de refus d'agrément ont ainsi pu être prises sans plus de motivation qu'une simple référence au fait que la personne était mentionnée dans un fichier d'antécédent. Deux exemples de courriers de refus d'agrément figurant en annexe illustrent des insuffisances de ce type⁽¹⁾. Le premier, datant de décembre 2004, renvoie simplement à des faits, non décrits, et à des dates de commission pour confirmer un refus à la suite d'un recours gracieux. Le second, datant d'avril 2006, est encore plus laconique puisqu'il se borne à informer l'employeur ayant fait la demande d'agrément que le candidat *« ne remplit pas les conditions de moralité requises par l'article 6 de la loi réglementant les activités privées de sécurité »*.

Ce type de pratique est particulièrement inacceptable en raison des **risques graves** qu'elle fait peser **en matière d'exclusion du marché du travail**. Or, le nombre de cas où un refus est opposé par l'autorité administrative n'est pas marginal. L'un des syndicats professionnels des entreprises de sécurité a ainsi fait état d'une quarantaine de retraits d'autorisation administrative par an et d'environ 150 refus de délivrance d'une autorisation préalable d'exercer la profession, sur un total de 8 000 à 9 000 embauches annuelles. Encore faut-il préciser qu'il ne s'agit pas là de statistiques exhaustives, mais seulement des affaires portées à la connaissance de cet organisme par ses adhérents.

Le juge administratif a déjà annulé des décisions de refus d'agrément préfectoral au seul motif que la personne figurait au STIC⁽²⁾. L'article 10 de la loi du 6 janvier 1978 prévoit en effet qu'*« aucune autre 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. »* Dans sa décision du 13 mars 2003 sur la loi pour la sécurité intérieure (n° 2003-467 DC du 13 mars 2003) le Conseil constitutionnel a considéré que la consultation des fichiers d'antécédents judiciaires était possible parce que *« les données recueillies dans les fichiers ne constitueront [...], dans chaque cas, qu'un élément de la décision prise, sous le contrôle du juge, par l'autorité administrative. »*

À la suite du premier rapport du groupe de travail sur les fichiers de police, le ministère de l'Intérieur a publié une circulaire relative au contentieux

⁽¹⁾ Annexe 9.

⁽²⁾ Arrêt du tribunal administratif de Marseille du 14 juin 2006 (n° 0500162), cité par la CNIL dans son rapport sur le STIC du 20 janvier 2009.

des autorisations et des agréments préfectoraux ⁽¹⁾, rappelant que tout acte pris sur le seul motif de la consultation du STIC risque d'être annulé par le juge administratif et que les décisions individuelles prises en application de la loi du 12 juillet 1983 doivent être motivées.

Au demeurant, bien que vos rapporteurs aient pu prendre connaissance de certains courriers lapidaires de préfets n'ayant manifestement pas exercé leur pouvoir d'appréciation, le rapport précité de la CNIL donne une vision d'ensemble soulignant **que les situations où la motivation est défailante revêtent un caractère exceptionnel**, les services de police prenant très au sérieux leur **devoir d'information** du préfet.

• Également parue à la suite des propositions du rapport précité du groupe de contrôle sur les fichiers de police, la **circulaire du 9 mai 2007 relative aux modalités de mise en œuvre du STIC** ⁽²⁾ rappelle que « *les éléments d'information communiqués par les services de police aux autorités administratives dans le cadre d'une enquête ne doivent pas se limiter à la simple transmission des éléments de la fiche STIC. Ils doivent comprendre une analyse et une appréciation critique issue de la consultation.* » Aussi incombe-t-il aux services de « ***vérifier la pertinence des informations recueillies en fonction de la nature de l'enquête sollicitée. Il y a lieu de s'appuyer sur le ou les dossiers de procédure judiciaire, en s'attachant notamment à la réalité des faits imputés au requérant, à leur gravité, à leur répétition éventuelle et à l'âge du mis en cause au moment de leur commission.*** »

Lors de leurs déplacements auprès des services de police chargés de la réalisation de ces enquêtes, vos rapporteurs ont pu constater que **ces prescriptions étaient bien observées**. Selon les mots d'un policier d'un SDIG, « *nous ne faisons pas ce travail à la légère, car ce qui est en jeu c'est un emploi et parfois une vocation.* » L'usage fait des fichiers est donc très prudent, et en cas de doute « *on creuse* ». Par exemple, pour un candidat à un poste d'adjoint de sécurité qui figurait au STIC en tant qu'auteur de dégradations volontaires, il s'est avéré qu'il s'agissait de l'encollage de serrures d'un lycée dans le cadre du mouvement contre le CPE. Il a été décidé de ne pas en faire mention dans la note à l'attention du préfet, laquelle donnait simplement un avis favorable.

Il reste que l'habitude de certains préfets de demander des enquêtes administratives à deux services de police différents d'un même ressort territorial semble ne pas s'être complètement perdue. Outre le fait qu'il y a là une déperdition d'énergie, cette situation est peu satisfaisante si l'on considère que l'enquête administrative est un métier très particulier, qui nécessite expérience et savoir faire. Il serait de ce point de vue des plus utiles d'en confier l'exclusivité aux SDIG.

⁽¹⁾ INT/D/08/00032/C du 11 février 2008.

⁽²⁾ INT/C/07/00059/C.

De fait, le **principal problème** des enquêtes administratives ne semble pas résider dans le soin apporté à leur réalisation, mais dans **les délais**. Il convient de relever que bien qu'éminemment nécessaire, la demande adressée systématiquement au parquet s'agissant des suites judiciaires pour les personnes figurant dans les fichiers d'antécédents allonge sensiblement la procédure. En outre, c'est la capacité des services de police à **faire face à la croissance du flux des enquêtes administratives** qui est désormais en cause. Fortement sollicité en raison de la présence de la plate-forme aéroportuaire d'Orly, le SDIG du Val-de-Marne a ainsi reçu près de 400 demandes d'enquêtes administratives entre le 1^{er} juillet et le 15 novembre 2008. Or, la réforme du renseignement s'est traduite par une diminution sensible des effectifs des anciens renseignements généraux, ce qui risque de rendre difficile en pratique le respect de délais courts pour l'instruction des demandes.

Proposition n° 47

Dans les cas où une enquête administrative doit être réalisée par la police nationale, celle-ci doit être confiée seulement au service départemental d'information générale.

Pour éviter que ces retards aient des conséquences très graves pour des personnes répondant à une offre d'emploi, une systématisation du caractère contradictoire de la procédure devrait être envisagée. Certains services enquêteurs ont déjà pour habitude de convoquer le demandeur afin de mieux comprendre son cas. Dès qu'il apparaît qu'une personne faisant l'objet d'une enquête administrative figure comme mis en cause dans un fichier d'antécédents judiciaires, elle devrait pouvoir être **avertie systématiquement** par courrier **de la possibilité qui lui est offerte d'être entendue par les services enquêteurs afin d'exposer sa situation**. Une telle procédure permettrait aux services enquêteurs **d'identifier les demandes particulièrement urgentes** et pour lesquelles un avis favorable peut être émis sans difficulté. Cette **généralisation d'une « bonne pratique »** jouerait un utile rôle d'alerte et contribuerait à éviter qu'un emploi échappe à un candidat pour des raisons de retard administratif.

Proposition n° 48

Avertir systématiquement toute personne figurant comme mis en cause dans un fichier d'antécédents judiciaires et faisant l'objet d'une enquête administrative de la possibilité d'être entendue par les services chargés de cette enquête, pour exposer son cas et, éventuellement, l'urgence de sa situation en termes d'accès à l'emploi.

C. LES ENJEUX D'UNE ADAPTATION AUX BESOINS ET DE LA MISE EN PLACE D'UNE VÉRITABLE DÉMARCHE PROSPECTIVE

L'adaptation des fichiers de police aux besoins des enquêteurs est une condition nécessaire de l'efficacité des services de sécurité intérieure. Force est de constater que les **délais de développement** de nouveaux projets sont très longs, puisqu'il faut souvent de l'ordre de **sept ans entre la décision initiale et la mise en service effective**. De ce fait et compte tenu du rythme d'évolution des technologies, la « péremption » technique des outils est souvent très rapide. En outre, leur durée d'utilisation est fort longue sans que des étapes de modernisation progressives soient nécessairement prévues. Il en résulte dans certains cas une obsolescence préoccupante de traitements d'autant plus utiles qu'ils sont spécialisés.

En sens inverse, on assiste à la création de nouveaux outils prometteurs dans le domaine du rapprochement. Si l'utilisation de l'informatique pour effectuer des recoupements d'informations est déjà une réalité depuis un certain temps afin de lutter contre certains crimes à caractère sériel particulièrement graves, les possibilités offertes par l'application d'une telle politique à une délinquance plus commune n'ont été prises en considération que très récemment. L'enjeu est pourtant de taille. Selon un rapport réalisé en commun par les inspections générales de la police et de la gendarmerie nationales, l'effet déterminant de l'identification criminalistique est nettement plus important pour les faits de petite et de moyenne délinquance (81 %) que pour les faits de grande criminalité (30 %) ⁽¹⁾. L'une des pistes d'amélioration du taux d'élucidation en matière de délinquance réside donc dans une utilisation plus efficace des données disponibles, tout particulièrement celles issues des activités de police technique et scientifique (PTS). Plusieurs expérimentations sont en cours dans la police et dans la gendarmerie.

Cette floraison d'initiatives, souvent locales, souligne avec une certaine acuité les insuffisances de la démarche prospective d'ensemble en matière de fichiers de police.

1. Un fichier des brigades spécialisées « à bout de souffle »

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** (terrorisme, stupéfiants, proxénétisme et grande délinquance financière). Il a par la suite fait l'objet d'une extension et est désormais utilisé par les offices centraux de police judiciaire ou de la direction centrale de la police aux frontières, les brigades centrales de la préfecture de police de Paris et les directions interrégionales de police judiciaire.

⁽¹⁾ *Rapport général de la mission d'audit sur le fonctionnement et les performances de la police technique et scientifique dans la lutte contre la délinquance de masse et la criminalité organisée, du contrôleur général Charles Diaz et du colonel Michel Venel, décembre 2007.*

Ce fichier répond à **deux vocations** :

— un **fichier d'objectifs**, visant à coordonner l'action des services concernés, très utile en termes d'information mutuelle des services de police sur les « cibles » et pour éviter des doublons en matière d'enquêtes, voire des interférences ;

— un **fichier de travail**, dans lequel est recensée et regroupée l'information relative à la criminalité organisée. Le FBS s'apparente sur ce point à un fichier de renseignement, alimenté par les informations collectées à l'occasion de la surveillance du milieu criminel, et son utilisation est très cloisonnée.

Créé en 1991, le FBS est « *arrivé en bout de course* » et **risque d'être frappé rapidement d'obsolescence technique**. Comme le relève le rapport du groupe de travail sur les fichiers de police paru en décembre 2008, le maintien en condition opérationnelle de ce traitement est désormais menacé pour plusieurs raisons : incompatibilité avec Internet Explorer 7, difficulté à faire évoluer les bases conformément à la réforme de la DCPJ et absence de personnels à la DSIC capables d'intervenir sur des langages informatiques devenus obsolètes.

Or, dans le premier rapport de ce groupe, paru en novembre 2006, il avait déjà été indiqué que ce fichier faisait l'objet d'une réflexion relative à sa modernisation. Celle-ci ne semble pas avoir progressé, alors qu'il s'agit d'un **outil particulièrement utile** permettant d'éviter que divers services travaillent sans le savoir simultanément sur la même affaire. Le FBS pourrait être utilisé, à terme, comme instrument permettant d'alimenter Europol en informations.

Proposition n° 49

Moderniser de toute urgence le fichier des brigades spécialisées, cet outil des plus utiles en étant malheureusement arrivé au point où son fonctionnement même est désormais compromis.

2. Les expérimentations en cours dans le domaine du rapprochement : « les fichiers c'est utile... quand on sait ce que l'on cherche ! »

a) LUPIN et CORAIL : les nouveaux outils de la police pour lutter contre la délinquance sérieuse

• Le projet de traitement automatisé **CORAIL (cellule opérationnelle de rapprochements et d'analyse des infractions)** a été lancé en 2005 et est entré en phase d'expérimentation en 2006 au sein de l'état-major de la direction de la police judiciaire de la préfecture de police de Paris.

Il s'agit d'un outil destiné à répondre à plusieurs besoins :

— rapprocher les faits entre eux à l'échelle régionale pour permettre l'élaboration de synthèses sur des affaires susceptibles d'être commises par des récidivistes notoires ayant commis des infractions graves au sens de l'article 21-1 de la loi du 18 mars 2003 (crimes ou délits portant atteinte aux personnes punis de plus de cinq ans d'emprisonnement ou portant atteinte aux biens et punis de plus de sept ans d'emprisonnement) ;

— moderniser le système de traitement et d'exploitation des télégrammes d'information, diffusés par le biais de la messagerie de commandement (RESCOM) ;

— mettre au point un outil ayant un objectif plus global de gestion de l'information ;

— diffuser l'information retraitée aux enquêteurs en fonction de leur niveau d'habilitation et de leurs besoins ⁽¹⁾.

CORAIL est alimenté par les télégrammes « 10 points » ou « 11 points » (pour les affaires élucidées) en provenance de Paris, des trois départements de la petite couronne et de celui des Yvelines. S'il apparaît que plusieurs faits sont susceptibles de présenter un intérêt pour établir par la suite un rapprochement avec d'autres affaires, une **fiche affaire** est créée, à laquelle seront ensuite ajoutés éventuellement les télégrammes qui lui semblent liés, ainsi que des éléments utiles à l'enquêteur (photographies de suspects issues de la vidéosurveillance, système de géo localisation des faits, dépêches de presse, éventuellement mention des prélèvements effectués par la PTS sur les scènes d'infraction, etc.). Le dossier affaire fournit donc une information structurée (*« c'est une révolution : en ouvrant leur ordinateur, nos enquêteurs ont accès à une information régionale retravaillée »*). Le tri est réalisé par les personnels de la cellule CORAIL, qui ont été choisis en raison de leur grande expérience en matière d'enquêtes judiciaires.

Les rapprochements entre affaires ne sont pas réalisés par le système informatique, et rarement par les personnels de la cellule CORAIL : ce sont le plus souvent **les enquêteurs eux-mêmes qui les signalent**, au vu des informations ordonnées qui leur sont transmises. L'enquêteur peut consulter CORAIL en fonction de sa spécialité (vols à main armée, vols astucieux, infractions sexuelles, etc.) ; de plus, en s'abonnant, il peut recevoir en temps réel sur son poste de travail les informations susceptibles de le concerner et diffusées par le système. Quand un rapprochement est effectué, il fait l'objet d'une **synthèse établie par la cellule**

(¹) Le travail sur la mise au point de la deuxième version de CORAIL est en passe de s'achever ; celle-ci permettra d'étendre l'utilisation de l'outil, actuellement réservée à environ 250 destinataires, à près de 2 000 fonctionnaires de la PJ ainsi qu'à des enquêteurs de la PUP. La décision de principe d'étendre le système sur l'ensemble du territoire au sein de chaque SRPJ a été prise, mais il reste à adapter un certain nombre de points techniques.

CORAIL ; celle-ci récapitule sous un nom de dossier évocateur ⁽¹⁾, les modes opératoires, le signalement du ou des auteurs, le service saisi, la liste des faits, leur localisation géographique, etc.

CORAIL remplace utilement le tri des masses de télégrammes sous forme papier, pour le moins encombrant. De surcroît, alors que ces documents étaient précédemment conservés très longtemps, la durée de conservation proposée pour CORAIL est de trois ans. De fait, la masse de données conservées a pu être diminuée par un facteur de l'ordre de 50, tandis que l'amélioration de l'efficacité a permis de réduire les effectifs de la cellule de tri des télégrammes. En 2008, 4 500 fiches ont été créées dans CORAIL. Depuis que le traitement existe, le nombre de synthèses réalisées par la cellule a été doublé. **L'impact sur le taux d'élucidation est significatif**, puisqu'à Paris il s'élève à 30 % dans le cas d'un fait individuel, mais atteint 40 % si un rapprochement a pu être effectué.

Trois points méritent également d'être soulignés.

Tout d'abord, l'existence d'un fichier centralisé apporte **davantage de garanties**. Faute d'un outil de ce type, il est de fait difficile d'empêcher les enquêteurs de créer leurs propres traitements de rapprochement pour les affaires qui les intéressent en utilisant des outils informatiques courants, sans contrôle sur la nature des données collectées ou sur leur durée de conservation. Selon un policier entendu à ce sujet, « *CORAIL signe l'arrêt de mort du tableau Excel* ».

Ensuite, la création de cet outil, directement réalisé au sein des services, **correspond très exactement aux besoins exprimés par les enquêteurs**. La conception du traitement a beaucoup évolué en cours de route car il était de fait impossible de spécifier au départ l'ensemble de ses caractéristiques ; de ce fait, le recours à un prestataire extérieur n'aurait sans doute pas pu donner un résultat de cette qualité.

Enfin, **l'homme reste au cœur du système**, à la fois pour le choix des informations à intégrer et pour la réalisation de rapprochements. CORAIL n'est pas capable de procéder à la recherche automatisée de liens entre des infractions, notamment parce que les champs ne sont pas renseignés de façon normée. Le système a été conçu en limitant volontairement les fonctions d'automatisation des recherches car, en allant au-delà, « *on se noierait* » dans le « bruit » généré dans le nombre de recoupements à trier.

• S'agissant du **logiciel d'uniformisation des procédures d'identification (LUPIN)**, très différent de CORAIL, ses concepteurs ont déclaré : « *nous sommes partis des besoins des collègues chargés des cambriolages* ».

(¹) La créativité du langage policier demeure vivace, comme en témoignent quelques exemples d'intitulés d'affaires : « *Les Bonnie and Clyde itinérants* », « *Les cardiaco dépressives* », « *L'élégant des grosses coupures* », ou « *L'escroc des cabines, le retour* ».

Mis en œuvre au sein du service d'investigation transversale de la direction de la police urbaine de proximité de la préfecture de police de Paris, ce traitement a pour objectif **l'utilisation des traces et informations relevées par la police technique et scientifique** en vue d'effectuer des **rapprochements entre affaires** ⁽¹⁾. Il s'agit de mieux combattre **certaines formes de délinquance**, essentiellement les **cambriolages** , et dans une moindre mesure les **vols par ruse sur la voie publique** et certains vols avec violences. Les antennes locales de police technique (ALPT) se déplacent et effectuent désormais des prélèvements pour environ 95 % des cambriolages constatés dans Paris *intra muros* (lesquels représentent près de 11 000 affaires en 2008). On notera qu'à l'échelle nationale ce taux est sensiblement moindre, puisqu'il s'établit à 61 % des cambriolages. Les indices relevés sont les traces papillaires ou les empreintes palmaires, mais aussi les traces biologiques. Sur l'ensemble des cambriolages traités par la PTS en 2008, 600 traces papillaires ou empreintes palmaires exploitables ont pu être relevées. En outre, le travail des personnels de la PTS a été élargi à la réalisation d'un **descriptif très détaillé du mode opératoire**. L'ensemble de ces données est saisi informatiquement dès le retour du fonctionnaire et alimente la base de données LUPIN en temps réel. La fiche d'intervention comprend des données relatives à l'infraction (grille de l'état 4001), au mode opératoire, à la victime (nom et prénom sont obligatoirement renseignés ; le reste est optionnel : adresse et éventuellement d'autres données, telles que l'âge, qui peut permettre d'identifier des délinquants ne s'en prenant qu'aux personnes âgées), au véhicule (cas des vols à la roulotte) et aux traces prélevées. Au 21 janvier 2009, 2 181 fiches d'intervention ont été réalisées par les ALPT, dont 43 % pour des vols avec effraction, 14 % pour des vols à la roulotte, 9 % pour des vols par escalade et 7 % pour des dégradations volontaires de véhicules.

Après découverte des traces sur les lieux de l'infraction, les empreintes digitales sont envoyées à l'identité judiciaire qui, en retour, communique l'identité du mis en cause en cas d'identification positive. S'agissant des limites actuelles du système, il faut relever que le FAED ne réalise pour l'instant pas de rapprochements de trace à trace. L'entrée en service de MetaMorpho devrait sur ce plan augmenter significativement l'efficacité du système. Par ailleurs, LUPIN ne permet pas encore d'utiliser pleinement les potentialités offertes par les prélèvements de traces biologiques en raison des retards de traitement par le FNAEG : les faits de petite délinquance ne sont pas prioritaires et les réponses ne reviennent pas assez rapidement compte tenu de délais d'analyse de près de dix-huit mois. Il reste que **l'outil ainsi bâti permet d'anticiper sur l'arrivée à maturité du FNAEG**.

LUPIN permet de **mieux prendre en compte la sérialité par le biais des modes opératoires**, souvent très répétitifs en matière de cambriolages, et de faire

(1) Un logiciel comparable de conception locale a été créé au sein d'un groupe « cambriolage » de la sûreté départementale des Bouches-du-Rhône. Baptisé SORPAC (synthèse opérationnelle pour une réponse adaptée à la criminalité), il permet de faire des rapprochements entre affaires, à partir du type d'infraction, du lieu de commission, du mode opératoire, des catégories de victimes, etc. Il permet également l'exploitation des traces relevées par la PTS sur les lieux d'infraction.

le lien entre plusieurs faits commis et un même auteur, ce qui n'est pas sans incidence sur la sanction pénale. Selon les responsables du projet, « *sans l'outil informatique, il est impossible de faire ce type de rapprochements.* » La PTS et l'outil informatique sont ainsi mis au service d'une culture de la preuve. LUPIN permet en effet une fois une identification réalisée, de **retrouver d'autres infractions anciennes commises par un même individu**, en effectuant une recherche par les modes opératoires et en reprenant à ce moment-là les relevés de traces précédents. Il permet également **d'identifier des séries cohérentes de faits** réalisés par un délinquant ou un groupe de délinquants identiques, par exemple des cambriolages commis sur un type précis de commerce avec un mode opératoire particulier et pour lesquels les comparaisons de trace à trace permettent de déterminer une unité d'auteur. Il constitue ainsi également un outil d'orientation des enquêtes. L'apport que représente un tel outil doit être mis en rapport avec le taux d'élucidation des cambriolages, particulièrement bas : malgré des efforts louables ayant permis son doublement depuis 2002, il reste de seulement 8 %.

EXEMPLE D'UNE AFFAIRE RÉSOLUE GRÂCE À LUPIN

Le 11 décembre 2008, les policiers de permanence de l'antenne de police technique de nuit se sont rendus rue Monceau à Paris 8^e, pour un vol commis par effraction.

Les auteurs se sont introduits dans les lieux en forçant la porte d'entrée au moyen d'un tournevis. À l'intérieur, ils ont dérobé divers objets. Les recherches techniques effectuées sur place ont permis de relever une trace papillaire exploitable sur la porte d'entrée. Les premières recherches entreprises, au début de décembre 2008, auprès du fichier automatisé des empreintes digitales (FAED) se sont avérées infructueuses.

Informé de cette affaire, un enquêteur de l'unité de police technique a constaté début janvier 2009 que le mode opératoire employé correspondait à celui utilisé par les auteurs d'un vol commis par effraction en décembre 2008. Lors de cette affaire, les empreintes digitales des nommés J, née en mai 1991 et S, né le 25 janvier 1994 (alias D né le 25 janvier 1993), avaient été identifiées. En conséquence, il a réalisé des comparaisons entre la trace et les empreintes digitales de J et de S. Elles ont permis d'identifier l'annulaire droit de la nommée J.

Par ailleurs, l'enquêteur a soupçonné les nommés J et S d'avoir réalisé neuf vols commis avec effraction entre le 5 décembre 2008 et le 2 janvier 2009. Le même mode opératoire avait été utilisé dans tous ces cas. En conséquence, il a comparé leurs empreintes digitales avec les traces papillaires relevées dans chacun des neuf cas précités. Ces comparaisons ont permis de nouveau d'identifier les doigts des mains droite et gauche des deux intéressés.

b) Les ambitions de la gendarmerie nationale

La gendarmerie nationale est également consciente du besoin d'un renforcement du rapprochement judiciaire, afin, d'une part, de lutter contre la logique de « niche » des investigations, qui se traduit par une mauvaise circulation transversale de l'information, et, d'autre part, d'améliorer la prise en compte du caractère sériel de certaines formes de délinquance.

Pour mettre en exergue ce caractère et accroître le taux d'élucidation, un traitement est actuellement en cours de développement. Il vise à **automatiser et à optimiser l'utilisation de l'information**. Baptisé « **application judiciaire dédiée à la révélation des crimes et délits sériels** » (AJDRCDs, parfois aussi désigné sous le nom de **Périclès**), ce projet est ambitieux. Il s'agit de la mise en place d'un **logiciel d'intelligence artificielle, et non d'une nouvelle base de données permanente**, alimenté par les pièces de procédure, les fichiers d'antécédents judiciaires, les sources ouvertes au public et les données figurant dans des systèmes d'informations détenus par d'autres administrations ou par des opérateurs privés de téléphonie (dans ces derniers cas, les informations ne pourront être obtenues que sur réquisition judiciaire). L'ensemble vise à obtenir des recoupements automatisés et temporaires de l'information. Ce type de recoupements est actuellement réalisé de façon manuelle et intuitive par les enquêteurs, notamment au sein de la division du rapprochement et investigations judiciaires du STRJD. En opérant des **rapprochements fondés sur des liens objectifs**, ce logiciel permettrait ainsi de mettre en exergue le caractère sériel de certaines infractions, d'élucider un plus grand nombre d'enquêtes, d'avoir une approche managériale de l'enquête (c'est-à-dire des réquisitions moins nombreuses et mieux ciblées) ainsi qu'une meilleure adaptation de la réponse pénale. Il fera l'objet d'un accès restreint, réservé à seulement 1 500 personnes habilitées.

Les projets des deux forces de sécurité intérieure en matière de logiciels de rapprochement reposent donc sur des **philosophies très différentes : exploitation ciblée** des sources d'information typiquement policières, avec une réalisation des **rapprochements reposant avant tout sur le travail de l'enquêteur** s'agissant de la police nationale ; confiance dans les perspectives ouvertes par **l'utilisation des moteurs de recherche appliquée au traitement d'une grande masse d'informations** afin de détecter automatiquement les phénomènes sériels pour la gendarmerie. Quoi qu'il en soit, les deux démarches de développement de fichiers de rapprochements en matière délictuelle sont également révélatrices d'une difficulté sérieuse : le cadre juridique actuel ne leur permet d'être déclarés à la CNIL. De manière plus générale, ces initiatives diverses révèlent un défaut d'anticipation des besoins techniques et financiers en matière de fichiers de police.

c) Un cadre législatif inadapté à l'utilisation accrue des fichiers de rapprochement

L'article 21-1 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure dispose qu'« *afin de faciliter la **constatation des crimes et délits présentant un caractère sériel**, d'en rassembler les preuves et d'en identifier les auteurs, grâce à l'établissement de liens entre les individus, les événements ou les infractions pouvant en mettre en évidence ce caractère sériel* », la police et la gendarmerie nationale peuvent mettre en œuvre des traitements automatisés de données à caractère personnel « *pour tout crime ou délit portant **atteinte aux personnes puni de plus de cinq ans d'emprisonnement ou portant atteinte aux biens et puni de plus de sept ans d'emprisonnement*** ».

Ces traitements peuvent contenir des données sur les personnes, sans limitation d'âge, contre lesquelles existent des indices graves ou concordants rendant vraisemblable qu'elles aient pu commettre une infraction de ce type, mais aussi celles à l'encontre desquelles existent seulement des « *raisons sérieuses de soupçonner qu'elles ont commis ou tenté de commettre* » une telle infraction. Peuvent également y figurer les victimes ainsi que les témoins. L'accès à ce type de fichiers fait l'objet d'une habilitation spéciale. La présence des témoins s'explique par le caractère très particulier des crimes en série. De fait, l'article 21-1 fournit un cadre juridique à des applications très spécialisées de lutte contre la criminalité sérielle, comme SALVAC pour la police (système d'analyse et de liens de la violence associée au crime) et ANACRIM pour la gendarmerie.

En revanche, **compte tenu des seuils de peines, les nouveaux logiciels** visant à améliorer le taux d'élucidation en matière de délinquance sérielle « courante » ne **correspondent pas aux critères fixés par la loi de 2003**. Ainsi, LUPIN traite exclusivement des faits de la petite et moyenne délinquance, réprimés par des peines d'emprisonnement médianes de trois ans et ne conjuguant que rarement deux circonstances aggravantes portant les peines encourues à sept ans d'emprisonnement.

En raison d'évidentes différences de gravité des faits, les garanties en termes de durée de conservation des données et de limitation de l'accès à un nombre très réduit d'agents prévues par l'article 21-1 ne peuvent pas être équivalentes pour les fichiers de rapprochement destinés à lutter contre la délinquance sérielle plus courante. En outre, la présence de témoins dans ces derniers est inutile. L'adaptation du cadre juridique ne passe donc pas par un simple abaissement des seuils de peines prévus par la loi précitée du 18 mars 2003. Il s'agit plutôt de **définir un cadre législatif particulier pour les nouvelles applications en matière délictuelle**, qui puisse tenir compte de la façon la plus appropriée de leurs spécificités, tout en préservant celles des fichiers destinés à la criminalité sérielle.

Proposition n° 50

Définir un cadre législatif approprié pour la mise en œuvre de traitements automatisés de données permettant des rapprochements destinés à la lutte contre la petite et moyenne délinquance sérielle.

3. Pour une véritable démarche prospective

• **L'empirisme actuel** présidant à la création de nouvelles applications n'est pas dépourvu d'avantages.

Tout d'abord, les systèmes précités récemment développés au sein des services de la préfecture de police de Paris sont caractérisés par une **prise en considération très étroite des besoins formulés par les enquêteurs eux-mêmes**.

Leurs spécifications se sont affinées en cours de développement, illustrant l'aspect très particulier des fichiers de police, pour lesquels aucun logiciel n'existe « sur étagère » sur le marché.

Ensuite, le développement de ces applications nouvelles souligne **l'ampleur des talents informatiques dont dispose la police**. LUPIN a ainsi été développé par un jeune gardien de la paix, en collaboration étroite avec les services de l'unité informatique et bureautique, de fin août à novembre 2008, et il a été mis en service le 1^{er} décembre de la même année, ce qui représente un temps très court au regard de la complexité de l'opération. Ce système n'a donc rien coûté au contribuable en dehors de la rémunération de ce fonctionnaire, qui a réalisé un travail très complet d'analyse des besoins des utilisateurs afin de livrer un système aussi efficace que possible. Il a été estimé que le même travail confié à une société de services informatiques aurait coûté de l'ordre de 400 000 euros. Ce cas n'est pas isolé : CORAIL a été réalisé selon un schéma sensiblement identique. Lors d'un déplacement auprès de la direction départementale de la sûreté publique du Val-de-Marne, vos rapporteurs ont également pu constater que la main courante informatisée utilisée par son centre d'information et de commandement avait été développée directement au sein des services en 2002. Un projet dit PEGASE est en cours pour uniformiser les applications utilisées en la matière par l'ensemble des DDSP, et il est directement inspiré du système mis en place dans le Val-de-Marne (une trentaine de sites doivent en être équipés cette année). De ce point de vue, vos rapporteurs ont du mal à comprendre pourquoi l'administration n'a pas fait le choix de généraliser tout simplement l'application conçue dans le Val-de-Marne, et ce gratuitement.

Une connaissance aussi précise que possible et **l'évaluation à l'échelle nationale des différentes initiatives locales** sont nécessaires à plus d'un titre. D'une part, il s'agit de détecter certains doublons éventuels ; d'autre part, il convient de valoriser ces réalisations en les généralisant lorsque cela est possible, en **évitant ainsi de lancer des appels d'offres à des prestataires de services extérieurs** dans les cas où un équivalent « maison » existe déjà.

• Plus largement, un certain nombre de problèmes rencontrés dans le développement de projets résulte du fait que la plupart des sociétés de services en ingénierie informatique subit un fort *turn over* des équipes, davantage au niveau des techniciens que des concepteurs de systèmes. Pour y faire face, il convient de **« recapitaliser en interne » une partie des connaissances techniques**, tout particulièrement s'agissant de la partie développement et intégration des systèmes, même si l'État n'a bien entendu plus vocation à **« héberger des arsenaux »**.

Par ailleurs, tous les bénéfices de la loi organique relative aux lois de finances (LOLF) n'ont, semble-t-il pas, été tirés en matière d'organisation interne du ministère de l'Intérieur et de circuits de prise de décision. Persiste un empilement de strates administratives intervenant à des degrés divers dans la définition des spécifications, sans qu'elles aient pour autant une compétence technique ou un regard d'utilisateur opérationnel. Selon les mots d'un responsable

des questions techniques, « *On occupe beaucoup de gens à faire du management administratif, sans avoir pour autant la compétence technique.* » À cette dispersion des responsabilités techniques s'ajoute le fait que les questions de gestion financière et de passation de marchés sont séparées des équipes de définition technique des programmes. Une unification de la gestion technique et de celle du marché pour un projet donné serait plus efficace.

Pour tirer les leçons du dossier ARIANE et mieux conduire les prochains projets de traitements communs à la police et à la gendarmerie, il serait utile de mettre en place une équipe légère intégrée associant ces deux forces, avec un seul chef, chargée de suivre l'ensemble du projet de la phase préparatoire à la mise en service. Un comité de pilotage rendant compte aux directions utilisatrices permettrait de prendre en compte l'ensemble des besoins exprimés et de gérer un seul contrat, avec une seule interface administrative avec l'industriel.

Proposition n° 51

Pour le développement de chaque nouveau fichier commun à la police et à la gendarmerie, créer une équipe intégrée associant les deux forces, avec un seul chef de projet assisté d'un comité où sont représentées toutes les directions intéressées, pour assurer le pilotage juridique, technique et financier du projet.

• Les **travaux d'anticipation** des besoins restent **encore très largement séparés entre la police et la gendarmerie.**

S'agissant de la prospective technologique à long terme, il n'existe pas de démarche intégrée associant formellement les travaux du service des technologies de la sécurité intérieure et ceux menés par l'Institut de recherches criminelles de la gendarmerie nationale.

En ce qui concerne les besoins à plus court terme pour ainsi dire logistiques, une réflexion est en cours dans le cadre du rapprochement entre police et gendarmerie afin d'améliorer la complémentarité entre les sites de Lognes et du fort de Rosny-sous-Bois, qui hébergent les serveurs de la police et de la gendarmerie. Se pose également la question d'une plus grande concentration des moyens à terme, notamment par le biais de l'acquisition de salles abritant des serveurs plus performants et mieux adaptées aux besoins. De ce point de vue, même si les contacts entre équipes de la police et de la gendarmerie sont de bonne qualité, selon les mots de responsables de la police entendus sur cette question « ***nous en sommes encore à faire connaissance*** ». Les réflexions sur les conséquences techniques et en termes d'organisation du rapprochement entre la police et la gendarmerie devraient s'étendre de 2009 à 2011. Elles devront notamment prendre en compte le fait que les relations entre la DSIC et la police nationale sont des rapports entre maître d'ouvrage et maître d'œuvre, alors qu'au sein de la gendarmerie l'organisation est plus « monolithique ».

L'accélération de ce processus paraît nécessaire au vu de l'ampleur des besoins en matière de modernisation de fichiers existants ou de développement de nouveaux systèmes. Il convient en effet de mettre en place une démarche de sélection des projets et des solutions aussi rationnelle que possible. Sur ce point, plusieurs responsables techniques ont relevé que, dans le cas d'ARIANE, une architecture commune centralisée aurait été techniquement préférable dans l'idéal au choix de créer deux bases séparées reliées par des passerelles. Cette dernière décision s'explique certes par une différence traditionnelle d'approche entre la gendarmerie nationale, très centralisée, et la police nationale, où l'organisation régionalisée a permis le développement de « *cultures de proximité* ». Il reste qu'à l'avenir les bénéfices du rapprochement entre les deux forces de sécurité intérieure ne pourront être véritablement tirés en matière d'investissements communs que si les choix techniques les plus rationnels sont retenus, et ce d'autant plus que le coût de réalisation et d'entretien des traitements automatisés est appelé à croître.

• À cet égard, vos rapporteurs ont souhaité disposer d'informations plus précises sur **l'évolution récente et les perspectives en matière de coût d'ensemble des fichiers** de police.

Les tendances récentes indiquent une **croissance très soutenue des crédits consommés** au titre des fichiers au sein de la mission Sécurité. S'agissant du programme police nationale, ils sont passés de 2,05 millions d'euros en 2003 à 10,76 millions d'euros en 2008, soit un **quintuplement** ⁽¹⁾. Pour 2009, ce sont 16,1 millions d'euros qui ont été prévus en loi de finances initiale, soit une croissance de 58,5 % par rapport à l'exécution 2008. Pour l'essentiel, cette progression d'ensemble s'explique par le coût croissant du FNAEG, les crédits consommés au titre de ce fichier étant passés de 1,8 million d'euros en 2003 à 7,6 millions d'euros en 2008, soit une croissance de 314 %. En 2009, le coût de ce fichier devrait représenter 13,9 millions d'euros en crédits de paiements. Quant à ARIANE, il s'agit d'un programme d'investissement important, puisque son coût d'ensemble s'élève à 15 millions d'euros. La police nationale a déjà consommé à ce titre près de 6,5 millions d'euros de crédits de paiement de 2007 à 2008, tandis que 2,2 millions d'euros sont prévus en 2009.

L'effet budgétaire de l'accroissement du nombre de personnes figurant dans le FNAEG est ainsi palpable. Au demeurant, **ce phénomène n'est pas prêt de ralentir** en raison de la volonté de procéder systématiquement à des analyses de traces sur des lieux d'infraction dans le cadre de la **politique de généralisation de l'utilisation de la PTS**. Même s'il est prévu de définir des protocoles très précis de relevé de traces ⁽²⁾, tant pour limiter les coûts que pour maximiser la probabilité de recueillir les éléments les plus utiles, pour faire face à la croissance

⁽¹⁾ Les éléments de réponse fournis à vos rapporteurs par le ministère de l'Intérieur figurent en annexe 10.

⁽²⁾ Il est prévu normalement trois prélèvements pour la petite délinquance ; la localisation des relevés peut être facile dans certains cas (vol de voiture, par exemple) mais fait appel à plus de réflexion dans d'autres (cambriolages).

considérable des flux, il faudra utiliser largement les capacités du secteur privé en matière d'analyse ⁽¹⁾.

Aussi est-il regrettable que les questions de vos rapporteurs relatives aux prévisions d'investissements à moyen terme n'ont, quant à elles, pas reçu de réponses. Dans le passé, **la mise en place et l'extension des finalités de fichiers s'est réalisée sans vision précise des coûts induits**, ce qui a conduit à des dysfonctionnements durables, le cas du FNAEG en constituant l'exemple le plus criant. Les conséquences de ce défaut d'anticipation se sont également manifestées de manière très prosaïque par des **problèmes d'alimentation électrique** constatés sur le site de Lognes. Désormais résolu par un doublement de la puissance des onduleurs, ils résultaient d'une **croissance de près de 40 % du nombre de serveurs en service sur une période de seulement deux ans**. Comme l'a relevé un responsable technique interrogé sur le sujet, « *on peut considérer que nous avons visé un peu bas* », même s'il faut aussi noter que les outils ont été conçus il y a une dizaine d'années, à un moment où l'utilisation de l'informatique n'avait pas du tout la même ampleur.

Les traitements informatisés sont un outil de travail quotidien et irremplaçable pour la police et la gendarmerie ; ils constituent de fait l'un des grands programmes d'investissement en matière de sécurité intérieure, non seulement en raison des coûts d'acquisition et de fonctionnement des matériels, mais aussi de la nécessité de disposer des ressources humaines nécessaires pour les exploiter et les faire évoluer dans de bonnes conditions. **L'« intendance suivra » ne peut plus être le mot d'ordre des politiques publiques dans ce domaine.**

Il n'est plus concevable de vouloir développer des fichiers adaptés aux véritables besoins, efficaces et bien contrôlés en feignant d'ignorer le coût certain, et qui ira croissant, de telles décisions. Aussi des évaluations financières sincères et complètes doivent-elles être présentées au Parlement, et à travers lui, plus largement, aux citoyens.

Proposition n° 52

Associer la police et la gendarmerie dans le cadre d'une véritable démarche intégrée de prospective technique et financière s'agissant des besoins futurs en matière de fichiers.

⁽¹⁾ Des améliorations techniques faciliteront toutefois l'absorption de ce surcroît d'activité, notamment grâce à l'utilisation d'écouvillons dotés d'un code-barres (à l'image de ce qui a été réalisé pour les kits de prélèvement FTA), alors que jusqu'ici les supports de prélèvement n'étaient pas normés. Il s'agit d'un nouveau produit destiné à répondre aux besoins du premier niveau d'intervention de police scientifique sur une scène d'infraction. Le marché, commun à la police et à la gendarmerie a été déclaré infructueux une première fois, aucun industriel français ne semblant malheureusement intéressé. Il faudra très probablement recourir aux services d'une société américaine, sans pouvoir faire jouer la concurrence.

D. AMÉLIORER L'ENCADREMENT DES TRANSFERTS INTERNATIONAUX DE DONNÉES

Les données figurant dans les différents fichiers de police nationaux sont devenues **un enjeu essentiel de la coopération policière et judiciaire internationale**, et singulièrement au sein de l'Union européenne. Les bases de données des différents États membres ont connu un fort développement, lié aux progrès de l'informatique, et constituent un **outil efficace de lutte contre une criminalité organisée de plus en plus transnationale**. Pourtant, les instruments juridiques permettant d'organiser les échanges en la matière sont demeurés très longtemps embryonnaires, et les textes les plus récents n'apportent pas encore de solutions à la hauteur des enjeux. Les suites des attentats du 11 septembre 2001 ont en effet placé l'échange d'informations au centre des préoccupations. Or, si nul ne conteste les nécessités d'un partage des renseignements pour lutter contre la menace terroriste, il convient pour autant de ne pas perdre de vue les nécessités d'une protection adaptée des données personnelles, afin de ne pas se retrouver dans une situation où l'on donne trop d'informations à des partenaires n'ayant pas le même niveau de protection des données⁽¹⁾. Cette question sous-tend d'ailleurs nombre de débats sur la protection des données à l'échelle européenne.

1. Une première étape minimale d'harmonisation dans le cadre du troisième pilier de l'Union

• Ainsi que cela a été rappelé dans la première partie du présent rapport, de manière générale, les règles applicables en matière de protection des données personnelles dans le cadre de l'Union européenne ne renvoient pas aux mêmes textes selon que l'on se trouve dans le cadre du premier pilier « communautés européennes » ou dans celui du troisième pilier « coopération policière et justice pénale ». Dans le premier cas, les règles applicables au contenu des fichiers, à leur contrôle, aux droits des personnes fichées et au transfert de données personnelles vers de pays tiers ont été fixées par la directive du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données⁽²⁾.

S'agissant des bases de données relevant du troisième pilier, et donc pour l'ensemble des fichiers de police, le seul encadrement juridique à l'échelle européenne était jusqu'à présent constitué par la convention STE 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, texte très général et succinct. Les dispositions européennes relatives aux fichiers de police et aux échanges d'informations sont donc restées pendant longtemps très limitées, ces questions relevant très largement de la souveraineté des États. Cette situation est apparue de plus en plus inadaptée et le programme de La Haye visant à renforcer

⁽¹⁾ On se reportera sur ce point aux analyses figurant dans le rapport d'information de M. Guy Geoffroy (n° 1447) s'agissant de l'« accord » conclu entre l'Union européenne et les États-Unis en juillet 2007 en matière de transfert de données des dossiers passagers dites PNR.

⁽²⁾ Directive 95/46/CE du Parlement et du Conseil, JOCE n° L 281, 23 novembre 1995.

la liberté, la justice et la sécurité dans l'Union européenne, adopté par le Conseil européen le 4 novembre 2004, a souligné la nécessité d'une approche innovante en matière de l'échange transfrontière d'informations en matière répressive. Dès lors, l'adoption d'un véritable cadre commun dans le cadre du troisième pilier devenait une condition préalable à la mise en œuvre du principe de disponibilité des informations. Tel est l'objet de la décision-cadre du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale ⁽¹⁾.

• Les ministres de la justice se sont mis d'accord à l'unanimité sur un **projet de décision-cadre relative à la protection des données personnelles** le 8 novembre 2007, après un débat qui a duré plus de deux ans. Ce texte représente un compromis, afin de disposer d'une première réglementation commune dont l'application puisse être contrôlée de façon bien plus efficace que dans le cadre du Conseil de l'Europe.

Il a fait l'objet de **nombreuses critiques**, tant de la part du Contrôleur européen à la protection des données (CEPD) que de la rapporteure du texte au sein de la commission des libertés civiles, de la justice et des affaires intérieures du Parlement européen, Mme Martine Roure. La CNIL a également publié un communiqué relevant un certain nombre d'insuffisances du texte ⁽²⁾. Le CEPD a publié trois avis sur ce projet de décision-cadre à différents stades de sa discussion. Dans celui du 23 juin 2007 (C 139/01), il a relevé que s'« *il est difficile de recueillir l'unanimité au Conseil [cela] ne saurait justifier une approche favorisant le plus petit dénominateur commun* ». À cet égard, la proposition revue à l'initiative de la présidence allemande ne prévoit selon lui pas un niveau suffisant de protection des données. Le texte ne couvre en effet que les données échangées par les États membres ou les organes de l'Union et « *les dispositions de la proposition n'instaurent aucune nécessité de protection adéquate et ne prévoient aucun critère commun ou mécanisme afin d'évaluer le caractère adéquat du niveau de protection. En d'autres termes, l'évaluation du caractère adéquat du niveau de protection fourni par l'État tiers ou l'instance internationale est laissée à la discrétion de chaque État membre.* »

Le Parlement européen a, pour sa part, souhaité modifier le projet de décision-cadre de façon substantielle. Il a demandé un champ d'application plus large, afin que le texte ne couvre pas seulement les données échangées entre États membres, mais s'applique aussi aux données traitées au niveau national, afin de renforcer la coopération entre les différentes autorités policières et judiciaires tout en garantissant un niveau équivalent de protection des données dans l'ensemble de l'Union européenne. Il a également souhaité renforcer les principes de finalité et de proportionnalité en limitant les cas dans lesquels les données peuvent être traitées ultérieurement par l'État qui a bénéficié d'informations. Le Parlement européen a aussi voulu encadrer plus strictement les conditions de transfert à des

⁽¹⁾ Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008, JOCE n° L 350/60 du 30 décembre 2008.

⁽²⁾ Communiqué du 16 août 2006.

pays tiers, notamment par le biais de l'évaluation par une autorité indépendante du « niveau adéquat » de protection des données personnelles offert par cet État tiers.

- Le texte définitivement adopté par le Conseil s'est très peu éloigné du consensus entre États membres de novembre 2007.

La **décision-cadre du 27 novembre 2008 ne porte en effet que sur les données à caractère personnel qui « sont ou ont été transmises ou mises à disposition entre les États membres »** (article premier), ou entre systèmes d'informations européens et États membres. Sont expressément exclus les « *intérêts essentiels en matière de sécurité nationale et des activités de renseignement spécifiques dans le domaine de la sécurité nationale* ».

L'article 11 prévoit que les données à caractère personnel transmises ou mises à disposition **peuvent être traitées ultérieurement pour des finalités autres que celles pour lesquelles elles ont été transmises** dans une liste de cas assez étendue, notamment « *pour prévenir un danger immédiat et sérieux pour la sécurité publique* » ou « *pour toute autre finalité, avec l'accord préalable de l'État membre qui transmet les données ou avec le consentement de la personne concernée, donné conformément au droit national* ».

Enfin, l'article 13 dispose que « *les États membres font en sorte que les données à caractère personnel qui sont transmises ou mises à disposition par l'autorité compétente d'un autre État membre ne puissent être transférées à des États tiers ou à des instances internationales* » qu'à certaines conditions : nécessité à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites ; l'autorité destinataire de l'État tiers doit être chargée des missions précitées ; l'État membre auprès duquel les données ont été collectées doit avoir donné son accord au transfert et l'État tiers concerné « *assure un niveau de protection adéquat* ». Toutefois, les **dérogations sont fort nombreuses**. Le 2 de l'article 13 prévoit en effet que le transfert sans accord préalable « *n'est autorisé que si le transfert de données est essentiel pour prévenir un danger immédiat et sérieux pour la sécurité publique d'un État membre ou d'un État tiers [...] L'autorité compétente pour donner son accord est informée sans délai.* » Par ailleurs, le 3 du même article prévoit par dérogation à la condition d'existence d'un niveau de protection adéquate que les données à caractère personnel peuvent être transférées si la législation nationale de l'État membre qui transfère les données le prévoit « *lorsque des intérêts légitimes prévalent, en particulier des intérêts publics importants* ». Ce transfert est également possible si « *l'État tiers ou l'instance destinataire prévoit des garanties qui sont jugées adéquates par l'État membre concerné conformément à sa législation nationale* ».

- Cette décision-cadre constitue donc un **consensus minimaliste**, très éloigné des ambitions initiales de la proposition de la Commission européenne, tant s'agissant du champ d'application du texte que des dispositions relatives aux échanges avec les États tiers. De fait, un certain nombre d'États membres restent

hostiles aux progrès de l'harmonisation communautaire dans le cadre du troisième pilier, et ils ont de surcroît souhaité rester aussi libres que possible en matière de coopération bilatérale en dehors de l'Union.

En tout état de cause, si le traité de Lisbonne entre en vigueur, les textes adoptés dans le cadre du troisième pilier de l'Union relèveront de la procédure de codécision ; il sera alors nécessaire de revoir l'ensemble de la réglementation relative à la protection des données et de prévoir un document commun couvrant à la fois le champ de la directive de 1995 et accroissant celui de la décision-cadre de 2008. La Commission européenne fera probablement une proposition dans ce sens à l'horizon 2010-2012, après avoir lancé le débat au travers d'un livre blanc ou vert. Même si ce travail ne se traduira donc pas par des résultats avant plusieurs années, une vigilance particulière s'impose dès maintenant en raison de l'ampleur des enjeux. À cet égard, la CNIL a relevé dans sa lettre d'information n° 3 datée de janvier 2008 que la composition du « groupe d'experts » chargé d'engager la réflexion sur la révision de la directive de 1995 était « surréaliste » et suscitait de très lourdes interrogations, puisque sur cinq personnes, quatre sont issues soit de sociétés américaines (Google et Intel), soit de cabinets d'avocats dont les principaux établissements sont basés aux États-Unis. Selon la CNIL, « *il est inconcevable qu'un groupe d'experts chargés de réfléchir sur les pouvoirs touchant au "troisième pilier" en Europe, et donc au domaine de la souveraineté, puisse être composé aux quatre-cinquièmes de personnalités représentant des intérêts privés américains.* »

2. La lente mise en œuvre du Traité de Prüm

- Le Traité de Prüm a été signé le 27 mai 2005 par sept États membres de l'Union européenne (Allemagne, Belgique, Espagne, France, Luxembourg, Pays-Bas et Autriche) ⁽¹⁾, selon le même processus que celui qui avait été suivi pour la première convention de Schengen. Lors du Conseil « Justice et affaires intérieures » du 15 février 2007, il a été décidé d'intégrer dans l'ordre juridique de l'Union les parties du Traité relatives à la coopération policière et judiciaire en matière pénale.

Afin d'améliorer l'échange d'informations transfrontières, les États parties s'autorisent un accès réciproque automatique à des bases de données nationales spécifiques, qu'il s'agisse des fichiers ADN (tant pour la comparaison entre profils que pour la comparaison de traces avec des profils enregistrés, articles 3 et 4), d'empreintes digitales (article 9) ou de registres d'immatriculation des véhicules (article 12). Le Traité va donc plus loin que la décision-cadre du 27 novembre 2008 : si cette dernière autorise la mise à disposition et la transmission d'informations figurant dans des fichiers nationaux policiers ou judiciaires, celle-ci n'est cependant pas réalisée de manière automatisée et donc quasi instantanée. Dans le cadre du Traité de Prüm, les informations sont transmises par

(¹) Huit autres États membres ont annoncé leur souhait d'adhérer à ce traité : Slovaquie, Italie, Finlande, Portugal, Bulgarie, Roumanie, Grèce et Suède.

l'intermédiaire du réseau de communication TESTA II. À ce stade, les données échangées restent anonymes, et c'est seulement en cas de constatations de concordance que peuvent être révélées les informations nominatives personnelles auxquelles correspondent les profils ADN ou les empreintes digitales. Si l'on prend l'exemple du FAED, les partenaires de la France n'auront accès qu'à une copie de cette base, exclusivement consacrée aux échanges internationaux d'informations. Cette réplique de la base sera mise à jour toutes les 24 heures. Ainsi, une des parties contractantes pourra faire ses recherches directement sur la copie de la base FAED et récupérer les données dactyloscopiques. Une fois la trace ou l'empreinte identifiée et rapprochée, le partenaire étranger en informera les autorités françaises, qui, en retour, lui transmettront l'ensemble des données nominatives.

Il ne s'agit donc en aucun cas de la mise en place d'une forme d'interconnexion des fichiers d'identification à l'échelle européenne, puisque la décision de fournir les informations reste entièrement de la responsabilité de l'État qui en est détenteur.

• **Les résultats obtenus lors des consultations croisées semblent prometteurs.** Ainsi, à l'occasion de la réunion informelle des ministres de la justice et des affaires intérieures qui s'est tenue à Dresde le 15 janvier 2007, des résultats du croisement réel de données entre ADN entre les bases allemande et autrichienne ont été présentés. Ce travail a permis de trouver 4 512 concordances sur un nombre total de traces croisées de 102 007, dont 31 concordances pour des meurtres ou homicides et 21 infractions à caractère sexuel.

La France a ratifié le Traité de Prüm le 12 janvier 2008, mais les deux décrets nécessaires à sa mise en œuvre pour le FAED et le FNAEG ne sont toujours pas parus. C'est d'autant plus regrettable que techniquement rien ne s'oppose à la mise à disposition de nos partenaires des informations contenues dans le FAED et le FNAEG, les logiciels nécessaires ayant d'ores et déjà été validés.

3. La longue marche vers l'adoption d'une décision-cadre sur l'utilisation des données passagers

• Les informations relatives aux transports aériens sont par nature susceptibles d'être très utiles dans le cadre de la lutte contre les formes graves de criminalité, notamment le trafic de drogue, et contre le terrorisme. L'article 7 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme autorise le ministère de l'Intérieur à procéder à la mise en œuvre de traitements automatisés de données à caractère personnel :

— figurant sur les cartes d'embarquement et de débarquement (données dites APIS – *Advanced Passenger Information System*) ;

— collectées à partir de la bande de lecture optique des documents de voyage (MRZ), de la carte nationale d'identité et des visas ;

— relatives aux passagers et enregistrées dans les systèmes de réservation et de contrôle lorsqu'elles sont détenues par les transporteurs (données dites PNR – *Passenger Name Records*).

Les données APIS et issues de la lecture optique des documents de voyages sont disponibles seulement au moment de l'embarquement du vol, qui servent à alimenter respectivement le fichier des passagers aériens (FPA) et le fichier national transfrontières (FNT). Dans les deux cas, les informations collectées sont limitées à quelques États de destination ou de provenance particulièrement sensibles. Selon les informations fournies à vos rapporteurs lors de leurs auditions, les expériences françaises et étrangères en la matière montrent que les fichiers reposant sur les données APIS sont assez peu efficaces, avec un taux de « hits » très faible et concernant généralement des infractions mineures.

En revanche, **les données PNR sont potentiellement bien plus intéressantes**, puisqu'elles sont enregistrées par le vendeur du billet dès la réservation et mentionnent le lieu d'achat, l'itinéraire, le mode de paiement, les réservations éventuelles de véhicules ou de chambres d'hôtel, parmi plus d'une trentaine d'autres informations qui peuvent être fournies par le passager. Ce système commercial a été développé initialement par les compagnies aériennes pour mieux gérer l'ensemble des prestations demandées par les passagers et ces informations standardisées circulent de façon très libre.

Sur un plan policier, l'exploitation de ces données est susceptible d'offrir des avantages sur trois plans :

— anticipation et analyse des risques présentés par certains vols au vu des passagers transportés ;

— utilisation des données conservées dans le cadre d'enquêtes de police ;

— réalisation d'analyses de risques par rapport aux tendances observées dans le passé en exploitant les données archivées.

De ce fait, **des programmes de traitement des PNR se développent rapidement**. Les États-Unis ont pris en la matière une avance certaine à la suite du 11 septembre 2001, mais d'autres États sont très actifs, tels que Bahreïn, le Qatar, l'Inde et la Corée du sud. Seulement trois États européens ont légiféré sur le sujet : la France, le Royaume-Uni et le Danemark. Ce dernier a prévu de répondre seulement à l'objectif de lutte contre le terrorisme, avec une durée de conservation des données limitée à un an. À ce stade, il n'a pas mis en place de système opérationnel. **Le seul fichier PNR actif a été mis en place par le Royaume-Uni** et il est d'une ambition certaine. **70 millions de livres** ont déjà été dépensés pour sa réalisation, alors même que le programme ne devrait atteindre l'ensemble de ces objectifs qu'en 2014. Les bénéfices retirés semblent substantiels en termes de

prévention du terrorisme. À cet égard, on peut également noter que selon les années les douanes françaises effectuent entre 60 et 80 % de leurs saisies de stupéfiants dans les aéroports internationaux de Paris directement grâce à l'exploitation ciblée des données PNR.

Il est apparu **nécessaire que l'Union se dote d'une doctrine commune et d'une véritable expérience en la matière** et ne se contente pas de réagir aux pressions extérieures au coup par coup. L'exemple des difficiles tractations entre l'Union européenne et les États-Unis à l'occasion de la conclusion des accords du 17 mai 2004⁽¹⁾ puis du 23 juillet 2007 souligne combien un texte encadrant le développement des fichiers d'exploitation des PNR permettrait de négocier dans de meilleures conditions.

• À la demande du Conseil européen des 25 et 26 mars 2004, la **Commission européenne a présenté le 6 novembre 2007 une proposition de décision-cadre relative à l'utilisation des données des dossiers passagers à des fins répressives**. Au cours de la présidence française, un important travail de consultation et de réexamen de ce **texte très critiqué**⁽²⁾ a été effectué, ce qui a permis la publication par la présidence tchèque le 23 janvier 2009 d'une nouvelle version de la proposition destinée à servir de base aux discussions ultérieures. Les négociations devraient s'étendre sur l'ensemble de l'année 2009, avec une perspective d'accord définitif en 2010, sous présidence espagnole ou belge.

La commission chargée des affaires européennes a examiné le rapport d'information de M. Guy Geoffroy sur la proposition de décision-cadre relative à l'utilisation des données PNR le mercredi 11 février 2009⁽³⁾. À l'initiative de son rapporteur, elle a adopté une proposition de résolution sur l'utilisation des dossiers passagers (n° 1448) le 11 février 2009. Vos rapporteurs s'en tiendront donc à des remarques factuelles sur les principales évolutions récentes du texte, tout en effectuant quelques observations sur l'impact pour le ministère de l'Intérieur que peut avoir la mise en œuvre d'un tel traitement de données en termes pratiques.

Deux questions principales restent à trancher : il s'agit, d'une part, de la **durée de conservation des informations** et, d'autre part, du **traitement des données sensibles**.

S'agissant de la conservation des données, le Royaume-Uni milite pour la durée la plus longue, soit dix ans (contre treize ans dans la proposition initiale de la Commission européenne, qui s'inspirait du système américain), avant tout en raison de la durée de conservation qu'il a déjà retenue pour son propre système. Il sera donc difficile d'obtenir une durée totale inférieure à dix ans tant que le

⁽¹⁾ Saisie par le Parlement européen au motif que cet accord violait les droits fondamentaux et était dépourvu de base juridique, la Cour européenne de justice a annulé les décisions du Conseil et de la Commission le 30 mai 2006.

⁽²⁾ On se référera à ce point à l'avis du CEPD en date du 20 décembre 2007, paru au JOCE du 1er mai 2008, ainsi qu'à la résolution du Parlement européen du 20 novembre 2008.

⁽³⁾ Utilisation des données des dossiers passagers (PNR) à des fins répressives. Bien concilier lutte contre le terrorisme et protection des libertés publiques, n° 1447.

troisième pilier relèvera de l'unanimité. La plupart des États membres s'accordent sur une durée de conservation minimale et de mise à disposition de trois ans ; reste à négocier la durée maximale de conservation pouvant être retenue par chacun d'entre eux.

En ce qui concerne les données sensibles, il est possible de faire progresser le dossier en définissant très précisément la finalité des données collectées et en faisant valoir l'apport que constitue la séparation entre les unités d'information passagers (UIP), autorités publiques chargées de la collecte et du traitement des données, et les autorités chargées de prévenir ou de combattre les infractions terroristes et les formes graves de criminalité. Enfin, il faudra donner une définition précise à la notion de profilage, afin de souligner qu'il s'agit avant tout de détecter des anomalies et en aucun cas de mettre en place des systèmes de filtres sur une base ethnique ou religieuse. L'un des points en débat reste précisément de savoir comment ces données sensibles seront filtrées par les UIP. Dans le cas où celles-ci procéderaient au « verrouillage » de ces données et non à leur effacement complet, il serait possible d'envisager leur exploitation ultérieure strictement encadrée, dans le cadre d'enquêtes policières ou judiciaires.

Il est également nécessaire de mettre en place une traçabilité aussi grande que possible des consultations et de prévoir des sanctions appropriées en cas d'utilisation à des fins non autorisées par le texte.

Il est encore trop tôt pour savoir quelle sera la solution retenue par la France pour respecter la séparation entre UIP et services opérationnels, ce principe ne correspondant pas aux habitudes acquises en matière de gestion des fichiers de police ou judiciaires. L'organisme auquel reviendra le rôle d'UIP devra probablement utiliser les compétences de policiers détachés de leurs services d'origine. Enfin, compte tenu de la masse des informations à traiter et du coût potentiellement très important de la mise en place d'un fichier PNR, il conviendra de mener une réflexion associant les différents services de police concernés afin de déterminer au mieux la nature des besoins réels et la dimension de l'outil à développer.

VI. CONTRÔLER LA TRANSITION ENTRE FICHIERS DE POLICE ET ACCOMPAGNER LEUR DESTRUCTION ÉVENTUELLE

Bien que la prolifération actuelle des fichiers de police puisse laisser penser qu'ils sont promis à un bel avenir, ils n'ont toutefois pas tous vocation à vivre éternellement : une fois la finalité qui avait présidé à leur création épuisée ou dépassée, ils perdent, en quelque sorte, leur raison d'exister.

Lorsqu'ils ne sont pas tout simplement détruits ou mis au rebut, ils sont parfois remplacés par des applications plus récentes et plus modernes. Qu'on décide de mettre fin à leur existence ou de la prolonger sous d'autres formes, les questions qui se posent sont de deux ordres. Tout d'abord, il convient de **déterminer quelles sont les informations qui peuvent être reprises et celles qui sont devenues sans objet**. Parmi ces dernières, il convient ensuite de définir les données qui doivent être détruites et celles qui, en revanche, doivent être versées aux archives.

La nécessité de reprendre à profit certaines données conservant une utilité opérationnelle et l'intérêt qui s'attache à certaines informations présentant un intérêt historique marqué font de la transition entre fichiers de police, comme de leur mort, des étapes clés où se joue la continuité de la mémoire policière.

A. LA DIFFICILE TRANSITION ENTRE FICHIERS DE POLICE

Les fichiers de police connaissent au cours de leur existence des évolutions contrastées. Alors que certains d'entre eux sont fusionnés, afin de réaliser, notamment, des économies d'échelle et des synergies entre la police et la gendarmerie nationales, d'autres, en revanche, sont démembrés et répartis entre plusieurs administrations. Dans les deux cas, se pose, de manière récurrente, le **délicat problème de la nécessaire reprise des informations**, présentant toujours un intérêt opérationnel et permettant aux services de police ou de renseignement d'accomplir pleinement leurs missions.

1. La fusion de deux fichiers de police : une reprise problématique de l'existant

Conformément à l'esprit de la loi du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure⁽¹⁾ qui prescrit la fusion des fichiers de la police et de la gendarmerie, **certaines traitements font actuellement l'objet d'un rapprochement stratégique**. Ainsi en est-il, par exemple, des fichiers d'antécédents judiciaires : STIC et JUDEX. Ils seront, à terme, réunis en une seule

⁽¹⁾ Loi n° 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure – Article annexe 1 : « Le rapprochement des grands fichiers de police criminelle de la police et de la gendarmerie nationales (STIC, JUDEX) sera favorisé, au besoin, en conférant une base législative aux échanges d'informations indispensables à l'efficacité des enquêtes judiciaires. ».

application, dénommée ARIANE (application de rapprochements, d'identification et d'analyse pour les enquêteurs).

Si les avantages attendus de cette opération en termes de rationalisation des moyens techniques et financiers ne sont pas minces, **le déploiement de l'application ARIANE a pris un certain retard** (de l'ordre de huit à neuf mois) et se heurte à quelques difficultés. La première d'entre elles réside dans **la complexité technique de la reprise des informations déjà contenues dans le STIC ou JUDEX**. En effet, le transfert de ces données implique, sur le plan technique, une vigilance particulière afin de sécuriser l'ensemble des informations. Il faut en effet reprendre et convertir dans un format informatique compatible avec ARIANE les 30 millions de procédures et les 2,5 millions de fichiers contenus dans JUDEX ainsi que les 5,6 millions de fiches contenues dans le STIC.

Ainsi, lors de son audition, M. Christian Lothion, directeur central de la police judiciaire, a souligné qu'une « *période de transition difficile* » était à prévoir afin, d'une part, de reprendre, sur le plan technique, l'ensemble des données déjà contenues dans le STIC et JUDEX et, d'autre part, de les « *toiletter* ». Cette tâche sera confiée aux services régionaux de documentation criminelle au sein de la police nationale et au service technique de recherches judiciaires et de documentation pour la gendarmerie nationale. **Ce constat, loin d'être isolé, est aujourd'hui largement partagé par l'ensemble des acteurs du projet.**

Du côté de la gendarmerie, le général Espinasse, sous-directeur des télécommunications et de l'informatique, a souligné, lors de son audition par vos rapporteurs, que le retard pris par rapport au projet initial s'explique effectivement par la difficulté à reprendre, sur le plan technique, toute l'information existante. Or, ce transfert de données vers ARIANE se fait à partir de JUDEX, une application jugée « *très ancienne* », et ce avec une tolérance zéro, dans la mesure où il s'agit d'informations judiciaires. La rentrée et la reprise de données depuis JUDEX vers ARIANE devraient ainsi durer six mois au cours de l'année 2009.

Du côté de la police nationale, c'est le même constat qui s'impose. Le commissaire divisionnaire, M. Sylvain Maubé, a également souligné, lors de son audition, l'exigence de sécurité qui préside au traitement de toute information judiciaire. Cette exigence de fiabilité expliquerait, comme pour la gendarmerie, le retard actuel du projet ARIANE, puisque **la volumétrie d'informations à transférer des fichiers STIC et JUDEX est « colossale ».**

En définitive, le fichier ARIANE devrait être pleinement opérationnel le 1^{er} septembre 2010, nombre de syndicats rencontrés, dont le syndicat national des officiers de police, jugeant la fusion du STIC et de JUDEX « *primordiale* », car elle permettra des échanges accrus d'informations.

2. Le démembrement d'un fichier de police : le délicat partage de l'héritage

Lorsqu'un fichier de police disparaît et est remplacé par de nouvelles applications plus modernes et plus efficaces, le partage de l'information devient plus complexe, dans la mesure où il convient de **trier l'ensemble des données pour pouvoir ensuite les transférer vers le bon fichier**. Or, certaines informations répondant à des finalités multiples, il s'avère souvent difficile de les répartir entre des applications dont les périmètres respectifs ne sont pas clairement délimités.

a) La question du partage du FRG entre SDIG et DCRI

Depuis le 1^{er} juillet 2008, le fichier des renseignements généraux n'est plus alimenté mais demeure consultable jusqu'au 31 décembre 2009⁽¹⁾. Cette période est consacrée, au niveau de chaque direction départementale, à l'examen complet du contenu détaillé de chaque dossier du fichier des renseignements généraux afin de **répartir les données entre EDVIRSP et CRISTINA**.

Ce partage vise à déterminer ce qui, sur le plan de la compétence et de la mise en œuvre, relève soit du fichier EDVIRSP, et donc de la responsabilité des services départementaux de l'information générale (SDIG), soit du fichier CRISTINA, et donc de la responsabilité des fonctionnaires des DCRI locales. Dans tous les cas, **l'examen se fait au cas par cas**. Le terme fixé à ce travail de répartition des données, parachevant la réforme du renseignement français intervenue à l'été 2008, est le **31 décembre 2009**, bien que le travail soit, selon M. Éric Le Douaron, directeur central de la sécurité publique, « *relativement bien avancé* ».

À l'inverse, certains fonctionnaires rencontrés par vos rapporteurs lors de leurs divers déplacements ont, pour leur part, souligné que « **la question du partage du FRG entre SDIG et DCRI reste entière** ». En premier lieu, certains dossiers sont susceptibles d'intéresser les deux services simultanément, la frontière entre les champs de compétences respectifs n'étant pas toujours aisée à déterminer. En second lieu, le partage des dossiers qu'il convient de réaliser constitue, sur le plan pratique, un « **travail de titan** ». S'il est vrai que certains départements ont d'ores et déjà achevé cette répartition, c'est principalement en raison du caractère « *sommaire* » du travail ainsi réalisé. En effet, nombre d'observateurs ont rappelé que si l'on entend conserver un maximum d'informations utiles et exploitables, **il est indispensable de reprendre et d'examiner tous les dossiers individuels un par un**.

Aujourd'hui, face aux difficultés de partage, les services rencontrés sont dans l'attente de consignes claires et précises de la part de la **mission confiée** à

(¹) Décret n° 2008-631 du 27 juin 2008 portant modification du décret n° 91-1051 du 14 octobre 1991 relatif aux fichiers gérés par les services des renseignements généraux et du décret n° 2007-914 du 15 mai 2007 pris pour l'application du 1 de l'article 30 de la loi n° 78-17 du 6 janvier 1978.

Mme Élisabeth Rabut qui vient d'être mise en place. Ainsi, la lettre de mission adressée par la ministre de l'Intérieur, Mme Michèle Alliot-Marie, lui confie le soin « *d'examiner les critères à retenir dans la répartition des données entre celles qui doivent être conservées par les services d'information générale, celles qui doivent être transférées et celles qui doivent être versées aux archives* ». En tout état de cause, il faudra, dans un département comme le Val-de-Marne, plusieurs années pour trier des dossiers qui remontent, pour les plus anciens d'entre eux, à la création du département en 1968.

b) L'impossibilité complète d'alimentation : l'imbroglio juridique entourant le retrait d'EDVIGE

Le décret du 27 juin 2008 modifiant le décret du 14 octobre 1991, qui avait créé le fichier des renseignements généraux ⁽¹⁾, dispose à son article premier que « ***la collecte et l'enregistrement de nouvelles données dans [le fichier des renseignements généraux] sont interdits à compter du 1^{er} juillet 2008*** ». Si le fichier des renseignements généraux ne peut plus être alimenté, il peut néanmoins être consulté jusqu'au 31 décembre 2009, date de sa disparition définitive.

Seul pouvait être alimenté, à partir du 1^{er} juillet 2008 et en remplacement du FRG, le traitement EDVIGE. Or, la décision de retrait de ce nouveau fichier de renseignement, prise en octobre 2008 par la ministre de l'Intérieur et définitivement actée par le décret n° 2008-1199 du 19 novembre 2008 ⁽²⁾, a été accompagnée par une note ⁽³⁾ du directeur de cabinet de la ministre de l'Intérieur ainsi que par une note ⁽⁴⁾ du directeur général de la police nationale, visant toutes deux à anticiper la décision de retrait et à en détailler les conditions. Dans sa note du 17 octobre 2008, le directeur de cabinet de la ministre de l'Intérieur rappelait ainsi que le retrait du décret du 27 juin 2008 ôtant « ***réroactivement toute existence juridique à EDVIGE*** », il fallait en anticiper tous les effets de manière préventive : « ***il convient [...] de cesser toute alimentation ou consultation du fichier, et de retirer de ce fichier les données qui ont pu y être intégrées depuis la publication du décret*** ». Cinq jours plus tard, le directeur général de la police nationale n'a fait que reprendre à son compte ces instructions : « ***l'accès à EDVIGE sous CHEOPS doit être immédiatement supprimé. Ce traitement ne doit plus pouvoir faire l'objet de consultation ou d'alimentation de la part des fonctionnaires de la sous-direction de l'information générale, de la direction centrale de la sécurité publique et des fonctionnaires affectés dans un service d'information générale des directions départementales de la sécurité publique ou, à Paris, de la préfecture de police*** ». Ainsi **étaient explicitement interdites l'alimentation et l'interrogation à partir des index du fichier EDVIGE**, le

⁽¹⁾ Le décret n° 2008-631 du 27 juin 2008 portant modification du décret du 14 octobre 1991 relatif au fichier des renseignements généraux.

⁽²⁾ Le décret n° 2008-1199 du 19 novembre 2008 portant retrait du décret n° 2008-632 du 27 juin 2008 portant création d'un traitement automatisé de données à caractère personnel dénommé « EDVIGE ».

⁽³⁾ Note du directeur du cabinet de la ministre de l'Intérieur à Monsieur le directeur général de la police nationale, en date du 17 octobre 2008.

⁽⁴⁾ Note du directeur général de la police nationale à Monsieur le directeur de l'administration de la police nationale, en date du 22 octobre 2008.

contenu de ce traitement de données n'ayant plus d'existence juridique. Se pose donc aujourd'hui le problème de la consultation et de la conservation des données produites pendant cette période ⁽¹⁾.

Néanmoins, en raison des consignes reçues à la suite des débats suscités par le fichier EDVIGE, les fonctionnaires des SDIG continuent de collecter et rassembler des informations, qu'ils ne peuvent intégrer ni dans le fichier EDVIGE, ni dans l'ancien fichier des renseignements généraux, qui est de fait gelé. De l'aveu de nombre d'acteurs au sein de la police nationale, « **la priorité opérationnelle ne semble pas avoir guidé cette décision** ». La situation est identique à la direction du renseignement de la préfecture de police. Si, depuis juillet 2008, des notes sont rédigées sur des faits ou agissements ne relevant pas de GESTEREXT, pendant de CRISTINA, il n'est pas possible de les intégrer dans le fichier GEVI, qui est juridiquement adossé au FRG. Au final, aussi bien dans les SDIG qu'à la DRPP, les données et informations diverses sont accumulées sous forme papier sans indexation informatique, affectant d'autant l'efficacité opérationnelle du travail réalisé. Compte tenu du retard accumulé à ce jour, il ne sera probablement pas possible de les intégrer par la suite dans GEVI ou EDVIRSP. Se pose là également **le problème de la consultation et de la conservation des données produites et collectées pendant cette période**.

Afin de prévenir une telle situation, dommageable à l'accomplissement de leurs missions par les services de renseignement, le retrait du décret du 27 juin 2008 portant création d'EDVIGE aurait dû être accompagné d'une disposition réglementaire **autorisant temporairement la collecte et l'enregistrement de données dans le fichier des renseignements généraux**. Guidés par un souci d'efficacité opérationnelle, vos rapporteurs proposent que le fichier des renseignements généraux puisse être de nouveau alimenté, dans l'attente de l'adoption d'une loi créant le futur fichier EDVIRSP. Cette proposition entend **permettre l'utilisation temporaire par les services de renseignement d'un outil de travail indispensable à l'accomplissement de leurs missions** et répondant à leurs attentes.

Proposition n° 53

Permettre, à titre provisoire et sur la base du décret du 14 octobre 1991, l'alimentation et la consultation du fichier des renseignements généraux, « gelé » depuis le 1^{er} juillet 2008, dans l'attente de l'adoption d'une loi autorisant la création du futur fichier EDVIRSP.

c) La désorganisation des services à la suite de la réforme des services de renseignements en 2008

Le 1^{er} juillet 2008, **la direction centrale du renseignement intérieur (DCRI)** a été créée. Elle exerce les attributions antérieurement dévolues à la

(1) Soit entre le 1^{er} juillet 2008 et le 19 novembre 2008.

direction de la surveillance du territoire (DST) ainsi que celles de la direction centrale des renseignements généraux (DCRG), relevant de sa mission de renseignement *stricto sensu* (lutte contre le terrorisme, contre les atteintes à la sûreté de l'État...).

Les autres missions des renseignements généraux ne relevant pas du renseignement (information générale sur l'activité politique, économique et sociale, surveillance des violences urbaines) sont dorénavant attribuées à la direction centrale de la sécurité publique (DCSP). Afin de réaliser cette mission, une nouvelle sous-direction a été créée en son sein : **la sous-direction de l'information générale** ainsi que des services départementaux d'information générale au sein des directions départementales de la sécurité publique.

Lors de son audition par vos rapporteurs, M. Éric Le Douaron, directeur central de la sécurité publique, a souligné **l'importance de la réforme du renseignement français intervenue à l'été 2008**. Le cloisonnement prégnant qui existait auparavant entre renseignements généraux, d'une part, et sécurité publique, d'autre part, ne permettait pas de « *chaînage vertueux* » entre le renseignement pur et le travail judiciaire, qui en constitue le prolongement naturel. Avec le nouveau dispositif mis en place à l'été dernier, le rattachement des SDIG à la Sécurité Publique constitue le signal fort d'**une orientation extrêmement nette de l'information générale vers l'opérationnel**. Ce rapprochement devrait permettre, selon le ministère de l'Intérieur, d'assurer une plus grande sécurité globale des citoyens : tous les aspects « *vie des quartiers* » et « *violences urbaines* », autrefois pris en charge par les renseignements généraux, sont désormais traités par les SDIG au sein de la Sécurité Publique, permettant ainsi une plus grande synergie avec les services chargés de la sûreté urbaine.

Toutefois, l'effet escompté de cette réorganisation des services de renseignement ne fait pas l'unanimité. Ainsi, le syndicat Alliance police nationale, lors de son audition, a jugé « **artificielle et inexistante** », **dans la pratique, la barrière entre la DCRI et les SDIG**. En outre, loin de l'objectif initialement visé, la tutelle de la DCSP sur l'information générale conduirait à une moins bonne circulation de l'information en matière de renseignement entre les SDIG et les services de la DCRI.

D'autres, comme le Syndicat général de la police, ont dressé **un premier bilan en demi-teinte de la réorganisation du renseignement intérieur**. Celui-ci se traduirait tout d'abord par une désorganisation considérable des services d'information générale. Si les SDIG comptent 260 implantations territoriales et 1 200 fonctionnaires, les effectifs sont jugés, dans certains cas, très insuffisants au regard des besoins. Ainsi, deux fonctionnaires seulement sont en poste à Manosque pour assurer l'ensemble de l'information générale des Alpes-de-Haute-Provence, empêchant tout fonctionnement normal de l'unité et nécessitant des renforts ponctuels en provenance d'autres SDIG notamment lors événements particuliers. De manière générale, **la réorganisation des services de renseignement semble avoir davantage profité à la DCRI** : à Marseille, les

effectifs de cette dernière sont dix fois supérieurs à ceux du SDIG. Au demeurant, **les SDIG sont aujourd'hui concurrencés par la gendarmerie** qui tend à les suppléer en travaillant directement avec les interlocuteurs traditionnels des renseignements généraux, y compris en zone police nationale, et en stockant nombre d'informations sans véritable contrôle.

LE SDIG DU VAL-DE-MARNE :

« nous vivons sur nos acquis et nous sommes en train de les perdre ».

Le SDIG de ce département a été plutôt « *bien servi* » dans le cadre de la réforme du renseignement intérieur, puisqu'il compte **vingt fonctionnaires de police et sept personnels administratifs**. Pour mémoire, les RG du Val-de-Marne, comptaient précédemment près de 60 personnels, y compris les antennes locales.

Le travail d'anticipation et d'analyse confié au SDIG s'exerce prioritairement sur les sujets suivants : racisme, xénophobie et antisémitisme ; phénomènes sectaires ; suivi des cultes ; activités extrémistes susceptibles d'avoir des répercussions en matière d'ordre public ; suivi des mouvements sociaux ; suivi des violences urbaines. Le travail est réalisé pour l'essentiel en milieu ouvert. **En raison de la réduction des effectifs, les personnels sont moins spécialisés que par le passé et, selon les personnels rencontrés, il existe, à terme, un risque non négligeable de perte d'expertise.** Cela est d'autant plus regrettable que ce sont les RG qui avaient identifié de façon anticipée des phénomènes comme les viols collectifs et les pitbulls.

En ce qui concerne l'activité des bandes, **le « gel » de l'alimentation du FRG conduit à l'absence totale d'outil permettant d'archiver le travail effectué.** Ainsi, une note a été réalisée en décembre 2008 sur quatre bandes du département : bien que mentionnant les noms des meneurs, ce document n'a pu être versé à leur dossier individuel, comme cela était pratiqué précédemment. Au total, le FRG du Val-de-Marne comprend près de 30 000 dossiers individuels et environ 40 000 fiches de référence.

À côté de la direction centrale de la sécurité publique (DCSP), chargée du renseignement ouvert, a été créée la direction centrale du renseignement intérieur (DCRI), qui prend en charge le renseignement fermé. **La DCRI, à l'instar de la DCSP, connaît une période de transition, M. Éric Le Douaron, estimant qu'« on en arrive au bout ».** Ainsi, l'arrivée de CRISTINA nécessitant un maillage plus performant et une sécurité accrue, le nouveau réseau informatique de postes cryptés est en cours de construction et de déploiement. À cet égard, M. Bernard Squarcini, directeur central du renseignement intérieur, a souligné qu'**il n'y avait pas en la matière « d'optimisation totale aujourd'hui ».**

B. ORGANISER LA DESTRUCTION DES FICHIERS DÉSUETS

Les activités de police et de renseignement évoluant rapidement, sous le double effet d'une diversification et d'une spécialisation accrue, certaines données qui, hier, présentaient encore un intérêt opérationnel marqué pour les services, deviennent aujourd'hui sans objet. Si le FAR est un exemple notable de ces fichiers obsolètes et dépassés, qui ne répondent plus à leur vocation originelle, se pose en dernier ressort la question de savoir si ces données devenues sans objet doivent être effectivement détruites ou s'il convient de leur donner une seconde vie, en les versant aux archives.

1. Archiver ou détruire, il faut choisir !

Les fichiers mis au rebut ou devenus sans objet, loin de connaître une fin de vie paisible, connaissent quelques dernières « convulsions », dont la cause est à rechercher dans le devenir incertain des données qu'ils contiennent. Alors que le **cadre juridique actuel reste flou sur les modalités de destruction et d'archivage**, la question se pose néanmoins de savoir suivant quels critères les données doivent être soit détruites, soit archivées. L'enjeu est de taille, tout particulièrement pour les renseignements généraux, qui ressemblent à bien des égards à « *un monde englouti sous les papiers* ».

a) La mission « Archives des renseignements généraux » : donner une seconde vie à des informations ne répondant plus aux besoins opérationnels

Parallèlement au processus en cours de répartition des données entre les fichiers CRISTINA et EDVIRSP, les autorités devront, dans les mois à venir, **définir au cas par cas ce qui, dans le fichier des renseignements généraux, doit être détruit ou versé aux archives nationales et/ou départementales**. En effet, le remplacement du fichier des renseignements généraux impose une mise à jour des anciens dossiers ainsi que la définition de critères de destruction, d'archivage et de transfert des données.

Pour ce faire, le 4 décembre 2008, la ministre de l'Intérieur a confié à Madame Élisabeth Rabut, chef de l'inspection générale des archives de France, une mission « *Archives des renseignements généraux* »⁽¹⁾. En effet, aux termes de la réorganisation des services de renseignement du ministère de l'Intérieur, **une partie importante des informations contenues dans le FRG est devenue sans objet** et devra donc être soit détruite, soit versée aux archives, suivant une clé de répartition qui reste à imaginer.

Aussi la ministre de l'Intérieur fixe-t-elle pour objectif final à la mission **la définition de « règles de tri, d'archivage et d'exploitation des données »** à partir « *d'une documentation riche et complexe, parfois très ancienne et parfois classée sans règles uniformes* ». Le rapport de la mission, qui sera remis en avril 2009, définira un ensemble de règles claires et opérationnelles encadrant les modalités de destruction, d'archivage et de transfert des données contenues dans le fichier des renseignements généraux. Les recommandations méthodologiques qui seront ainsi faites pourront en outre être adoptées pour d'autres fichiers de police et de gendarmerie voués à disparaître.

Afin de définir les critères de répartition des données entre celles qui doivent être conservées par les SDIG, celles qui doivent être transférées et celles qui doivent être versées aux archives, la mission conduite par Mme Élisabeth Rabut devra **analyser dans le détail le champ de compétences ainsi que le fonctionnement des différents services**, qu'il s'agisse de l'information générale

(1) Les lettres de cadrage de la mission « Archives des renseignements généraux » figurent en annexe 11.

ou du renseignement intérieur. La composition élargie de cette mission, comprenant notamment des fonctionnaires de l'IGPN, de la DLPAJ, de la préfecture de police, de la DCSP et de l'IGA, doit permettre de faire émerger une conception globale et collective du traitement des archives et de repenser « *toutes les règles de l'amont vers l'aval* ». Outre le versement de certaines données aux archives, la mission examinera également de quelle manière sont produites, classées, indexées et consultées les données dans les SDIG. Les durées de conservation des données dans les services qui les produisent, en fonction des besoins de consultation par ceux-ci dans le temps, feront également l'objet d'un cadre normé commun à l'ensemble des services. **C'est toute la chaîne de vie des données, de leur production jusqu'à leur archivage, qui sera étudiée et fera l'objet de recommandations méthodologiques.**

Au-delà de cette ambition générale, la mission devra avant tout définir les critères de répartition entre les données qui doivent être détruites et celles qui seront archivées. Au regard de **la difficulté à définir avec précision l'intérêt historique justifiant la conservation de certaines données**, la mission réfléchit actuellement à la possibilité de verser aux archives les données du FRG dans leur intégralité et non par échantillonnage.

Il convient toutefois de rappeler que cette tentative de définition des critères de destruction, d'archivage et de transfert des données contenues dans les fichiers de police n'est pas nouvelle. En effet, le ministre de l'Intérieur et le ministre de la culture avaient publié en 2001 une circulaire conjointe ⁽¹⁾ définissant les modalités de tri et de conservation des documents produits ou reçus par les directions régionales et départementales des renseignements généraux. Ainsi, à chaque type de document correspondaient une durée d'utilité administrative (DUA) ainsi qu'un sort final à l'expiration de la DUA, qui pouvait être de trois ordres : conservation, destruction ou tri.

Proposition n° 54

Rédiger un guide méthodologique à l'attention des services, détaillant avec précision les critères et les modalités de production, de traitement, de transfert, de destruction et d'archivage des données contenues dans les fichiers de police.

b) Trier les archives centrales de la préfecture de police : « un monde englouti sous les papiers »

À la suite des décisions des préfets de police successifs de recentrer l'activité des renseignements généraux parisiens sur les activités policières, à savoir les violences urbaines, l'ordre public et la lutte contre les extrémismes violents, **décision a été prise en 2001**, lors de l'informatisation des fichiers de

⁽¹⁾ La circulaire AD 2001-1 du 3 juillet 2001 relative au tri et à la conservation des documents produits ou reçus par les directions régionales et départementales des renseignements généraux figure en annexe 12.

renseignements généraux de la préfecture de police, **de mettre fin à l'activité traditionnelle de fichage nominatif des personnes en fonction de leurs activités politiques, économiques, sociales ou religieuses**. Ainsi, depuis le début des années 2000, le fichier manuel et mécanographique, dénommé « *archives centrales* » n'est plus alimenté.

La préfecture de police doit donc désormais s'atteler au chantier du « *classement définitif et de l'archivage du fichier manuel des renseignements généraux* ». Le Préfet de Police, dans sa lettre adressée à la ministre de l'Intérieur en date du 23 décembre 2008 et portant sur la mise en conformité des fichiers mis en œuvre par la préfecture de police ⁽¹⁾, a rappelé « *l'attention toute particulière* » qui est portée sur ce chantier.

Depuis janvier 2009, en vertu d'un arrêté du Préfet de Police ⁽²⁾, ce fonds documentaire « *archives centrales* » a été soustrait à la gestion de la direction du renseignement pour être placé sous le statut d'archives, qui ne sont dès lors consultables que par dérogation spéciale « *délivrée par une autorité hiérarchique de rang élevé, selon une procédure garantissant une traçabilité exhaustive* » ⁽³⁾.

Au regard du **volume considérable de ces archives**, comprenant 3,5 millions de fiches cartonnées d'indexation ⁽⁴⁾, renvoyant à 787 129 dossiers ⁽⁵⁾, le Préfet de Police a fixé **un délai de trois ans** pour « *procéder méthodiquement au reversement définitif de ce fonds documentaire important au service des archives historiques de la préfecture de police* ». Vos rapporteurs, en visitant les rayonnages poussiéreux des sous-sols de la préfecture de police, où sont stockés ces 787 129 dossiers, ont pu se faire une idée du « **travail considérable** », que représente ce processus de tri commencé en novembre 2008. Bien que prévu initialement pour trois ans, le travail d'apurement et de versement aux archives devrait en réalité durer probablement bien davantage (soit cinq *a minima*, voire plus). Les dossiers actuellement traités sont ceux couvrant la période des années 1930 et 1940. À cet effet, les **trois fonctionnaires affectés à ce travail de tri** vont être renforcés par quatre réservistes civils ⁽⁶⁾. Si l'on se réfère aux nouvelles catégories d'informations pouvant figurer dans la future application EDVIRSP, entre 60 et 70 % des données relèvent du suivi des activités politiques,

⁽¹⁾ La lettre du Préfet de Police à la ministre de l'Intérieur, en date du 23 décembre 2008 et ayant pour objet la mise en conformité des fichiers mis en œuvre par la préfecture de police, figure en annexe 13.

⁽²⁾ L'arrêté n° 2009-00038 du 14 janvier 2009 relatif au versement au service des archives des données contenues dans le fichier manuel des renseignements généraux de la préfecture de police figure en annexe 15.

⁽³⁾ Si les « *archives centrales* » ne sont plus alimentées depuis 2001, elles pouvaient être consultées par certains fonctionnaires de la direction du renseignement de la préfecture de police habilités à cet effet ainsi que par quelques fonctionnaires autorisés par le Préfet de Police, de la DCRI ou de la brigade criminelle de la direction de la police judiciaire de Paris.

⁽⁴⁾ Dont 3 millions de fiches cartonnées d'indexation pour les personnes physiques et sur 500 000 pour les personnes morales.

⁽⁵⁾ Ces dossiers sont subdivisés en dossiers individuels (personnes physiques et morales), de principe (essentiellement composés de synthèses relatives à des problèmes d'ordre général) et de synthèse (regroupant des notices individuelles résultant d'une enquête).

⁽⁶⁾ Il s'agira le plus souvent de personnes retraitées des renseignements généraux parisiens, connaissant bien les méthodes de travail de ce service.

économiques et sociales *stricto sensu*, qui devraient être expressément exclu du champ des données pouvant être désormais collectées.

Comme le ministère de la Défense et le ministère des Affaires étrangères, la préfecture de police dispose de la faculté de reverser ses documents à son propre service des archives et à son musée. La sélection des documents conservés va être réalisée par les personnels de la DRPP, sous la tutelle du conservateur du service des archives. En tout état de cause, il ne sera procédé à aucune destruction tant que les conclusions de la mission nationale d'appui confiée à la chef de l'inspection générale des archives de France, Mme Élisabeth Rabut, n'auront été rendues. Au vu des premiers travaux, **les documents présentant un véritable intérêt historique sont rares, « de l'ordre d'un sur dix mille »**. Une fois les dossiers archivés ou détruits, les fiches d'indexation seront détruites, car elles ne présentent en elles-mêmes pas d'intérêt historique.

2. La fin programmée du FAR : la nouvelle « Arlésienne » ?

Le fichier alphabétique de renseignements de la gendarmerie est **un fichier atypique** : bien que ne répondant plus à l'ambition originelle qui avait présidé à sa création, les gendarmes ne peuvent se résigner à s'en séparer. Cet attachement quasi affectif conduit actuellement à **l'impréparation totale de la fin du FAR programmée au 24 octobre 2010**. Ainsi, alors qu'il doit disparaître dans à peine dix-huit mois, les modalités de transfert, de destruction et d'archivage n'ont toujours pas été définies à ce jour.

a) Un fichier au fonctionnement obsolète et inadapté

Le fichier alphabétique de renseignements (FAR) est un fichier administratif géré par la gendarmerie nationale, largement obsolète et archaïque. Se présentant sous forme de **fiches manuscrites individuelles, gérées au niveau de chaque brigade territoriale**, le FAR a pour vocation première de permettre aux gendarmes d'acquérir une connaissance approfondie de la population résidente et, notamment, de son éventuelle dangerosité. Les informations recensées dans le FAR sont également utilisées dans le cadre des enquêtes de police administrative, comme les enquêtes de moralité pour les candidats aux concours de la fonction publique, l'ouverture d'un débit de boissons ou l'autorisation de détention d'armes.

Le FAR concerne actuellement **trois types de publics**, à savoir les personnes nées dans le ressort de la brigade territoriale, celles y résidant présentement ainsi que celles y ayant résidé. Afin de bien identifier et de recenser l'ensemble des populations visées, les fiches du FAR se répartissaient, jusqu'à une période récente, en trois catégories. En premier lieu, les « *fiches 15* », de couleur jaune, concernaient **les personnes nées dans le ressort géographique de la brigade territoriale**. En second lieu, les « *fiches 24* », de couleur marron, concernaient **les personnes nées à l'extérieur du ressort géographique de la brigade territoriale**. Enfin, les « *fiches 25* », de couleur verte, concernaient **les**

personnes nées à l'étranger. Depuis 2006, l'ensemble des fiches du FAR sont blanches et sont directement téléchargeables depuis l'Intranet de la gendarmerie nationale. Une fois la fiche téléchargée, l'agent a ensuite la charge de l'imprimer et de la conserver dans l'armoire de sa brigade.

S'agissant des données contenues dans le FAR, **une fiche individuelle comporte trois volets**, suivant une logique de signalisation. Le premier volet de la fiche est composé de **données nominatives**, portant tant sur la personne visée ⁽¹⁾ que son conjoint ⁽²⁾. Le deuxième volet de la fiche constitue **la partie « renseignement » proprement dite** : les gendarmes y recensent tous les procès-verbaux et autres renseignements (plaintes, etc.) concernant la personne, qu'elle soit mise en cause, victime ou témoin. Y figurent également les mentions d'une éventuelle inscription dans d'autres fichiers, comme le fichier des personnes recherchées (FPR). Le troisième volet, enfin, concerne **la vérification d'identité de la personne**, réalisée par la brigade du lieu de résidence auprès de la brigade du lieu de naissance. En effet, toutes les fiches FAR établies sur le lieu de résidence sont transmises par courrier à la brigade territoriale du lieu de naissance afin que celle-ci détermine si l'identité mentionnée est ou non exacte. La certification de la vérification de l'identité de la personne concernée est attestée par la mention, sur la fiche FAR du lieu de résidence, du numéro de l'acte de naissance. De manière générale, les gendarmes estiment que les fiches du FAR contiennent uniquement des « *éléments factuels et objectifs* ». C'est pourquoi, les fiches étaient auparavant triées et indexées suivant la gravité des faits commis. Ce mode de classement a été abandonné depuis une vingtaine d'années, au profit d'un classement par ordre alphabétique.

Il apparaît, en revanche, bien regrettable que **l'alimentation du FAR ne réponde pas au même formalisme que le classement par ordre alphabétique**. Les gendarmes rencontrés par vos rapporteurs, lors de leur déplacement à la brigade territoriale d'Auvers-sur-Oise, ont rappelé que **le FAR est alimenté « en cas de besoin »** et quand la nature des faits présente un « *intérêt* ». Ainsi, les critères d'inscription dans le FAR ne sont pas clairement établis et semblent laissés à la libre appréciation de chaque gendarme. En outre, le FAR est actuellement dans une phase transitoire, avant sa disparition définitive fixée au 24 octobre 2010. Cette fin annoncée du FAR nécessiterait que les services de gendarmerie anticipent d'ores et déjà la disparition de ce fichier, notamment en réduisant son alimentation. Or, sur le terrain, les gendarmes n'ont pas le sentiment « *d'avoir levé le pied dans l'alimentation du FAR* ». Ce constat a été corroboré par certaines personnes auditionnées par vos rapporteurs, dont l'une d'elles a affirmé : **« la destruction du FAR n'a pas commencé ».**

⁽¹⁾ Les données nominatives comprennent pour la personne visée les informations suivantes : nom, prénom, surnom, date et lieu de naissance, noms et prénoms des parents, domicile, téléphone, profession, employeur.

⁽²⁾ Les données nominatives relatives au conjoint de la personne visée comprennent les informations suivantes : nom, prénom, date et lieu de naissance, date et lieu de mariage.

De la même manière, **la gestion du FAR n'est pas empreinte d'un formalisme excessif**, dans la mesure où elle reste **entièrement manuelle** et dépendante de la bonne volonté de chaque brigade territoriale. Il appartient en effet à chaque militaire de tenir à jour le fichier de son unité **au fil des procédures établies ou des interventions réalisées**. La consultation par les militaires reste par ailleurs libre au sein de l'unité. Lors du déplacement de vos rapporteurs à Auvers-sur-Oise, le casier du FAR était placé au sous-sol, sous les escaliers, à côté de la salle de repos des gendarmes de la brigade. De manière générale, **les FAR sont d'accès libre et ne sont pas placés sous coffre**, bien que les militaires cherchent à les installer dans des « *endroits discrets* ». Le manque de rigueur en la matière est d'autant plus regrettable qu'en l'absence d'informatisation du FAR, aucune traçabilité des consultations n'est possible.

Les conditions d'apurement des fiches sont néanmoins plus strictes, en théorie, et ont été définies une instruction initiale de 1971. Ainsi, les personnes décédées ou ayant plus de 80 ans ne peuvent normalement plus être répertoriées dans le FAR. De la même manière, les personnes ayant déménagé ne doivent plus figurer dans le FAR de l'unité de leur ancienne domiciliation. Or, au hasard de la consultation du FAR lors du déplacement à la brigade territoriale d'Auvers-sur-Oise, vos rapporteurs ont pu constater que **des personnes décédées, certaines en 1988, continuaient d'être répertoriées...**

Au final, en l'absence totale de procédure automatisée et formalisée, **l'apurement des fiches n'est pas réellement possible en raison des volumes à traiter**, estimés à 60 millions de fiches sur l'ensemble du territoire national. S'agissant de l'apurement et du respect de la durée de conservation des données, les gendarmes ont souligné à plusieurs reprises qu'il leur était quasiment impossible de réaliser ces opérations manuellement. C'est donc, par défaut, que l'apurement des fiches se fait « *au fil du travail quotidien* », suivant la disponibilité des gendarmes.

b) Un fichier auquel la gendarmerie est attachée et dont elle n'arrive pas à se détacher : « c'est la mémoire de la brigade qui va s'en aller »

Bien que le FAR soit **un fichier complètement désuet**, les gendarmes restent sentimentalement attachés à ce fichier.

En premier lieu, le FAR fait l'objet d'**une gestion très lourde**. Les échanges d'informations entre brigades, aux fins de mises à jour, se font exclusivement par courrier. Ainsi, la brigade du lieu de résidence envoie la fiche à la brigade du lieu de naissance, en vue de compléter et de mettre à jour les informations nécessaires. Cette logique axée autour de la brigade du lieu de naissance, qui remonte à 1922, a vocation à centraliser en un point unique l'ensemble des informations relatives à une personne, mais produit autant de doublons entre les brigades.

En second lieu, avec l'apparition des fichiers d'antécédents judiciaires (STIC ou JUDEX), **le FAR s'est révélé être un outil de travail inadapté**. Bien que son existence ait été signalée à la CNIL, le décret visant à le doter d'une base juridique claire et précise n'a jamais vu le jour. Le groupe de travail sur les fichiers de police, présidé par M. Alain Bauer, avait demandé en 2006 la régularisation juridique de ce fichier, que la gendarmerie nationale n'a jugé ni utile, ni nécessaire. En effet, cette dernière a préféré à la régularisation la disparition du dispositif d'ici 2010, les fiches devant être archivées ou broyées.

En dépit des critiques régulièrement adressées à **ce fichier « d'un autre temps »**, vos rapporteurs ont pu constater, lors de leurs divers déplacements, l'attachement des gendarmes pour cet outil de travail. À cet égard, les militaires rencontrés à la brigade territoriale d'Auvers-sur-Oise ont souligné que le FAR constitue pour eux une base de travail indispensable, dont ils font usage quotidiennement. Ainsi, lorsqu'une personne se présente à la brigade de gendarmerie, elle fait systématiquement l'objet d'une fiche au FAR, si toutefois elle ne fait pas partie des vingt millions de personnes qui y sont déjà répertoriées.

En outre, alors même que le rapport rédigé par le groupe de travail de M. Alain Bauer rendu public en décembre 2008, a récemment rappelé que **« l'obsolescence du FAR [...] ainsi que les contraintes légales relatives au respect des libertés individuelles, obligent la gendarmerie nationale à arrêter l'exploitation et l'administration de ce traitement ⁽¹⁾ »**, vos rapporteurs ont pu constater que le FAR était toujours alimenté et consulté, comme s'il ne devait jamais disparaître. De l'aveu même de certains gendarmes, ce n'est que contraints et forcés qu'ils se sépareront, le moment venu, du FAR. Or, l'échéance fixée au 24 octobre 2010 exige que les brigades intègrent dans leur fonctionnement la fin programmée du FAR.

De manière générale, vos rapporteurs ont en effet pu constaté, au cours de la mission, un profond décalage entre, d'une part, les discours officiels, plutôt optimistes, assurant que tout sera mis en œuvre pour une disparition effective du FAR au 24 octobre 2010 et, d'autre part, le manque d'information des gendarmes sur le terrain, qui n'ont reçu, à ce jour, **aucune directive détaillant les modalités et les critères de destruction, d'archivage et de transfert des 60 millions de fiches existantes**. Cette absence de directives claires et précises sur le devenir du FAR soulève d'autant plus d'inquiétudes et de doutes sur la fin programmée du FAR que le travail de tri des informations existantes ⁽²⁾ s'annonce très long et laborieux. Certains gendarmes ont même affirmé qu'il était **« impossible de trier le FAR »**. Ainsi, lorsque des brigades territoriales fusionnent, les armoires contenant les FAR des différentes brigades sont simplement juxtaposés, à défaut de pouvoir réaliser un véritable tri de chacune des fiches individuelles. Si ce travail de tri et d'apurement ne peut être réalisé au niveau local, il est difficilement

⁽¹⁾ Au terme de la période transitoire qui a commencé en 2004 et dont l'échéance est fixée au 24 octobre 2010, le FAR sera supprimé.

⁽²⁾ 60 millions de fiches, impliquant 20 millions de personnes.

imaginable qu'il puisse être mené à bien au niveau national, et ce avant le 24 octobre 2010.

Proposition n° 55

Définir au plus vite la nature du fichier qui aura vocation à remplacer le fichier alphabétique de renseignements (FAR) en octobre 2010, en déterminant avec précision la finalité assignée à ce nouveau traitement ainsi que la description générale de ses fonctions, les catégories de données à caractère personnel enregistrées, leur origine et les catégories de personnes concernées.

c) La fin du FAR : une annonce sans véritable anticipation

Si la disparition du FAR ressemble à l'horizon, s'éloignant au fur et à mesure que l'on s'en rapproche, la gendarmerie nationale envisage aujourd'hui **deux perspectives pour régler la question du devenir du FAR.**

La première repose sur l'idée de **la *tabula rasa*** : il serait procédé, d'une part, à la destruction complète des 60 millions de fiches existantes dans le FAR et, d'autre part, à l'alimentation *ab initio* d'un nouveau fichier vierge. En tout état de cause, **cette hypothèse de travail reste peu convaincante.** En effet, l'affaiblissement durable de la mémoire et de la connaissance de la gendarmerie, qui résulterait de la destruction complète du FAR, serait dommageable à l'action des gendarmes de manière générale et notamment à la sécurité de leurs interventions sur le terrain.

La deuxième hypothèse de travail consiste dans **l'examen et le tri manuels de chacune des soixante millions de fiches**, afin de déterminer celles qui doivent être détruites et celles qui doivent être archivées. Si, à ce jour, aucune directive spécifique n'a été édictée afin de définir les modalités de transfert, de destruction et d'archivage, **seules seraient reprises et conservées**, en l'état actuel, **les fiches des personnes susceptibles de troubler la sécurité des interventions des gendarmes.** Or, selon les estimations de la gendarmerie, seules 10 % des fiches existantes répondraient à ce critère. Si des directives doivent être prochainement diffusées et publiées par la direction générale de la gendarmerie nationale en ce sens, le général Jean-Régis Vechambre, lors de son audition par vos rapporteurs, a suggéré que les données qui ne seront pas reprises dans la nouvelle application en remplacement du FAR seront probablement détruites. En effet, il apparaît de manière assez nette que ces données ne seront pas versées aux archives nationales. Cette hypothèse est d'autant plus vraisemblable que **Mme Élisabeth Rabut, chef de l'inspection générale des Archives de France, a insisté, lors de son audition, sur le fait que le périmètre de sa mission** visant à définir les modalités de transfert, d'archivage et de destruction du fichier des renseignements généraux **ne porte pas sur le FAR**, même si les recommandations méthodologiques de la mission pourront ensuite être adoptées par la gendarmerie, pour autant qu'elle en formule la demande.

Proposition n° 56

Établir dans les meilleurs délais des directives, à l'attention de l'ensemble des brigades territoriales de la gendarmerie nationale, précisant les critères ainsi que les modalités de transfert, de destruction et d'archivage des données contenues dans le FAR, afin que sa disparition soit pleinement effective au 24 octobre 2010.

Quelle que soit l'hypothèse de travail retenue, **l'objectif est de parvenir, en 2010, à un fichier informatique, à la voilure et à la volumétrie réduites**, ne reposant plus sur la logique de la brigade du lieu de naissance et **recentré sur deux publics prioritaires**. Le premier serait constitué par les personnes présentant un risque pour la sécurité des interventions des gendarmes ainsi que la population en général (détenteurs de chiens dangereux, détenteurs d'armes, personnes violentes, etc.). Les informations concernant ces personnes auraient une visibilité nationale. Le second public visé concernerait les personnes qui, nécessitant des mesures de sécurité ou de surveillance particulières, demandent à être recensées (opération « *Tranquillité vacances* », personnes âgées isolées, résidences secondaires). Ces informations auraient, pour leur part, une visibilité seulement départementale.

Ce nouvel outil, qui contiendrait **au maximum 5 millions de fiches**, serait intégré dans le futur fichier d'« *aide au traitement harmonisé de la protection de la population et de la prévention des troubles* », connu sous le nom d'ATHÉNA. Cette application comporterait, entre autres, un « module FAR », qui offrirait un cadre général normé commun à l'ensemble des brigades. L'ambition qui préside à la mise en œuvre de ce module FAR est double : sécuriser, au niveau national, les interventions des gendarmes et approfondir, au niveau local, la connaissance de la circonscription dans laquelle est implantée la brigade territoriale.

L'enjeu est donc, à terme, d'**assurer une traçabilité parfaite et globale de toutes les consultations du module FAR**, à vocation tantôt locale, tantôt nationale, ce qui nécessite au préalable de clarifier les besoins et de distinguer ce qui relève ou non d'un échelon de proximité.

Alors que le système actuel permet de fichier « *le tout venant* » en raison d'une gestion uniquement manuelle, **le FAR rénové définira précisément les catégories de personnes qui pourront effectivement être recensées** dans le futur fichier. Ainsi, les personnes ne correspondant pas à ces catégories préalablement définies, tant sur le plan juridique qu'informatique, ne pourront être fichées, le logiciel disposant d'un dispositif de contrôle informatique des données saisies. À cet égard, les gendarmes rencontrés lors des divers auditions et déplacements ont exprimé leur **Crainte d'assister à un « affaiblissement de la mémoire et de la connaissance »**, dommageable à l'action de la gendarmerie.

En effet, les finalités du FAR évoluant et se recentrant notamment sur la sécurisation des interventions, certaines informations ne seront plus recensées.

Alors qu'à l'échelon de chaque brigade territoriale, les nouveaux résidents étaient tous fichés au FAR à leur arrivée, ils ne seront plus recensés à l'avenir avec le nouveau système. De la même manière, une personne qui se présentera en 2010 à la gendarmerie, par exemple pour déclarer le vol de son véhicule, ne sera plus référencée au FAR. La seule trace qui sera conservée de son passage et de l'infraction dont elle a été victime se trouvera dans la plainte ou la procédure (procès-verbal intégré dans l'application BB 2000 et bientôt PULSAR). Ainsi, certains gendarmes ont avancé l'idée que la connaissance du terrain et de la population acquise par la gendarmerie à l'échelon de chaque brigade est susceptible d'être remise en cause par le nouveau système. Il convient toutefois de rappeler que le bulletin de service retrace d'ores et déjà cette activité (à savoir, les noms et identités des personnes qui se présentent à la brigade) et que **la perte d'information et de mémoire, souvent invoquée, relève plus de la nostalgie que de la réalité.**

3. La mort des fichiers de police

La disparition d'un fichier de police n'est jamais neutre, puisqu'elle touche directement les services de police et de gendarmerie dans l'accomplissement de leurs missions et qu'elle implique le plus souvent la mise en place d'un nouvel outil, jugé plus performant. La polémique suscitée par la création d'EDVIGE, en remplacement du fichier des renseignements généraux, et la confusion qui entoure la fin annoncée du FAR sont autant d'exemples de la **nécessité de porter au cœur du débat public la question de la disparition des fichiers de police.**

Aussi vos rapporteurs proposent-ils que **la disparition des fichiers de police, devenus obsolètes et ne répondant plus à leur vocation originelle, ne puisse être prononcée que par une loi expresse.** En effet, le législateur, pour chaque fichier de police dont la disparition est envisagée, doit pouvoir débattre publiquement des besoins et des attentes des services opérationnels de police et de gendarmerie, au regard notamment de l'évolution des nouvelles technologies de l'information et de la communication. En outre, **faire de la loi le seul vecteur normatif pouvant mettre fin à l'existence d'un fichier de police** permettra au législateur d'évaluer la pertinence et l'efficacité de ce traitement de données, au regard des finalités qui avaient initialement présidé à sa création.

Proposition n° 57

Prononcer la destruction des fichiers par la loi. En conséquence, compléter l'article 26 de la loi du 6 janvier 1978, afin que seule la loi puisse mettre fin à l'existence des fichiers intéressant la sécurité publique et ceux qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.

EXAMEN EN COMMISSION

Au cours de la réunion du mardi 24 mars 2009, la Commission examine le rapport d'information de M. Jacques Alain Bénisti et Mme Delphine Batho sur les fichiers de police.

M. le président Jean-Luc Warsmann. À la suite de la polémique sur le fichier EDVIGE, la commission des Lois avait procédé à une série d'auditions, à l'issue desquelles elle avait adopté neuf recommandations, à l'unanimité. Il avait alors été décidé de poursuivre nos réflexions sur ce sujet en chargeant deux rapporteurs, l'un appartenant à la majorité, l'autre à l'opposition, de procéder à un travail d'ensemble sur les fichiers de police. Pour la première fois le Parlement traite de cette question de façon approfondie, et je souligne combien le travail réalisé s'appuie largement sur des déplacements, qui ont permis de s'attacher au fonctionnement concret des fichiers.

M. Jacques Alain Bénisti, rapporteur. Lorsque la commission des Lois, à l'initiative de son Président, nous a confié ce rapport d'information sur les fichiers de police, je dois avouer que je ne m'attendais pas à découvrir un sujet aussi vaste, mais combien passionnant. Le travail a été de ce fait un peu plus long qu'initialement prévu, et la liste des personnes auditionnées et des déplacements témoigne de notre volonté de disposer d'une vision aussi complète que possible du sujet. Nous avons ainsi, entre autres, visité une brigade territoriale de gendarmerie, une direction départementale de la sécurité publique, plusieurs services de la préfecture de police de Paris, deux parquets de TGI en région parisienne, des services techniques, sans oublier la CNIL, en assistant à deux séances de droit d'accès indirect, sur le STIC et sur le fichier des renseignements généraux.

C'était d'autant plus nécessaire qu'il s'agit du premier travail d'information sur le sujet réalisé par le Parlement ; de plus, nous n'avons pas voulu nous cantonner à l'audition des principaux responsables administratifs. Les déplacements dans les services, sur le terrain, nous ont permis de rencontrer les personnels qui alimentent, exploitent ou contrôlent les fichiers, ce qui nous a donné une vision plus vivante et concrète du sujet.

C'est d'ailleurs d'une certaine manière autour de l'idée de vie des fichiers que nous avons réalisé le rapport, en nous attachant aux différentes étapes logiques que sont notamment la création, l'alimentation, le contrôle et, éventuellement, la destruction des fichiers. Je peux d'ores et déjà souligner que, même si Delphine Batho et moi-même n'avons naturellement pas été toujours d'accord, nous avons pu arriver aux mêmes conclusions pragmatiques dans bien des cas, et sur un point en particulier qui est au cœur de l'ensemble de notre démarche. D'ailleurs, sur les 57 propositions, nous n'avons que quatre

divergences. D'une part, les services de police et de gendarmerie ont besoin de fichiers efficaces, d'autre part ceux-ci doivent respecter les libertés publiques, les deux points étant parfaitement complémentaires. La fiabilité et la performance des outils que sont les fichiers sont indissociables de la meilleure protection des libertés publiques et des données.

Je crois que le plus simple est d'exposer dès à présent les principales propositions du rapport, tout en soulignant les quelques points sur lesquels nous différons.

La première proposition, et sans doute la plus emblématique, concerne la clarification du cadre juridique. Actuellement, la création d'un fichier de police peut emprunter deux voies : la première est celle de la création par un acte réglementaire, après avis de la CNIL, conformément à la loi de 1978 relative à l'informatique et aux libertés. La seconde est celle de l'autorisation par un texte de loi spécifique, comme ce fut le cas pour le FNAEG ou, plus récemment, pour l'expérimentation du fichier des passagers aériens et pour le traitement automatisé des données signalétiques de véhicules (tous deux autorisés par la loi du 23 janvier 2007 relative à la lutte contre le terrorisme). En pratique, le recours à la loi est de plus en plus fréquent. Si seulement 17 % des fichiers de police ont été créés par la loi, la moitié des fichiers ayant une base législative l'ont été au cours des cinq dernières années. À notre sens, l'autorisation par la loi correspond davantage à l'article 34 de la Constitution, qui prévoit que la loi fixe les règles « *concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques* ». Une telle solution permettra, grâce au débat parlementaire, de bien exposer les objectifs poursuivis et de désamorcer des inquiétudes qui sont le plus souvent, selon moi, disproportionnées. En outre, cela sera l'occasion d'analyser les moyens consacrés effectivement au fonctionnement des outils, les études d'impact devant à ce titre être un instrument précieux.

Une fois le fichier autorisé par la loi, il restera naturellement une phase d'élaboration technique et réglementaire d'application. Plusieurs propositions visent à améliorer les rapports entre la CNIL et les services de police, ces derniers n'étant pas des plus satisfaisants, et c'est un euphémisme. Cette situation s'explique en partie par des différences d'approche, mais aussi par un cadre juridique qui ne favorise pas le dialogue entre l'autorité de contrôle et les utilisateurs de fichiers que sont la police et la gendarmerie. Il en résulte parfois de véritables blocages, coûteux en temps et en argent. Afin d'y remédier, il s'agira notamment de prévoir une mise en application par étape, associant ces deux partenaires très en amont, de façon à ne plus avoir à subir la situation actuelle où les services présentent à la CNIL un projet quasiment « bouclé » et pratiquement opérationnel. Celle-ci n'a, dès lors, le choix qu'entre accepter une forme de fait accompli ou demander des modifications qui peuvent parfois se révéler coûteuses et techniquement difficiles. De manière plus générale, il s'agit d'étendre une forme de procédure contradictoire entre les ministères et la CNIL, de façon à favoriser un dialogue constructif, un peu à la manière de ce qui existe pour les relations entre la Cour des comptes et les administrations qu'elle contrôle.

Nous nous sommes ensuite attachés à l'épineuse question de la protection des données sensibles, ce qui nous a amenés tout d'abord à préciser les caractéristiques de l'outil devant succéder au fichier des renseignements généraux (FRG). Par commodité, nous avons continué à le désigner sous l'appellation « EDVIRSP », puisque tel est le sigle prévu dans le projet de décret transmis au Conseil d'État.

Nous sommes arrivés à deux points de consensus. D'une part, il n'y a pas d'utilité à continuer à collecter dans le cadre d'un « fichier des personnalités » des données sur les personnes physiques ayant sollicité, exercé ou exerçant un mandat politique, syndical ou économique ou qui jouent un rôle institutionnel, économique, social ou religieux significatif. D'autre part, le futur fichier EDVIRSP autorisé par la loi visera deux finalités : d'une part, le fichage des personnes, groupes ou organisations qui, en raison de leur activité individuelle ou collective, peuvent porter atteinte à la sécurité des personnes et des biens, par le recours ou le soutien actif apporté à la violence, ainsi que les personnes entretenant ou ayant entretenu un lien direct et non fortuit avec celles-ci. D'autre part, un fichier des enquêtes administratives, en ne conservant que les dossiers ayant fait l'objet d'une décision défavorable. Nous avons en effet découvert que certains SDIG procédaient ainsi et la généralisation de cette pratique semble souhaitable.

En revanche, nous continuons à diverger sur quelques points s'agissant de ce fichier. Pour ma part, je considère qu'il faut conserver la notion d' « origine géographique » comme élément de signalement des personnes. Ensuite, s'agissant des mineurs, je suis favorable à la possibilité de les inscrire dans le fichier à partir de treize ans, y compris dans l'application très efficace développée par la préfecture de police de Paris et dénommée GEVI (pour gestion des violences urbaines). Celle-ci mérite d'ailleurs d'être mise à la disposition des autres SDIG. Il s'agit avant tout de jouer un rôle préventif en matière de délinquance et de criminalité des bandes, l'actualité récente en ayant largement souligné la nécessité. La ministre de l'Intérieur a annoncé la création d'un nouveau fichier pour lutter contre les bandes ; nous proposons de répondre à cet objectif tout simplement en procédant à la généralisation de GEVI.

Sur cette question des mineurs, nous sommes d'accord sur la création d'un droit à l'oubli, avec un effacement de l'élément au bout de trois ans à défaut de nouvel événement, le tout sous le contrôle d'un magistrat référent.

Enfin, pour terminer sur cette question des données sensibles, après bien des débats, nous sommes convenus de la nécessité de l'abandon de la typologie ethno- raciale actuellement utilisée dans le cadre des fichiers d'antécédents judiciaires STIC et JUDEX. La ministre de l'Intérieur a d'ailleurs lancé à cet effet une expérimentation d'une forme de portrait-robot, dans lequel la couleur de la peau est une composante au même titre que celle des yeux ou des cheveux. Il s'agit de remplacer par des critères objectifs et opérationnels une typologie

relevant seulement de l'usage et posant à l'évidence de nombreux problèmes, aussi bien juridiques que philosophiques.

J'en viens maintenant à des questions plus pratiques, portant sur le fonctionnement des fichiers.

De ce point de vue, les déplacements dans les services nous ont permis de mesurer les très nombreuses difficultés qui existent pour leur alimentation, et de faire en conséquence de nombreuses propositions. Pour le fichier des empreintes digitales (FAED), le principal problème réside dans le fait que la gendarmerie n'est pas dotée des terminaux de signalisation modernes dont dispose la police. Mais c'est dans le cas du STIC que les problèmes sont les plus frappants, le système étant daté techniquement et reposant largement sur des flux considérables de papiers et de nombreuses ressaisies manuelles, sources d'erreurs et consommatrices de ressources. Cette analyse est d'ailleurs conforme aux conclusions du rapport de contrôle que la CNIL a consacré récemment à ce fichier. Pour sortir de cette situation, il faut agir à la fois sur le flux et sur le stock.

En ce qui concerne le premier, il n'y a aucun intérêt à « stiquer » une personne dont le parquet a annoncé dans le cadre du traitement en temps réel qu'elle ne sera pas poursuivie compte tenu de l'insuffisance de charges. Les policiers doivent donc tenir compte de ces décisions, qui figurent d'ailleurs au procès-verbal, la plupart du temps. Pour le stock, nous avons constaté de visu la masse impressionnante des procédures à traiter, qui atteint par exemple presque deux ans de retard à Versailles dans le service régional chargé du contrôle de la qualité. Le recrutement ponctuel de contractuels s'impose, comme cela a d'ailleurs été fait pour réduire les retards accumulés dans la gestion du FNAEG. De même, il faut éviter que l'application ARIANE, qui doit remplacer le STIC et JUDEX, hérite du stock des erreurs accumulées. Le passage à un nouveau système plus moderne doit être l'occasion de repartir sur des bases plus saines, en engageant une forme d'« opération vérité » des fichiers d'antécédents, dont il ne faut pas se cacher qu'elle sera fort lourde.

Après la création et l'alimentation, le contrôle.

Dans le cas des fichiers d'antécédents judiciaires, il n'apparaît pas satisfaisant en pratique, qu'il s'agisse des mises à jour effectuées par les parquets au vu des suites judiciaires ou du contrôle exercé par la CNIL dans le cadre du droit d'accès indirect.

En ce qui concerne le rôle des parquets, il faudra véritablement améliorer CASSIOPEE de manière à ce que les échanges d'information soient plus efficaces lorsqu'il y a requalification des faits et pour mieux tenir compte des suites judiciaires. Par ailleurs, dans certains cas, les retards observés dans la mise à jour peuvent créer des situations très préjudiciables. Ainsi en est-il tout particulièrement pour les personnes voulant exercer un emploi dans le domaine de la sécurité privée et voyant l'emploi convoité leur échapper en raison de lourdeurs

administratives différant la décision sur l'agrément préalable. Il convient donc de réduire de trois mois à un mois le délai de traitement du dossier en cas de demande de mise à jour et, surtout, de créer une procédure de traitement en temps réel pour répondre aux demandes de mise à jour présentant un degré d'urgence particulièrement élevé. Cette tâche serait confiée à un magistrat référent des fichiers d'antécédents, d'une certaine manière sur le modèle de celui contrôlant le FNAEG.

C'est sur la question du contrôle par le procureur de la République que se situe notre dernier sujet de divergence. Dans l'état actuel de la législation, qui reprend sur ce point le décret de 1991, le procureur peut demander le maintien dans un fichier d'antécédent des données d'une personne qui a fait l'objet d'une relaxe ou d'un acquittement. À mon sens, il convient de maintenir une telle possibilité, qui peut s'avérer utile dans certains cas, notamment lorsqu'il s'agit de multirécidivistes.

Le deuxième contrôle exercé sur les fichiers revient à la CNIL, au travers de l'exercice du droit d'accès indirect. Là encore, le retard est considérable et il convient de s'attaquer au « stock » des recours par l'embauche ponctuelle de personnels. On peut également penser que le maintien de la lourde procédure de droit d'accès indirect ne se justifie pas s'agissant des victimes, qui devraient pouvoir bénéficier d'un droit d'accès direct à leurs données personnelles. Enfin, dans le cas particulier du contrôle des fichiers des services de renseignement dont les textes portant création ne sont pas publiés au *Journal Officiel*, comme dans sur le fichier CRISTINA exploité par la DCRI, nous proposons une transmission systématique de ces textes à la délégation parlementaire au renseignement.

Convaincus de l'utilité des fichiers, nous souhaitons que leurs finalités soient bien respectées.

Cela passe par un contrôle étroit des utilisations afin de lutter notamment contre la vente d'information, mieux connue en argot policier sous le nom de « tricoche ». En l'espèce, l'informatique est un atout car elle permet une grande traçabilité, ce qui n'était pas le cas avec les fichiers papiers. Les sanctions disciplinaires prononcées en la matière sont de plus en plus sévères et la publicité qui leur est donnée contribue à l'effet extrêmement dissuasif. Il reste à se doter en ce domaine d'outils plus modernes de détection en temps réel des comportements anormaux. Respecter les finalités, c'est aussi s'assurer que l'utilisation des fichiers d'antécédents judiciaires dans le cadre d'enquêtes administratives obéisse à une exigence particulière de discernement. À cet égard, nous pensons qu'il est utile de systématiser la pratique existant déjà dans certains départements et consistant, pour les services enquêteurs, à entendre la personne faisant l'objet d'une enquête administrative et figurant dans un fichier d'antécédent. Il s'agit ainsi qu'une simple « erreur de jeunesse » n'ait pas des conséquences démesurées.

Le respect des finalités doit aussi passer par la mise en place de fichiers ayant un objet bien défini et correspondant à un besoin clairement identifié des

enquêteurs. De ce point de vue, j'ai été impressionné par la qualité de deux outils développés récemment par la préfecture de police de Paris et destinés à opérer des rapprochements entre infractions. Le premier, CORAIL, vise à moderniser le traitement des télégrammes internes à la police judiciaire dits « dix points » ou « onze points », qui décrivent des infractions. Le second, LUPIN, permet de mieux lutter contre les cambriolages en mettant en évidence leur caractère sériel et en exploitant les données concernant les modes opératoires, recueillies par la police technique et scientifique sur les lieux d'infraction. Les deux démarches présentent des points communs : elles ont été initiées par les utilisateurs, pour répondre très précisément à leurs besoins ; les projets ont été réalisés en interne et très rapidement pour un coût modique, en utilisant les compétences informatiques des personnels. Il s'agit, à mon sens, d'un bon exemple du type de démarches à encourager pour améliorer le taux d'élucidation.

Pour terminer mon propos, je considère qu'il y a des cas où il faut assurer une bonne transition d'un fichier à l'autre, voire où il faut régler les conditions de la disparition d'un fichier.

Nous avons abordé ces questions, une fois encore, avec la volonté très claire de permettre aux services de police et de gendarmerie de travailler dans de bonnes conditions.

De ce point de vue, il faut mettre fin à un imbroglio juridique qui empêche actuellement les SDIG de fonctionner efficacement.

L'article premier du décret du 27 juin 2008 dispose que « *la collecte et l'enregistrement de nouvelles données dans [le fichier des renseignements généraux] sont interdits à compter du 1^{er} juillet 2008* ». Si le fichier des renseignements généraux ne peut plus être alimenté, il peut néanmoins être consulté jusqu'au 31 décembre 2009, date de sa disparition définitive. Seul pouvait donc être alimenté, à partir du 1^{er} juillet 2008 et en remplacement du FRG, le traitement EDVIGE. Or, la décision de retrait de ce nouveau fichier de renseignement, prise en octobre 2008 par la ministre de l'Intérieur et définitivement actée par le décret du 19 novembre 2008, a été accompagnée par une note de son directeur de cabinet rappelant que le retrait du décret du 27 juin 2008 ôtant « *rétroactivement toute existence juridique à EDVIGE* », il fallait en anticiper tous les effets de manière préventive et que de ce fait, je cite : « *il convient [...] de cesser toute alimentation ou consultation du fichier, et de retirer de ce fichier les données qui ont pu y être intégrées depuis la publication du décret* ». Au cours de nos déplacements, plusieurs agents et responsables des SDIG ont indiqué combien cette situation pratique et juridique était délicate et démotivante pour les services.

Nous proposons donc, dans l'attente d'une loi autorisant la création du futur fichier EDVIRSP, de permettre à titre provisoire et sur la base du décret de 1991, l'alimentation et la consultation du FRG.

Le second point délicat concerne la disparition programmée au 24 octobre 2010 du fichier alphabétique de renseignements (FAR) de la gendarmerie. Il s'agit d'un immense fichier papier qui fait, pour ainsi dire, partie des traditions de la gendarmerie. Or, alors que sa disparition est programmée par la loi, nous avons pu constater qu'il est toujours alimenté et que les personnels sont inquiets de la disparition de cet outil. Il faut dans les meilleurs délais, d'une part définir la nature du fichier destiné à succéder au FAR, d'autre part établir des directives précises à l'attention des brigades territoriales pour le transfert, l'archivage et la destruction de l'immense masse de données figurant dans ce fichier (60 millions de fiches et 20 millions de personnes...).

Mme Delphine Batho, rapporteure. Comme l'a noté mon collègue, nos travaux se sont étendus sur une durée de six mois et il s'agit d'une « première » dans l'histoire du Parlement. Pour autant, le sujet est tellement vaste que nous n'avons pas pu traiter de manière également exhaustive l'ensemble des fichiers. Nous nous sommes particulièrement attachés à des fichiers emblématiques des difficultés rencontrées, comme le STIC ou le FRG, mais de nombreux autres fichiers mériteraient à eux seuls un autre rapport d'information, notamment ceux qui concernent la politique d'immigration.

Si un rapporteur de la majorité et une rapporteure de l'opposition sont parvenus à se mettre d'accord sur 53 propositions communes sur un total de 57, c'est avant tout parce que nous avons porté une attention toute particulière aux réalités du fonctionnement des fichiers et, plus généralement, que nous partageons la conviction qu'un contrôle démocratique accru est nécessaire sur ce sujet.

Le constat de départ de nos travaux reposait sur les inquiétudes croissantes des citoyens résultant de la propension à créer de plus en plus de fichiers et du phénomène de massification de ces derniers. Les ambiguïtés et le manque de transparence du cadre juridique alimentent d'ailleurs ces inquiétudes, car il existe une grande diversité des modes de création de fichiers, par la loi, par le règlement, voire sans base juridique assez souvent.

Ensuite, il y a dans certains de ces fichiers des erreurs, tout particulièrement dans les fichiers d'antécédents judiciaires STIC et JUDEX, où figurent indûment de nombreuses personnes. Or, ces erreurs peuvent avoir des conséquences terribles, qu'il s'agisse de l'accès à des professions nécessitant un agrément administratif, que l'on estime à environ un million d'emplois, ou de l'obtention de la nationalité française. Nous avons également constaté une situation de blocage entre la CNIL et le ministère de l'Intérieur, préjudiciable tant à la qualité des textes réglementaires qu'à l'avancement des projets. Enfin, nous avons relevé des défaillances des contrôles, souvent faute de moyens, mais pas toujours.

L'idée centrale du rapport est que l'amélioration des droits des citoyens et des garanties va de pair avec une meilleure performance des outils. Or, les policiers et gendarmes ne disposent pas des instruments modernes nécessaires à

l'exercice de leurs missions. La proposition de réserver au législateur l'autorisation des fichiers de police aura une conséquence immédiate : s'agissant du successeur d'EDVIGE, nous demandons qu'il ne puisse être créé que par une loi, après un véritable débat parlementaire. En l'espèce, nous proposons de mettre fin au « mélange des genres » qui a été à l'origine des inquiétudes concernant EDVIGE, ce fichier mêlant alors plusieurs finalités très différentes : enquêtes administratives tout d'abord, fichage de militants politiques et associatifs ensuite, et nécessaire évaluation des menaces pour mieux anticiper la protection des personnes et des biens enfin. Il s'agira désormais de clairement distinguer les finalités et de ne pas les mélanger au sein d'un même fichier. S'agissant des violences urbaines, il n'y a pas lieu de créer un nouveau fichier, car il existe effectivement déjà un outil moderne au sein de la préfecture de police de Paris, permettant d'étudier les structures des réseaux et de l'économie souterraine. À notre grande surprise, la sous-direction de l'information générale n'en connaissait pas l'existence. La généralisation de cette application, développée en interne, évitera de lourdes procédures de passation de marché.

Je ne reviendrai pas en détail sur nos divergences, qui sont exposées dans le rapport, mais je souhaite souligner que j'estime nécessaire, pour faire face aux violences urbaines, que les SDIG, qui remplacent les renseignements généraux, puissent inscrire dans GEVI les mineurs de plus de treize ans qui figurent déjà dans des fichiers d'antécédents judiciaires. Cette proposition s'explique par le fait que nous avons demandé à plusieurs responsables policiers quel pourrait être le critère objectif permettant l'inscription d'un mineur dans un tel fichier de renseignement et qu'aucune réponse satisfaisante ne nous a été apportée. Nous souhaitons que le Gouvernement retienne cette proposition.

Par-delà la nécessité de renforcer les contrôles, avec, d'une part, la mise en place d'une procédure de traitement en temps réel des demandes de mises à jour en fonction des suites judiciaires et, d'autre part, l'accroissement des moyens de la CNIL – la France étant mal classée en Europe si l'on s'attache au ratio entre personnels des autorités de contrôle et population – je souhaite faire encore deux remarques.

Dans le rapport, 20 propositions sur 57 portent sur le STIC et sur JUDEX. Le STIC est le plus massif, puisque 5,4 millions de personnes mises en cause y figurent aujourd'hui, et il s'agit de loin du fichier qui pose le plus de problèmes. Lors de la visite du service régional de documentation judiciaire de Versailles, nous avons pu constater ce que les deux ans de retard représentent : quatre grandes pièces entièrement consacrées, du sol au plafond, au stockage de piles de papiers. Nous l'avons décrit dans le rapport, au même titre de l'ensemble des processus qui peuvent conduire à des erreurs. Selon moi, on ne peut pas séparer les défaillances du STIC de la « politique du chiffre » qui a été mise en place dans la police nationale. En effet, l'un des problèmes majeurs est que l'outil d'alimentation du STIC et l'outil statistique sont identiques, ce qui conduit trop souvent en pratique à inscrire dans le fichier des personnes placées en garde à vue, alors même que les investigations menées à cette occasion ont pu contribuer à les mettre hors de

cause. Ainsi, dans certaines affaires où plusieurs personnes étant placées au même moment en garde à vue pour des violences, celles qui sont relâchées immédiatement à l'initiative du parquet faute de charges demeurent en fait plus longtemps dans les fichiers d'antécédents que celles pour lesquelles la décision de classement sans suite intervient plus tard, la décision du procureur de la République se traduisant dans ce dernier cas plus rapidement par un effacement des données. De même, nous avons reproduit des échanges de courriers édifiants qui montrent qu'alors que les fichiers d'antécédents sont placés sous le contrôle du procureur de la République, il peut arriver que les services gestionnaires refusent de tenir compte des demandes que ceux-ci leur adressent.

Ma deuxième remarque porte sur les enjeux internationaux considérables en matière de fichiers et de protection des données personnelles, comme par exemple pour les données PNR (*Passenger Name Records*), lesquelles ont d'ailleurs donné lieu à un rapport d'information de notre collègue Guy Geoffroy. Dans ce contexte, la France a tout intérêt à faire valoir sa propre approche des fichiers et de la protection des données personnelles. Notre modèle est en effet très différent de celui mis en œuvre dans le monde anglo-saxon ; ainsi, nous n'avons pas suivi le modèle britannique en matière de fichier ADN et disposons de ce fait d'un outil bien mieux encadré et bien plus fiable. Nous devons davantage mettre en avant cette conception à l'échelle internationale, ainsi que le fait que nous faisons davantage confiance à l'enquêteur qu'à la machine, laquelle ne pourra jamais le remplacer. Ce modèle français du fichier de police existe de fait empiriquement, mais il n'est pas clairement assumé.

Enfin, par-delà les défaillances relevées dans le rapport, même sous réserve de l'organisation d'une « opération nettoyage » des fichiers d'antécédents, force est de constater que le ministère de l'Intérieur a du mal à gérer l'acquisition ainsi que la mise en place de nouveaux systèmes modernes et à faire face à leur coût croissant. Si l'on souhaite une meilleure protection des données personnelles et des libertés et en même temps des outils plus pointus et plus modernes pour les policiers, cela nécessitera d'y consacrer les moyens budgétaires nécessaires. À cet égard, il faut souligner que c'est le fichier des brigades spécialisées, qui constitue l'outil chargé de traiter la criminalité et la délinquance organisées les plus dangereuses, qui fait face à l'obsolescence la plus certaine.

M. le Président. Le document issu des réflexions de nos rapporteurs comporte un certain nombre de points remarquables. J'attire votre attention sur le tableau classant les fichiers en fonction de leur base juridique, qui recense un nombre de fichiers supérieur à celui recensé par le rapport Bauer, ce qui illustre l'exhaustivité des investigations auxquelles nos collègues ont procédé.

De même, je constate que les rapporteurs ont mis en exergue des outils performants, développés en interne par certains services de l'État, au sein de la préfecture de police de Paris notamment, sans que les administrations centrales aient connaissance de l'utilité de ces instruments. De la sorte, ce rapport d'information devrait permettre de généraliser ces outils qui, si notre Commission

ne s'était pas saisie du sujet, seraient probablement restés sous-exploités et méconnus de leurs utilisateurs potentiels.

M. Philippe Gosselin. Je tiens à saluer le travail des rapporteurs. Je représente notre assemblée à la CNIL et je peux vous assurer que le sujet des fichiers de police nous intéresse et nous concerne. Un rapport de la CNIL, remis au Premier ministre le 20 janvier 2009, a été consacré au STIC. Il pointe les mêmes problèmes que les rapporteurs et formule les mêmes critiques à l'encontre de ce fichier, qui a un impact sur l'accès de nos concitoyens à un million d'emplois.

Je souscris à la nécessité de développer le contrôle parlementaire sur les fichiers de police. Le principe de leur création par la loi me paraît pertinent, même si l'on peut débattre du degré de détail des dispositions législatives à adopter.

La suggestion de renforcement du rôle de la CNIL constitue également une bonne proposition. Depuis 1978, cette autorité administrative indépendante a démontré de la qualité de son travail. Il faut néanmoins la doter de moyens adaptés. Ses contrôles sont aujourd'hui pour l'essentiel cantonnés à l'Île-de-France et à la région de Marseille. Il serait utile qu'elle puisse être en mesure d'intervenir aussi sur l'ensemble du territoire national.

M. le Président. Les rapporteurs se prononcent en faveur d'une base législative pour tous les fichiers de police. Il me semble que nous sommes appelés à prendre clairement position sur ce sujet.

M. Christophe Caresche. Lors de sa venue devant notre Commission, le président de la CNIL, M. Alex Türk, s'est plutôt prononcé en faveur du Parlement en présentant la CNIL comme le « bras armé » de celui-ci sur les questions relatives aux données à caractère personnel.

M. Jacques Alain Bénisti, rapporteur. La création des fichiers par la loi ne se fera pas sans consultation de la CNIL, tout en permettant au nécessaire débat de se tenir en toute transparence.

M. Bernard Derosier. Je suis personnellement favorable à ce que la loi garantisse de manière démocratique le fonctionnement de tout instrument nécessaire à la protection de la République, comme c'est le cas des moyens à la disposition de la police. Il faut que le Parlement, qui représente la Nation, soit désormais à l'origine de la création de fichiers de police, tout particulièrement au regard des déviances qui ont pu être constatées.

Tirant les leçons de mon expérience du fonctionnement de la commission nationale de contrôle des interceptions de sécurité, où majorité et opposition sont représentées de manière à garantir le pluralisme de l'institution, j'estime néanmoins que la CNIL gagnerait à faire davantage de place à l'opposition.

Mme Delphine Batho et M. Jacques Alain Bénisti, rapporteurs. C'est la proposition n^o 1 du rapport.

M. Bernard Derosier. Pour le reste, l'indépendance de la CNIL ne retire rien à la nécessité d'une intervention du législateur sur la question des fichiers.

M. Sébastien Huyghe. À l'instar de Philippe Gosselin, je suis membre de la CNIL. Je m'associe donc bien volontiers aux propos de mon collègue.

Je souhaiterais tout d'abord savoir si nos rapporteurs ont des divergences d'appréciation par rapport au rapport de la CNIL sur le STIC.

Je me félicite ensuite de l'appui exprimé par nos rapporteurs au travail du président Alex Türk s'agissant de l'accroissement des moyens de financement de la CNIL. La mise en place d'un système de redevance me semble constituer une piste intéressante de financement complémentaire, sans affecter l'indépendance de l'institution. Je salue donc la contribution des rapporteurs à cette réflexion.

Je suis également favorable à la création des fichiers de police par la loi. Les membres de la CNIL sont même plus ambitieux, puisqu'ils militent pour une constitutionnalisation du principe de protection des données à caractère personnel, dans le cadre d'une révision du Préambule de la Constitution.

S'agissant enfin de la proposition relative à la composition de la CNIL, je forme le vœu que cette idée ne marque pas une certaine forme de défiance à l'égard de son travail. L'indépendance des avis que celle-ci a formulé ces dernières années n'a jamais été mise en doute. J'ajoute que le Sénat a désigné un représentant de l'opposition, lors du dernier renouvellement. Enfin, même si les appartenances politiques ne sont pas affichées par ses membres non parlementaires, je peux vous assurer que la représentation des différentes sensibilités et opinions au sein de la CNIL est très équilibrée.

M. Noël Mamère. Un certain consensus semble se dégager sur l'intérêt de confier exclusivement à la loi le soin de créer les fichiers de police. Cela ne doit pas nous empêcher de nous insurger contre l'inflation de ces instruments. L'un des rapporteurs a, à cet égard, cité des chiffres effrayants en évoquant le nombre de 60 millions de fiches et 20 millions de personnes concernées.

Compte tenu de l'évolution des technologies, nous ne pouvons que constater que la CNIL n'a pas les moyens de contrôler de manière efficace le recours de plus en plus étendu à de tels instruments. Même si le FNAEG ne présente pas un caractère aussi intrusif que les fichiers génétiques anglo-saxons, il reste en soi très dangereux. Il a notamment fait l'objet de détournements par certains laboratoires procédant à des recherches sur les origines ethniques des personnes qui y figurent.

Au total, la représentation nationale doit tout entreprendre pour éviter la multiplication de ces fichiers de police. À cet égard, le rapport d'information qui

vient de nous être présenté doit constituer un point d'appui nous permettant d'aller plus loin.

Mme Delphine Batho, rapporteure. S'agissant du rapport de la CNIL sur le STIC, nous y faisons bien évidemment référence dans notre rapport. Nous avons procédé aux mêmes constatations que la CNIL même si nous n'avons pas eu les moyens de faire un contrôle global, permettant d'établir des statistiques d'erreurs. En revanche, nous avons souhaité étudier précisément quel est le processus qui aboutit aujourd'hui à ces erreurs tant au stade de l'alimentation, de l'enrichissement que de la prise en compte de la requalification juridique des faits, cette dernière n'étant pas neutre en termes de durée de conservation des données. Nous allons dans le même sens que la CNIL en ce qui concerne le STIC, tout en allant plus loin dans notre rapport.

S'agissant de la nécessité d'une loi pour créer tout fichier de police, il aurait pu être possible bien auparavant de s'interroger sur le point de savoir si la question des fichiers de police ne relève pas de l'article 34 de la Constitution. Mais, c'est la loi du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés qui renvoie elle-même à la voie réglementaire pour la création des fichiers de police. En outre, l'un des problèmes vient de ce que la loi du 6 août 2004 a changé la nature l'avis de la CNIL : désormais, il est simplement rendu public et ne lie plus le Gouvernement. Lors des débats, Alex Türk avait alors considéré que la simple publicité de cet avis, désormais consultatif, aurait un effet suffisamment dissuasif sur le Gouvernement. Or, cela n'a pas toujours été le cas, comme pour le fichier EDVIGE ou le fichier DELPHINE relatif aux passeports biométriques. Notre proposition vise à ce que, lors de l'élaboration de tout projet ou proposition de loi autorisant la création d'un fichier de police, l'avis de la CNIL soit publié, afin d'éclairer le débat parlementaire. C'est d'une certaine manière ce qui s'est passé à l'occasion des débats sur la loi du 23 janvier 2006 relative à la lutte contre le terrorisme, dans la mesure où le rapporteur, dans le cadre de ses travaux préparatoires, avait auditionné la CNIL et où le législateur avait tenu compte de certaines de ses observations.

Je voudrais également faire deux remarques. La première sur l'inflation des fichiers. On parle souvent de « prolifération » des fichiers de police. Mais, en réalité, le plus important problème réside dans la massification du nombre de personnes inscrites dans les fichiers de police. Si nous ne voulons pas avoir un méta fichier qui mélange toutes les finalités, il faut se résoudre à avoir des outils différents, répondant chacun à l'objectif qui leur est assigné. Le nombre de fichiers ne pose ainsi pas de problème en soi, à partir du moment où chacun d'eux répond à une finalité précise.

Par ailleurs, de ce que nous avons pu constater au cours de nos travaux, il n'y a pas actuellement d'interconnexions entre les fichiers de police. Les seules qui existent sont des interconnexions en quelque sorte humaines. Ainsi, lorsqu'ils veulent vérifier, dans le cadre de leurs enquêtes, dans quels fichiers une personne est inscrite, les policiers doivent actuellement passer par le portail CHEOPS pour

consulter successivement et de manière séparée les différents fichiers : STIC, FNAEG, FAED, FIJAIS, etc.

Je voudrais également revenir sur le FNAEG. Si la remarque de M. Noël Mamère sur les détournements des prélèvements génétiques par certains laboratoires procédant à des recherches sur les origines ethniques des personnes figurant au FNAEG est avérée, c'est très inquiétant. Cependant, à ce jour, ne sont inscrits dans le FNAEG que les segments non codants. Ainsi, le seul élément qui peut être identifié est le sexe de l'individu. Pour le reste, il est impossible de faire des sélections ou des recherches à partir d'autres caractéristiques, comme l'origine ethno-raciale.

En outre, le FNAEG offre des garanties importantes. L'inscription dans ce fichier se fait suivant une saisie en double aveugle, pour éviter tout risque d'erreur. Tous les dossiers pour lesquels il existe une suspicion de risque d'erreurs sont bloqués et ne peuvent être inscrits dans le fichier. Enfin, ce n'est pas l'ordinateur qui associe une trace à un individu, mais c'est un expert biologiste qui fait les rapprochements. L'ordinateur ne fait que proposer des choix de rapprochements, qui sont validés ou non par l'expert biologiste. Le FNAEG a cependant connu des problèmes. Il a notamment dû faire face à une croissance rapide en raison de l'extension de son domaine par la loi du 18 mars 2003 pour la sécurité intérieure. Il faut également reconnaître que beaucoup de délinquants portent aujourd'hui des gants et, à l'avenir, l'ADN va progressivement remplacer les empreintes digitales. Enfin, tenant compte de la jurisprudence de la Cour européenne des droits de l'homme et d'une récente circulaire du ministère de la Justice, nous faisons une proposition visant à mettre fin à des prélèvements biologiques qui sont manifestement disproportionnés pour certains délits.

M. Jacques Alain Bénisti, rapporteur. Pour être complémentaire, j'ajouterai que nous faisons des propositions allant dans le sens d'un renforcement des moyens de la CNIL avec l'instauration d'une petite redevance sur les utilisateurs de l'informatique, du secteur privé comme du secteur public. En revanche, nous sommes opposés à la régionalisation de la CNIL, pour éviter que les effectifs du siège ne soient dilués sur l'ensemble du territoire et que le contrôle de la CNIL perde ainsi en efficacité. S'agissant de la constitutionnalisation de la protection des données personnelles, il faudra attendre une éventuelle réforme de la Constitution pour y procéder. Concernant le pluralisme de la composition de la CNIL, nos travaux, qui ont associé un rapporteur de la majorité et une rapporteure de l'opposition, qui semblaient au départ très éloignés, prouvent que, grâce à ce pluralisme, on arrive à « déminer » les problèmes en matière de création des fichiers de police. Enfin, je suis d'accord avec Mme Delphine Batho sur le fait que les dérives ethno-raciales, évoquées par M. Noël Mamère, ne peuvent se manifester dans le cadre du FNAEG en raison de l'enregistrement des seuls segments non codants. Mais nous sommes prêts à examiner les faits qui viennent de nous être rapportés.

M. Sébastien Huyghe. Je tiens à souligner que le projet de régionalisation des services de la CNIL ne vise pas à dépouiller le siège de ses moyens, mais bien à allouer des personnels supplémentaires dans les régions, au plus près des besoins. La création d'antennes régionales permettra à la CNIL de se projeter sur tout le territoire et de pallier ainsi la carence soulignée précédemment par M. Philippe Gosselin.

M. le Président. Avant que nos échanges s'achèvent, la question du traitement en temps réel des demandes de mise à jour des données figurant dans les fichiers d'antécédents judiciaires mérite d'être évoquée. Il importe effectivement de prévoir une telle mesure, afin d'éviter d'éventuels préjudices pour des personnes innocentes y figurant par erreur.

Sur proposition du président Jean-Luc Warsmann, la Commission autorise conformément à l'article 145 du Règlement, le dépôt du rapport d'information en vue de sa publication et charge les rapporteurs de l'élaboration d'une proposition de loi reprenant les mesures d'ordre législatif qu'ils ont recommandées.

SYNTHÈSE DES PROPOSITIONS

CLARIFIER LE CADRE JURIDIQUE

Proposition n° 1

Modifier l'article 13 de la loi du 6 janvier 1978 relatif à la composition de la CNIL, afin que les deux députés et les deux sénateurs, membres de l'autorité de contrôle, soient désignés respectivement par l'Assemblée nationale et par le Sénat, « *de manière à assurer une représentation pluraliste* ».

Proposition n° 2

Seule la loi doit pouvoir autoriser la création d'un fichier de police. En conséquence, modifier l'article 26 de la loi du 6 janvier 1978, afin que les fichiers ou toute catégorie de fichiers intéressant la sécurité publique et ceux qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ne soient autorisés que par la loi.

Proposition n° 3

Toute loi autorisant la création d'un fichier de police devra au minimum préciser l'identité du responsable du traitement, la finalité et la dénomination du traitement ainsi que la description générale de ses fonctions, le service chargé de la mise en œuvre, le service auprès duquel s'exerce le droit d'accès (direct ou indirect), les catégories de données à caractère personnel enregistrées, leur origine et les catégories de personnes concernées par le traitement, les catégories de personnes qui ont accès aux informations enregistrées, les destinataires des informations, les rapprochements et interconnexions, la durée de conservation des données.

Proposition n° 4

L'avis de la CNIL sur tout projet de loi autorisant la création de fichiers de police est rendu public et transmis au Parlement simultanément au dépôt, sur le bureau de l'Assemblée nationale ou du Sénat, du projet de loi autorisant la création d'un fichier de police.

Proposition n° 5

Les projets ou propositions de loi autorisant la création de fichiers de police doivent être accompagnés d'une étude d'impact appréciant le volume du fichier considéré ainsi que sa finalité, au regard de l'ensemble des fichiers d'ores

et déjà existants. La CNIL sera associée à la réalisation de ces études d'impact préalables.

Proposition n° 6

Les projets de loi autorisant la création de fichiers de police doivent prévoir une clause de rendez-vous dans le temps, afin que le Parlement opère à moyen et long terme une évaluation du fichier considéré. Au terme de cette évaluation, qui doit faire l'objet d'un débat en séance publique, le Parlement peut décider de mettre fin, par la loi, au fichier concerné, si la finalité qui avait initialement présidé à sa création n'est plus démontrée.

Proposition n° 7

Améliorer les relations de travail entre la CNIL et le ministère de l'Intérieur grâce à la transmission systématique de l'avant-projet de rapport annuel de la CNIL au Ministère de l'Intérieur, afin qu'il puisse formuler toutes les réponses nécessaires aux différentes observations de la CNIL le concernant. L'objectif est de créer, sur le modèle de la Cour des Comptes, une procédure contradictoire entre l'autorité de contrôle et les services de police et de gendarmerie, où la première, avant la publication de son rapport définitif, recueille les réponses des seconds aux observations qui leur sont adressées.

Proposition n° 8

Étendre la procédure écrite et contradictoire, entre la CNIL et le ministère de l'Intérieur, à l'ensemble des traitements de données à caractère personnel mis en œuvre pour le compte de l'État.

Proposition n° 9

Créer une procédure de mise en application par étapes des fichiers de police sous le contrôle de la CNIL. En conséquence, introduire dans la loi du 6 janvier 1978 une disposition nouvelle prévoyant que les fichiers relevant de l'article 26 (ceux intéressant la sécurité publique et ceux ayant pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté), une fois autorisés par le législateur et en amont de la publication du décret d'application de la loi, font l'objet, sur le plan technique, d'une procédure de mise en application par étapes, afin qu'ils puissent, à chaque étape clé de leur élaboration et lors de rendez-vous obligatoires, faire l'objet d'une validation conjointe entre la CNIL et le ministère de l'Intérieur.

MIEUX PROTÉGER LES DONNÉES SENSIBLES

Proposition n° 10

Seule la loi peut autoriser un fichier de police à déroger à l'interdiction de principe, posée par l'article 8 de la loi du 6 janvier 1978, de contenir des données sensibles (origines raciales ou ethniques, opinions politiques, philosophiques ou religieuses, appartenance syndicale et données relatives à la santé et à la vie sexuelle) et ce dans la stricte mesure où les finalités du fichier l'exigent. Modifier en conséquence le IV de l'article 8 de la loi du 6 janvier 1978.

Proposition n° 11

Le futur fichier EDVIRSP devra être créé par la loi.

Proposition n° 12

D'une part, le fichier EDVIRSP ne concernera que « *les personnes, groupes, organisations et personnes morales qui, en raison de leur activité individuelle ou collective, peuvent porter atteinte à la sécurité des personnes et des biens, par le recours ou le soutien actif apporté à la violence, ainsi que les personnes entretenant ou ayant entretenu un lien direct et non fortuit avec celles-ci* ».

D'autre part, un fichier distinct, relatif aux personnes « *faisant l'objet d'enquêtes administratives* » sera créé. Ce traitement de données ne recensera que les personnes ayant fait l'objet d'une décision administrative défavorable.

Proposition n° 13

Prévoir que la collecte et la conservation de données sensibles, dont celles enregistrées dans la catégorie « *signalement* », soient strictement interdites dans le fichier relatif aux enquêtes administratives défavorables.

Proposition n° 14 de votre Rapporteur

Conserver, au titre des données sensibles susceptibles d'être collectées et conservées dans EDVIRSP, la notion d'« *origine géographique* » comme élément de signalement des personnes.

Proposition n° 14 bis de votre Rapporteur

Limiter les données sensibles collectées et conservées dans EDVIRSP au titre du signalement aux seuls « *signes physiques particuliers, objectifs et inaltérables* ».

Proposition n° 15

Abandonner définitivement l'inscription dans tout fichier, quelles que soient sa nature et sa portée, des personnes physiques ayant sollicité, exercé ou exerçant un mandat politique, syndical ou économique ou qui jouent un rôle institutionnel, économique, social ou religieux significatif.

Proposition n° 16 de votre Rapporteur

Pourront être collectées et conservées dans le futur fichier EDVIRSP les données relatives aux mineurs de plus de treize ans lorsqu'« *en raison de leur activité individuelle ou collective, ils peuvent porter atteinte à la sécurité des personnes et des biens* ».

Proposition n° 16 bis de votre Rapporteur

Ne pourront être collectées et conservées dans le futur fichier EDVIRSP et à la seule fin de les inscrire dans l'application « Gestion des violences urbaines » (GEVI), que les données relatives aux mineurs de plus de treize ans qui, d'une part, sont référencés dans un fichier d'antécédents judiciaires (STIC ou JUDEX) et, d'autre part, peuvent, « *en raison de leur activité individuelle et collective, porter atteinte à la sécurité des personnes et des biens, par le recours ou le soutien actif apporté à la violence, ainsi que les personnes entretenant ou ayant entretenu un lien direct et non fortuit avec ceux-ci* ».

Proposition n° 17 de votre Rapporteur

Élargir l'application GEVI, actuellement développée et gérée par la préfecture de police, aux mineurs qui, « *en raison de leur activité individuelle ou collective, peuvent porter atteinte à la sécurité des personnes et des biens* ».

Proposition n° 17 bis de votre Rapporteur

Élargir l'application GEVI, actuellement développée et gérée par la préfecture de police, aux mineurs de plus de treize ans, qui, d'une part, sont référencés dans un fichier d'antécédents judiciaires (STIC ou JUDEX) et qui, d'autre part, peuvent, « *en raison de leur activité individuelle et collective, porter atteinte à la sécurité des personnes et des biens, par le recours ou le soutien actif apporté à la violence, ainsi que les personnes entretenant ou ayant entretenu un lien direct et non fortuit avec ceux-ci* ».

Proposition n° 18

Doter les services départementaux d'information générale (SDIG), situés dans des départements particulièrement confrontés à la gestion des violences urbaines, d'un fichier GEVI à vocation départementale.

Proposition n° 19

Dans le cas plus spécifique de l'Île-de-France, mettre en place un fichier GEVI à vocation régionale, en permettant l'alimentation et la consultation du fichier GEVI par les fonctionnaires spécialement habilités des services départementaux d'information générale de la région d'Île-de-France.

Proposition n° 20

Introduire, dans les fichiers de renseignement, un droit à l'oubli pour les mineurs de plus de treize ans avec effacement de l'élément enregistré le jour du troisième anniversaire de son enregistrement, à défaut de nouvel événement.

Proposition n° 21

Nommer un magistrat référent au plan national, chargé de veiller au respect du droit à l'oubli pour les mineurs à la date du troisième anniversaire de l'inscription dans le fichier. En l'absence de nouvel événement justifiant la conservation des données concernant le mineur, le magistrat s'assure que celles-ci sont effectivement effacées. Si, au regard de tout nouvel événement, les services gestionnaires souhaitent le maintien des informations concernant le mineur, ils doivent alors présenter au magistrat l'ensemble des raisons le justifiant.

Dans le cas où un tel maintien des données au-delà du troisième anniversaire est autorisé par le magistrat, les services gestionnaires et le magistrat référent doivent se réunir tous les ans, afin d'étudier de nouveau les raisons justifiant le maintien dans le fichier. S'il estime que la demande de maintien est insuffisamment motivée, le magistrat peut ordonner l'effacement des données.

Proposition n° 22

Remplacer la typologie ethno- raciale du STIC-Canonge et de son équivalent JUDEX par les éléments du portrait-robot, dont la couleur de peau est une composante au même titre que la couleur des yeux et des cheveux, par exemple.

GARANTIR L'EXACTITUDE DES FICHIERS DE POLICE

Proposition n° 23

Afin de garantir une meilleure alimentation du fichier automatisé des empreintes digitales, déployer de bornes de signalisation T1 et T4 dans les unités de la gendarmerie nationale, aussi bien dans les 100 brigades départementales de renseignements et d'investigations judiciaires que dans les unités territoriales les plus chargées.

Proposition n° 24

Lorsqu'il est possible de réaliser un prélèvement biologique à des fins de comparaison sur une personne à l'encontre de laquelle il existe une « *raison plausible* » de soupçonner qu'elle a commis un crime ou un délit, la loi n'énumère pas actuellement les infractions concernées. Il est nécessaire de renvoyer explicitement à la liste des infractions pour lesquelles l'enregistrement d'un profil génétique est possible. En conséquence, modifier l'alinéa 3 de l'article 706-54 du code de procédure pénale.

Proposition n° 25

Mettre en place une politique de formation adaptée au profit des agents administratifs affectés à l'alimentation des fichiers.

Proposition n° 26

Enjoindre les services de police de tenir compte sans délai des décisions de classement sans suite formulées par les parquets dans le cadre du traitement en temps réel par le biais d'une circulaire du ministre de l'Intérieur rappelant les conditions d'inscription d'une personne mise en cause dans les fichiers d'antécédents.

Proposition n° 27

Remettre à toute personne placée en garde à vue un document d'information précisant que d'éventuelles poursuites judiciaires peuvent entraîner l'inscription dans un fichier d'antécédent judiciaire et récapitulatif de manière pratique les différentes possibilités qui sont offertes aux citoyens en matière de droit d'accès, de demande de mise à jour et de rectification des données.

Proposition n° 28

Recruter des contractuels en nombre suffisant pour permettre aux services régionaux de documentation criminelle de résorber le stock de procédures en attente de traitement s'agissant du STIC.

Proposition n° 29

Mettre en place une politique de revalorisation, d'intéressement et de validation des acquis de l'expérience en direction des personnels administratifs chargés de l'alimentation et du contrôle de la qualité des fichiers d'antécédents.

Proposition n° 30

Définir un processus de contrôle qualité et d'enrichissement des données dans le cadre du déploiement d'ARIANE.

Proposition n° 31

Prévoir un remplacement rapide du logiciel ARDOISE, en tenant compte en amont des réalités du travail des utilisateurs.

Proposition n° 32

Confier à une commission, présidée par un procureur général et associant l'IGPN, l'IGGN et la CNIL, le soin de définir les modalités de reprise de l'ensemble des données figurant dans le STIC et dans JUDEX, de telle sorte qu'ARIANE n'hérite pas du stock d'erreurs accumulées dans les traitements actuellement en service. Consacrer les moyens et le temps nécessaires à la réalisation effective de ce chantier considérable.

RENDRE LES CONTRÔLES PLUS EFFICACES

Proposition n° 33

L'utilisation des fichiers d'antécédents judiciaires dans le cadre d'un procès pénal doit respecter la règle du contradictoire. Dans le cas où le ministère public mentionne les affaires pour lesquelles un prévenu ou un mis en examen a été mis en cause, la fiche correspondante doit être versée au dossier.

Proposition n° 34

Mettre en place au plus vite le dispositif d'échanges d'informations entre CASSIOPÉE et ARIANE, afin de tenir compte plus rapidement et plus efficacement des changements de qualification et des suites judiciaires.

Proposition n° 35

Garantir la transmission systématique des décisions judiciaires d'effacement des fichiers d'antécédents afin de procéder aux effacements correspondants dans le fichier Canonge et dans le FNAEG.

Proposition n° 36

Réduire à un mois le délai de traitement du dossier en cas de demande de mise à jour émanant d'une personne figurant dans un fichier d'antécédents judiciaires.

Proposition n° 37

Mettre en place une procédure de traitement en temps réel auprès d'un magistrat référent des fichiers d'antécédents afin de répondre aux demandes de mise à jour présentant un degré d'urgence particulièrement élevé.

Proposition n° 38 de votre Rapporteur

Maintenir la faculté accordée au procureur de la République de prescrire le maintien dans un fichier d'antécédent judiciaire des données personnelles concernant les personnes mises en cause en cas de décision de relaxe ou d'acquittement devenue définitive.

Proposition n° 38 bis de votre Rapporteur

Supprimer la faculté accordée au procureur de la République de prescrire le maintien dans un fichier d'antécédent judiciaire des données personnelles concernant les personnes mises en cause en cas de décision de relaxe ou d'acquittement devenue définitive (modification du III de l'article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure).

Proposition n° 39

Élargir le nombre de cas dans lesquels le procureur de la République peut ordonner l'effacement des données personnelles en modifiant le III de l'article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure.

Proposition n° 40

Installer au plus vite dans les parquets des TGI des terminaux permettant l'accès direct aux données figurant dans les traitements STIC et JUDEX, afin d'assurer un véritable contrôle par le procureur de la République et d'accélérer le traitement des mises à jour en fonction des suites judiciaires.

Proposition n° 41

Prévoir l'engagement de personnels contractuels ponctuellement nécessaires à la CNIL pour traiter le stock des recours accumulés et garantir ainsi des délais convenables d'exercice du droit d'accès indirect.

Proposition n° 42

Instituer un droit d'accès direct des victimes aux fichiers d'antécédents judiciaires.

Proposition n° 43

Engager une réflexion sur la création au profit de la CNIL d'une redevance modeste, acquittée par les utilisateurs de l'informatique, en vue d'adapter les moyens de l'autorité de contrôle à la croissance continue des recours.

Proposition n° 44

Assurer une transmission systématique à la délégation parlementaire au renseignement de l'ensemble des textes relatifs à la mise en place de traitements automatisés de données à caractère personnel par les services de renseignement, lorsque les textes portant création des fichiers intéressant la sûreté de l'État et la défense ne sont pas publiés au *Journal Officiel*.

RESPECTER LES FINALITÉS DES FICHIERS

Proposition n° 45

Remplacer par un contrôle d'accès sécurisé au moyen de cartes à puce la multitude de codes attribués aux policiers et gendarmes pour utiliser les différentes applications dont ils disposent.

Proposition n° 46

S'orienter vers la mise en place de systèmes d'alerte en temps réel fondés sur l'analyse du comportement de l'utilisateur et permettant de mieux réprimer les détournements de données personnelles figurant dans les fichiers de police.

Proposition n° 47

Dans les cas où une enquête administrative doit être réalisée par la police nationale, celle-ci doit être confiée seulement au service départemental d'information générale.

Proposition n° 48

Avertir systématiquement toute personne figurant comme mis en cause dans un fichier d'antécédents judiciaires et faisant l'objet d'une enquête administrative de la possibilité d'être entendue par les services chargés de cette enquête, pour exposer son cas et, éventuellement, l'urgence de sa situation en termes d'accès à l'emploi.

Proposition n° 49

Moderniser de toute urgence le fichier des brigades spécialisées, cet outil des plus utiles en étant malheureusement arrivé au point où son fonctionnement même est désormais compromis.

Proposition n° 50

Définir un cadre législatif approprié pour la mise en œuvre de traitements automatisés de données permettant des rapprochements destinés à la lutte contre la petite et moyenne délinquance sérielle.

Proposition n° 51

Pour le développement de chaque nouveau fichier commun à la police et à la gendarmerie, créer une équipe intégrée associant les deux forces, avec un seul chef de projet assisté d'un comité où sont représentées toutes les directions intéressées, pour assurer le pilotage juridique, technique et financier du projet.

Proposition n° 52

Associer la police et la gendarmerie dans le cadre d'une véritable démarche intégrée de prospective technique et financière s'agissant des besoins futurs en matière de fichiers.

**CONTRÔLER LA TRANSITION ENTRE FICHIERS DE POLICE ET ACCOMPAGNER
LEUR DESTRUCTION ÉVENTUELLE**

Proposition n° 53

Permettre, à titre provisoire et sur la base du décret du 14 octobre 1991, l'alimentation et la consultation du fichier des renseignements généraux, « gelé » depuis le 1^{er} juillet 2008, dans l'attente de l'adoption d'une loi autorisant la création du futur fichier EDVIRSP.

Proposition n° 54

Rédiger un guide méthodologique à l'attention des services, détaillant avec précision les critères et les modalités de production, de traitement, de transfert, de destruction et d'archivage des données contenues dans les fichiers de police.

Proposition n° 55

Définir au plus vite la nature du fichier qui aura vocation à remplacer le fichier alphabétique de renseignements (FAR) en octobre 2010, en déterminant avec précision la finalité assignée à ce nouveau traitement ainsi que la description générale de ses fonctions, les catégories de données à caractère personnel enregistrées, leur origine et les catégories de personnes concernées.

Proposition n° 56

Établir dans les meilleurs délais des directives, à l'attention de l'ensemble des brigades territoriales de la gendarmerie nationale, précisant les critères ainsi que les modalités de transfert, de destruction et d'archivage des données contenues dans le FAR, afin que sa disparition soit pleinement effective au 24 octobre 2010.

Proposition n° 57

Prononcer la destruction des fichiers par la loi. En conséquence, compléter l'article 26 de la loi du 6 janvier 1978, afin que seule la loi puisse mettre fin à l'existence des fichiers intéressant la sécurité publique et ceux qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.

GLOSSAIRE

ACC	Autorité de contrôle commune
AGRIPPA	Application nationale de gestion du répertoire informatisé des propriétaires et possesseurs d'armes
ANACRIM	Analyse criminelle
ARDOISE	Application de recueil de la documentation opérationnelle et d'informations statistiques sur les enquêtes
ARIANE	Application de rapprochements, d'identification et d'analyse pour les enquêteurs
BDRIJ	Brigade départementale de renseignements et d'investigations judiciaires
CASSIOPÉE	Chaîne applicative supportant le système d'information orienté procédure pénales et enfants
CEPD	Contrôleur européen de la protection des données
CHEOPS	Circulation hiérarchisée des enregistrements opérationnels de police sécurisés
CNIL	Commission nationale de l'informatique et des libertés
CORAIL	Cellule opérationnelle de rapprochements et d'analyse des infractions liées
CREI	Comptes rendus d'enquête après identification
CRI	Centre de ressources informatiques
CRISTINA	Centralisation du renseignement intérieur pour la sécurité du territoire et les intérêts nationaux
DCRB	Division du contrôle et de la réglementation bancaires
DCRI	Direction centrale du renseignement intérieur
DCSP	Direction centrale de la sécurité publique
DELFI	Division des études, des liaisons et de la formation
DLPAJ	Direction des libertés publiques et des affaires juridiques
DSDC	Division de la statistique et de la documentation criminelle
DST	Direction de la surveillance du territoire

EDVIGE	Exploitation documentaire et valorisation de l'information
EDVIRSP	Exploitation documentaire et la valorisation de l'information relative à la sécurité publique
FAED	Fichier automatisé des empreintes digitales
FAR	Fichier alphabétique de renseignements
FBS	Fichier des brigades spécialisées
FIJAIS	Fichier judiciaire national automatisé des auteurs d'infractions sexuelles
FNAEG	Fichier national des empreintes génétiques
FNFM	Fichier national du faux monnayage
FNI	Fichier national des immatriculations
FNPC	Fichier national des permis de conduire
FNT	Fichier national transfrontière
FPA	Fichier des passagers aériens
FRG	Fichier des renseignements généraux
FVV	Fichier des véhicules volés
GESTEREXT	Gestion du terrorisme et des extrémismes à potentialité violente
GEVI	Gestion des violences urbaines
HALDE	Haute autorité de lutte contre les discriminations
IGA	Inspection générale de l'administration
IGPN	Inspection générale de la police nationale
JUDEX	Système judiciaire de documentation et d'exploitation
LUPIN	Logiciel d'uniformisation des procédures d'identification
NAFIS	<i>National Automated Fingerprint Information System</i>
NDNAD	<i>National DNA Database</i>
NIR	Numéro identifiant au répertoire
PTS	Police technique et scientifique
SAFARI	Système automatisé pour les fichiers administratifs et le répertoire des individus
SALVAC	Système d'analyse des liens de la violence associée aux crimes

SCPPB	Service central de préservation des prélèvements biologiques
SDIG	Sous-direction de l'information générale
SDIG	Service départemental de l'information générale
SIS	Système d'information Schengen
SRDC	Service régional de documentation criminelle
STIC	Système de traitement des infractions constatées
STRJD	Service technique de recherches judiciaires et de documentation

LISTE DES PERSONNES AUDITIONNÉES

Commission nationale de l'informatique et des libertés

- M. Alex TÜRK, président ;
- M. Yann PADOVA, secrétaire général ;
- Mme Florence FOURETS, directrice des relations avec les usagers et du contrôle ;
- Mme Carina CHATAIN-MARCEL, chef de cabinet, chargée des relations avec les institutions ;
- M. Guillaume DESGENS-PASANAU, chef du service des affaires juridiques.

Médiateur de la République

- M. Jean-Paul DELEVOYE, médiateur de la République ;
- M. Luc CHARRIÉ, administrateur civil, conseiller Réforme.

Commission nationale de déontologie de la sécurité

- M. Roger BEAUVOIS, président ;
- Mme Nathalie DUHAMEL, secrétaire générale.

Commission Nationale Consultative des Droits de l'Homme

- M. Joël THORAVAL, président ;
- Mme Nicole QUESTIAUX, présidente de la sous-commission « *droits de l'Homme et évolutions de la société* ».

Ministère de l'Intérieur, de l'Outre-Mer et des collectivités territoriales

- *Direction générale de la police nationale*

- M. Frédéric PÉCHENARD, directeur général ;
- M. Jean MAFART, chef du pôle juridique du cabinet du directeur général.

- Direction des libertés publiques et des affaires juridiques

- M. Laurent TOUVET, directeur.

- Inspection générale de la police nationale

- M. Dominique BOYAJEAN, chef de l'inspection générale.

- Direction centrale de la police judiciaire

- M. Christian LOTHION, directeur.

- Direction centrale de la police judiciaire, division des relations internationales

- M. Bernard PETIT, contrôleur général, chef de la division.

- Direction centrale de la sécurité publique

- M. Éric Le DOUARON, directeur ;
- M. Serge GUILLEN, sous-directeur à l'information générale.

- Direction centrale de renseignement intérieur

- M. Bernard SQUARCINI, directeur.

- Service des technologies de la sécurité intérieure

- M. Patrick GUYONNEAU, ingénieur en chef de l'armement, directeur ;
- M. Julien GENTILE, commissaire divisionnaire, adjoint au directeur.

Ministère de la Défense

- Direction générale de la gendarmerie nationale

- général Roland GILLES, directeur général ;
- M. Jean-Pierre BONTHOUX, conseiller juridique du directeur général ;

- Inspection générale de la gendarmerie nationale

- général Edmond BUCHHEIT, inspecteur général.

- Sous-direction des télécommunications et de l'informatique

- général François ESPINASSE, sous-directeur des télécommunications et de l'informatique ;

- Audition relative aux fichiers administratifs de la gendarmerie nationale

- général Jean-Régis VÉCHAMBRE, chef de cabinet du directeur général ;

- Colonel Denys MORÉE, chef du bureau du renseignement ;
- Colonel Claude LORENT, chef du bureau des systèmes d'information.

Ministère de la Justice

- Direction des affaires criminelles et des grâces

- M. Thierry POCQUET du HAUT-JUSSÉ, chef de service, adjoint au directeur.

- Projet CASSIOPÉE

- M. Stéphane HARDOUIN, directeur de projet, direction des services judiciaires ;
- M. Luc FERRAND, magistrat, secrétariat général.

Projet ARIANE

- M. Sylvain MAUBÉ, commissaire divisionnaire, pour la police nationale ;
- Colonel Jacques-Charles FOMBONNE, pour la gendarmerie nationale.

Observatoire national de la délinquance et groupe de contrôle sur les fichiers de police

- M. Alain BAUER, président.

Institut national de la police scientifique

- M. Hubert WEIGEL, directeur.

Fichier national automatisé des empreintes génétiques (FNAEG)

- M. Christian HASSENFRTZ, magistrat référent, procureur général près la Cour d'appel de Nancy.

Groupe de suivi du « plan d'action 2008-2010 pour une police technique et scientifique plus performante »

- M. Charles DIAZ, contrôleur général de la police nationale ;
- Colonel Jacques HÉBRARD, directeur de l'Institut de recherches criminelles de la gendarmerie nationale (IRCGN).

Institut National des Hautes Études de Sécurité

- M. Pierre MONZANI, directeur.

Mission « *Archives des Renseignements généraux* »

- Mme Elisabeth RABUT, chef de la mission, chef de l'inspection générale des archives nationales ;
- M. Gilles SANSON, rapporteur général, inspecteur général de l'administration ;
- Mme Nacera HADDOUCHE, rapporteure, inspecteur de l'administration ;
- M. Sylvain MANVILLE, rapporteur, chef de la mission des archives de France.

Ligue des Droits de l'Homme

- Mme Danièle LOCHAK, vice présidente ;
- M. Jean-Claude VITRAN, responsable du groupe de travail « *Libertés et TIC* ».

Avocats

- Pour le Conseil national des barreaux

- Mme Andréanne SACAZE, ancien Bâtonnier d'Orléans ;
- M. Didier LIGER, président de la commission libertés et droits de l'Homme, avocat à Versailles.

- Pour le Barreau de Paris

- M. Dominique TRICAUD, avocat à Paris ;
- M. Vincent NIORE, avocat à Paris.

- Pour la Conférence des Bâtonniers

- M. Jean-François MORTELETTE, ancien Bâtonnier de Blois.

Syndicats de police

- UNSA-police

- M. Paul LE GUENNIC, secrétaire général adjoint ;
- Mme Francie CHASSAGNE, déléguée nationale pour le corps des commissaires ;
- M. Frank FIEVEZ, délégué national.

- Syndicat général de la police

- M. Nicolas COMTE, secrétaire général ;
- M. Frédéric GALÉA, secrétaire national.

- Syndicat Synergie-officiers

- M. Christophe GESSET, conseiller technique ;
- M. Francis NEBOT, conseiller technique.

- Syndicat des commissaires de la police nationale

- M. Emmanuel ROUX, secrétaire général adjoint ;
- M. Grégory CORNILLON, commissaire à la sécurité publique à Clichy-la-Garenne.

- Alliance police nationale

- M. Jean-Yves BUGELLI, secrétaire général adjoint ;
- M. Laurent CACLAU LACROUTS, secrétaire national adjoint.

- Syndicat national des officiers de police

- Mme Chantal PONS-MESOUAKI, secrétaire nationale ;
- M. Carlos GARCIA, secrétaire pour l'Île-de-France.

- Syndicat national indépendant des personnels administratifs et techniques (SNIPAT)

- M. Bernard MEYNIER, secrétaire général ;
- Mme Sylvie GAGU, secrétaire générale adjointe ;
- M. Georges KNECHT, secrétaire général adjoint.

Collectif « Non à Edvige »

- M. Jean-Claude VITRAN, responsable du groupe de travail « Libertés et TIC » de la Ligue des Droits de l'Homme ;
- Mme Meryem MARZOUKI, pour l'association « Imaginons un Réseau Internet Solidaire » ;

- M. Philippe CASTEL, représentant de la FSU au sein de l'association « *Inter LGBT* » ;
- M. Laurent BELLINI, pour l'association « *L'Autre cercle* ».

Intelligence économique et sécurité privée

- Syndicat national des entreprises de sécurité

- M. Jean-Pierre MALGUY, délégué général.

- Fédération professionnelle de l'intelligence économique (FPIE)

- général (CR) Jean-Bernard PINATEL, président ;
- M. Hervé SÉVENO, secrétaire général ;
- M. Brice de GLIAME, vice-président ;
- M. Béchir MANA, membre du conseil d'administration.

- Société Iris Consultants

- M. Patrick BAPTENDIER.

LISTE DES DÉPLACEMENTS EFFECTUÉS

Service technique de recherches judiciaires et de documentation à Rosny-sous-Bois (9 octobre 2008)

- Colonel Francis HUBERT, chef du service technique de recherches judiciaires et de documentation ;
- Chef d'escadron Hubert CHARVET, chef de la division des fichiers du service technique de recherches judiciaires et de documentation.

Préfecture de police de Paris

- Brigade criminelle du 36 quai des Orfèvres à Paris (16 octobre 2008)

- M. Jean-Jacques HERLEM, directeur-adjoint chargé des brigades centrales à la direction de la police judiciaire ;
- M. Loïc GARNIER, commissaire divisionnaire, chef de la brigade criminelle.

- Division de la statistique et de la documentation criminelle (4 décembre 2008)

- M. Christian FLAESCH, directeur de la police judiciaire de la préfecture de police ;
- M. Richard MARLET, commissaire divisionnaire, chef de la division de la statistique et de la documentation criminelle ;
- M. Renaud VEDEL, directeur-adjoint du cabinet du Préfet de police.

- Sections techniques de recherche et d'investigation de l'identité judiciaire (4 décembre 2008)

- M. Philippe BUGEAUD, sous-directeur des ressources humaines et de la logistique ;
- M. Vianney DYEUVRE, commissaire divisionnaire, chef des sections techniques de recherche et d'investigation de l'identité judiciaire.

- Direction du renseignement de la préfecture de police (DRPP) de Paris (16 octobre 2008 et 15 janvier 2009)

- M. Bruno LAFFARGUE, directeur du renseignement ;
- M. Roland DOMGIN, commandant de police à l'emploi fonctionnel ;
- Mme Marie-José ABAD-MARTIN, commandant de police.

- Présentation du fichier LUPIN (3 février 2009)

- M. Philippe CARON, contrôleur général, sous-directeur de la police territoriale ;
- M. Maurice SIGNOLET, commissaire divisionnaire, chef du service d'investigation transversale (SIT) ;
- Mme Odette DOS REIS BEGENT, capitaine de police, chef de l'unité d'analyse et des synthèses opérationnelles (UASO) au SIT ;
- Mme Estelle STAMM, lieutenant de police, adjoint au chef de l'UASO ;
- M. Fiorello SALA, brigadier de police, affecté à l'UASO, conception et développement de LUPIN ;
- M. Patrice COUILLON, gardien de la paix, affecté à l'UASO, conception et développement de LUPIN.

- Présentation du fichier CORAIL (11 février 2009)

- M. Jean-Jacques HERLEM, contrôleur général, directeur adjoint de la DPJ, chargé des brigades centrales de la police judiciaire de Paris ;
- M. Denis COLLAS, commissaire divisionnaire, chef d'état-major de la direction régionale de la police judiciaire de Paris ;
- M. Éric FRANCELET, commissaire principal, chef du service informatique de la direction régionale de la police judiciaire de Paris ;
- M. Jean-Pierre DAL POZZOLO, capitaine de police et concepteur de « CORAIL 1 » ;
- M. Sylvain JAMES, brigadier chef de police et développeur de « CORAIL 2 ».

M. Philippe DALBAVIE, conseiller technique au cabinet du Préfet de police, a assisté vos rapporteurs lors de chacun des déplacements à la préfecture de police de Paris.

**Brigade territoriale de la Gendarmerie Nationale d'Auvers-sur-Oise (95)
(6 novembre 2008)**

- Colonel Philippe CAUSSE, commandant le groupement de gendarmerie départementale du Val-d'Oise ;
- Chef d'escadron Jean-Marc MICHELET, commandant la compagnie de Cergy ;
- Lieutenant Thierry LOURY, commandant la compagnie d'Auvers-sur-Oise ;

- Adjudant Éric LAFONTAINE, adjoint au commandant de brigade d'Auvers-sur-Oise.

Sous direction de la police technique et scientifique à Écully (69) (27 novembre 2008)

- Commission nationale de l'informatique et des libertés

- M. Jean MASSOT, président de section honoraire au Conseil d'État, magistrat en charge du droit d'accès indirect ;
- Mme Bérengère MONEGIER du SORBIER, responsable de la cellule « *Droit d'accès indirect* » ;

- Sous-direction de la police technique et scientifique

- M. Bruno PEREIRA-COUTINHO, contrôleur général, sous-directeur de la police technique et scientifique de la DCPJ ;
- M. Éric BRENDEL, chef du service central de documentation criminelle ;
- M. Guillaume LE MAGNEN, chef du service central d'identité judiciaire ;
- M. Bernard MANZONI, adjoint au chef du service central d'identité judiciaire ;
- Mme Florence MOURARET, adjointe au chef de la division des études, des liaisons et de la formation.

Département des Deux-Sèvres (8 et 19 décembre 2008)

- M. Xavier PAVAGEAU, procureur de la République du tribunal de grande instance de Niort ;
- M. Laurent DUFOUR, directeur départemental de la sécurité publique ;
- Lieutenant-colonel Frédéric BONNEVAL, commandant le groupement de gendarmerie départementale ;
- Lieutenant Christophe BARRAUD, commandant la communauté de brigades de gendarmerie de Melle.

Service régional de documentation criminelle (SRDC) de Versailles (18 décembre 2008)

- M. Bruno PEREIRA-COUTINHO, contrôleur général, sous-directeur de la police technique et scientifique de la DCPJ ;

- M. Jean ESPITALIER, contrôleur général, directeur régional de la police judiciaire à Versailles ;
- M. Philippe GUICHARD, commissaire principal, chef de la division des affaires criminelles de la DRPJ Versailles ;
- M. Christophe HIRSCHMANN, commissaire de police, chef de la division de police technique de la DRPJ Versailles ;
- Mme Isabelle RENARD, secrétaire administrative de classe exceptionnelle, chef du service régional de documentation criminelle (SRDC) de la DRPJ Versailles ;
- M. Romain JEANNIN, secrétaire administratif, adjoint au chef du SRDC ;
- Mme Sandrine DELHOUME, adjoint administratif principal de 2e classe, responsable du "contrôle qualité" de la base STIC au sein du SRDC.

Commission nationale de l'informatique et des libertés (CNIL) (12 janvier 2009)

- M. Emmanuel DE GIVRY, membre de la CNIL, conseiller à la cour de cassation ;
- Mme Bérengère MONEGIER du SORBIER, responsable du droit d'accès indirect.

Tribunal de grande instance d'Evry (12 janvier 2009)

- M. Jean-François PASCAL, procureur de la République auprès du tribunal de grande instance d'Evry ;
- M. Pascal LE FUR, adjoint au procureur ;
- Mme Maryse LELEU, greffière en chef.

Direction Départementale de la Sécurité Publique (DDSP) du Val de Marne (21 janvier 2009)

- M. le contrôleur général Éric DRAILLARD, directeur départemental de la sécurité publique du Val-de-Marne ;
- M. le commissaire divisionnaire Jean-Yves OSES, adjoint du directeur
- M. le commissaire divisionnaire Jean-René CURTA, chef d'état-major par intérim (centre d'information et de commandement) ;

- M. le commissaire divisionnaire Richard SRECKI, chef de la sûreté départementale ;
- M. le commissaire de police Jean-Michel AVON, chef du service départemental d'information générale ;
- Mme le commissaire de police Anouck FOURMIGUE, commissaire central adjoint de Créteil.

Direction des systèmes d'information et de communication (DSIC) de Lognes (22 janvier 2009)

- M. Reynald BOUY, directeur adjoint des systèmes d'information et de communication du ministère de l'Intérieur ;
- M. Mathieu JEANDRON, sous-directeur de l'exploitation et du soutien ;
- M. Daniel FLEURENCE, chef du bureau de la supervision et du soutien utilisateurs ;
- M. Antoine DELOUVRIER, chef de projet PASSAGE à la sous-direction des études et projets.

Bruxelles (26 janvier 2009)

Commission européenne

- M. Jonathan FAULL, Directeur général de la DG « Justice, liberté et sécurité » ;
- M. Alain BRUN, chef de l'unité de protection des données.

Représentation permanente de la France auprès de l'Union européenne

- M. Daniel LECRUBIER, chef du service « Justice et affaires intérieures »
- Mme Claire ROCHETEAU, conseiller « Justice et affaires intérieures » ;
- M. Jean-Philippe MOCHON, conseiller juridique.

Contrôleur européen à la protection des données

- M. Peter HUSTINX, contrôleur européen de la protection des données ;
- M. Giovanni BUTARELLI, adjoint du CEPD ;
- Mme Bénédicte HAVELANGE, conseiller juridique.

Tribunal de grande instance de Bobigny (2 février 2009)

- M. François MOLINS, procureur de la République ;
- M. Patrick POIRRET, procureur de la République adjoint ;
- M. Denis FAURIAT, secrétaire général du parquet ;
- M. Pierre-Olivier AMEDÉE-MANESME, substitut du procureur affecté à la division de l'exécution des peines ;
- Mme Nathalie BRILOT, greffière en chef, services du parquet ;
- Mme Sophie GREMY, greffière en chef, service de l'exécution des peines ;
- Mme Monique POMPIU, greffière en chef, service pénal.

ANNEXES

Annexe 1 : Tableau des fichiers de police ou ayant un usage de police.....	237
Annexe 2 : Évolution du volume des principaux fichiers de police	273
Annexe 3 : Réponse du magistrat de liaison au Royaume-Uni au questionnaire des rapporteurs.....	277
Annexe 4 : Réponse de l’ambassade de France aux Pays-Bas au questionnaire des rapporteurs	291
Annexe 5 : Formulaire à remplir par les candidats à un emploi dans la police du Kent.....	301
Annexe 6 : Circulaire du ministère de la Justice du 9 juillet 2008 relative au refus du prélèvement biologique.....	303
Annexe 7 : Échange de courriers entre un commandant de groupement de gendarmerie et deux procureurs de la République	309
Annexe 8 : Exemples de courriers s’agissant du contrôle exercé par les parquets sur les fichiers d’antécédents judiciaires.....	315
Annexe 9 : Exemples de refus d’agrément préfectoral pour l’accès à une profession dans le domaine de la sécurité privée.....	325
Annexe 10 : Coût des fichiers de police – mission sécurité – programme police nationale.....	329
Annexe 11 : Lettres de cadrage de la mission « Archives des renseignements généraux ».....	331
Annexe 12 : Circulaire du ministère de l’Intérieur du 3 juillet 2001 relative aux règles de tri et de conservation des documents produits par les services des renseignements généraux.....	337
Annexe 13 : Lettre du préfet de police de Paris sur la mise en conformité des fichiers	347
Annexe 14 : Réponses au questionnaire des rapporteurs sur les fichiers de la préfecture de police de Paris	353
Annexe 15 : Arrêté du préfet de police de Paris relatif à l’archivage du fichier manuel des renseignements généraux.....	369

**ANNEXE 1 : TABLEAU DES FICHIERS DE POLICE OU
AYANT UN USAGE DE POLICE**

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Convention internationale								
Accord de Schengen du 9 juin 1990 (décret n° 95-577 du 6 mai 1995)	Système d'information Schengen (SIS)	Direction générale de la police nationale (DCPJ)	Recensement : - des personnes recherchées, sous surveillance ou indésirables ; - des véhicules ou objets recherchés.	Informatique	Judiciaire	- 3 ans renouvelables pour les données relatives aux personnes et aux véhicules ; - 5 ans pour les documents d'identité et les billets de banque ; - 10 ans pour les autres objets.	Mixte	Alimenté par le fichier des véhicules volés, le fichier des personnes recherchées et le STIC.
Loi								
Loi n° 90-1131 du 19 décembre 1990 (articles L. 330-1 à L. 330-8 du code de la route)	Fichier national des immatriculations (FNI)	Ministère de l'Intérieur (DLPJA)	Connaître à tout moment la situation administrative et juridique d'un véhicule et d'identifier son propriétaire, notamment dans le cadre de recherches de police	Informatique	Administratif	Les informations sont conservées jusqu'à la destruction ou au retrait du véhicule, plus cinq ans.	Direct	Le FNI comprend environ 30,6 millions de voitures particulières immatriculées.
Loi n° 98-468 du 17 juin 1998 (modifiée par les lois n° 2001-1062 et n° 2003-239)	Fichier national automatisé des empreintes génétiques (FNAEG)	Direction générale de la police nationale (DCPJ) - fichier commun à la police et à la gendarmerie	Enregistrement et comparaison des empreintes génétiques.	Informatique	Judiciaire (fichier d'identification)	De 25 à 40 ans	Direct	

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Loi n° 2004-204 du 9 mars 2004 (modifiée par les lois n° 2005-1549 et n° 2006-399)	Fichier judiciaire national automatisé des auteurs d'infractions sexuelles (FIJAIS)	Ministère de la justice	Prévenir la récidive d'infractions sexuelles ou violentes et faciliter l'identification de leurs auteurs.	Informatique	Judiciaire (fichier d'identification)	De 20 à 30 ans	Direct	
Loi n° 2005-1549 du 12 décembre 2005 (créant l'article 21 -1 de la loi n° 2003-239 du 18 mars 2003)	Logiciel d'analyse criminelle (ANACRIM)	Gendarmerie nationale	Opérer des rapprochements pour établir des liens entre procédures judiciaires et mettre en évidence leur caractère sérieux.	Informatique	Judiciaire. Fichiers temporaires liés à des investigations sur des crime ou délit contre les personnes punies de plus de cinq ans d'emprisonnement ou aux biens et punis de plus de sept ans d'emprisonnement.	Doit être fixée par décret en Conseil d'Etat après avis de la CNIL.	Indirect	La loi du 12 décembre 2005 a donné une base juridique à ce type de traitements informatiques. Les décrets en Conseil d'Etat ne sont pas encore parus.

Texte de référence initial	Loi n° 2005-1549 du 12 décembre 2005 (créant l'article 21-1 de la loi n° 2003-239 du 18 mars 2003)
Nom du fichier	Système d'analyse et de liens de la violence associée au crime (SALVAC)
Administration gestionnaire	Police et gendarmerie nationale
Objet	Opérer des rapprochements pour établir des liens entre procédures judiciaires et mettre en évidence leur caractère sériel.
Nature du fichier	Informatique
Type	Judiciaire. Fichiers temporaires liés à des investigations sur des crime ou délit contre les personnes punies de plus de cinq ans d'emprisonnement ou aux biens et punis de plus de sept ans d'emprisonnement.
Durée de conservation des données	Doit être fixée par décret en Conseil d'Etat après avis de la CNIL.
Droit d'accès	Indirect
Observations	La loi du 12 décembre 2005 a donné une base juridique à ce type de traitements informatiques. Les décrets en Conseil d'Etat ne sont pas encore parus.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Loi n° 2006-64 du 23 janvier 2006 (article 7), transposant la directive 2004/82/CE du 29 avril 2004, décret n° 2006-1630 du 19 décembre 2006 et arrêté daté du même jour.	Fichier des passagers aériens (FPA)	Direction générale de la police nationale (direction centrale de la police aux frontières)	Fichier des données collectées par les entreprises de transport international au moment de l'enregistrement (données dites APIS), envoyées dès la clôture du vol.	Informatique	Administratif	5 ans (à l'exception de la mention « connu » ou « inconnu » au FPR ou au SIS, qui n'est conservée que 24 heures). Dans le cadre de la lutte contre l'immigration clandestine, les données ne peuvent être consultées que dans les 24 heures qui suivent leur transmission.	Direct auprès de la PAF, sauf pour la mention « connu » ou « inconnu » au fichier des personnes recherchées (dans ce cas droit d'accès indirect).	Autorisé à titre expérimental pour deux ans, il fait l'objet actuellement d'une nouvelle déclaration à la CNIL pour une reprise de l'expérimentation. Ce fichier est interconnecté avec le FPR et, à l'avenir, le sera avec le SIS.
Loi n° 2006-64 du 23 janvier 2006 (article 8) arrêté du 2 mars 2007	Traitement automatisé de contrôle des données signalétiques des véhicules	Police, gendarmerie et douanes	Rapprochement des données issues des dispositifs de lecture automatisés de plaques d'immatriculation (L-API) embarqués dans des véhicules avec le fichier des véhicules volés et signalés (FVV).	Informatique	Judiciaire (fichier d'identification)	- huit jours en l'absence de rapprochement positif ; - un mois en cas de rapprochement positif.	Indirect	Expérimentation autorisée pour une durée de deux ans

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Article L. 611-3 à L. 611-5 du code de l'entrée et du séjour des étrangers et du droit d'asile (article R. 611-18 à R. 611-24 du même code)	Traitement automatisé de données à caractère personnel de ressortissants étrangers qui, ayant été contrôlés à l'occasion du franchissement de frontières, ne remplissent pas les conditions d'entrée requises ou « fichier des non-admis » (FNAD)	Ministère chargé de l'immigration	Lutter contre l'entrée et le séjour irrégulier des étrangers.	Informatique	Administratif et judiciaire	- 5 ans à compter de leur inscription ; - 32 jours pour les données relatives aux procédures administratives ou judiciaires de refus d'entrée sur le territoire et, le cas échéant, de maintien en zone d'attente.	Direct	Fichier créé à titre expérimental pour une durée de deux ans à compter du 25 juillet 2007. Il est accessible aux agents habilités de la police aux frontières et aux agents de la police, de la gendarmerie et des services de renseignement du ministère de la Défense chargés de missions de prévention et de répression des actes de terrorisme.
Article L. 611-3 du code de l'entrée et du séjour des étrangers et du droit d'asile (articles R. 611-25 à R. 611-34 du même code – décret n° 2007-1890 du 26 décembre 2007)	Traitement automatisé de données à caractère personnel relatives aux étrangers faisant l'objet d'une mesure d'éloignement (ELOI)	Ministère chargé de l'immigration	Enregistrement des données à caractère personnel relatives aux étrangers faisant l'objet d'une mesure d'éloignement.	Informatique	Administratif et judiciaire	3 ans à compter de la date de l'éloignement ou de la fin de la rétention.	Direct	Ce fichier est accessible aux agents de la direction centrale de la police aux frontières et de la direction centrale de la sécurité publique habilités, ainsi qu'aux agents habilités de la police et de la gendarmerie en charge de la gestion des centres

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Article L. 611-6 du code de l'entrée et du séjour des étrangers et du droit d'asile (articles R. 611-8 à R. 611-15 du même code).	Traitement automatisé de données à caractère personnel relatives aux étrangers sollicitant la délivrance d'un visa (VISABIO)	Ministère des affaires étrangères et ministère chargé de l'immigration	Notamment faciliter sur le territoire national les vérifications d'identité opérées par les services de la police et de la gendarmerie en vertu de l'article 78-3 du CPP.	Informatique	Administratif	5 ans à compter de leur inscription.	Direct	de rétention administrative et de l'exécution des procédures d'éloignement. Outre les OPJ habilités (pour les missions de vérification d'identité), ce fichier est également accessible aux agents habilités de la police, de la gendarmerie et des services de renseignement du ministère de la Défense chargés de missions de prévention et de répression des actes de terrorisme.

Décret								
Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Décret n° 55-1397 du 22 octobre 1955	Fichier relatif à la carte nationale d'identité	Ministère de l'intérieur (DLPAJ)	<ul style="list-style-type: none"> - Mettre en œuvre les procédures de délivrance et de renouvellement ; - Limiter les risques de contrefaçon et de falsification ; - Faciliter l'action des policiers et gendarmes lors du franchissement des frontières. 	Informatique	Fichier d'identification administrative	15 ans	Direct	<p>L'informatisation du fichier a été réalisée en 1987.</p> <p>Le décret n° 2007-391 du 21 mars 2007 pris en application de la loi du 23 janvier 2006 rend les services de lutte contre le terrorisme destinataires des données contenues dans ce traitement.</p>
Décrets n° 87-249 du 8 avril 1987 et n° 2005-585 du 27 mai 2005	Fichier automatisé des empreintes digitales (FAED)	Direction générale de la police nationale (DCPJ) - fichier commun à la police et à la gendarmerie	Enregistrement et comparaison des empreintes digitales.	Informatique	Judiciaire (fichier d'identification)	25 ans	Direct	Depuis 2005, ce fichier peut également comprendre des empreintes palmaires et des clichés anthropométriques

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Décret n° 91-1051 du 14 octobre 1991	Fichiers des renseignements généraux (FRG)	Direction générale de la police nationale (renseignements généraux)	<p>Centralisation des informations sur les personnes :</p> <ul style="list-style-type: none"> - pouvant porter atteinte à la sûreté de l'État ou à la sécurité publique par la violence ; - ayant sollicité ou sollicitant l'accès à des informations protégées ; - exerçant ou ayant exercé un mandat électif ou jouant un rôle politique, économique, social ou religieux significatif. 	Système d'indexation informatique de dossiers papiers	Fichier de renseignement	Les données ne peuvent être conservées que pour autant qu'elles sont toujours nécessaires eu égard aux finalités du fichier. (examen tous les 5 ans, sous le contrôle de la CNIL, de la justification et du bien-fondé des informations nominatives détenues).	Indirect	Le décret n° 91-1051 est abrogé à compter du 31 décembre 2009 en vertu de l'article 3 du décret n° 2008-631 du 27 juin 2008. L'article 1 ^{er} de ce dernier dispose que « la collecte et l'enregistrement de nouvelles données [...] sont interdits à compter du 1 ^{er} juillet 2008 ». Seul le transfert de données vers les nouvelles applications se substituant au FRG est autorisé jusqu'au 31 décembre 2009.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
<p>Décret n° 91-1051 du 14 octobre 1991 (créé en 1996). GEVI a pour base juridique le décret de 1991, sa conformité avec ce texte ayant été reconnue par la CNIL dans sa décision du 19 novembre 1996).</p>	<p>Gestion des violences (GEVI)</p>	<p>Préfecture de police de Paris (RGPP et, depuis 2008, DRPP – pôle phénomènes urbains violents)</p>	<p>Recueil des informations sur les individus majeurs ou les personnes morales susceptibles d'être impliquées dans des actions de violences urbaines ou de violences sur les terrains de sport pouvant porter atteinte à l'ordre public et aux institutions.</p>	<p>Informatique</p>	<p>Renseignement</p>	<p>Les données ne peuvent être conservées que pour autant qu'elles sont toujours nécessaires eu égard aux finalités du fichier.</p>	<p>Indirect</p>	<p>Le fichier GEVI a été autorisé sur l'avis conforme de la CNIL (délibération n° 96-098 du 19 novembre 1996). Le fichier GEVI ne couvre que Paris, alors même que la DRPP coordonne l'action des sept SDIG de la région parisienne (les DDRG de la région parisienne utilisaient le FRG jusqu'en juillet 2008). Une réflexion sur l'extension de GEVI aux autres départements de la région parisienne est en cours.</p>

<p>Texte de référence initial</p> <p>Décret du 29 mars 1993 (article D. 611-1 à D. 611 -7 du code de l'entrée et du séjour des étrangers et du droit d'asile)</p>	<p>Nom du fichier</p> <p>Système informatisé de gestion des dossiers des ressortissants en France (AGDREF)</p>	<p>Administration gestionnaire</p> <p>Ministère chargé de l'immigration (fichier national) et préfectures (fichiers départementaux)</p>	<p>Objet</p> <p>Notamment permettre aux services de la police et de la gendarmerie de vérifier la régularité du séjour en France (article D. 611-3).</p>	<p>Nature du fichier</p> <p>Informatique</p>	<p>Type</p> <p>Administratif</p>	<p>Durée de conservation des données</p> <p>- un an après le décret de naturalisation pour les personnes devenues françaises ; - 5 ans pour les personnes décédées, pour les étrangers ayant fait l'objet d'un refus de séjour, d'un arrêté de reconduite à la frontière ou dont le titre de séjour est venu à expiration.</p>	<p>Droit d'accès</p> <p>Direct</p>	<p>Observations</p> <p>- Les services de police et de gendarmerie ne peuvent accéder qu'au fichier national et seulement en vue de vérifier la régularité du séjour. - Les articles 9 et 33 de la loi n° 2006-64 permettent l'accès aux données par les agents de la police, de la gendarmerie et des services de renseignement du ministère de la Défense chargés de missions de prévention et de répression des actes de terrorisme.</p>
--	--	--	---	---	---	---	---	---

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
<p>Décret n° 2001-583 du 5 juillet 2001, modifié par le décret n° 2006-1258 du 14 octobre 2006. L'article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure a donné une base législative aux fichiers d'antécédents.</p>	<p>Système de traitement des infractions constatées (STIC)</p>	<p>Direction générale de la police nationale</p>	<p>Faciliter la constatation des infractions pénales, le rassemblement des preuves et la recherche de leurs auteurs, ainsi que l'exploitation de ces données à des fins statistiques.</p>	<p>Informatique</p>	<p>Fichier d'antécédents judiciaires</p>	<p>De 5 ans (cas général pour les mineurs) à 40 ans (infractions présentant une particulière gravité).</p>	<p>Indirect</p>	<p>- La loi n° 2003-239 relative à la sécurité intérieure a autorisé la consultation de ce fichier dans le cadre d'enquêtes administratives. - Ce fichier est destiné à être remplacé par ARIANE, application commune à la police et à la gendarmerie.</p>
<p>Décret n° 2005-1726 du 30 décembre 2005</p>	<p>Fichier relatif aux passeports (Delphine et TES)</p>	<p>Ministère de l'Intérieur (DLPAJ)</p>	<p>- Mettre en œuvre les procédures d'établissement, de délivrance et de renouvellement des passeports ; - Prévenir et détecter leur falsification ou contrefaçon.</p>	<p>Informatique</p>	<p>Fichier d'identification administrative</p>	<p>- 15 ans pour les majeurs ; - 10 ans pour les mineurs.</p>	<p>Direct</p>	<p>En application de l'article 9 de la loi du 23 janvier 2006, les services de lutte contre le terrorisme à la DGPJ, la DGGN et la DGSE sont destinataires des données contenues dans ce traitement.</p>

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Décret n° 2006-1411 du 20 novembre 2006. L'article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure a donné une base législative aux fichiers d'antécédents.	Système judiciaire de documentation et d'exploitation (JUDEX)	Gendarmerie	Faciliter la constatation des infractions pénales, le rassemblement des preuves et la recherche de leurs auteurs.	Informatique	Fichier d'antécédents judiciaires	De 5 ans (cas général pour les mineurs) à 40 ans (infractions présentant une particulière gravité).	Indirect	- La loi n° 2003-239 relative à la sécurité intérieure a autorisé la consultation de ce fichier dans le cadre d'enquêtes administratives. - Ce fichier est destiné à être remplacé par ARIANE, application commune à la police et à la gendarmerie.
Décret du 27 juin 2008, non publié au <i>Journal officiel</i>	Centralisation du renseignement intérieur pour la sécurité du territoire et les intérêts nationaux (CRISTINA)	Direction générale de la police nationale (DCRI)	Lutte contre toutes les activités susceptibles de constituer une atteinte aux intérêts fondamentaux de la nation.	Informatique	Renseignement	Les données ne peuvent être conservées que pour autant qu'elles sont toujours nécessaires eu égard aux finalités du fichier.	Indirect	Fichier destiné à reprendre les données des anciens fichiers de la DST et certaines données des fichiers gérés par les RG (dont notamment le fichier automatisé du terrorisme [FIT], abrogé par l'article 4 du décret n° 2008-631 du 27 juin 2008).

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Décret n° 2008-1109 du 29 octobre 2008	Traitement de données « pré-plainte en ligne » (PPL)	Direction générale de la police nationale	Permettre à la victime ou à son représentant de faire une déclaration en ligne, pour certaines infractions, et d'obtenir un rendez-vous pour la signature de la plainte.	Informatique	Application bureautique	Données à caractère personnel effacées à la signature de la plainte (à défaut de signature, effacement automatique après 30 jours).	Direct.	Traitement en cours d'expérimentation dans les Yvelines et la Charente-Maritime.
Arrêté								
Arrêté du 20 décembre 1972 (la base juridique actuelle est constituée par l'article L. 225-1 à L. 225-9 du code de la route)	Fichier national des permis de conduire (FNPC)	Ministère de l'Intérieur (DLP/ADJ)	Enregistrer et gérer toutes les informations relatives aux permis de conduire, en particulier les droits de conduire de tout conducteur.	Informatique	Fichier d'identification administrative	De manière générale, les informations relatives aux condamnations judiciaires, aux compositions pénales, aux amendes forfaitaires et aux mesures administratives affectant le permis de conduire doivent être effacées lorsque s'est écoulé un délai de 10 ans sans que soit à nouveau intervenue une nouvelle décision.	Direct	

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Arrêté du 29 août 1991, modifié par l'arrêté du 3 novembre 2006 (traitement régi par l'article 7 de la loi n° 2006-64 du 23 janvier 2006)	Fichier national transfrontière (FNT)	Direction générale de la police nationale (direction centrale de la police aux frontières)	Collecte des informations concernant les embarquements et débarquements de passagers aériens à destination ou en provenance de pays « sensibles ».	Informatique	Administratif	3 ans	Direct	La loi de 2006 a donné une base législative au FNT, créé auparavant par l'arrêté du 29 août 1991. Fonctionnant jusque-là sous une forme manuelle, son fonctionnement et son fonctionnement étaient devenus très aléatoires, ce qui a conduit à une informatisation du FNT.
Arrêté du 28 octobre 1992 (modifié par l'arrêté du 13 mai 1998)	Traitement automatisé d'informations nominatives de gestion et de suivi des procédures et du courrier dans les unités élémentaires de la gendarmerie – Brigade Bureautique 2000 (BB 2000)	Gendarmerie (au sein de chaque brigade territoriale)	Application locale destinée à gérer le service et les registres et de permettre un partage de l'information sur la connaissance de la circonscription de l'unité.	Informatique	Application bureautique	- 2 ans pour le registre et les amendes forfaitaires ; - toute mise à jour du dossier de circonscription entraîne la suppression des données précédentes (pas d'historique).	- Indirect pour les données relevant de l'article 11 du code de procédure pénale (secret de l'instruction) - Direct pour toutes les autres informations	En cours de remplacement par l'application PULSAR, ce fichier comprend notamment le dossier de circonscription, qui recense les personnes y travaillant ou y résidant devant être connues du fait de leurs responsabilités, de « leur attachement au milieu militaire » ou de décisions de justice.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Arrêté du 22 mars 1994 (modifié par l'arrêté du 28 février 2005)	Fichier de suivi des titres de circulation délivrés aux personnes sans domicile ni résidence fixe (FSDRF)	Gendarmerie (STRJD)	Suivi des titres de circulation délivrés aux personnes sans domicile ni résidence fixe, soumises aux dispositions de la loi n° 69-3 du 3 janvier 1969.	Informatique	Fichier d'identification administrative	- données conservées 6 mois après la sédentarisation ; - conservées jusqu'à l'âge de 80 ans en l'absence de sédentarisation ; - effacées en cas de décès.	Direct	
Arrêté du 19 décembre 1994 (modifié par l'arrêté du 30 juillet 2002)	Fichier de suivi des personnes faisant l'objet d'une rétention administrative (SUICRA)	Gendarmerie	Assurer le suivi des personnes faisant l'objet d'une décision de rétention.	Informatique	Administratif	2 ans à compter du prononcé de la dernière mesure de rétention.	Direct auprès du groupe-ment de gendarmerie local ou du responsable de la gestion du centre de rétention administrative (CRA)	Ce fichier ne concerne que les CRA du Mesnil-Geisposheim, rattachés aux groupements de gendarmerie locaux. La mise en œuvre du fichier ELO, qui permet une gestion commune inter-services des étrangers, a entraîné l'abandon en 2008 de l'application SUICRA par la gendarmerie.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Arrêté du 24 février 1995	Main courante informatisée (MCI)	Direction générale de la police nationale	Gérer l'emploi des effectifs, les événements et les déclarations des usagers.	Informatique	Application bureautique	Tant qu'elles sont nécessaires eu égard aux finalités du fichier.	Direct auprès du commissariat .	Le fichier des personnes en cause comprend des données personnelles : identité des personnes, catégorie (requérant, témoin, victime, auteurs), filiation, adresse. La procédure de remplacement de la MCI par un nouveau logiciel est en cours ; le projet d'arrêté définit les durées de conservation des données.
Arrêté du 15 mai 1996 (modifié par l'arrêté du 2 septembre 2005)	Fichier des véhicules volés (FVV)	Police et gendarmerie	Faciliter les recherches : - pour la découverte et la restitution de véhicules volés ; - la surveillance de véhicules signalés dans le cadre d'activités répressives ou préventives ; - des personnes susceptibles	Informatique	Judiciaire	La radiation des véhicules volés ou surveillés doit être effectuée sans délai avant restitution du véhicule volé ou dès que la mesure de surveillance devient sans objet.	Mixte : - direct pour les véhicules volés ; - indirect pour les véhicules surveillés.	

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Arrêté du 15 mai 1996 (modifié par l'arrêté du 2 septembre 2005)	Fichier des personnes recherchées (FPR)	Police et gendarmerie	d'utiliser un véhicule volé ou signalé. Faciliter la recherche de personnes recherchées (au titre de décisions judiciaires, faisant l'objet d'une enquête, étrangers faisant l'objet d'une décision d'expulsion, mineurs en fugue, personnes disparues, etc.).	Informatique	Judiciaire (fichier d'identification)	La radiation des personnes inscrites doit être effectuée sans délai en cas de découverte ou d'extinction du motif de la recherche.	Mixte.	Le décret n° 96-417 du 15 mai 1996 autorise à traiter, dans le cadre du FPR, des informations nominatives concernant « les signes physiques particuliers objectifs et permanents et comme élément de signalement des personnes ».
Arrêté du 28 octobre 1996 (modifié par l'arrêté du 20 février 2003)	Fichier national automatisé des personnes incarcérées	Administration pénitentiaire	Gestion des affectations des détenus et production de statistiques sur la population pénale.	Informatique	Judiciaire	Quinze mois à compter de la levée d'écrou.	Direct en ce qui concerne les personnes incarcérées	L'article 5 de l'arrêté dispose que les officiers de police judiciaire de la police nationale et de la gendarmerie nationale sont autorisés à consulter, à des fins de police judiciaire, les informations relatives à l'identité des personnes incarcérées et à l'incarcération.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Arrêté du 13 septembre 2002	Service central de préservation des prélèvements biologiques (SCPBP)	Gendarmerie	Assurer la gestion des prélèvements biologiques effectués dans le cadre d'affaires judiciaires concernant l'une des infractions mentionnées à l'article 706-55 du code de procédure pénale et entrainant l'enregistrement au FNAEG.	Informatique	Application bureautique	40 ans, dans la limite des 80 ans de l'individu ayant fait l'objet des prélèvements.	Direct	
Arrêté du 28 août 2007	Fichier national des interdits de stade (FNIS)	Direction générale de la police nationale (DCSP)	Prévenir et lutter contre les violences lors des manifestations sportives, notamment en garantissant la pleine exécution des mesures administratives et judiciaires d'interdiction de stade.	Informatique	Administratif	5 ans à compter de l'expiration de la dernière mesure prononcée.	Indirect	Ce fichier est alimenté par les fiches judiciaires ou administratives des interdits de stade inscrites dans le FPR. En vertu de l'article L. 332-16 du code des sports et du décret n° 2006-1549 du 8 décembre 2006, les préfets peuvent communiquer aux fédérations sportives certaines informations figurant dans le FNIS.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Arrêté du 15 novembre 2007	Application de gestion du répertoire informatisé des propriétaires et possesseurs d'armes (AGRIPPA)	Ministère de l'Intérieur (DLPAJ)	Traitement automatisé de données à caractère personnel concernant les détenus d'armes et de munitions.	Informatique	Administratif	20 ans.	Direct	La délibération n° 2006-231 de la CNIL portait sur un projet de décret en Conseil d'État.
Autres								
Aucun texte (créé en 1942)	Fichier de la batellerie	Gendarmerie (STRJD)	Suivi des mariniers ainsi que des bateaux affectés au transport fluvial de marchandises.	Manuel (fichier papier)	Administratif	La procédure d'épurent manuel mise en place en 1974 consiste en la destruction des fiches concernant les mariniers décédés ou de plus de 80 ans, ainsi que celles des bateaux détruits.		Ce fichier obsolète contient 52 000 fiches. Conservé en l'état dans l'attente d'une décision relative à la création d'un fichier informatique pour le suivi des activités du milieu fluvial.

Texte de référence initial	Instruction initiale de 1971	Nom du fichier	Fichier alphabétique de renseignements (FAR)	Administration gestionnaire	Gendarmerie	Objet	Permettre aux brigades de gendarmerie d'acquies une connaissance approfondie de la population, notamment en vue de la réalisation d'enquêtes administratives.	Nature du fichier	Manuel local (fiches papiers)	Type	Renseignement	Durée de conservation des données	Épurement manuel : - les personnes décédées ou de plus de 80 ans ne doivent plus figurer dans le FAR ; - les personnes ayant déménagé ne doivent plus figurer dans le fichier de l'unité de leur ancienne domiciliation.	Droit d'accès	Indirect	Observations	- Le FAR doit être détruit en 2010. - Il comprend environ 60 millions de fiches. - Entièrement manuel, il n'assure aucune traçabilité des consultations.
Texte de référence initial	Aucun texte (créé en 1975)	Nom du fichier	Fichier des personnes nées à l'étranger (FPNE)	Administration gestionnaire	Gendarmerie (STRJD)	Objet	Enregistrement de toute personne née à l'étranger entrant en contact avec la gendarmerie.	Nature du fichier	Manuel (fichier papier)	Type	Administratif	Durée de conservation des données	Épurement manuel : les personnes décédées ou de plus de 80 ans ne doivent plus figurer dans le FPNE.	Droit d'accès	Indirect	Observations	Ce fichier sera supprimé en octobre 2010. Il comprend actuellement environ 7 millions de fiches, mais n'est plus alimenté ni consulté depuis septembre 2007.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Aucun texte (créé en 1982)	Fichier des avis de condamnations pénales (FAC)	Gendarmerie	Compléter le FAR avec les renseignements collectés auprès des greffes des tribunaux (condamnations exécutoires inscrites au bulletin n° 2 du casier judiciaire).	Manuel local (fiches papiers)	Judiciaire	Épurement manuel à partir des informations collectées auprès des greffes ou lors de la promulgation de lois d'amnistie.	Inconnu	Classé comme « <i>fichier obsolète en cours</i> » dans le rapport Bauer de 2006. L'accès direct au bulletin n° 2 du casier judiciaire n'est en effet pas autorisé aux services de police judiciaire.
Aucun texte.	Fichier de travail de la police judiciaire (FTPJ)	Direction générale de la police nationale (SRPJ)	Collecte d'informations sur des délinquants spécialisés.	Informatique (bases locales au sein des SRPJ)	Judiciaire	Données conservées tant qu'elles sont nécessaires eu égard à la finalité des fichiers.		Créé en 1987 et déclaré à la CNIL en 1991, le FTPJ n'a fait l'objet d'aucun texte réglementaire. À la différence du fichier des brigades spécialisées, cette application ne permet pas l'échange d'informations entre applications locales. Le FTPJ n'est plus utilisé que par quelques services de P.J.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Aucun texte	Fichier des brigades spécialisées (FBS)	Direction générale de la police nationale (seuls les personnels disposant d'une habilitation spéciale, en nombre réduit, ont accès à ce fichier)	Fichier de travail des services de police spécialisés luttant contre la grande délinquance et le crime organisé. Il a pour objectif d'utiliser au mieux les diverses informations collectées à l'occasion de la surveillance du milieu criminel, de permettre des échanges confidentiels entre services spécialisés et d'autoriser tous les croisements de recherche possibles entre les informations figurant dans la base.	Informatique	Judiciaire	Données conservées tant qu'elles sont nécessaires eu égard à la finalité des fichiers.		Mise en place en 1991, cette application a beaucoup vieilli techniquement et sa modernisation a été annoncée. Une réflexion est également entamée sur la nécessité de lui donner une base législative distincte de celle de l'article 21 de la loi pour la sécurité intérieure du 18 mars 2003.
Aucun texte (déclaré à la CNIL simultanément à la déclaration du STIC)	Logiciel de rédaction des procédures (LRP)	Direction générale de la police nationale	Rédiger les procès-verbaux et les rapports administratifs ou judiciaires.	Informatique	Application bureautique.	Épurement tous les cinq ans.		Ce logiciel doit être remplacé par ARDOISE pour l'alimentation d'ARANE.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Règlement (CE) n° 1338/2001 du 28 juin 2001 définissant des mesures nécessaires à la protection de l'euro contre le faux monnayage	Fichier national du faux monnayage (FNFM)	Police et gendarmerie	Recenser les affaires relatives au faux monnayage commises sur le territoire national (données relatives à l'affaire, à l'infraction, aux coupures saisies, à l'identité des mis en cause et à leur signalement).	Informatique	Judiciaire			Mis en service lors de la mise en circulation de l'euro, le 1 ^{er} janvier 2002. Il permet de satisfaire aux obligations de centralisation au niveau national des informations relatives au faux monnayage ainsi qu'à celles d'information d'Europol (article 8 du règlement).
Aucun texte	Fichier des objets signalés (FOS)	Gendarmerie	Vérifier si un objet bien identifié a été signalé par les unités de gendarmerie à l'occasion d'une enquête judiciaire ou par le SIS comme étant volé.	Informatique	Judiciaire	Épurement automatique des données en fonction des durées de conservation des objets.		Sous-ensemble de JUDEX, ce fichier devenu autonome n'a pas été déclaré à la CNIL et doit être fusionné avec le STIC-objets dans le cadre de la mise en place du fichier des objets et véhicules signalés (FOVES).

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Procédure de déclaration en cours auprès de la CNIL	Gestion du terrorisme et des extrémismes violents (GESTEREXT)	Préfecture de police de Paris (RGPP et depuis 2008, DRPP – service chargé de la lutte contre le terrorisme et les extrémismes à potentialité violente)	- Prévenir les actes de terrorisme ; - Surveiller les individus, groupes, organisations et phénomènes de société susceptibles de porter atteinte à la sûreté nationale.	Informatique	Renseignement	Les données ne peuvent être conservées que pour autant qu'elles sont toujours nécessaires eu égard aux finalités du fichier.	Indirect	GESTEREXT constitue l'équivalent de CRISTINA pour la DRPP, celle-ci ayant conservé les missions de renseignement intérieur à Paris. Cette application remplacera GESTER, créé en 1996
Aucun texte (créé en 2008)	Outil de centralisation et de traitement opérationnel des procédures et des utilisateurs de signatures (OCTOPUS)	Préfecture de police de Paris (direction de la police de proximité – brigade des réseaux ferrés de la sous direction de la police régionale des transports)	Recherche des auteurs de « tags » (identification des auteurs de dégradations, établissement de synthèses de faits et de recoupements).	Informatique	Judiciaire (fichier d'identification)	10 ans à partir du dernier fait.	Indirect	Le fichier comprend des informations sur les mineurs sans limitation d'âge (en application de l'article 21 de la loi n° 2003-239 pour la sécurité intérieure). Il comprend 237 fiches au 10 novembre 2008. OCTOPUS doit faire l'objet d'une procédure de déclaration à la CNIL au cours de l'année 2009.

<p>Texte de référence initial</p> <p>Aucun texte (en phase d'expérimentation depuis décembre 2008)</p>	<p>Nom du fichier</p> <p>Logiciel d'uniformisation des prélèvements et identification (LUPIN)</p>	<p>Administration gestionnaire</p> <p>Préfecture de police de Paris (service d'investigation transversale de la direction de la police urbaine de proximité)</p>	<p>Objet</p> <p>Lutter contre les cambriolages en procédant à des rapprochements à partir des données de police technique et scientifique et relatives aux modes opératoires recueillies sur les scènes d'infraction.</p>	<p>Nature du fichier</p> <p>Informatique</p>	<p>Type</p> <p>Fichier de traitement du renseignement judiciaire</p>	<p>Durée de conservation des données</p> <p>Trois ans (épurement manuel). Le projet d'arrêté prévoit une durée de cinq ans et le logiciel va évoluer vers un épurement automatique</p>	<p>Droit d'accès</p>	<p>Observations</p> <p>LUPIN doit faire l'objet d'une procédure de déclaration à la CNIL, mais le projet d'arrêté ne pourra être transmis à celle-ci que sous réserve d'une modification de la loi du 18 mars 2003, qui réserve actuellement les traitements d'infractions à caractère sériel aux crimes et délits punis de plus de cinq ans d'emprisonnement (atteintes aux personnes) ou de plus de sept ans (atteintes aux biens).</p>
---	--	---	--	---	---	---	-----------------------------	--

<p>Texte de référence initial</p>	<p>Aucun texte (en phase d'expérimentation depuis 2006)</p>	<p>Cellule opérationnelle de rapprochement et d'analyse d'infractions liées (CORAIL)</p>	<p>Administration gestionnaire</p> <p>Préfecture de police de Paris (DPJ)</p>	<p>Objet</p> <p>Diffuser aux services d'enquêtes les fiches relatives à des faits sériels, sous la forme d'états opérationnels tirés des infractions, afin de faciliter les rapprochements.</p>	<p>Nature du fichier</p> <p>Informatique</p>	<p>Type</p> <p>Fichier de traitement du renseignement judiciaire</p>	<p>Durée de conservation des données</p> <p>- 3 ans pour les fiches et les états opérationnels ; trois ans à compter du fait le plus récent pour les synthèses ; - les synthèses élucidées sont conservées jusqu'au terme de la période incluant la possibilité d'une « récidive légale » de l'auteur condamné ; - 5 ans pour les circulaires régionales.</p>	<p>Droit d'accès</p> <p>Indirect</p>	<p>Observations</p> <p>CORAIL a pour objectif de faciliter l'identification de récidivistes notoires ayant commis des infractions graves (crime ou délit contre les personnes punis de plus de cinq ans d'emprisonnement ou aux biens et punis de plus de sept ans d'emprisonnement)</p>
<p>Aucun texte</p>	<p>Système de traitement des images des véhicules volés (STIV)</p>	<p>Gendarmerie (STRJD – cellule de traitement des images des véhicules volés)</p>	<p>Objet</p> <p>Exploiter à des fins judiciaires les photographies de certains véhicules prises par les radars automatisés (véhicules volés, mis sous surveillance, etc.).</p>	<p>Nature du fichier</p> <p>Informatique</p>	<p>Type</p> <p>Judiciaire (fichier d'identification)</p>	<p>Durée de conservation des données</p> <p>Non prévue pour le moment.</p>	<p>Droit d'accès</p>	<p>Observations</p> <p>Ce traitement est en phase préparatoire de déclaration auprès de la CNIL. Compte tenu d'un risque de redondance avec le futur système central de traitement du LAPI (SCTL), il est envisagé de l'abandonner.</p>	

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Aucun texte	ARAMIS	Gendarmerie	Système de traitement des informations présentant un caractère opérationnel (gestion des interventions ; messagerie interne de suivi des situations ; renseignement pour le suivi de l'ordre public).	Informatique	Application bureautique.	- 3 mois pour les données relatives aux appelants ; - 2 ans pour les fiches d'appel et les interventions associées ; - 2 ans et demi pour les messages de renseignement et les points de situation.		Les destinataires des informations sont les patrouilles en cours et leurs autorités hiérarchiques immédiatement supérieures.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Aucun texte (dossier de déclaration déposé en avril 2008 à la direction des affaires juridiques du ministère de la Défense)	ATHENA	Gendarmerie	<ul style="list-style-type: none"> - Améliorer l'accueil du public et les relations avec les usagers ; - Aider et sécuriser les interventions ; - Optimiser le traitement du renseignement d'ordre public et de défense. 	Informatique	Renseignement	De 2 à 15 ans selon le type de données.		ATHENA est destiné à remplacer le FAR et le module ARAMIS. Il comprendra un module « FAR » comprenant des fiches de renseignement sur certaines personnes inscrites d'autorité (personnes violentes, détenteurs d'armes ou de chiens dangereux, etc.) ou à la demande de certaines personnes (« tranquillité vacances », personnes âgées...).

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Aucun texte. Sa mise en œuvre suppose la modification de l'article 21-1 de la loi du 18 décembre 2003 et l'élaboration d'un décret pris après avis de la CNIL.	Application judiciaire dédiée à la révélation des crimes et délits en série (AJDRCDs)	Gendarmerie	Faciliter la détection : - des crimes et délits de même nature et imputables à un même auteur ou groupe d'auteurs ; - des infractions ou comportements délinquants réitérés par un même auteur ou groupe d'auteurs.	Informatique	Fichier de traitement du renseignement judiciaire	Fonction du délai de prescription de l'action publique, du statut des personnes inscrites dans le système et de toute décision de justice définitive connue d'ARIANE. Un système d'apurement automatique est prévu.	Direct, auprès du magistrat référent du fichier.	Cette application en phase de conception recueillera tout type de données en rapport direct avec une affaire judiciaire (procédures judiciaires, données issues d'autres fichiers de police, sources ouvertes au public...).
Projet de décret en cours d'examen par le Conseil d'Etat.	Exploitation documentaire et valorisation de l'information relative à la sécurité publique (EDVIRSP)	Direction générale de la police nationale (direction centrale de la sécurité publique – sous direction de l'information générale)	Collecte, conservation et traitement des données relatives : - aux personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique ; - aux personnes faisant l'objet d'enquêtes administratives.	Informatique	Renseignement	- Les données ne peuvent être conservées que pour autant qu'elles sont toujours nécessaires eu égard aux finalités du fichier s'agissant de la première finalité ; - 5 ans pour les données concernant les enquêtes administratives à compter de leur enregistrement ou de la cessation des fonctions ou	Indirect	La CNIL a rendu sa délibération sur le projet de décret EDVIRSP le 20 octobre 2008. Le décret sur l'application EDVIRSP servira de base juridique à la nouvelle version de l'application GEVI de la direction du renseignement de la préfecture de police de Paris.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Aucun texte. Un décret en Conseil d'État est prévu.	Application de rapprochements d'identification et d'analyse pour les enquêteurs (ARIANE)	Police et gendarmerie	Faciliter la constatation des infractions, le rassemblement des preuves et la recherche des auteurs.	Informatique	Fichier d'antécédents judiciaires	des missions au titre de laquelle l'enquête est menée ; - trois ans pour les données concernant les mineurs (treize ans et plus) pouvant porter atteinte à la sécurité publique après l'intervention du dernier événement ayant justifié un enregistrement.	Indirect	ARIANE est une application destinée à fusionner le STIC et JUDEX dans le cadre du rapprochement entre la police et la gendarmerie. La déclaration d'ARIANE à la CNIL est en cours d'élaboration.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Aucun texte (projet de décret et déclaration à la CNIL en cours d'élaboration)	Fichier des objets volés et signalés (FOVES)	Police et gendarmerie	Vérifier si un objet ou un véhicule ont été signalés ou déclarés volés. L'ensemble des objets et véhicules sera classé en 12 catégories.	Informatique	Judiciaire (fichier d'identification)	Épurement automatique des données en fonction des durées de conservation des objets.		Issu de la fusion entre le STIC – objets, le FVV et le FOS, ce fichier devrait être mis en place au deuxième trimestre 2009. Il sera alimenté directement par les applications ARDOISE et ICARE.
Aucun texte	Application de recueil de la documentation opérationnelle et d'informations statistiques sur les enquêtes (ARDOISE)	Direction générale de la police nationale	Collecter et archiver les informations recueillies lors des missions de police judiciaire ou administrative (données issues de procès-verbaux, comptes rendus d'enquêtes et rapports administratifs ou judiciaires).	Informatique	Application bureautique	5 ans à compter de la transmission à l'autorité judiciaire ou administrative compétente.	Indirect	ARDOISE est destiné à terme à remplacer le logiciel de rédaction des procédures et à alimenter le fichier ARIANE. La déclaration d'ARDOISE est en cours (avis de la CNIL rendu et Conseil d'État saisi).

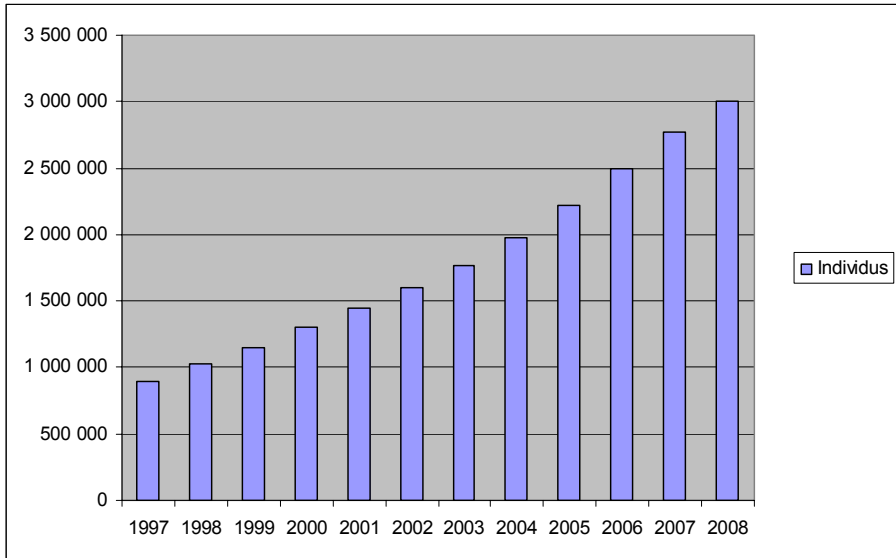
Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Aucun texte	ICARE	Gendarmerie	Assister les militaires de la gendarmerie dans la rédaction de leurs procès-verbaux.	Informatique	Application bureautique	Les données à caractère personnel sont conservées jusqu'à la clôture de la procédure et transmission aux autorités judiciaires compétentes. Elles ne sont accessibles qu'au niveau de l'unité de rattachement de la procédure.		ICARE constituera l'outil d'alimentation des fichiers JUDEX et FVV et à terme, d'ARIANE par la gendarmerie. Il alimentera également la future application CASSIOPEE du ministère de la Justice. Le dossier de déclaration a été déposé en juillet 2008 à la direction des affaires juridiques du ministère de la Défense.
Aucun texte	PULSAR	Gendarmerie	- Gérer le service et les registres ainsi que les amendes forfaitaires ; - Créer des messages d'information statistique et les bulletins d'analyse des accidents.	Informatique	Application bureautique	Variable selon les modules, sans excéder 3 ans.		PULSAR est une évolution de l'application BB 2000, déclarée à la CNIL. Dans certains modules, PULSAR comprendra des informations relatives aux personnels, aux victimes (y compris mis en cause. Son déploiement est prévu en 2009.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Nature du fichier	Type	Durée de conservation des données	Droit d'accès	Observations
Aucun texte	Gestion des étrangers en situation irrégulière (GESI)	Préfecture de police de Paris (DRPP – sous direction chargée de la lutte contre l'immigration irrégulière et le travail illégal des étrangers)	Assurer une gestion en temps réel, de l'interpellation jusqu'à la reconduite, des étrangers en situation irrégulière interpellés par les services de la préfecture de police.	Informatique	Administratif et judiciaire	2 ans.	Direct	
Aucun texte	GREGOIRE	Ministère de l'immigration, de l'intégration, de l'identité nationale et du développement solidaire.	Refonte complète de l'application AGDREF. Il vise notamment : - le traitement interministériel des dossiers des étrangers dans les préfectures, avec un périmètre étendu aux consulats, services de police et unités de gendarmerie ; - l'introduction de la biométrie à des fins de lutte contre la fraude.	Informatique	Administratif			Le calendrier de mise en oeuvre prévoit un développement en 2009, la migration des données figurant dans AGDREF et le déploiement opérationnel de l'application étant prévus entre la fin 2009 et l'été 2010.

ANNEXE 2 : ÉVOLUTION DU VOLUME DES PRINCIPAUX FICHIERS DE POLICE

FICHER AUTOMATISÉ DES EMPREINTES DIGITALES

Années	Individus	Variations
1997	889 755	-
1998	1 022 043	132 288
1999	1 152 171	130 128
2000	1 299 043	146 872
2001	1 442 239	143 196
2002	1 597 751	155 512
2003	1 761 315	163 564
2004	1 981 615	220 300
2005	2 217 524	235 909
2006	2 493 079	275 555
2007	2 766 283	273 204
2008 ^(a)	2 998 523	232 240

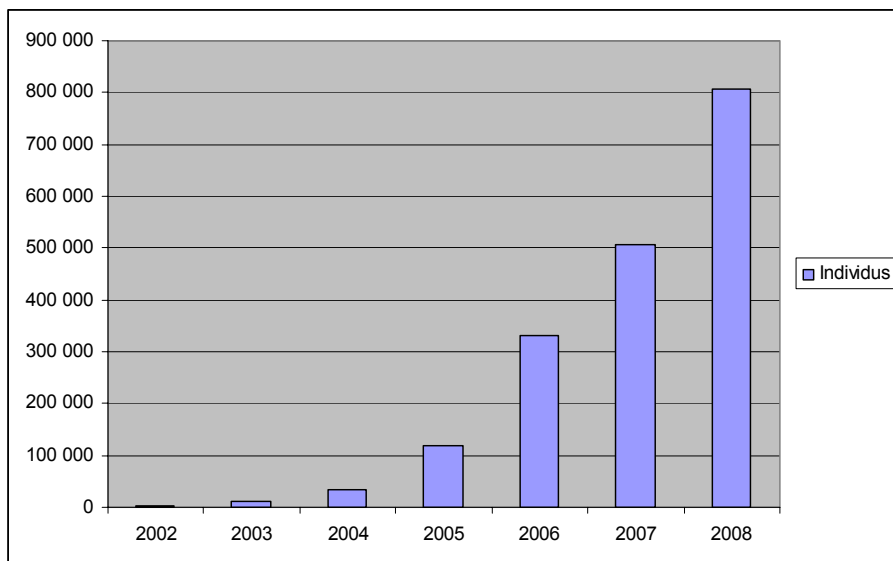


(a) Au 1^{er} octobre

FICHER NATIONAL DES EMPREINTES GÉNÉTIQUES ^(a)

Années	Individus	Variations
2002	2 635	-
2003	11 796	9 161
2004	33 917	22 121
2005	119 612	85 695
2006	331 348	211 736
2007	506 085	174 737
2008	806 356	300 271

^(a) Hors profils génétiques issus des prélèvements sur suspects aux fins de comparaison et hors traces ou profils enregistrés dans le cadre de recherches pour l'identification d'une victime anonyme ou de recherches après une disparition de personnes.

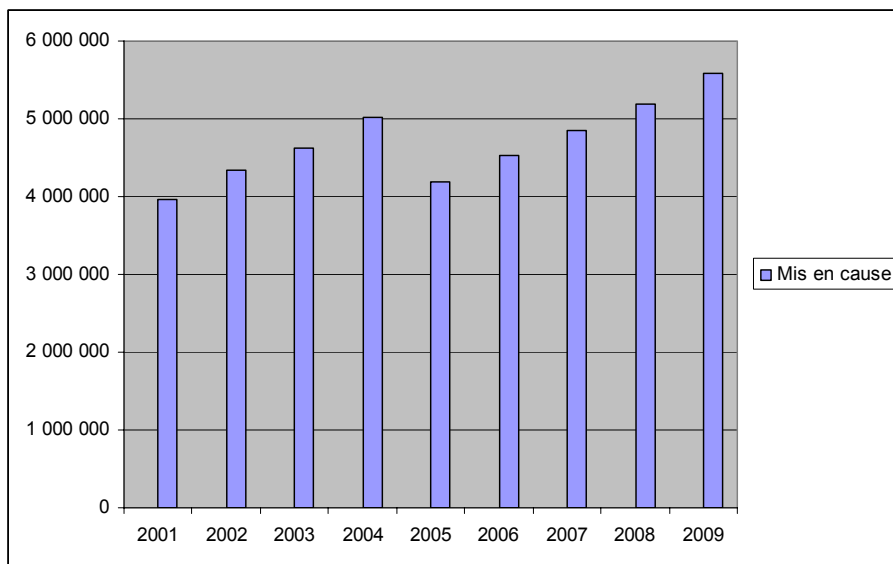


SYSTÈME DE TRAITEMENT DES INFRACTIONS CONSTATÉES ^(a)

Au 1 ^{er} janvier	Nombre de mis en cause	Évolution ^(b)
2001	3 957 453	-
2002	4 334 184	376 731
2003	4 614 820	280 636
2004	5 020 856	406 036
2005	4 194 126	- 826 730
2006	4 527 891	333 765
2007	4 854 958	327 067
2008	5 192 831	337 873
2009	5 580 677	387 846

^(a) Aucune donnée relative au nombre d'individus inscrits en qualité de mis en cause chaque année n'est disponible. Les données figurant dans le tableau correspondent à la volumétrie totale des mis en cause arrêtée à un instant donné, à savoir le 1^{er} janvier de chaque année.

^(b) La progression de la volumétrie ne reflète pas le nombre de personnes distinctes nouvellement inscrites dans une année, mais traduit le résultat net entre inscriptions et épurements effectués au cours de l'année considérée. La baisse constatée fin 2004 est consécutive à la mise en place de la fonction d'épurement automatique.



Sources : rapport de la mission d'audit sur le fonctionnement et les performances de la police technique et scientifique dans la lutte contre la délinquance de masse et la criminalité organisée ; ministère de l'Intérieur, de l'outre-mer et des collectivités territoriales.

ANNEXE 3 : RÉPONSE DU MAGISTRAT DE LIAISON AU ROYAUME-UNI AU QUESTIONNAIRE DES RAPPORTEURS

Magistrat de liaison

LONDRES

Le 18 décembre 2008

FICHIERS DE POLICE AU ROYAUME-UNI

INTRODUCTION

Avant de répondre au questionnaire, il nous est apparu essentiel de décrire rapidement les fichiers de police les plus importants existant au Royaume-Uni.

1) Le National Police Computer

Le NPC est un système (fichier) informatique commun aux polices d'Angleterre, du Pays de Galles et de l'Irlande du Nord.

Il a été créé en 1974 et était alors utilisé pour l'enregistrement des véhicules volés. Aujourd'hui, il se compose de plusieurs fichiers, consultables 24 heures sur 24 comportant des informations aussi bien locales que nationales.

Ainsi, les policiers peuvent avoir accès à la liste des véhicules volés, des empreintes digitales, des propriétaires de véhicules (y compris assurances, contrôles techniques...), des délinquants, des personnes recherchées ou disparues, à des analyses sur des rapprochements d'affaires criminelles, aux condamnations, à la liste objets volés, des armes à feu, des mises en garde sur les plaques minéralogiques, des délinquants sexuels...

Il est également possible de faire des recherches et des rapprochements sur les noms, des noms similaires, des prénoms, des parties de noms ou alias et encore d'autres signalements d'individus ou de véhicules.

En juillet 2006, 97 millions d'informations étaient regroupées dans ces fichiers (y compris les personnes, les permis de conduire et les véhicules).

Ce fichier est relié au fichier d'empreintes génétiques (ADN).

2) Le Fichier ADN

Ce fichier a été créé en 1995.

À la fin de l'année 2005, il contenait le profil d'environ 3,4 millions de personnes dont 585 000 sont des mineurs de moins de 16 ans.

À la fin de 2006, ce chiffre a atteint 4 millions de personnes ce qui en fait le plus important fichier ADN au monde. Chaque mois, 30 000 échantillons sont ajoutés en provenance de scène de crime ou de prélèvements sur les personnes arrêtées.

Ainsi, 5,2 % de population du Royaume-Uni se trouve dans ce fichier.

Entretenir et développer ce fichier est une des premières priorités du Gouvernement britannique. C'est pourquoi le Gouvernement et la Police ont investi dans ce fichier près de 300 millions de Livres dans les cinq dernières années.

Une unité du *Home Office* est en charge de réguler le fichier informatique. Une commission composée de fonctionnaires du *Home Office* et de membres de l'*Association of Chief Police Officers* et de l'*Association of Police Authorities* est chargée de contrôler le fonctionnement de ce fichier informatique. La *Human Genetics Commission* est aussi représentée et des discussions sont en cours pour l'établissement d'un groupe d'éthique (*ethics group*) dans le but de contribuer et d'offrir des conseils.

La gestion de ce fichier a été confiée à la police scientifique (*Forensic Science Service*) depuis décembre 2005.

3) *Le National Automated Fingerprint Information System (NAFIS)*

Ce fichier permet de connecter entre elles 43 forces de police et autres agences, 500 postes de travail et près de 200 unités de scanners à travers l'Angleterre et le Pays de Galles.

Ces bureaux sont capables d'enregistrer les empreintes digitales et de transmettre leur image dans la base de données nationale.

Elle contient aujourd'hui près de 5 millions d'empreintes relevées sur des scènes de crimes non résolus ou de personnes mises en cause.

4) *Le Footwear Intelligence Tool*

Le *Forensic Science Service* a lancé la première base de données nationale d'empreintes de chaussures récupérées sur des scènes de crime le 15 février. Cette base de données est désormais accessible à toutes les forces de police.

Ce fichier contient déjà les données concernant les chaussures d'environ 20 000 suspects dont les empreintes ont été retrouvées sur les scènes de crime à travers les pays et peut en accueillir 30 000 autres.

Il est mis à jour quotidiennement et reçoit les empreintes des forces de police qui les ont relevées lors de gardes à vue et celles retrouvées sur les lieux d'infractions.

Légalement, des suspects peuvent désormais voir un profil de leur chaussure enregistré. Cela implique alors une photographie de la chaussure et une impression avec de l'encre sur le sol.

5) *Les MAPPAs (Multi Agency Public Protection Arrangements)*

Les MAPPAs ont été créés par le *Criminal and Justice Act* de 2000 : l'établissement de MAPPAs locaux est devenu une obligation pour la police, le service de probation et l'administration pénitentiaire.

Ces autorités coopèrent avec les services sociaux, de santé, du travail, du logement... afin d'évaluer et de prendre en compte les risques posés par les délinquants sexuels et les personnes violentes.

6) *Le VISOR (Violent and Sex Offender Register)*

Ce fichier est accessible aux officiers de police et au personnel du Service de probation.

Dans le VISOR sont enregistrés le nom, l'adresse, la photographie, une évaluation, le risque que la personne représente, le *modus operandi* de chaque délinquant sexuel.

Ce fichier est relié au *National Police Computer*.

Le CEOP (*Child Exploitation and Online Protection*), qui dépend de la SOCA, collabore à l'« alimantation et au fonctionnement de ce fichier en ce qui concerne les abus sexuels sur mineurs.

7) *Le fichier concernant le terrorisme*

Il existe une base de données qui peut regrouper tous les renseignements sur une personne et ce, sans aucune restriction (ethnie, âge, couleur de peau, déplacements...). Ces renseignements en tant que tels ne peuvent toutefois pas être utilisés lors de la procédure « judiciaire ».

Ce fichier est géré par le SO15 de la Metropolitan Police de Londres et les renseignements sont collectés par les policiers et le MI5.

8) *Le Knowledge Desk*

Ce fichier est tenu par la SOCA (*Serious Organised Crime Agency*). Il recueille des renseignements sur différentes affaires relatives à la criminalité organisée traitées non seulement par la SOCA mais également par les autres unités de police.

9) *Le fichier des condamnations (correspondant à notre casier judiciaire)*

Le *Criminal Record* est géré par le *Criminal Record Bureau* (CRB), dépendant du *Home Office*, qui a un accès partiel au *Police National Computer*.

Le « casier judiciaire » n'est pas accessible au public. Toutefois, un employeur peut faire une demande pour avoir accès à certaines informations avec l'autorisation du *Chief police Officer*.

10) *Le fichier « Ordre Public » (tenu par la National Public Order Intelligence Agency)*

Ce fichier contient les données sur les mouvements extrémistes et peut comporter des données politiques, syndicales, ou encore sur le militantisme associatif tels que les altermondialistes, les mouvements de défense des animaux particulièrement actifs en Angleterre et les mouvements hooligans.

11) *Les fichiers immigration tenus par la UK Border Agency (département du Home Office chargé de l'immigration)*

La UKBA alimente un fichier qui, sous la réserve exprimée ci-après, ressemble à notre Fichier National des Étrangers. Il existe, en effet, une grande différence avec le fichier français qui est accessible aux fonctionnaires de police ; au Royaume Uni ce fichier des étrangers est géré par les services du UKBA et les policiers ne peuvent pas y accéder directement ; bien entendu, ils peuvent obtenir des informations qu'il contient, mais ils doivent au préalable solliciter les services d'immigration

La UKBA dispose désormais de deux outils supplémentaires :

- Le Programme *e-border*

Ce fichier a été créé en 2006 suite aux attentats de Londres en 2005.

Il regroupe un certain nombre de données sur les passagers arrivant, sortant ou transitant par le Royaume-Uni et en provenance ou à destination de zones considérées comme potentiellement à risques.

Ce programme regroupe deux sortes de données :

- les données PNR qui sont exploitables dès la réservation du billet (numéro de vol, nom, mode de paiement).

- les données APIS qui sont transmises au moment de l'embarquement. Aujourd'hui les secondes sont beaucoup plus utilisées que les premières en matière de contrôle.

La police a accès à toutes ces données.

Les informations sur les passagers sont conservées pendant 10 ans.

- Le Programme *Semaphore*

Il a été lancé en novembre 2004 et constituait le préambule du programme *e-border*. Il prévoit la transmission de toutes les données biométriques.

Le programme IRIS en fait donc partie.

Le *JBOC (Joint Border Operation Center)* est l'outil opérationnel de *Semaphore* et du programme *e-border* décidé en janvier 2005. Il collecte et analyse les données des passagers et permet de faire des recherches croisées avec les différents fichiers de police. Il fonctionne 24 heures sur 24. Le personnel de *JBOC* est constitué d'officiers de l'*UK Border Agency* et de la police.

La reconnaissance de l'iris est un programme mis en place pour les passagers réguliers britanniques et résidents longue durée. On compte 10 points de passage (points équipés pour la reconnaissance de l'iris dans les aéroports) sur 9 points de frontières qui permettent aux passagers enregistrés de passer au contrôle automatique

Le programme est opérationnel dans les aéroports suivants : les 5 terminaux d'Heathrow, les terminaux 1 et 2 de Manchester, le terminal 1 de Birmingham et les terminaux nord et sud de Gatwick.

Grâce à ce programme, en mars 2008, 909.000 opérations de contrôle avaient été effectuées et 181.460 personnes enregistrées dans le programme. De plus, sur 20.000 alertes sur des profils passagers, 1.600 ont permis une arrestation (meurtre, kidnapping, fraude, viol et agression...).

*

* *

À ce stade et pour une meilleure compréhension, il paraît également nécessaire de fournir quelques précisions :

– *Her Majesty's Inspectorate of Constabulary* est un organisme composé d'inspecteurs nommés par la Reine, sur proposition du Ministre de l'Intérieur, chargé d'évaluer et éventuellement d'améliorer l'efficacité des services de police. Ils diffusent les codes de bonnes pratiques.

– Le *Chief Officer* est responsable des officiers non gradés.

– Le *Chief Constable* est l'équivalent du commissaire de police.

I - Les principes généraux s'appliquant en matière de mise en place et d'utilisation des fichiers de police

Le Parlement a voté des lois relatives à l'utilisation des fichiers ; elles ont pour but d'assurer la protection et la confidentialité des informations contenues dans ces fichiers, qu'elles aient un caractère personnel, qu'elles aient un impact sur la sécurité nationale, l'économie ou qu'elles concernent des poursuites ou enquêtes en cours.

• Le *Data Protection Act* de 1998 : il régleme la manière dont toutes les organisations (et pas seulement la police) doivent protéger les données personnelles. L'*Information Commissioner* a le pouvoir d'initier des inspections en cas de nécessité.

• Le *Regulation of Police Investigatory Act* de 2000 : cette loi vise entre autres, l'interception et la révélation de données concernant les communications téléphoniques, la surveillance, l'utilisation de personnes particulières (informateurs), l'acquisition de moyens permettant le décryptage de données codées et de mots de passe.

Sur le fondement de ce texte, ont été publiés des codes de bonnes de pratiques (*Codes of Practise*) dont le but est de faire prendre conscience aux personnes responsables de l'importance de la sécurité des données spécialement lorsque les données sont transférées aux autorités publiques (police et mise en application de la loi).

Ces codes font un certain nombre de recommandations pour l'utilisation et la conservation des données.

Les autorités de police et les «agences» en charge de la mise en application des lois peuvent faire l'objet d'inspections par le *Interception Communication Commissioner*.

- Le Criminal Procedure and Investigations Act de 1996 : cette loi contient des règles de procédure pénale ainsi qu'un code de bonnes pratiques qui établit la manière dont les officiers de police enregistrent, conservent et révèlent au Procureur les éléments obtenus dans le cadre d'une enquête pénale.

- Le Freedom of Information Act de 2000: cette loi encadre les conditions de divulgation des informations détenues par les autorités publiques ou par des personnes leur fournissant un service.

Le législateur a par ailleurs décidé que dans certaines circonstances les informations peuvent être révélées au public.

- Le Police and Criminal Evidence Act de 1984 : ces dispositions détaillent les moyens de conservation des données recueillies au cours de perquisitions, d'interpellations et de rétention de personnes, d'investigations et d'interrogatoires de détenus.

II - Les modalités d'alimentation, de mise à jour et de consultation des fichiers de police

a) La nature des modes d'alimentation

Selon nos interlocuteurs, ces fichiers peuvent être alimentés soit par des informations papier soit par des données informatisées.

b) Les modalités de mise à jour

Le Ministre de l'Intérieur a établi des lignes directrices relatives à la gestion des informations par la police (*Code for Management of Police Information - MoPI*), qui sont entrées en vigueur le 14 novembre 2005. Le Code MoPI énonce les principes qui régissent les procédures d'obtention et d'enregistrement des informations, les procédures destinées à s'assurer de la précision des informations, les procédures en vue de réexaminer la nécessité de conserver les informations et de les détruire lorsqu'elles ne sont plus utiles, les procédures de partage d'informations entre les diverses forces de police et entre la police et d'autres organismes publics. Le Code MoPI s'applique directement à toutes les forces de police d'Angleterre et du Pays de Galles et à la SOCA.

Le respect des principes énoncés par le Code MoPI par les forces de police est mis en œuvre par les *HM Inspectors of Constabulary*.

Les *Retention Guidelines*, qui font partie du Code MoPI, régissent la conservation des informations contenues dans le PNC. Ces lignes directrices encadrent l'accès aux données du PNC plutôt que leur suppression, notamment en imposant des périodes strictes au terme desquelles les informations ne peuvent plus être conservées en vue d'être utilisées à l'encontre de la personne.

Comme il vient d'être dit, ces informations sont toutefois conservées et peuvent être consultées par la police et utilisées comme de simples informations.

Les fichiers pourraient être également consultés par l'autorité (dépendant du *Home Office*) en charge des «casiers judiciaires», lorsqu'un individu fait l'objet d'une procédure de vérification approfondie du *Criminal Records Bureau*. Dans ce cas précis, les données ne seraient également utilisées que comme de simples informations.

Ainsi la police jouit d'un accès continu aux données, tandis que leur accès est restreint pour les utilisateurs non policiers.

Les infractions susceptibles de faire l'objet d'un enregistrement au sein d'un fichier sont classées en catégories A, B et C, et sont fondées sur la gravité de l'infraction (A désignant les infractions les plus graves). Les fichiers sont en principe conservés jusqu'à ce que la personne ait atteint l'âge de 100 ans, mais leur accès peut être restreint, aux fins d'utilisation par la police uniquement.

– Pour les infractions de catégorie A, lorsqu'un individu a fait l'objet d'une peine privative de liberté d'au moins 6 mois, l'historique de la condamnation ne sera jamais en « accès restreint ». En revanche, la condamnation sera en « accès restreint » après une période de 35 ans pour une infraction de catégorie B, et de 30 pour les infractions de catégorie C.

– Pour les mineurs, l'infraction de catégorie A ne sera jamais en « accès restreint », l'infraction de catégorie B le sera après 30 ans, et l'infraction de catégorie C après 25 ans.

– Pour les adultes ayant fait l'objet d'une peine privative de liberté de moins de 6 mois, l'infraction de catégorie B est en « accès restreint » après 20 ans, et après 15 ans pour les infractions de catégorie C.

– Pour les mineurs ayant fait l'objet d'une peine privative de liberté de moins de 6 mois, l'infraction de catégorie B est en « accès restreint » après 15 ans, et après 10 ans pour les infractions de catégorie C.

– Pour les adultes ayant fait l'objet d'une peine non privative de liberté en relation avec une infraction de catégorie A, l'infraction est en « accès restreint » après 20 ans, 15 ans pour les infractions de catégorie B, et après 12 ans pour les infractions de catégorie C.

– Pour les mineurs ayant fait l'objet d'une peine non privative de liberté en relation avec une infraction de catégorie A, l'infraction est en « accès restreint » après 15 ans, après 12 ans pour les catégories B, et 10 ans pour les catégories C.

– Pour les adultes qui ont fait l'objet d'un avertissement de la police en relation avec une infraction de catégorie A, l'infraction sera en « accès restreint » après 10 ans, 5 ans pour les catégories B et C.

– Pour les mineurs qui ont fait l'objet d'une réprimande ou d'un avertissement en relation avec une infraction de catégorie A, l'infraction sera en « accès restreint » après 10 ans, 5 ans pour les infractions de catégorie B et C.

Pour les personnes acquittées par un tribunal ou les personnes à l'encontre desquelles aucune charge n'a été retenue, l'historique de l'infraction sera en « accès restreint » après que le résultat est entré dans le fichier nominatif.

Si les faits sont dépenalisés, ils seront en « accès restreint » après leur reclassification.

Pour les personnes faisant l'objet d'une ordonnance, l'historique de l'infraction sera en « accès restreint » après l'expiration de cette ordonnance.

En cas d'appel à l'encontre de la décision d'un tribunal, le fichier sera mis à jour en fonction du résultat de cet appel. Si la condamnation est infirmée, l'historique ne sera pas retiré mais il sera en « accès restreint ».

La procédure de mise à jour des fichiers peut être à la fois manuelle et automatique. Par exemple, la plupart des personnes arrêtées et détenues au poste de police voient leurs données enregistrées dans le fichier de la police locale lors de leur mise en garde à vue. Ces systèmes locaux sont reliés au *PNC (Police National Computer)* qui viennent l'alimenter électroniquement et automatiquement.

La plupart des éléments contenus dans les fichiers sont modifiés manuellement.

c) La nature et le statut des autorités en charge de l'alimentation, de la consultation et de la mise à jour des fichiers

Aux termes du MoPI, la responsabilité de la gestion et de l'usage des informations par les services de police relève du *Chief Officer* du service de police qui détient l'information. Ils jouissent d'un pouvoir discrétionnaire, dans des circonstances exceptionnelles, pour autoriser le retrait d'informations concernant une condamnation, un avertissement (*penalty notice for disorder*), un acquittement ou une arrestation dont ils possèdent les détails, c'est-à-dire de toute procédure qui aurait été initiée par les forces de police de la zone géographique que dirige le *Chief Officer*.

Les *Chief Officers* ont le devoir d'obtenir et de gérer les informations nécessaires à des fins policières, et de s'assurer du respect des lignes directrices du code MoPI. Dans le cadre de la gestion des informations, ils doivent s'assurer de l'existence de procédures destinées à prévenir un accès non autorisé ou accidentel à ces informations, ainsi que leur modification ou leur destruction. Les *Chiefs Officers* sont chargés de la sélection et de la formation des personnes occupant des postes-clé dans la gestion des fichiers de police. Ces personnes seront enregistrées sur le registre professionnel destiné à cet effet.

Les informations doivent être enregistrées seulement si elles sont nécessaires à des fins policières. Les *Chiefs Officers* établiront les procédures d'enregistrement : la source de l'information, la nature de la source, une évaluation de la fiabilité de la source, et la possibilité d'un réexamen, d'une réévaluation et d'un audit. En effet, le code MoPI pose que les informations doivent être réexaminées et qu'au cours de ce réexamen, la conservation ou la suppression de l'information doivent être envisagées. L'information doit être supprimée s'il a été démontré qu'elle est inexacte ou qu'elle n'est plus considérée comme nécessaire à la police.

Depuis sa mise en place, le *National DNA Database (NDNAD)* était géré par le *Forensic Science Service (FSS)* au nom de l'*Association des Chief Police Officers (ACPO)*. En 2005, le FSS a changé de statut pour devenir une société gérée par le Gouvernement avec une possibilité de privatisation dans le futur.

L'établissement de standards et le contrôle de la base de données NDNAD ont été transférés au *National Policing Improvement Agency (NPIA)*.

Le *National DNA Database Strategy Board* contrôle l'opération du NDNAD et de la NPIA.

Le *National DNA Database Ethics Group* a été créé en réponse aux critiques qui ont dénoncé le manque de contrôle éthique de la base de données.

Le 1^{er} rapport annuel date de cette année.

De nombreuses organisations de défense des droits fondamentaux ont estimé que la loi relative au NDNAD devrait être modifiée dans le sens d'un meilleur contrôle. *Justice UK*, une organisation britannique de défense des droits de l'homme, a déclaré que la NDNAD devrait être contrôlée par un organisme indépendant de la police et du *Home Office*.

III - Les modalités de contrôle du contenu et de l'utilisation des fichiers

a) Le statut et la nature des autorités en charge du contrôle

Les 43 *Chiefs Constables* d'Angleterre et du Pays de Galles sont en charge du contrôle des fichiers (*Data Controllers*).

La *National Policing Improvement Agency (NPIA)* est en charge du traitement des fichiers au nom des *Chiefs Constables* et elle est également responsable de la maintenance des systèmes.

La UKBA est responsable du contrôle des fichiers afférents à la réglementation sur les étrangers.

b) Les conditions d'accès et de rectification des données par les personnes concernées

L'accès au fichier PNC est étroitement contrôlé par un groupe de personnes appelé le *PNC Information Access Panel*. L'accès au fichier peut seulement être accordé et utilisé dans un but et pour une raison très précis.

Les agences ne faisant pas partie de la police qui veulent accéder au fichier doivent le demander à l'*Information Access Panel*.

L'information fournie peut être une donnée spécifique qui sera téléchargée et remise ou bien un accès direct au fichier. Chaque agence doit s'engager à signer un accord concernant cet accès (*Data Access Agreement*), écrit par le NPIA qui est responsable de la maintenance du fichier PNC.

Un citoyen peut écrire au chef de police compétent pour connaître la nature et le contenu des données contenues dans un fichier (voir ci-dessous)

*

* *

Exemple concernant le National DNA Database :

Le *Criminal Justice and public Order Act 1994* a permis la création du NDNAD.

Le *Criminal Justice and Police Act 2001* a supprimé l'exigence, posée par le *PACE 1984*, de détruire les échantillons ADN et les empreintes digitales concernant des personnes ayant été acquittées par un tribunal ou n'ayant pas été poursuivies.

Le *Criminal Justice Act 2003* a donné à la police le pouvoir supplémentaire de collecter des échantillons ADN et des empreintes digitales sans leur consentement, de toutes les personnes détenues dans un poste de police qui ont été arrêtées pour une infraction susceptible de faire l'objet d'un enregistrement dans un fichier de police (*recordable offence*), ce qui couvre une large gamme d'infractions (état d'ébriété, mendicité...). En revanche, la loi écossaise ne permet pas la rétention l'ADN de manière permanente pour les personnes qui ont été innocentes, mais elle permet la rétention permanente pour des infractions mineures (trouble à l'ordre public - *Breach of the Peace*).

Justice UK a déclaré que la rétention d'échantillons ADN de personnes à l'encontre desquelles aucune charge n'a été retenue ou des personnes qui ont été acquittées constitue une ingérence grave du droit à la vie privée, ce qui n'avait pas été l'avis de la Chambre des Lords dans *R v Chief Constable of South Yorkshire (ex parte S et Marper) [2004] UKHL 39*. Le 4 décembre 2008, la Cour européenne des droits de l'homme a déclaré que la rétention de l'ADN de S. et Marper violait leurs droits fondamentaux en vertu de l'article 8 de la CEDH. Le Gouvernement a jusqu'en mars 2009 pour appliquer le jugement.

c) Les difficultés pratiques observées

Les problèmes rencontrés par les utilisateurs du PNC quant à l'exactitude des données sont immédiatement signalés par les utilisateurs qui ont autorité dans ce domaine.

Si le problème concerne la manière dont l'information est enregistrée dans le PNC, il est possible de présenter une requête (une *Request For Change*) ; s'ensuit une procédure pour s'assurer que le problème est résolu (généralement cela consiste en la rectification d'une donnée) dans les plus brefs délais.

Certains problèmes sont si simples et peuvent être résolus si rapidement qu'il n'est pas utile d'en référer au *Data Controller* (par exemple le *Chief Officer* de la police ayant créé le fichier).

Les problèmes les plus sérieux sont examinés par les *Working Parties* constituées d'experts et de techniciens spécialisés qui discutent des différents problèmes et appliquent la solution appropriée. Les *Working Parties* se rencontrent deux fois par mois.

Lorsque le problème concerne un individu que les données du fichier affectent personnellement, il doit se renseigner auprès des *Data Controllers* sur l'application des textes concernant la protection des données.

Le *Data Controller* a l'obligation de répondre à la personne dans les 40 jours. Par la suite, si la personne dont la donnée personnelle enregistrée dans le PNC n'est pas satisfaite de la réponse donnée, elle peut porter l'affaire à la connaissance de l'*Information Commissioner*. Sa demande sera alors examinée devant l'*Information Tribunal*. Si un accord ne peut toujours pas être trouvé, le cas de la personne peut être entendu devant la *Court of Appeal*.

En dernier recours, la personne peut porter sa demande devant la Cour européenne des droits de l'homme.

Depuis 2006, tous les fichiers de police relatifs à l'arrestation sont désormais conservés dans le PNC pour une durée indéfinie à moins que l'individu concerné ne démontre l'existence de circonstances exceptionnelles en faveur de la suppression des données. Le *Chief Constable* peut refuser la suppression au motif que la personne ne fournit

pas la preuve de l'existence de circonstances exceptionnelles. Il n'existe aucun recours contre cette décision, mais l'organisation *Genewatch* conseille d'écrire à nouveau.

Si une personne, acquittée ou non poursuivie, estime que son dossier fait partie des circonstances exceptionnelles et qu'elle désire supprimer son ADN du fichier, elle peut écrire au *Chief Constable* de la police qui a prélevé l'échantillon pour lui demander de supprimer les données et de détruire cet échantillon, à la lumière de la décision de la CEDH dans l'affaire *Marper*. La décision précitée s'applique à toutes les personnes ayant été acquittées ou à l'encontre desquelles aucune charge n'a été retenue. Toutefois son application à des personnes sujettes à un avertissement est discutable. *Genewatch* conseille aux personnes concernées d'envoyer une copie de leur lettre à leur parlementaire.

L'organisation britannique de défense des droits l'homme, *Justice UK*, estime que la police doit notifier à l'individu que son profil ADN sera enregistré dans la NDNAD et conservé de manière permanente. Par ailleurs, selon *Justice UK*, dans les cas où aucune charge n'est retenue contre la personne arrêtée, ou que la personne est acquittée par la suite, elle peut écrire au *Chief Constable* afin de demander que leur profil ADN soit supprimé. Si le *Chief Constable* refuse, la personne devrait avoir la possibilité de remettre en cause sa décision devant un tribunal, ce qui n'est pas possible sous l'empire de la loi actuelle.

d) Les statistiques concernant l'utilisation frauduleuse des fichiers de police et les sanctions effectivement prononcées à l'encontre d'agents publics

Aucune statistique n'est en ce domaine disponible. Toutefois, la sécurité des données personnelles contenues dans le PNC est prise très au sérieux. Quiconque commettant une violation des données enregistrées, qu'il soit officier de police ou agent ayant un accès légitime à ces informations mais l'utilisant de façon frauduleuse peut être traduit en justice. Les peines encourues sont variées et une incarcération est possible.

Il existe une « disposition » de *Common Law* qui énonce l'obligation de conserver les données personnelles en sécurité et de ne pas les révéler en dehors d'une autorisation spéciale et d'un contrôle approprié.

Plusieurs lois s'appliquent en la matière :

– le *Data Protection Act* de 1998 ;

– le *Misuse of Computer Act* de 1990.

• Les échantillons prélevés au poste de police en Angleterre et au Pays de Galles sont ensuite envoyés à des laboratoires commerciaux pour analyse. Les informations ne peuvent être supprimées que dans des circonstances exceptionnelles, à défaut elles sont conservées jusqu'au 100^e anniversaire de la personne concernée. En Écosse, les données ADN sont supprimées si aucune charge n'a été retenue contre la personne ou que celle-ci a été acquittée ; la police se réserve le droit de conserver ces données dans le cas d'une infraction grave ou d'une infraction sexuelle mais pour une durée limitée (3 ans plus 2 ans sur demande du Sheriff).

Des personnes peuvent volontairement donner leur ADN afin d'être écartées de l'enquête (afin d'être « discriminées », selon le terme utilisé dans le domaine de la police technique et scientifique). Si en Écosse les donateurs volontaires peuvent demander à être effacés de la base de données, ce droit est refusé en Angleterre et au Pays de Galles.

Toutefois, en avril 2008, le Groupe éthique du NDNAD a recommandé que l'ADN des volontaires soit détruit à la fin de l'affaire.

Dans la mesure où les échantillons ADN contiennent des informations génétiques illimitées, l'accès à de telles informations est une question très sensible. Les organisations de défense des droits de l'homme, ainsi que certains laboratoires chargés de l'analyse et de la conservation des échantillons ADN (LGC Ltd), ont fait part aux parlementaires de leurs inquiétudes quant à l'envoi à des laboratoires privés d'informations sensibles. *Genewatch* s'est inquiétée de l'utilisation du NDNAD, sans le consentement des personnes concernées, pour des recherches génétiques controversées, et de la conservation par ces laboratoires de copies d'informations génétiques. L'organisation a notamment dénoncé un manque de transparence sur l'objet des recherches, l'approbation de recherches controversées sur l'éthnie, le manque de contrôle éthique, le manque de contrôle de la recherche effectuée par ces laboratoires et le manque de contrôle démocratique concernant les nouvelles utilisations opérationnelles telles que la recherche de membres de la famille de la personne. Par ailleurs, la plupart des données sont conservées sur le NDNAD alors même que les fichiers du PNC ont été supprimés.

Justice UK a critiqué le manque de transparence concernant l'utilisation des échantillons du NDNAD à des fins de recherche et demande à ce que le langage de la section 64(1A) du *PACE 1984* donne une définition plus stricte l'utilisation (en vue de la comparaison, de l'identification). *Justice UK* a notamment dénoncé le fait que la commission NDNAD pour l'Angleterre et le Pays de Galles a approuvé des projets de recherche fondés sur les échantillons contenus dans la base de données en vue d'une identification possible de comportements liés aux caractéristiques ethniques et familiales (*ethnic and familial traits*) et ce, sans le consentement des personnes concernées.

Selon *Justice UK*, l'utilisation de données médicales privées aux fins d'application de la loi peut être assimilée à une mauvaise utilisation d'informations personnelles sensibles même si le partage est exercé à des fins légitimes.

L'usage de NDNAD et des échantillons à des fins de recherche a été suspendu en attendant que le *NDNAD Ethics Board* (comité éthique) élabore des lignes directrices sur leur usage.

Genewatch souhaite la création d'un organe indépendant, transparent et responsable dont le rôle serait de s'assurer qu'il n'y a pas d'abus dans l'utilisation des données et que les nouvelles garanties sont bien respectées.

En vertu du *Data Protection Act 1998*, les données personnelles doivent être obtenues et utilisées pour des besoins spécifiques et leur traitement doit être « juste » (notion peu claire).

Les individus ont le droit de savoir quelles informations la police détient sur eux. Il suffit d'écrire au poste de police local mentionnant une '*subject access request*'.

Le Conseil de la bioéthique (*Nuffield Council on Bioethics*) a mené une consultation sur l'utilisation par la police des fichiers AND et empreintes digitales. Le rapport, publié en septembre 2007, demande que l'ADN des personnes soit supprimé en cas d'acquiescement et recommande la mise en place de garanties procédurales afin de prévenir des abus dans l'utilisation des informations génétiques.

La ministre de l'Intérieur, Jacqui Smith, a annoncé que le Gouvernement devait s'intéresser à la question de la durée de la conservation des données ADN ; elle a, par ailleurs, annoncé une future consultation. Elle a également indiqué que l'ADN des mineurs de moins de 10 allait être rapidement supprimé de la base de données.

Selon elle, « *la force de la base de données ADN ne peut être maintenue que si elle jouit de la confiance du public* ». Les changements seront exprimés dans un Livre blanc qui proposera une approche plus proportionnée, plus juste et qui relèverait davantage du bon sens. Elle souhaite plus de garanties, plus de transparence.

IV - La consultation des fichiers à vocation judiciaire dans le cadre d'enquêtes administratives

Selon nos interlocuteurs, les fichiers peuvent être utilisés dans le cadre d'enquêtes administratives. C'est le cas pour l'ouverture de certains établissements, pour la délivrance d'autorisations de détention d'armes à feu ou avant la conclusion d'un contrat de travail.

Les autorités britanniques sont particulièrement sensibles aux problèmes liés aux infractions à caractère sexuel dont les victimes sont des mineurs. Les exemples qui nous ont été donnés, dans cette hypothèse, concernent l'embauche de personnes qui travaillent en contact avec ou à proximité de jeunes enfants. Ceci signifie que les futurs employeurs – même individuels – peuvent obtenir des renseignements sur les personnes qu'ils vont embaucher, par exemple pour s'occuper de leurs enfants.

Cette possibilité ne peut étonner dans un pays où les voisins de délinquants sexuels sont avisés de cette proximité et où il y a, quelques semaines, a été évoquée la possibilité d'obliger ces délinquants à porter en évidence mention de leur condamnation....

V - Les solutions retenues s'agissant de l'utilisation de données sensibles sur les personnes dans les fichiers de police

Les données « sensibles » ne peuvent être utilisées que dans un cadre policier. Ces informations ne peuvent pas être révélées à un employeur ni à des tierces personnes.

Force est de rappeler que tant le Gouvernement que la population britanniques n'ont pas les mêmes préoccupations que les autorités ou l'opinion publique françaises. Il est, en effet, parfaitement admis que ces éléments sensibles soient répertoriés dans des fichiers ou dévoilés par un étudiant lors de son inscription à l'université ou par une personne souhaitant entrer dans la police ou encore par un détenu, lors des formalités d'entrée en prison.

Est joint, à titre d'exemple, le questionnaire remis aux personnes qui souhaitent devenir des fonctionnaires de police ou qui s'inscrivent à l'université.

ANNEXE 4 : RÉPONSE DE L'AMBASSADE DE FRANCE AUX PAYS-BAS AU QUESTIONNAIRE DES RAPPORTEURS

AMBASSADE DE FRANCE

AUX PAYS-BAS

Service de Sécurité Intérieure



La Haye, le 18 décembre 2008

OBJET : Pays-Bas, questionnaire sur les fichiers de police
REF : commande parlementaire (A.N., commission des lois) adressée au Magistrat de Liaison.

– principes généraux concernant la mise en place des fichiers de police :

Loi dite « *Wet politiregisters* » ou « *Wpolr* » du 21 juillet 2007 et règlement d'application daté du 14 décembre 2007.

– modalités d'alimentation, de mise à jour et de consultation :

Alimentation, mise à jour et consultation informatiques.

La loi impose une vérification semestrielle pour contrôler la nécessité de maintenir une donnée en mémoire (suppression dès que « non nécessaire » et au plus tard 5 ans après la première saisie pour le fichier de renseignement criminel)

– modalités de contrôle du contenu et de l'utilisation :

Une autorité indépendante, le *College bescherming persoonsgegevens* ou « CBP », est chargée de suivre l'application des textes légaux concernant la protection des données. Il est donc compétent pour les fichiers de police.

Le CBP considère que l'autorégulation est une condition de base pour une bonne application de la loi. De ce fait, il préconise la création d'une fonction d'Officier de protection des données dans chaque organisme privé ou public qui dispose d'un fichier contenant des données personnelles. Ce superviseur interne doit disposer d'un statut particulier au sein de sa structure d'emploi, garantissant son indépendance. La liste de ces Officiers est tenue à jour par le CBP. Par ailleurs, l'Autorité encourage les organismes concernés à rédiger un code de bonne conduite concernant l'usage de ses fichiers.

Conformément à ce principe général, concernant précisément les fichiers de police, la Loi « *Wpolr* » prévoit expressément dans son article 34 la désignation de ce Contrôleur

interne qui doit fournir un rapport annuel au « CBP », lequel est désigné pour « superviser » les fichiers de police.

Enfin, la loi sur les fichiers précise (art. 47) que les Ministres de la Justice, de l'Intérieur et de la Défense (autorité sur la Maréchaussée Royale) doivent faire procéder en commun à une évaluation de l'application de son contenu cinq ans après sa publication puis à intervalle régulier de 4 ans (à noter que la pratique néerlandaise de l'audit implique dans sa réalisation des experts extérieurs, tels des universitaires, chercheurs...).

– consultation des fichiers à vocation de police judiciaire dans le cadre administratif (encadrement et difficultés) :

La fourniture d'informations dites « données de police » à des organisations ou autorités agissant dans le cadre administratif est autorisée et régulée par les articles 16, 18 et suivants de la Loi « Wpolr », dispositions complétées par le paragraphe 4 du règlement d'application.

L'idée qui se dégage de ces textes est que toute transmission à des services tiers doit être justifiée par un intérêt public supérieur et dans le cadre de missions précises. Une liste des organisations bénéficiaires doit être définie par un texte réglementaire.

À noter que les maires sont cités dans la loi et accèdent aux données dans le cadre de leur autorité sur la police et leurs rôles en matière d'ordre public.

– utilisation de données sensibles sur les personnes dans les fichiers de police, et, analyse des évolutions récentes, réactions politiques et opinion publique :

Tous les fichiers interdisent de saisir de façon systématique l'orientation sexuelle, même si cette information peut se trouver ponctuellement dans une main courante ou dans une audition. Aucun système ne permet d'exécuter une requête sur ce critère. Il est, par contre, totalement interdit d'entrer dans un fichier l'appartenance à un parti politique/syndicat ou des choix philosophique et religieux.

Aucune réaction publique particulière n'a été récemment relevée, concernant les fichiers de police.

En 2007, le CBP avait attiré l'attention sur sa volonté d'engager des contrôles d'initiative. Il ne comptait plus se contenter de recevoir et exploiter les plaintes individuelles. Il considère que les seules actions portées par des individus ne suffisaient pas à couvrir l'intérêt général.

Il avait également souligné la nécessité d'assurer, sans citer particulièrement une défaillance, une sécurité à haut niveau sur les transferts d'informations au profit des autorités de justice ou de police des autres États.

Concernant les données personnelles, à noter des débats :

– début 2007, débat sur le projet de loi relatif à la conservation des données par les opérateurs de téléphonie et les fournisseurs d'accès internet ;

– actuellement, le dossier médical individuel informatisé, qui est un sujet de réflexion.

ANNEXE

Liste alphabétique des fichiers accessibles en direct par les services de police néerlandais

BPS : Système d'information et d'enregistrement local pour les procédures de police (main courante, procès-verbaux)

Blue view : Système de recherche nationale permettant d'accéder à toutes les informations BPS

BVV/VBS : Système des étrangers utilisé par la police des frontières

CIV : Fichier national des personnes et supporters liés à des incidents et infractions commises à l'occasion de rencontre de football

CJIB : Fichier d'information concernant les méthodes d'encaissement des amendes

COMPAS : fichier de recherche et de poursuite de l'administration du parquet

CRB : Fichier national des permis de conduire

EDISON : Fichier recensant tous les sécurités des documents administratifs permettant de faire des comparaisons

HKS : Fichier national des antécédents criminels (similaire au STIC-JUDEX)

- **DEX module** : Module d'extraction permettant d'effectuer des statistiques de consultation-saisies sur HKS

- **CVI** : Module de consultation national de HKS limité aux noms et objets

FCM : Fichier regroupant les photographies de suspects

FGMV : Fichier des véhicules volés

GBA : Fichier national des personnes enregistrées auprès des mairies (aux Pays-Bas, l'immatriculation auprès de sa mairie de domicile est obligatoire. Ce fichier permet donc en théorie d'avoir en direct l'adresse de n'importe quel habitant des Pays-Bas)

JDS : Registre des condamnations des personnes physiques et morales (fichier du ministère de la Justice, accessible à certains policiers spécialement habilité)

KADASTER : Registre national du cadastre

KVK : Registre de la chambre du commerce (fichiers des commerces et associations)

LDM : Fichier national des dossiers d'homicide

LEXIS NEXIS : Fichier de news et d'éléments légaux au sens large (journaux, actualité des sociétés etc)

LIST : Interface de requête simultanée dans les fichiers NSIS, OPS, CVI et RDW

LORS : Registre national des *modus operandi* et suspects pour les infractions de violences

LURIS : Registre d'enregistrement national des requêtes échangées avec les autorités étrangères

NSIS : Accès national au système SIS (*Schengen Info System*)

OPS : Fichier national des personnes recherchées

PAPOS : Fichier des amendes impayées

PSHV : Fichier national des étrangers

PSO PLATEAU : Interface de requête simultanée dans les fichiers BPS et RBS

RBS : Système de base des enquêtes.

RI online : Système national d'information sur les enquêtes en cours (permettant d'entrer des photos et autres éléments pouvant aider à l'identification des suspects)

TOBIAS : Système d'information sur les procès-verbaux

VERONA : Système des armes à feu et des permis de chasse

VICLAS : Système d'analyse des dossiers de crime violents

VIP : Fichier des personnes en détention

VIS (nouveau nom NDS) : Fichier des documents perdus, volés et non existant

VOS : Fichier local des heures de fermeture et ouverture des débits de boissons

VROS : Index de toutes les procédures en cours ou récemment terminées aux Pays-Bas

Il existe également un fichier à l'usage exclusif de l'UCTA (unité judiciaire anti terrorisme), fichier centralisant les informations judiciaires liées au terrorisme.

QUESTIONNAIRE SUR LES FICHIERS DE POLICE

– RÉPONSES DU MINISTÈRE DE LA JUSTICE DES PAYS-BAS –

1. Principes généraux s'appliquant en matière de mise en place et d'utilisation des fichiers de police. Rôle joué par le Parlement pour l'autorisation de créer de tels fichiers.

Les Pays-Bas connaissent une loi spécifique pour le traitement de données personnelles en matière de tâches de police (application pénale de l'État de droit, maintien de l'ordre public et aide) : c'est la loi sur les données policières. La loi sur les données policières s'applique aux données personnelles mentionnées dans un fichier ou destinées à l'être. Cette loi définit les principes suivants :

- la loi sur les données policières suit de près la loi sur la protection des données personnelles, en application dans le droit néerlandais de la Directive 95/46/CE ;
- les données policières ne sont employées que dans la mesure où c'est indispensable pour une bonne exécution des tâches de police ;
- les données à employer ont été recueillies légalement et sont exactes ; elles sont corrigées ou détruites dès qu'il apparaît qu'elles ne sont pas correctes ;
- les données ne sont employées que dans des buts bien définis et justifiés et dans la mesure où leur emploi est proportionné au but ;
- on distingue un emploi ciblé et un emploi non ciblé des données. Plus leur emploi est ciblé, plus grande est la protection offerte contre les atteintes à la vie privée ; les délais d'emploi dépendent des buts dans lesquels les données sont employées dans le cadre des tâches de police ;
- l'accès aux données de police est limité par des autorisations. Le point de départ étant en l'occurrence que les données ne sont communiquées qu'à des officiers de la police judiciaire, pour exécution des tâches dont ils sont chargés ;
- les données policières employées dans différents buts dans le cadre d'une tâche de police peuvent être combinées conditionnellement entre elles ;
- les données policières peuvent être échangées avec des instances extérieures à la police à condition que ce soit expressément réglé ou qu'il soit question d'un intérêt général de poids ;
- la personne concernée a le droit de prendre connaissance des données la concernant, à moins qu'il n'y ait des motifs légaux de refus ;
- une autorité de surveillance indépendante veille à l'emploi licite et minutieux des données ;

- la police est tenue d'établir un procès-verbal des données recueillies et de faire procéder périodiquement à des audits pour les besoins de la surveillance ;
- excepté l'approbation parlementaire de la loi sur les données policières, le système néerlandais ne connaît pas d'approbation particulière du Parlement pour la mise en place d'un fichier de police.

2. Modalités d'alimentation, de mise à jour et de consultation des fichiers de police (nature des modes d'alimentation, de mise à jour, statut et nature des autorités en charge de l'alimentation, consultation et mise à jour)

a. Modalités d'alimentation et de consultation

* Les objectifs de la police.

Sur la base du principe que les données policières ne sont employées que dans des buts bien définis et justifiés, on distingue plusieurs buts dans le cadre desquels il est permis d'alimenter des fichiers informatiques. Ce sont les buts suivants, définis par la loi sur les données policières :

– Exécution des tâches quotidiennes de police (article 8)

Il s'agit des tâches de base telles que la surveillance, les conseils de prévention, le traitement de problèmes de circulation, les investigations élémentaires et l'aide. Cela concerne souvent des données sur des personnes qui ne font pas (encore) l'objet de suspicions et des données qui ne découlent pas d'investigations approfondies. La police peut rapprocher ces données librement. Elles sont supprimées au bout de cinq ans.

– Emploi ciblé de données policières (articles 9 et 10)

Par emploi ciblé de données on entend l'emploi structuré ou à grande échelle de données sur certaines personnes.

Tout d'abord, la police peut faire un usage important de données personnelles à la suite d'un événement, par exemple un meurtre, un hold-up ou une situation de nuisance grave. Pour l'alimentation de fichiers sur la base de ces articles il n'y a pas de restrictions concernant le statut des personnes (suspects, personnes non encore suspectées mais faisant l'objet d'une enquête, témoins, victimes etc.) ; il n'est pas nécessaire que l'implication précise de ces personnes soit déjà établie. Le but des investigations doit être établi par écrit. Un aperçu de ces investigations doit être disponible pour l'autorité de surveillance. Les données doivent être supprimées dès qu'elles ne sont plus nécessaires pour le but dans lequel elles ont été recueillies. Si les investigations donnent lieu à des poursuites pénales le but des investigations ne sera atteint que lorsque les tribunaux auront pris une décision irrévocable.

Ensuite, l'emploi ciblé de données personnelles pour servir à obtenir des informations concernant l'implication de certaines personnes dans certains faits répressibles ou dans des actes constituant une violation grave de l'ordre public. Dans ce cas ce n'est pas tellement l'événement qui est au centre de l'enquête, mais le rassemblement d'informations par la police.

– Tâches de soutien (article 13)

La loi édicte des règles complémentaires pour l'emploi de données policières pour l'exécution de tâches de soutien. Ces données sont centralisées et largement disponibles au sein de la police. On peut songer à des données concernant le signalement de personnes et de biens – telles que le registre de recherche -, l'identification et la vérification de personnes et d'antécédents.

Les délais d'emploi dépendent du but spécifique de l'usage des données. Ces délais doivent être établis par écrit.

* La disponibilité des données au sein de la police (articles 11 et 15).

Il peut aussi arriver dans la pratique que des données utilisées dans un certain but dans le cadre d'une tâche de police doivent aussi être employées dans un autre but. Sur ce point, la loi sur les données policières fournit des « liens croisés », de sorte que cet autre usage est possible si c'est nécessaire. La loi édicte des règles spécifiques pour la comparaison informatique et l'emploi combiné de données dans un autre but.

* Retrait de données (article 14)

Les données sont retirées à l'échéance des délais mentionnés ci-dessus. Les données retirées sont conservées pendant cinq ans, afin de pouvoir traiter d'éventuelles réclamations et rendre compte des activités de la police. Un droit de communication peut par ailleurs être exercé. Durant cette période les données, dans des cas particuliers, peuvent de nouveau être employées de façon ciblée (articles 9 et 10 de la loi). Au delà, les données sont détruites ou archivées si elles ont une grande valeur pour le patrimoine culturel et la recherche historique.

* La communication de données de police à des tiers (articles 18, 19 et 20)

Article 18 : des données de police peuvent être communiquées à une personne ou une instance exerçant une tâche publique ou privée. Il faut pour cela qu'il y ait un intérêt général de poids. L'application de ce critère implique qu'on pèse le pour et le contre, en tenant notamment compte des principes de proportionnalité et de subsidiarité. Les personnes et instances concernées sont désignées par la réglementation inférieure (décret sur les données de police).

La loi sur les données policières offre cependant deux possibilités spécifiques de communiquer des données à des personnes ou instances que le décret sur les données de police ne désigne pas :

– article 19 : dans des cas occasionnels, des données de police peuvent être communiquées à des tiers. Cette communication est liée à certains buts compatibles avec les tâches de la police. Par ailleurs il doit y avoir un intérêt général de poids – exigence mentionnée ci-dessus – et il faut l'approbation du procureur, s'il s'agit de données sur le maintien pénal de l'ordre de droit ;

– article 20 : des données de police peuvent être communiquées dans le cadre de coopérations avec d'autres instances. L'exigence d'intérêt général de poids, la compatibilité avec les tâches de la police et l'approbation du procureur s'appliquent également dans ces cas.

* La loi s'applique aux données employées sur support papier aussi bien qu'aux données informatisées.

b. Statut et nature des autorités en charge de l'alimentation, consultation et mise à jour

Les données de police sont accessibles aux policiers autorisés. La police peut être considérée comme un circuit fermé, c'est-à-dire qu'un policier est légalement obligé de tenir ses données à la disposition d'autres fonctionnaires de la police. Ce n'est que dans des cas exceptionnels qu'il peut refuser. La communication de données de police à des tiers dépend d'une décision préalable. Ce système a été décrit plus haut.

3. Modalités de contrôle du contenu et de l'utilisation des fichiers (statut et nature des autorités en charge de ce contrôle, modalités d'accès et de rectification des données et difficultés pratiques, statistiques concernant l'utilisation frauduleuse et sanctions)

a. Modalités de contrôle du contenu et de l'utilisation des fichiers – autorités en charge du contrôle)

Article 33 : le gestionnaire est tenu de faire procéder périodiquement à un audit sur la protection de la vie privée. Cet audit est effectué par un expert indépendant. Les résultats de cet audit sont envoyés à l'autorité de surveillance. S'il s'avère que les prescriptions légales ne sont pas respectées, le gestionnaire est obligé de faire effectuer un deuxième contrôle.

Article 34 : un corps de police est tenu de nommer un fonctionnaire chargé de la protection de la vie privée, qui conseille le gestionnaire du corps et qui veille au respect de la loi en son nom.

Article 35 : un organe indépendant, le Collège pour la protection des données personnelles, veille au respect de la loi. Ce collège peut enquêter de son propre gré, peut employer certains moyens coercitifs et imposer des sanctions.

Nous ne disposons pas d'informations statistiques sur l'usage illicite ou abusif de données de police et les sanctions imposées à des fonctionnaires publics dans ce contexte.

b. Modalités d'accès et de rectification des données par les personnes concernées – difficultés observées.

Article 25 : la personne concernée a le droit de prendre connaissance des données de police la concernant. Une décision est prise dans les quatre semaines suivant la demande. Cette décision peut être reportée pour une période de quatre ou six semaines.

Article 27 : la communication des données peut être refusée dans l'intérêt de la bonne exécution des tâches de la police, en raison d'importants intérêts de tiers ou de la sécurité de l'État.

On n'a pas connaissance de problèmes spécifiques concernant l'application du droit de communication. Il est cependant fréquent que plusieurs corps de police soient impliqués, du fait de la structure régionalisée de la police néerlandaise. Dans un tel cas, les corps de police concernés doivent coordonner leur action, ce qui demande beaucoup de temps. Il est alors possible de reporter une demande de communication pour une période supplémentaire de six semaines (Art. 25, deuxième paragraphe, WPG).

Article 28 : la personne à qui on a communiqué des données de police la concernant peut demander leur rectification, leur retrait ou leur protection. Une décision est prise dans les quatre semaines suivant la demande.

Article 29 : Il est possible de faire appel auprès d'un tribunal d'un refus de communication ou de correction.

4. Possibilités de consultation des fichiers à vocation de police judiciaire dans le cadre d'enquêtes administratives – difficultés pratiques et juridiques.

En principe, les données de police peuvent uniquement être employées pour l'exécution d'une tâche de police concernant des faits répressibles. Elles ne peuvent donc pas être consultées librement dans le cadre de tâches de surveillance. Il est toutefois possible de fournir des données à certaines instances de surveillance, si elles ont été désignées par la loi. Par ailleurs, certaines données de police – qui n'ont pas fait l'objet d'une utilisation ciblée – peuvent être fournies aux fonctionnaires chargés de contrôler l'application de certaines lois, si ces données concernent le respect de ces lois et si des accords ont été passés sur l'utilisation de ces données. On n'a pas connaissance aux Pays-Bas de problèmes pratiques concernant l'utilisation de données de police pour des enquêtes administratives.

5. Solutions retenues s'agissant de l'utilisation des données sensibles sur les personnes dans les fichiers de police – évolutions récentes

La loi sur les données de police offre la possibilité d'utiliser des données sensibles en complément d'autres données de police, dans la mesure où c'est indispensable pour le but de leur emploi. On ne connaît pas de problèmes ou développements récents concernant l'utilisation de données sensibles par la police.

ANNEXE 5 : FORMULAIRE À REMPLIR PAR LES CANDIDATS À UN EMPLOI DANS LA POLICE DU KENT

RESTRICTED staff (when complete)

Equal Opportunities Form

Kent Police values diversity in its workforce and aims to recruit and value a workforce that reflects the diverse make-up of the community of Kent.

As part of our recruitment / promotion process you are required to complete this monitoring form. This page will be detached and will not form part of the selection process. We expect all our employees, and prospective employees, to support our aim to build a diverse and representative workforce

<p>Age: Up to 21 <input type="checkbox"/> 22-25 <input type="checkbox"/> 26-30 <input type="checkbox"/> 31-35 <input type="checkbox"/> 36-40 <input type="checkbox"/> 41-45 <input type="checkbox"/> 46-50 <input type="checkbox"/> 51-55 <input type="checkbox"/> 56-60 <input type="checkbox"/> 61-65 <input type="checkbox"/> over 65 <input type="checkbox"/></p>	<p>Sexual Orientation: Bisexual <input type="checkbox"/> Gay/Lesbian <input type="checkbox"/> Heterosexual <input type="checkbox"/> Prefer not to say <input type="checkbox"/></p>
<p>Gender: Male <input type="checkbox"/> Female <input type="checkbox"/> Transgender <input type="checkbox"/> Transexual <input type="checkbox"/> Intersex <input type="checkbox"/> Prefer not to say <input type="checkbox"/></p>	<p>Religious Belief: Buddhist <input type="checkbox"/> Christian <input type="checkbox"/> Hindu <input type="checkbox"/> Jewish <input type="checkbox"/> Muslim <input type="checkbox"/> Sikh <input type="checkbox"/> None <input type="checkbox"/> Other (please state) <input type="checkbox"/></p>
<p>Disability: Yes <input type="checkbox"/> No <input type="checkbox"/> Prefer not to say <input type="checkbox"/></p>	<p>Prefer not to say <input type="checkbox"/></p>
<p>Ethnic Origin:</p> <p>White British <input type="checkbox"/> Irish <input type="checkbox"/> Any other White Background <input type="checkbox"/></p> <p>Mixed White and Black Caribbean <input type="checkbox"/> White and Black African <input type="checkbox"/> White and Asian <input type="checkbox"/> Any other mixed background <input type="checkbox"/></p> <p>Asian and Asian British Indian <input type="checkbox"/> Pakistani <input type="checkbox"/> Bangladeshi <input type="checkbox"/> Any other Asian background <input type="checkbox"/></p> <p>Black and Black British Caribbean <input type="checkbox"/> African <input type="checkbox"/> Any other black background <input type="checkbox"/></p> <p>Gypsy & Traveller English Gypsy <input type="checkbox"/> Irish Traveller <input type="checkbox"/> European Roma <input type="checkbox"/></p> <p>Chinese or other ethnic group Chinese <input type="checkbox"/> Other ethnic group (please specify) <input type="checkbox"/></p>	

RESTRICTED staff (when complete)

ANNEXE 6 : CIRCULAIRE DU MINISTÈRE DE LA JUSTICE DU 9 JUILLET 2008 RELATIVE AU REFUS DU PRÉLÈVEMENT BIOLOGIQUE



Paris, le 09 JUL. 2008

MINISTÈRE DE LA JUSTICE

Le Garde des Sceaux, Ministre de la Justice

DIRECTION
DES AFFAIRES CRIMINELLES ET DES GRÂCES

à

Le Directeur

Mesdames et Messieurs les procureurs généraux
près les cours d'appel

OBJET : Refus de prélèvement FNAEG.

N/R E F : CRIM-PJ N° 08-28.H 5

Une alimentation rigoureuse du fichier national automatisé des empreintes génétiques (FNAEG) dans tous les cas prévus par la loi est nécessaire pour garantir la pleine efficacité de ce traitement : le nombre de rapprochements susceptibles d'être opérés par ce fichier est subordonné au volume des données que ce dernier contient.

A cette fin, il m'apparaît nécessaire que soient systématiquement poursuivies les personnes qui s'opposent à leur prélèvement aux fins d'identification génétique, faits prévus et réprimés au paragraphe II de l'article 706-56 du code de procédure pénale : *« Le refus de se soumettre au prélèvement biologique prévu au premier alinéa du I est un délit puni de 1 an d'emprisonnement et de 15000 euros d'amende, peine portée à 2 ans d'emprisonnement et 30000 euros d'amende lorsque le refus est opposé par une personne condamnée pour un crime »*

Or, mon attention a été appelée à plusieurs reprises sur des décisions de relaxe rendues par différentes juridictions de première instance ou d'appel saisies de faits de cette nature, au motif qu'elles n'étaient pas en mesure d'apprécier la régularité de la décision de prélèvement.

Dans ces affaires, qui ont jusqu'à présent toutes concerné des « suspects » et non pas des condamnés, les magistrats ont estimé ne pas disposer des éléments suffisants pour apprécier s'il existait réellement des indices graves ou concordants, ou une ou plusieurs raisons plausibles, de soupçonner que l'individu prélevé avait commis un crime ou un délit figurant à l'article 706-55 du code de procédure pénale. Plusieurs juridictions ont ainsi considéré que la simple information selon laquelle l'intéressé faisait l'objet d'une garde à vue ne suffisait pas à caractériser en quoi il était suspect au sens de l'alinéa 3 de l'article 706-54 du code de procédure pénale.

/.

Afin d'éviter que de telles décisions de relaxe ne se multiplient, il y a lieu de rappeler que le premier élément constitutif du délit de refus de prélèvement est la régularité du prélèvement lui-même. Le parquet et le tribunal doivent donc être en mesure de l'apprécier.

La présente dépêche-circulaire vise ainsi à rappeler, dans un premier temps, dans quel cadre procédural un prélèvement ADN peut être régulièrement réalisé et, dans un second temps, quels éléments doivent en être versés à la procédure suivie pour refus de prélèvement.

1- La régularité du prélèvement initial

La régularité des opérations de prélèvement génétique s'apprécie au regard de la situation de la personne prélevée, de l'infraction qui lui est reprochée et du consentement de l'intéressé.

1-1- Quant à la personne prélevée

Les personnes qui peuvent faire l'objet d'un prélèvement et qui, partant, sont susceptibles d'être poursuivies pour avoir refusé de s'y soumettre, sont celles mentionnées aux premier, deuxième et troisième alinéas de l'article 706-54 du code de procédure pénale :

- les personnes condamnées pour l'une des infractions listées à l'article 706-55,
- les 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,
- les personnes à l'encontre desquelles il existe une ou plusieurs raisons plausibles de soupçonner qu'elles ont commis un crime ou un délit.

1-1-1- Les personnes condamnées

Seules les condamnations devenues définitives doivent être prises en compte. En effet, contrairement au fichier judiciaire national automatisé des auteurs d'infractions sexuelles (FIJAIS), le législateur n'a pas prévu la prise en compte des condamnations « même non définitives ». Le principe d'interprétation stricte de la loi pénale impose donc que seules les condamnations définitives soient considérées.

Bien qu'une réflexion interministérielle soit actuellement en cours pour envisager d'inclure les personnes dispensées de peine dans le champ du fichier, les personnes ayant été déclarées coupables mais dispensées de peine ne peuvent faire, en l'état du droit, l'objet d'un prélèvement en vue d'un enregistrement au FNAEG.

Les mineurs ayant fait l'objet d'une mesure ou d'une sanction éducative ou d'une mise sous protection judiciaire prévue aux articles 8, 15, 15-1, 16, 16 bis de l'ordonnance du 2 février 1945 relative à l'enfance délinquante, ne peuvent être prélevés en qualité de condamnés, puisque ces décisions ne s'analysent pas juridiquement comme des condamnations.

En conséquence, en application de l'article 2 de l'ordonnance susvisée qui prévoit qu'une peine ne peut être prononcée qu'à l'égard des mineurs de 13 à 18 ans, les mineurs de moins de 13 ans ne peuvent faire l'objet d'un prélèvement en vue d'établir leur profil génétique.

1-1-2- Les suspects aux termes de l'alinéa 2 de l'article 706-54 du code de procédure pénale

Il s'agit 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 code de procédure pénale.

Si la notion d'indices graves ou concordants renvoie au critère retenu à l'article 80-1 de ce code pour rendre possible la mise en examen par le juge d'instruction, le législateur n'exige pas le cumul d'indices à la fois graves et concordants qui rend, aux termes de l'article 105 du code précité, la mise en examen obligatoire.

La régularité du prélèvement sur le fondement de l'alinéa 2 de l'article 706-54 du code de procédure pénale, suppose donc, soit l'existence de plusieurs indices, même légers dès lors qu'ils sont concordants, soit l'existence d'un seul indice, à la condition qu'il soit grave.

Ainsi, une personne contre laquelle le seul indice de culpabilité résulte de sa mise en cause par la victime ou par un témoin, si cette mise en cause n'est ni circonstanciée ni corroborée par d'autres éléments de la procédure, ne peut être prélevée sur ce fondement car un tel indice ne peut être considéré comme grave à lui seul.

1-1-3- Les suspects aux termes de l'alinéa 3 de l'article 706-54 du code de procédure pénale

Il s'agit des personnes à l'encontre desquelles il existe **une ou plusieurs raisons plausibles de soupçonner** qu'elles ont commis ou tenté de commettre une infraction visée à l'article 706-55 du code de procédure pénale.

La notion de raison plausible renvoie au critère retenu aux articles 63 et 77 de ce code pour permettre le placement en garde à vue.

Cette catégorie de suspects recouvre donc des personnes dont l'implication est moins établie que dans l'hypothèse de ceux visés à l'alinéa 2 de l'article 706-54 du code de procédure pénale, puisqu'il suffit de l'existence d'une seule raison plausible permettant de soupçonner la personne pour permettre le prélèvement de cette dernière sur le fondement de l'alinéa 3 de cet article : des indices matériels, une mise en cause par la victime, un coauteur, un complice ou un témoin, le comportement suspect de la personne.

Il y a lieu de rappeler que les suspects visés à l'alinéa 3 de l'article 706-54 du code de procédure pénale ne peuvent faire l'objet d'un prélèvement qu'aux fins de comparaison au FNAEG, et non pas d'enregistrement dans le fichier.

1-1-4- Le cas particulier des suspects mineurs

Ainsi que je l'indiquais dans ma dépêche-circulaire du 23 juin 2006, et comme pour les mineurs condamnés, il convient de faire preuve de prudence en matière de prélèvement des mineurs en qualité de suspects dans un souci de conciliation entre la finalité du FNAEG, d'une part, et les dispositions de l'ordonnance du 2 février 1945 relative à l'enfance délinquante, d'autre part : le prélèvement de matériel biologique aux fins d'alimentation ou de comparaison au FNAEG ne se justifie que si des condamnations pénales sont possibles.

Ainsi ne sauraient être prélevés les mineurs de moins de 13 ans, qui ne peuvent, aux termes de l'article 2 de l'ordonnance précitée, faire l'objet que de mesures ou sanctions éducatives, mais pas de condamnations pénales.

S'agissant des mineurs âgés de plus de 13 ans, l'opportunité du prélèvement doit être appréciée avec rigueur, à l'issue d'un dialogue entre l'officier de police judiciaire et le parquet.

1-2- Quant à l'infraction concernée

Pour les condamnés et les suspects visés à l'alinéa 2 de l'article 706-54 du code de procédure pénale, la possibilité de prélever est expressément limitée aux infractions listées à l'article 706-55 du même code. Cette liste, initialement limitée aux infractions à caractère sexuel, a été considérablement étendue par la loi du 18 mars 2003 pour la sécurité intérieure à la plupart des infractions prévues au code pénal, et notamment aux délits contre les biens, tels que les vols ou les dégradations.

En revanche, la possibilité de prélever les suspects visés à l'alinéa 3 de l'article 706-54 du code de procédure pénale n'est pas expressément limitée à cette liste d'infractions.

Il convient pourtant de considérer que le champ d'application de ce dernier alinéa est également circonscrit aux infractions de l'article 706-55 du code précité. En effet, les débats parlementaires montrent que telle est la volonté du législateur, et une interprétation différente tendrait à détourner le texte de son esprit.

L'alinéa 3 de l'article 706-55 du code précité n'a pas, par exemple, vocation à permettre de soumettre à un prélèvement ADN les personnes interpellées pour un délit routier ou une infraction à la législation contre les étrangers. En effet, dans ce type de contentieux, il existe contre la personne dès l'interpellation des indices graves ou concordants tels qu'ils impliquent que le prélèvement se fasse sur le fondement de l'alinéa 2 de l'article précité, dont le champ d'application est expressément limité.

Cette analyse présente également l'avantage de ne pas multiplier la détermination coûteuse de profils génétiques qui n'ont pas vocation à enrichir la base FNAEG.

Enfin, et compte-tenu de la vocation initiale de ce traitement, une politique pénale de prélèvements systématiques de personnes mises en cause pour tout crime ou délit ne pourrait qu'alimenter les critiques portées sur le fichier et multiplier les comportements de refus de prélèvements, dont la poursuite et le jugement pourront se révéler problématiques compte-tenu d'un fondement juridique fragile.

J'ajoute que j'ai fait part de ces éléments d'analyse aux directeurs de la police et de la gendarmerie nationales par notes des 25 juin 2007 et 21 janvier 2008.

1-3- Quant au consentement au prélèvement

Sans être exprès, l'accord des personnes faisant l'objet d'un prélèvement ADN est nécessaire.

En effet, il ressort certes de l'article 16-11 du code civil qu'en matière civile ou lorsque l'identification génétique est effectuée à des fins médicales ou de recherche scientifique, l'identification par empreinte génétique ne peut être recherchée qu'après avoir recueilli le consentement exprès de l'intéressé, tandis qu'aucune exigence de cette nature n'est imposée en matière pénale.

Pour autant, une interprétation a contrario de l'alinéa 5 de l'article 706-56 du code de procédure pénale conduit à conclure à la nécessité de recueillir l'accord de l'intéressé, quoique de manière non expresse. En effet, en application de cette disposition, les prélèvements ADN peuvent être faits sans l'accord de l'intéressé lorsqu'ils sont effectués sur un condamné pour un crime ou un délit dont la peine encourue est de 10 ans d'emprisonnement. A contrario, ils ne peuvent être faits par la force dans les autres situations, ce qui suppose donc l'accord de la personne qui en fait l'objet.

S'agissant plus spécifiquement des mineurs, il appartient au mineur lui-même, et non pas à ses représentants légaux, de donner ce consentement. En effet, le respect du principe général de l'inviolabilité du corps humain nécessite que l'intéressé puisse s'opposer au prélèvement dont il fait lui-même l'objet. Il ressort en outre clairement du libellé de l'infraction de refus de prélèvement prévue et réprimée à l'article 706-56, alinéa 6, du code de procédure pénale, que celle-ci est constituée lorsque la personne à prélever, et non pas une autre, refuse de se soumettre à l'opération.

Sous réserve de l'application du cinquième alinéa précité de l'article 706-56 du code de procédure pénale, en application duquel il peut être procédé à un prélèvement de force sur les condamnés à un crime ou un délit puni d'une peine de 10 ans d'emprisonnement, il appartient donc au seul mineur d'accepter ou de refuser le prélèvement effectué sur sa personne.

En leur qualité de représentants légaux, les parents du mineur doivent cependant être informés de ce qu'un prélèvement a été effectué sur leur enfant ou de ce que ce dernier s'y est opposé.

2- Les éléments de la procédure nécessaires à l'appréciation de la régularité du prélèvement initial

Afin d'exercer des poursuites et de statuer sur les faits de refus de prélèvement, la procédure soumise aux magistrats du parquet et du siège doit comporter tous les éléments utiles à l'appréciation de la régularité du prélèvement initial.

En effet, l'autorité judiciaire doit pouvoir clairement appréhender sur quel fondement juridique (alinéa 1, 2 ou 3 de l'article 706-54 du code de procédure pénale) et pour quelle infraction reprochée (issue de la liste de l'article 706-55 du code de procédure pénale) le prélèvement a été décidé.


S'agissant des refus de prélèvement opposés par des personnes condamnées, la décision de condamnation définitive doit impérativement être versée à la procédure.

S'agissant des refus de prélèvement opposés par des personnes suspectes, les éléments de nature à permettre aux magistrats d'apprécier l'existence « *d'indices graves ou concordants* » ou d' « *une ou plusieurs raisons plausibles* » doivent être joints à la procédure.

Il convient de relever, à cot égard, que la simple mention de ce que la personne prélevée faisait l'objet d'une mesure de garde à vue ou d'une mise en examen ne saurait informer complètement les magistrats.

Pour autant, il n'est pas nécessaire que soit versée à la procédure établie pour le refus de prélèvement, l'intégralité de celle dans le cadre de laquelle le prélèvement initial a été effectué. Un procès-verbal de synthèse suffisamment détaillé permettant de caractériser la ou les raisons plausibles de soupçonner la personne, ou les indices graves ou concordants rendant vraisemblable sa participation aux faits peut suffire. Dans l'hypothèse où le parquet poursuivant les faits de refus de prélèvement est distinct de celui qui avait dirigé l'enquête initiale, et pour éviter toute insécurité juridique, il est souhaitable que, sur demande du premier, le second fournisse les éléments nécessaires à la rédaction d'un procès-verbal de synthèse précis.

Vous voudrez bien me rendre compte, sous le timbre du bureau de la police judiciaire, des procédures suivies pour refus de prélèvement ADN dans lesquelles une difficulté particulière vous apparaît, ainsi que des problèmes que vous seriez amenés à rencontrer dans l'exécution des présentes instructions.



Jean-Marie HUET

ANNEXE 7 : ÉCHANGE DE COURRIERS ENTRE UN COMMANDANT DE GROUPEMENT DE GENDARMERIE ET DEUX PROCUREURS DE LA RÉPUBLIQUE



MINISTÈRE DE LA DÉFENSE



RÉGION DE GENDARMERIE :

le 21 juillet 2008

Groupe ment

Le lieutenant colonel commandant par suppléance le groupement de gendarmerie départementale

à M. le procureur de la République à

OBJET: - Mise à jour du système judiciaire de documentation et d'exploitation (JUDEX), par intégration des suites judiciaires.
REFERENCE: - - Circulaire N° 51992 DEF/GEND/OE/SDP/PJ du 10 août 2007.
PIECE JOINTE : - - Fiche navette « suites judiciaires ».

J'ai l'honneur de vous informer des directives adressées en diffusion générale à l'ensemble des unités de la gendarmerie nationale. Il s'agit de la mise à jour des données contenues dans le fichier JUDEX, par intégration des décisions de justice. Dans l'attente du déploiement de l'application informatique « CASSIOPEE » du ministère de la justice, un protocole détermine le rôle de chaque intervenant et instaure la mise en oeuvre d'une fiche navette intitulée « suites judiciaires » (voir pièce jointe).

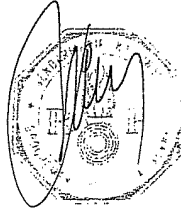
Toute procédure judiciaire alimentant le fichier JUDEX et transmise au parquet compétent doit être systématiquement accompagnée d'une ou de plusieurs fiches navettes « suites judiciaires » dûment renseignées.

Pour les procédures dont il est saisi, le procureur de la République peut ordonner que certaines informations soient rectifiées, complétées ou effacées. Il doit, en outre, transmettre au gestionnaire du fichier les décisions judiciaires favorables aux personnes mises en cause (décisions de relaxe ou de non-lieu devenues définitives - décisions de classement sans suite pour insuffisance de charges).

Les fiches navettes sont complétées et transmises par le procureur de la République au commandant de la B.D.R.I.J, qui les adresse au S.T.R.J.D., tenu de procéder aux mises à jour demandées.

Ces éléments vous sont adressés à toutes fins utiles, pour toutes directives ou précisions que vous estimeriez devoir communiquer aux enquêteurs

Veillez agréer, Monsieur le procureur de la République, l' expression de ma considération la plus distinguée.



GENDARMERIE NATIONALE					ANNEXE
Compagnie					ANNEXE SUITES JUDICIAIRES
unité					
Code Unité	P.V.	Année	N° pièce	Feuille 4/2	N° dossier Justice

Imprimé à retourner le cas échéant par le parquet au Commandant de Groupement de gendarmerie départementale (Brigade Départementale de Renseignements et d'Investigations Judiciaires)

INFRACTION(S)

<i>Analyse et références</i>		NATIF
Fait		
Commis le	Code Postal, Commune	
	<i>Adresse de commission du fait</i>	
Prévu		
Réprimé		

MIS(E) EN CAUSE

Nom	Prénoms	Nom Maternel	
Sexe	Situation de Famille	Date Naissance	Code Postal de Commune, Naissance
Filiation			
père :		mère :	
Adresse			
Code Postal et Commune	N° de Téléphone	Profession	Résidence (si étranger)

PROCEDURE

Transmise à M. [Nom Magistrat], Magistrat à [Commune tribunal] .
le / /

REPONSE PARQUET

Le procureur de la République
du Tribunal de Grande Instance
de [ville]

Le procureur général
près la Cour d'Appel
de [ville]

L'honneur d'informer le commandant de groupement de gendarmerie départementale
[ville] :

Il a été intervenu au profit de la personne mise en cause dans la procédure judiciaire concernant la ou les infractions mentionnées ci-dessus, lesquelles ont fait l'objet d'une inscription dans JUDEX :

- une décision de relaxe en date du
- une décision de classement sans suite en date du pour⁽¹⁾
- une décision de non-lieu en date du
- une décision d'acquiescement en date du
- le procureur de la République prescrit l'effacement des informations directement ou indirectement nominatives concernant cette personne.
- le procureur de la République prescrit l'ajout de la mention de ⁽²⁾ concernant cette personne

saïse du motif en clair pour code 1) absence d'infraction - code 2) infraction insuffisamment caractérisée
relaxe/classement/non lieu

PV n°

Pièce n°

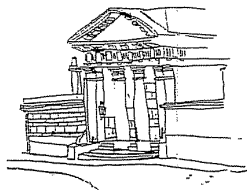
Feuillet n° 2/2

Autres observations :

.....
.....
.....

Cachet de la juridiction et signature de l'autorité

TRIBUNAL DE GRANDE INSTANCE DE
rue du Palais - Cédex 9 - Tél : - FAX :
TRIBUNAL DE GRANDE INSTANCE DE
PARQUET



Le Procureur de la République de

Le Procureur de la République de

A

M. le Commandant Groupement de
Gendarmerie

, le 25 septembre 2008

Objet : fiche navette JUDEX

V/Réf : circulaire N° 51992 DEF/GEN/OE/SDPJ/P du 10 août 2007

Nous avons l'honneur, en réponse à votre note susvisée du 4 juillet 2008 ; de vous informer que pour permettre les mises à jour indispensables du fichier JUDEX en cas de classement sans suite (11 = absence d'infraction ou 21 = infraction insuffisamment caractérisée), de non-lieu ou de relaxe, nous vous prions de bien vouloir inviter vos services à joindre en tête de procédure, après les bordereaux de transmission et les convocations délivrées, la fiche-navette de suites judiciaires.

Cette fiche ne doit apparaître que si une ou plusieurs personnes sont identifiées comme auteur dans la procédure concernée.

Une fiche navette devra être jointe par prévenu.

En cas de classement (code 11 ou 21), de non-lieu ou de relaxe, nos services feront retour à la BDRJ de la fiche dûment remplie afin qu'il soit procédé à l'effacement nécessaire sur le JUDEX.


LE PROCUREUR DE LA
RÉPUBLIQUE DE

LE PROCUREUR DE LA
RÉPUBLIQUE DE

ANNEXE 8 : EXEMPLES DE COURRIERS S'AGISSANT DU CONTRÔLE EXERCÉ PAR LES PARQUETS SUR LES FICHIERS D'ANTÉCÉDENTS JUDICIAIRES

2007 SC
B - 2007/00
30 NOV 2007

EVRY - PARQUET
11 DEC. 2007
BUREAU CENTRAL



Liberté - Égalité - Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INTÉRIEUR,
DE L'OUTRE-MER
ET DES COLLECTIVITÉS TERRITORIALES

Ecully, le

DIRECTION GÉNÉRALE
DE LA POLICE NATIONALE

DIRECTION CENTRALE
DE LA POLICE JUDICIAIRE

SOUS-DIRECTION
DE LA POLICE TECHNIQUE
ET SCIENTIFIQUE

DIVISION DES ÉTUDES
DES LIAISONS
ET DE LA FORMATION

T.G.I. EVRY

10 DEC. 2007

SERVICE COURRIER

Le sous-directeur chargé
de la police technique et scientifique

à

Monsieur le procureur de la République
près le tribunal de grande instance
d'Evry

REF PIN / DCPJ / PTS / DELF / IF 31419
AFFAIRE SUIVIE PAR

OBJET : Droit d'accès au fichier STIC.

REF. : Votre décision en date du 11/09/2007 faisant suite à la requête de monsieur _____, par laquelle il sollicite l'effacement des données à caractère personnel le concernant enregistrées dans le STIC.

Par courrier référencé ci-dessus adressé à Monsieur le directeur régional de la police judiciaire de Versailles, vous avez ordonné l'effacement des données à caractère personnel concernant Monsieur _____, né le _____ à Paris _____, inscrit au système de traitement des infractions constatées (STIC) en qualité de mis en cause pour usage de stupéfiants datant de 2006.

L'article 3 du décret n° 2001-583 du 5 juillet 2001 modifié prévoit que les décisions de classement sans suite pour insuffisance de charges entraînent l'ajout d'une mention dans le fichier, sauf si le procureur de la République en prescrit l'effacement. L'effacement, aux termes de la circulaire du ministère de la justice en date du 26 décembre 2006 ne devrait être ordonné que si la personne a été totalement mise hors de cause et que le maintien des informations n'est plus justifié au regard des finalités du fichier.

Je vous informe, qu'après examen du dossier, il n'a pas été procédé à l'effacement des données pour la procédure considérée dans laquelle les faits d'usage de stupéfiants sont avérés et reconnus par le requérant, ce dernier s'étant vu de surcroît notifier un rappel à la loi par officier de police judiciaire.

Par ailleurs, en application des dispositions du nouvel article 87-1 du décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi du 6 janvier 1978 modifiée, je vous informe que la commission nationale de l'informatique et des libertés a été tenue informée de la suite réservée à cette requête, à charge pour cette autorité d'en informer directement le requérant.

P/le sous-directeur chargé de la
police technique et scientifique

ADRESSE POSTALE : 31, avenue Franklin Roosevelt 69134 ECULLY CEDEX
Téléphone : 04 72 86 89 00 - Télécopie : 04 72 86 89 50

commissaire principal



B. Sol.

2007

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

Ecully, le 18 DEC. 2007

DIRECTION GENERALE
DE LA POLICE NATIONALE

DIRECTION CENTRALE
DE LA POLICE JUDICIAIRE

SOUS-DIRECTION
DE LA POLICE TECHNIQUE
ET SCIENTIFIQUE

DIVISION DES ETUDES
DES LIAISONS
ET DE LA FORMATION

Le sous-directeur chargé de la police
technique et scientifique

à

Monsieur le procureur de la République
près le tribunal de grande instance
d'EVRY

REF PN / DCPJ / PTS / DLF / N°
AFFAIRE SUIVIE PAR

OBJET : Droit d'accès au fichier STIC.

REF. : Votre décision en date du 11/09/2007 faisant suite à la requête de monsieur
par laquelle il sollicite l'effacement des données à caractère personnel
le concernant enregistrées dans le STIC

Par courrier référencé ci-dessus adressé à Monsieur le directeur régional de la police
judiciaire de Versailles, vous avez ordonné l'effacement des données à caractère personnel
concernant monsieur , né le à , inscrit au
système de traitement des infractions constatées (STIC) en qualité de mis en cause pour
dégradation de biens privés datant de 2003.

L'article 3 du décret n° 2001-583 du 5 juillet 2001 modifié prévoit que les décisions de
classement sans suite pour insuffisance de charges entraînent l'ajout d'une mention dans le fichier,
sauf si le procureur de la République en prescrit l'effacement. L'effacement, aux termes de la
circulaire du ministère de la justice en date du 26 décembre 2006, ne devrait être ordonné que si la
personne a été totalement mise hors de cause et que le maintien des informations n'est plus justifié
au regard des finalités du fichier.

Je vous informe, qu'après examen du dossier, il a été procédé à l'ajout de la mention de
classement sans suite et non à l'effacement des données pour la procédure considérée dans
laquelle les faits de dégradations de biens privés sont avérés et reconnus par le requérant.

Par ailleurs, en application des dispositions du nouvel article 87-1 du décret n° 2005-
1309 du 20 octobre 2005 modifié pris pour l'application de la loi du 6 janvier 1978 modifiée, je
vous informe que la commission nationale de l'informatique et des libertés a été tenue informée de
la suite réservée à cette requête, à charge pour cette autorité d'en informer directement le
requérant.

P/le sous-directeur chargé de la
police technique et scientifique

commissaire principal

4/4

OBJET
29 JAN. 2008
SECRETARIAT CENTRAL



MINISTÈRE DE L'INTÉRIEUR,
DE L'OUTRE-MER
ET DES COLLECTIVITÉS TERRITORIALES

ÉVALUÉ
29 JAN. 2008
E. - ION DES PEINES

DIRECTION GÉNÉRALE
DE LA POLICE NATIONALE

DIRECTION CENTRALE
DE LA POLICE JUDICIAIRE

SOUS-DIRECTION
DE LA POLICE TECHNIQUE
ET SCIENTIFIQUE

DIVISION DES ÉTUDES
DES LIAISONS
ET DE LA FORMATION

Ecully, le 24 JAN. 08

Le sous-directeur chargé de la police
technique et scientifique

à

Monsieur le procureur de la République
près le tribunal de grande instance
d'EVRY

REF PH / DCPJ / PTS / DELF / MP /
AFFAIRE SUIVIE PAR

OBJET : Droit d'accès au fichier STIC.

REF. : Votre décision en date du 11/09/2007 faisant suite à la requête de monsieur
, par laquelle il sollicite l'effacement des données à caractère personnel le
concernant, enregistrées dans le STIC

Par courrier référencé ci-dessus adressé à Monsieur le directeur régional de la police
judiciaire de Versailles, vous avez ordonné l'effacement des données à caractère personnel
concernant monsieur , né le } à } inscrit au système de
traitement des infractions constatées (STIC) en qualité de mis en cause pour dégradation de biens
privés datant de 1996, pour vol avec effraction et pour dénonciation mensongère à autorité
judiciaire ou administrative entraînant des recherches inutiles datant de 1997.

Je vous informe qu'à la suite d'une procédure d'accès indirect aux données à caractère
personnel le concernant, conduite sous le contrôle de la commission nationale de l'informatique et
des libertés (CNIL), des vérifications en vue de la mise à jour de la fiche de l'intéressé ont été
effectuées, notamment auprès de votre parquet, saisi le 23/10/2006 dans le cadre d'une demande
de communication des suites judiciaires pour les deux procédures visées.

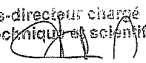
Par courrier retourné le 08/03/2007, dont une copie est jointe au présent, votre service a
prescrit pour l'affaire de dégradations volontaires datant de 1996 (E) l'ajout de la
mention de classement sans suite et a indiqué que la procédure datant de 1997 (E) a
fait l'objet d'une décision judiciaire de nature autre que celles énumérées par le décret du 5 juillet
2001 portant création du fichier STIC.

La procédure de vérification s'est achevée le 08/06/2007, après présentation du dossier de monsieur [redacted] à la commission nationale de l'informatique et des libertés (CNIL) qui a été informée de l'ajout de la mention de classement sans suite apportée par le gestionnaire du fichier pour la procédure de dégradation de biens privés datant de 1996.

En revanche, les données personnelles relatives à la procédure de vol avec effraction et de dénonciation mensongère à autorité judiciaire ou administrative, entraînant des recherches inutiles datant de 1997 ont été maintenues au fichier (conservation 20 ans).

Vu ce qui précède, j'ai le regret de vous informer que je ne peux accéder à la nouvelle requête en effacement des données à caractère personnel de monsieur [redacted], la fiche de l'intéressé ayant déjà fait l'objet d'une mise à jour pour les deux procédures considérées.

P/le sous-directeur chargé de la
police technique et scientifique



commissaire principal



Evry, le 2 décembre 2008

MINISTÈRE DE LA JUSTICE

TRIBUNAL DE GRANDE INSTANCE
EVRY
Le procureur de la République
Secrétariat Central - STIC

Le Procureur de la République

à

Monsieur le sous-directeur chargé de la police
technique et scientifique

31 avenue Franklin Roosevelt
69134 ECULLY Cedex

RAPPEL

LRAR

- OBJET** : Droit d'accès au fichier STIC
- V/Réf.** : Votre décision en date du 11/09/2007 faisant suite à la requête de monsieur par laquelle il sollicite l'effacement des données à caractère personnel le concernant, enregistrées dans le STIC.
- N/Réf.** : B501A-2006/C
Mon précédent courrier du 22 septembre 2008

J'ai l'honneur de vous rappeler que j'ai pris connaissance de votre transmission en date du 24 janvier 2008 reprise en références, qui appelle les observations suivantes :

- s'agissant de l'affaire de dégradations volontaires datant de 1996 (E)

Vous m'indiquez que cette procédure a fait l'objet d'une décision judiciaire de nature autre que celle énumérée par le décret du 5 juillet 2001 portant création du fichier STIC.

J'observe cependant que la décision prise par ce parquet le 29 janvier 1997 repose sur le motif suivant : l'enquête n'a pas permis de rassembler des preuves. Il apparaît donc clairement qu'aucune charge n'a pu être retenue à l'encontre de Monsieur et il serait pour le moins paradoxal qu'au seul prétexte que ce motif ne soit pas expressément visé, au sens littéral, par le décret pour que l'intéressé ne puisse pas bénéficier d'un effacement de cette mention.

En effet, notre parquet a considéré que rien dans la procédure ne permettait d'engager de poursuites à son encontre et il convient de s'en tenir à l'esprit des dispositions réglementaires et de considérer qu'aucune infraction ne peut lui être reprochée, le motif "absence d'infraction" repris dans mes réquisitions initiales est donc parfaitement caractérisé.

Dans ces conditions, je maintiens mes réquisitions initiales du 11 septembre 2007 et ordonne en conséquence l'effacement de la mention inscrite au fichier STIC de la police nationale sous la référence PV n° 1997/C.

- s'agissant de l'affaire de vol aggravé par deux circonstances datant de 1997
(E)

Les explications que vous avez bien voulu me donner ne peuvent pas davantage recevoir mon approbation.

En effet, il ressort clairement de la procédure dressée par le commissariat de Montgeron que Monsieur [redacted] - qui est d'ailleurs à l'origine de la dénonciation des faits qui ont permis de diligenter une enquête - a certes été entendu, pour autant, aucune charge n'a été retenue à son encontre puisque seuls Madame [redacted] Monsieur [redacted] et Monsieur [redacted] ont été renvoyés devant le tribunal correctionnel.

Ces derniers ont d'ailleurs bénéficié par un jugement du 4 juin 1998 d'une relaxe.

Il serait donc pour le moins paradoxal que les personnes impliquées dans la procédure et qui ont comparu devant le tribunal correctionnel puissent bénéficier d'un effacement de leur inscription au fichier STIC à la suite d'une décision de relaxe alors que, dans le même temps, une personne pour laquelle le parquet a considéré qu'il n'y avait pas lieu d'engager de poursuites à son encontre se verrait refuser le même effacement.

C'est la raison pour laquelle j'ai formalisé cette absence de poursuites par une décision de classement sans suite, aucune infraction ne pouvant être reprochée à Monsieur [redacted].

Dans ces conditions, je maintiens également mes réquisitions initiales du 11 septembre 2007 et ordonne en conséquence l'effacement de la mention inscrite au fichier STIC de la police nationale sous la référence : PV n° 1997/C. Cariat de Montgeron.

Je vous remercie de bien vouloir me rendre compte de vos diligences avant le 15 janvier 2009 à défaut je me verrais contraint de saisir la commission nationale de l'informatique et des libertés.

314 c



Evry, le 22 septembre 2008

MINISTÈRE DE LA JUSTICE

TRIBUNAL DE GRANDE INSTANCE
EVRY
Le procureur de la République
Secrétariat Central - STIC

Le Procureur de la République

à

Monsieur le sous-directeur chargé de la police
technique et scientifique

31 avenue Franklin Roosevelt
69134 ECULLY Cedex

OBJET : Droit d'accès au fichier STIC.

V/Réf. : Votre décision en date du 11/09/2007 faisant suite à la requête de monsieur par laquelle il sollicite l'effacement des données à caractère personnel le concernant, enregistrées dans le STIC.

N/Réf. : B501A-2006/C

J'ai pris connaissance de votre transmission en date du 24 janvier 2008 reprise en références, qui appelle les observations suivantes :

- s'agissant de l'affaire de dégradations volontaires datant de 1996 (E)

Vous m'indiquez que cette procédure a fait l'objet d'une décision judiciaire de nature autre que celle énumérée par le décret du 5 juillet 2001 portant création du fichier STIC.

J'observe cependant que la décision prise par ce parquet le 29 janvier 1997 repose sur le motif suivant : l'enquête n'a pas permis de rassembler des preuves. Il apparaît donc clairement qu'aucune charge n'a pu être retenue à l'encontre de Monsieur et il serait pour le moins paradoxal qu'au seul prétexte que ce motif ne soit pas expressément visé, au sens littéral, par le décret pour que l'intéressé ne puisse pas bénéficier d'un effacement de cette mention.

En effet, notre parquet a considéré que rien dans la procédure ne permettait d'engager de poursuites à son encontre et il convient de s'en tenir à l'esprit des dispositions réglementaires et de considérer qu'aucune infraction ne peut lui être reprochée, le motif "absence d'infraction" repris dans mes réquisitions initiales est donc parfaitement caractérisé.

Dans ces conditions, je maintiens mes réquisitions initiales du 11 septembre 2007 et ordonne en conséquence l'effacement de la mention inscrite au fichier STIC de la police nationale sous la référence : PV n°

- s'agissant de l'affaire de vol aggravé par deux circonstances datant de 1997
(Erf)

Les explications que vous avez bien voulu me donner ne peuvent pas davantage recevoir mon approbation

En effet, il ressort clairement de la procédure dressée par le commissariat de que Monsieur - qui est d'ailleurs à l'origine de la dénonciation des faits qui ont permis de diligenter une enquête - a certes été entendu ; pour autant, aucune charge n'a été retenue à son encontre puisque seuls Madame Monsieur et Monsieur ont été renvoyés devant le tribunal correctionnel

Ces derniers ont d'ailleurs bénéficié par un jugement du 4 juin 1998 d'une relaxe

Il serait donc pour le moins paradoxal que les personnes impliquées dans la procédure et qui ont comparu devant le tribunal correctionnel puissent bénéficier d'un effacement de leur inscription au fichier STIC à la suite d'une décision de relaxe alors que, dans le même temps, une personne pour laquelle le parquet a considéré qu'il n'y avait pas lieu d'engager de poursuites à son encontre se verrait refuser le même effacement.

C'est la raison pour laquelle j'ai formalisé cette absence de poursuites par une décision de classement sans suite, aucune infraction ne pouvant être reprochée à Monsieur

Dans ces conditions, je maintiens également mes réquisitions initiales du 11 septembre 2007 et ordonne en conséquence l'effacement de la mention inscrite au fichier STIC de la police nationale sous la référence : PV n°

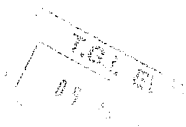
Je vous remercie de bien vouloir me rendre compte de vos diligences.

114

es



MINISTÈRE DE L'INTERIEUR,
DE L'OUTRE-MER
ET DES COLLECTIVITÉS TERRITORIALES



DIRECTION GÉNÉRALE
DE LA POLICE NATIONALE

DIRECTION CENTRALE
DE LA POLICE JUDICIAIRE

SOUS-DIRECTION
DE LA POLICE TECHNIQUE
ET SCIENTIFIQUE

DIVISION DES ÉTUDES
DES LIAISONS
ET DE LA FORMATION



Evry, le 08 JAN 2009

Le sous-directeur chargé de la police technique
et scientifique

à

Monsieur le procureur de la République
près le tribunal de grande instance d'Evry

REF PN / DCP / PTS / DELF / N°
AFFAIRE SUIVIE PAR

O B J E T : Droit d'accès au fichier STIC.
REFERENCE : Votre courrier N/Réf. B501A-2006/ en date du 22/09/2008 faisant suite à la décision DCPJ/PTS/DELF en date du 11/09/2007.

Par courrier cité en référence, vous confirmez votre demande d'effacement de la fiche concernant monsieur [nom], né le [date] à [lieu], inscrit au système de traitement des infractions constatées (STIC) en qualité de mis en cause, dans une affaire datant du 07/12/96 ([nom]) et une autre datant du 11/06/97 [nom] au motif que cette personne a bénéficié de deux décisions de classement sans suite, l'une motivée par une infraction insuffisamment caractérisée, l'autre par une absence d'infraction.

Je vous informe que le service central de documentation criminelle, direction d'application du STIC, a procédé à l'effacement des données à caractère personnel relatives aux affaires considérées.

Par ailleurs, vous évoquez une décision de relaxe prononcée le 4/06/98 par le tribunal correctionnel, en faveur de madame [nom], monsieur [nom] et monsieur [nom], suite à leur mise en cause dans l'affaire établie par le commissariat de [lieu].

A ce jour, la consultation du STIC, sous la référence susvisée, fait apparaître que ces trois personnes y figurent en qualité de mis en cause.



En vertu du III de l'article 21 de la loi du 18 mars 2003, une telle décision conduit en principe à l'effacement des données personnelles concernant les personnes mises en cause, sauf si le procureur de la République en prescrit le maintien pour des raisons liées à la finalité du fichier.

Les termes de votre lettre du 22/09/08 indiquaient que ces trois personnes pouvaient « bénéficier d'un effacement de leur inscription au fichier STIC à la suite de la décision de relaxe ».

C'est la raison pour laquelle, je vous informe également de l'effacement des données à caractère personnel de madame _____ monsieur _____ et monsieur _____ relatives à l'affaire établie par le commissariat de _____ 61007.

P/le sous-directeur chargé de la
police technique et scientifique

~~_____~~
commissaire divisionnaire

ANNEXE 9 : EXEMPLES DE REFUS D'AGRÉMENT PRÉFECTORAL POUR L'ACCÈS À UNE PROFESSION DANS LE DOMAINE DE LA SÉCURITÉ PRIVÉE



PREFECTURE DES HAUTS-DE-SEINE

27 AVR 2006

CABINET DU PREFET
Service de la sécurité intérieure et de la police générale
Bureau des polices administratives
Affaire suivie par : Mlle
Tél : 01
Fax : 01
Courriel : cabinet@hauts-de-seine.pref.gouv.fr
Recommandée avec A.R.

Nanterre, le 25 AVR 2006

SECURITAS
162/166 boulevard de Verdun
92413 COURBEVOIE CEDEX

Monsieur,

Vous avez souhaité recruter Monsieur [redacted] au sein de votre entreprise, en qualité d'agent de surveillance.

J'ai le regret de vous informer que celui-ci ne remplit pas les conditions de moralité prévues à l'article 6 de la loi réglementant les activités privées de sécurité n° 83-629 du 12 juillet 1983 modifiée.

Je vous serais obligé de bien vouloir, sans délai, notifier cette décision à l'intéressé en le faisant émarger sur le présent document, et de lui en remettre copie.

Je vous précise que Monsieur [redacted] peut présenter, dans un délai de deux mois à compter de la présente notification :

- soit un recours gracieux auprès de mes services,
- soit un recours hiérarchique auprès de Monsieur le Ministre d'Etat, Ministre de l'Intérieur et de l'Aménagement du Territoire (direction des libertés publiques et des affaires juridiques – sous-direction des libertés publiques, 7^{ème} bureau – 11 rue des Saussaies - 75800 Paris Cedex 08),
- soit un recours contentieux devant le Tribunal Administratif de Versailles (56 avenue de St Cloud - 78011 Versailles Cedex).

Si celui-ci estime devoir utile de former un recours, selon les modalités ci-dessus exposées, il devra joindre à sa correspondance un exemplaire du présent document.

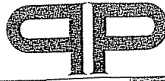
Je vous prie de croire, Monsieur, à l'assurance de ma considération distinguée.

Pour le Préfet,
L'Adjointe à la Directrice de Cabinet

M. [redacted] reconnaît avoir pris connaissance de la décision de la Préfecture des Hauts-de-Seine.

Date et signature :

4/05/2006



PREFECTURE DE POLICE
DIRECTION DE LA POLICE GENERALE

4^{ème} Bureau
36, rue des Morillons - 75015 Paris
Affaire suivie par : M. ...
REF : 1764
Tél. : 01
Mél. : prefpol.dpg-4eb-gardiennage@interieur.gouv.fr

Paris, le 04 SEP 2004

M.
78500 Sartrouville

Lettre recommandée avec A.R.

Monsieur,

Par lettre parvenue dans mes services le 15 décembre 2004, vous m'avez saisi d'un recours gracieux contre ma décision du 1^{er} décembre vous signifiant, ainsi qu'à votre employeur, la société "GROUP 4 FALCK", votre incapacité à exercer la profession d'agent de surveillance.

Vous joignez à votre courrier copie d'une décision du Tribunal de Grande Instance de Paris du 12 mai 2003 mentionnant l'exclusion du bulletin numéro 2 du casier judiciaire d'une condamnation prononcée à votre encontre le 7 juin 2000 par la 16^{ème} Chambre Correctionnelle du même Tribunal.

J'en prends bonne note.

L'article 6 de la loi n° 83-629 du 12 juillet 1983 modifiée réglementant les activités de sécurité privée précise les conditions à respecter pour être employé par une société les exerçant.

Or, bien que votre casier judiciaire soit vierge suite à l'exclusion de la condamnation du 7 juin 2000, vous ne remplissez pas ces conditions, eu égard aux faits commis le 19 septembre 1990 à Paris (75), les 1^{er} mai 1995 et 1^{er} août 1999 à Bondy (Seine-Saint-Denis) et le 6 décembre 1999 à Paris (75019) figurant dans les traitements automatisés de données personnelles gérés par les autorités de police.

REPUBLIQUE FRANÇAISE
Liberté Egalité Fraternité

PREFECTURE DE POLICE - 9, boulevard du Palais - 75195 PARIS CEDEX 04 - Tél : 01 53 71 53 71 ou 01 53 73 53 73
Serveur vocal : 08 91 01 22 22 (0,225 € la minute)

3611 PREFECTURE DE POLICE (gratuit les trois premières minutes puis 0 112 € par tranche de deux minutes)
<http://www.prefecture-police-paris.interieur.gouv.fr> - mél : cabcom.prefecturepoliceparis@interieur.gouv.fr

Ces mentions emportant incapacité d'exercer l'emploi d'agent de sécurité, j'ai le regret de vous faire connaître qu'il ne m'est pas possible de revenir sur la décision prise à votre rencontre

Je vous informe toutefois que vous disposez d'un droit d'accès aux informations vous concernant inscrites dans ce traitement informatisé qui s'exerce par l'intermédiaire de la CNIL, conformément à l'article 41 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

Il convient pour ce faire de formuler une demande écrite auprès de cette autorité sise *21 rue Saint Guillaume à Paris (75340)*, laquelle est par ailleurs **uniquement** habilitée à solliciter la mise à jour de données éventuellement **inexactes**.

Il est précisé que si vous estimez devoir contester la présente décision, il vous appartient d'utiliser les voies de droit encore offertes telles qu'elles vous ont été initialement indiquées.

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

Le DIRECTEUR de la POLICE GÉNÉRALE
L'Administrateur CIVIL
Chargé de Mission
auprès du Directeur de la Police Générale

ANNEXE 10 : LE COÛT DES FICHIERS DE POLICE - MISSION SÉCURITÉ - PROGRAMME POLICE NATIONALE

(action 6)

(en euros)

Totaux	Crédits inscrits au PLF		Crédits consommés	
	AE	CP	AE	CP
2002			2 258 842	2 258 842
2003			2 049 513	2 049 513
2004			2 351 140	2 351 140
2005			4 777 312	5 248 475
2006			16 507 027	5 749 640
2007	9 460 000	10 000 000	8 305 07	11 230 311
2008	4 150 000	6 985 000	18 719 900	10 760 317
2009	13 300 000	16 100 000	-	-

ARIANE	Crédits inscrits au PLF		Crédits consommés	
	AE	CP	AE	CP
2006			6 692 340	-
2007	1 000 000	3 300 000	3 795 962	4 379 228
2008	1 000 000	4 085 000	175 896	2 106 966
2009	1 700 000	2 200 000	-	-

ARDOISE	Crédits inscrits au PLF		Crédits consommés	
	AE	CP	AE	CP
2008			641 148	179 391

FAED	Crédits inscrits au PLF		Crédits consommés	
	AE	CP	AE	CP
2002			2 258 842	2 258 842
2003			1 834 504	1 834 504
2004			2 134 301	2 134 301
2005			4 710 527	5 181 690
2006			9 640 653	5 710 032
2007			3 214 769	6 454 784
2008	3 150 000	2 900 000	16 929 878	7 601 321
2009	11 600 000	13 900 000		

FNAEG	Crédits inscrits au PLF		Crédits consommés	
	AE	CP	AE	CP
2003			215 009	215 009
2004			216 839	216 839
2005			66 785	66 785
2006			174 035	39 608
2007	8 460 000	6 700 000	128 880	183 749
2008			406 613	183 824

PHAROS	Crédits inscrits au PLF		Crédits consommés	
	AE	CP	AE	CP
2007			506 083	-
2008			223 471	566 710

N-MCI	Crédits inscrits au PLF		Crédits consommés	
	AE	CP	AE	CP
2007			659 376	212 551
2008			342 893	122 106

Source : Ministère de l'Intérieur, de l'outre-mer et des collectivités territoriales.

ANNEXE 11 : LETTRES DE CADRAGE DE LA MISSION « ARCHIVES DES RENSEIGNEMENTS GÉNÉRAUX »



MINISTÈRE DE L'INTÉRIEUR
DE L'OUTRE-MER
ET DES COLLECTIVITÉS TERRITORIALES

Cabinet du Ministre

Le Préfet, Directeur du
Cabinet

Paris, le 18 décembre 2008

Réf. : SJ/MD

NOR : INTK08301235

**Le Ministre de l'Intérieur, de l'Outre-mer
et des Collectivités Territoriales**

à

**Monsieur le Directeur Général de la Police Nationale
Monsieur le Préfet de Police
Mesdames et Messieurs les Préfets de département
(Métropole et Outre - Mer)**

OBJET : Mission "Archives des Renseignements Généraux"

P. J. : 1

Aux termes de la réorganisation des services de renseignement du ministère de l'Intérieur, de l'Outre-mer et des Collectivités Territoriales une partie du contenu des fichiers de ces services, notamment ceux des anciens renseignements généraux, est aujourd'hui sans objet. Un nombre important de données devront être versées aux Archives.

Ces changements nécessitent, à partir d'une documentation riche et complexe, parfois très ancienne et parfois classée sans règles uniformes, de définir des règles de tri, d'archivage et d'exploitation des données.

J'ai confié à Elisabeth RABUT, Chef de l'Inspection Générale des Archives de France une mission qui nous permettra de bénéficier d'un ensemble de règles clair et opérationnel, à la fois pour la période transitoire qui les conduira à un nouveau cadre juridique et pour l'exercice ultérieur de leur activité. Elle sera assistée, pour sa mission de fonctionnaires du Ministère de la Culture et de la Communication et du Ministère de l'Intérieur, de l'Outre-mer et des Collectivités Territoriales. Gilles SANSON, Inspecteur Général de l'Administration en sera le rapporteur général. Vous trouverez, joint à la présente, copie de la lettre de mission ainsi que la composition du groupe de travail.

.../

- 2 -

Cette mission peut être amenée à se rendre dans des services de préfectures ou de DDSP. Elle vous en informera préalablement et je vous demande de bien vouloir lui réserver le meilleur accueil.

Je vous rappelle enfin, qu'il ne doit être procédé à aucune destruction de fichiers avant que les conclusions de cette mission soient rendues publiques.

**Pour le Ministre et par délégation
Le Préfet, Directeur du Cabinet**

A handwritten signature in black ink, appearing to be 'M. Delpuech', written over a faint circular stamp or watermark.

Michel DELPUECH



MINISTÈRE DE L'INTÉRIEUR,
DE L'OUTRE-MER
ET DES COLLECTIVITÉS TERRITORIALES

Le Ministre

Paris, le 4/12/08
Réf : CAB/SJ n°48

Madame l'Inspecteur Général,

La réorganisation des services de renseignement du Ministère de l'Intérieur, de l'Outre-mer et des Collectivités Territoriales qui a pris effet le 1^{er} juillet dernier, s'est traduite par la création de la Direction Centrale du Renseignement Intérieur (DCRI), chargée des missions de sécurité nationale assurées auparavant par la Direction de la Surveillance du Territoire (DST) et la Direction Centrale des Renseignements Généraux (DCRG).

De son côté, la Direction Centrale de la Sécurité Publique (DCSP) est désormais chargée, entre autre, d'une mission dite d'information générale et bénéficie pour se faire, en son sein d'une Sous-Direction de l'Information Générale (SDIG) qui se décline au niveau départemental. Cette mission était auparavant assurée, avec des attributions plus larges, par la DCRG.

Aux termes de ces réorganisations, une partie du contenu des fichiers de ces services est aujourd'hui sans objet. Un nombre important de données devront être versées aux Archives.

Ces changements nécessitent, à partir d'une documentation riche et complexe, parfois très ancienne et parfois classée sans règles uniformes, de définir des règles de tri, d'archivage et d'exploitation des données.

.../...

Madame Elisabeth RABUT
Chef de l'inspection générale des Archives de France
Direction des Archives de France
Inspection générale
56 rue des Francs-Bourgeois
75141 Paris Cedex 03

La mission que j'ai souhaité vous confier, et que je vous remercie d'avoir acceptée, permettra à mes services de bénéficier d'un ensemble de règles clair et opérationnel, à la fois pour la période transitoire qui les conduira à un nouveau cadre juridique et pour l'exercice ultérieur de leur activité.

Je vous prie de trouver ci-joint la composition de la mission que vous présidez. Vous serez assistée, chaque fois que nécessaire, par les services de la Direction Générale de la Police Nationale et de la Préfecture de Police.

A partir d'une évaluation de la situation existante, qu'il s'agisse des fonds documentaires détenus par les SDIG, la DCSP et la préfecture de police ou des règles d'archivage et de traitement qui y sont appliquées, il conviendra notamment d'examiner :

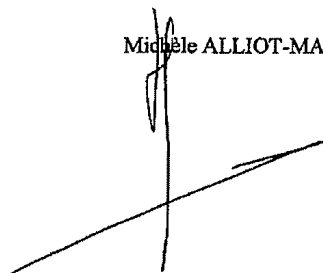
- les critères à retenir dans la répartition des données entre celles qui doivent être conservées par les services d'information générale, celles qui doivent être transférées et celles qui doivent être versées aux archives ;
- l'intérêt d'un versement intégral ou d'un versement par échantillonnage dans les services publics d'archives ;
- les modes de classement et d'indexation, les méthodes de traitement et de consultation des données détenues par les SDIG ;
- les durées de conservation des données dans les services qui les produisent, en fonction des besoins de consultation par ceux-ci dans le temps.

Votre rapport devra m'être remis le 15 mars 2009. Je vous remercie de me présenter un rapport d'étape d'ici le 1er février 2009.

Je vous prie, Madame l'Inspecteur Général, d'agréer l'expression de ma considération distinguée.

*et de mon souvenir très
fidèle et cordial*

Michèle ALLIOT-MARIE



PJ : Composition des membres de la mission

Copie : Madame Christine ALBANEL
Ministre de la Culture et de la Communication

Composition de la Mission "Archives des Renseignements Généraux"

Chef de la mission : - Elisabeth RABUT, Chef de l'inspection générale des Archives de France,

Rapporteur Général : - Gilles SANSON, Inspecteur Général de l'Administration : Inspection Générale de l'Administration,

Membres :

• **Archives de France** :

- Hélène SERVANT, conservateur au Département de la politique archivistique et de la coordination interministérielle (direction des Archives de France)
- Evelyne VAN DEN NESTE, conservateur responsable du service des missions (direction des Archives de France)

• **Ministère de l'Intérieur, de l'Outre-mer et des Collectivités Territoriales** :

- Laurent TOUVET, Conseiller d'Etat, Direction des Libertés Publiques et des Affaires Juridiques,
- Xavier PENEAU, Chef de Service, Directeur-Adjoint de la Direction de la Modernisation et de l'Action Territoriales,
- Jérôme LEONNET, Inspecteur Général, Coordonnateur des services de l'Inspection Générale de la Police Nationale,
- Véronique LEFAURE, commissaire divisionnaire, Direction Centrale de la Sécurité Publique,
- Jean-Pierre LESGOURGUES commissaire divisionnaire, Direction du Renseignement de la Préfecture de Police,
- Pierre MONTASTIER, commissaire divisionnaire, Inspection Générale de la Police Nationale,
- Philippe BERTRAND, attaché au bureau des libertés publiques, Direction des Libertés Publiques et des Affaires Juridiques,

Rapporteurs : - Nacera HADDOUCHE, Inspecteur de l'Administration, Inspection Générale de l'Administration :

- Sylvain MANVILLE, Chef de la mission des archives de France, Ministère de l'Intérieur, de l'Outre-mer et des Collectivités Territoriales,

ANNEXE 12 : CIRCULAIRE DU MINISTÈRE DE L'INTÉRIEUR DU 3 JUILLET 2001 RELATIVE AUX RÈGLES DE TRI ET DE CONSERVATION DES DOCUMENTS PRODUITS PAR LES SERVICES DES RENSEIGNEMENTS GÉNÉRAUX

Archives de France

CIRCULAIRE AD 2001-1 DU 3 JUILLET 2001

Tri et conservation des documents produits ou reçus par les directions régionales et départementales des renseignements généraux

Le ministre de l'Intérieur

La ministre de la Culture et de la Communication

à

Mesdames et Messieurs les Préfets (directions régionales et départementales des renseignements généraux)

Mesdames et Messieurs les Présidents des Conseils généraux (archives départementales)

Monsieur le Directeur central des renseignements généraux

Références : Nos précédentes circulaires :

- AD 94-3 du 17 janvier 1994, relative au traitement et à la conservation des documents produits ou reçus par les services de police

- NOR/INT/C/95/00225/C (AD 95-6) du 28 juillet 1995, relative au traitement et à la conservation des archives publiques des compagnies républicaines de sécurité

- NOR/INT/C/98/00156/C (AD 98-4) du 6 juillet 1998, relative au tri et à la conservation des documents produits ou reçus par les commissariats de police

La présente circulaire se situe dans la continuité de la circulaire AD 94-3 du 17 janvier 1994 portant sur le traitement et la conservation des documents produits ou reçus par les services de police. Les principes énoncés dans le cadre de cette circulaire s'appliquent aux directions régionales et départementales des renseignements généraux. Aussi convient-il de se reporter à ce document pour prendre connaissance des règles générales concernant les archives et la documentation, des modalités de versement des archives du service aux archives départementales et des conditions de communication des archives versées.

1. Rappel historique sur les directions régionales et départementales des renseignements généraux

Depuis l'apparition des États organisés, les souverains et gouvernements de toute nature désirent être informés des activités des populations qu'ils dirigent susceptibles d'intéresser, voire d'entraver, la conduite de leur politique. L'une des tâches confiées par les gouvernants à l'administration est donc d'organiser la collecte et l'exploitation des renseignements concernant la sécurité des hautes personnalités de l'État et la mise en cause de l'action de celles-ci, allant de l'opposition dans le cadre légal aux agissements clandestins visant à renverser le régime en place. En France, cette mission incombe aux services des renseignements généraux, qui constituent l'une des composantes de l'administration de la police.

Archives de France

Si l'ancien régime n'a pas méconnu les activités de surveillance de l'état de l'opinion, notamment par le biais du " cabinet noir ", chargé de l'interception des correspondances privées, c'est au Consulat et à l'Empire que l'on doit la naissance du premier service organisé en charge de la police de renseignement. L'une des six divisions du ministère de la police générale, dirigé par Fouché, est chargée de la sûreté générale et de la police secrète. Elle est confiée à Pierre-Marie Desmarest, qui en gardera la tête jusqu'à la Restauration.

Après la chute de Napoléon 1^{er}, la police de renseignement connaît peu d'évolutions notables jusqu'au second Empire. Ce régime décide de développer cette fonction en s'appuyant sur la police spéciale des chemins de fer, dont la création avait été décidée par la Monarchie de Juillet afin d'organiser la sécurité des voyageurs dans ce nouveau moyen de locomotion. Les décrets impériaux du 22 février et du 15 décembre 1855 créent trente commissaires spéciaux de police qui résident aux extrémités ou aux points intermédiaires importants des réseaux ferrés. Ces fonctionnaires sont chargés non seulement de la répression des infractions de droit commun, mais aussi de la surveillance de l'état de l'opinion quant aux questions politiques, économiques et sociales. Rattachés au ministère de l'Intérieur, ces commissaires spéciaux constituent la première implantation territoriale stable de la police de renseignement.

En complément de ces décrets fondateurs, d'autres directives impériales viennent élargir les prérogatives des commissaires spéciaux, dont l'action est de moins en moins confinée à la seule police des chemins de fer. Ainsi, un décret du 15 mars 1861 confie à ceux-ci la surveillance des mouvements des étrangers et la police des ports et des frontières. Une circulaire du 1^{er} octobre 1862 met ces mêmes commissaires à la disposition des préfets pour toute mission que ces derniers jugeraient opportun de leur confier. Ces attributions sont aujourd'hui encore, pour bon nombre d'entre elles, exercées par les directions régionales et départementales des renseignements généraux.

L'outil mis en place par le second Empire sera maintenu et même renforcé par la troisième République. C'est à ce régime que l'on doit l'installation d'un commissaire spécial dans chaque chef-lieu de département, par circulaire du 17 janvier 1894 : le maillage territorial initié par Napoléon III est ainsi complété. De nouvelles et importantes missions sont également confiées à ce service de police : le contre-espionnage interne, dont l'armée est dessaisie à la suite de l'affaire Dreyfus, par décret du 1^{er} mai 1899 ; la surveillance des jeux, par décret du 18 mai 1909 ; enfin la police de l'air et des aérodromes, par décret du 15 juin 1930. On doit enfin à la troisième République l'apparition de l'appellation " renseignements généraux ", employée pour la première fois dans une circulaire de 1907 et la création, par décret du 26 avril 1937, d'une direction des services de renseignements généraux.

Parallèlement à cette action nationale, le gouvernement républicain encourage le développement, à Paris, d'une police de renseignement tout aussi structurée et possédant des attributions identiques, dans le cadre de la préfecture de police.

La loi du 23 avril 1941, qui met en place les structures de la police nationale telles qu'elles existent encore de nos jours, crée un service des renseignements généraux rattaché à la direction générale de la police nationale. Les prérogatives de ce service sont confirmées par le gouvernement de Vichy. L'ordonnance du 16 novembre 1944, manifestant la reprise en mains de la police nationale par les autorités de la France libre, confirme l'existence d'une direction des renseignements généraux, désormais distincte de la nouvelle direction de la surveillance du territoire.

La cinquième République est à l'origine de l'appellation actuelle de direction centrale des renseignements généraux, qui désigne, depuis un arrêté du 16 octobre 1968, le service chargé de la police de renseignement. Celui-ci connaît des modifications dans la répartition de ses missions : une circulaire du 10 novembre 1972 érige la police de l'air et des frontières en service autonome. Ses compétences territoriales sont étendues aux départements et territoires d'outre mer par circulaire interministérielle du 21 mars 1979. Enfin, depuis une dizaine d'années, les attributions des directions régionales et départementales des renseignements généraux font l'objet d'importantes évolutions, qui conduisent ces services à abandonner le suivi de l'activité et du fonctionnement interne des partis politiques au profit de l'intelligence économique et de la police de proximité.

2. Le tri et la conservation des documents produits ou reçus par les directions régionales et départementales des renseignements généraux

Archives de France

Fruit d'une réflexion menée conjointement par des archivistes et des agents de la police nationale affectés dans les services des renseignements généraux, le tableau d'archivage joint à la présente circulaire est un outil de travail concret devant permettre à chacun d'accomplir aisément les tâches qui lui incombent concernant les archives. Il est divisé en quatre colonnes qui apportent les informations suivantes :

- colonne 1 : la **typologie des documents** ; le nom sous lequel chaque document est désigné reflète l'appellation actuelle de ce document ;
- colonne 2 : la **durée d'utilité administrative (D.U.A.)**, soit la période pendant laquelle le service doit conserver sous sa responsabilité les dossiers d'utilisation fréquente (archives courantes) ou épisodique (archives intermédiaires) ;
- colonne 3 : le **sort final** à expiration de la D.U.A., qui peut être de trois ordres :
 - la **conservation** définitive aux archives départementales (C), pour les archives possédant une valeur historique majeure ;
 - la **destruction (D)** par les soins du service producteur des archives au terme de la D.U.A. et après signature d'un visa d'élimination par le directeur des archives départementales ;
 - le **tri (T)** pour les documents dont l'intérêt historique ne justifie pas une conservation intégrale ;
- colonne 4 : les **observations** ; elles s'appliquent à un document précis et peuvent porter sur chacune des trois colonnes du tableau.

Le tableau prend en compte les documents actuellement produits ou reçus par les directions régionales et départementales des renseignements généraux au cours de leur activité. Il ne peut englober l'intégralité des archives conservées au sein d'une direction donnée, dont la production a pu être générée par des attributions aujourd'hui disparues. Lorsque l'analogie entre un document conservé dans la direction concernée et la typologie offerte par le tableau s'avère impossible, il convient de développer une réflexion commune associant les responsables des directions concernés et ceux des archives afin de déterminer le traitement adapté au document en question.

Pour le ministre de l'Intérieur
et par délégation,
le directeur général de la police nationale
Patrice BERGOUGNOUX

Pour la ministre de la Culture et de la
Communication
et par délégation,
la directrice des archives de France
Martine de BOISDEFRE

DOCUMENTS	D.U.A.	SORT FINAL	OBSERVATIONS
-----------	--------	------------	--------------

1. ADMINISTRATION DE LA POLICE			
1. 1. Instructions générales et correspondances			
Circulaires administratives et instructions provenant du ministère de l'intérieur ou, le cas échéant, d'autres ministères	Validité	D (1)	(1) Ces documents sont archivés au niveau des administrations centrales.
Notes de service	Validité	C	
Registres du courrier arrivée et départ	10 ans à compter de la clôture du registre	D	
Messages reçus (ou " arrivée ") : chronos	2 ans	D	
Les messages proviennent essentiellement de la direction centrale des RG, des directions régionales, des autres directions départementales des RG, du secrétariat général pour l'administration de la police (S G A P), de la délégation régionale au recrutement et à la formation (D R R F), des directions départementales de la sécurité publique ou de la préfecture.			
Messages émis (ou " départ ") : chronos	10 ans	C	
Ces messages ont pour principaux destinataires les correspondants habituels des services des RG mentionnés ci-dessus. Ils peuvent aussi avoir un caractère exclusivement interne, lorsqu'ils portent sur l'administration ou le fonctionnement du service. Les messages ont tout d'abord été transmis par télégramme ou télex, puis par fax. Ces modes de diffusion s'étant avérés peu sécurisés, les services des RG ont par la suite adopté des réseaux propres au ministère de l'intérieur (réseau Rescom). A présent, les RG bénéficient d'un réseau de diffusion spécifique, le réseau de bureautique nationale (R B N), dont l'accès est entièrement contrôlé.			
Synthèses thématiques :			
Ces synthèses peuvent porter sur les violences urbaines, les mouvements sociaux, les manifestations de contestation, etc			
- réalisées par la direction centrale des RG	5 ans	D (1)	(1) Ces documents sont archivés au niveau des administrations centrales
- réalisées par la direction régionale des RG	5 ans	C	
- réalisées par la direction départementale des RG	5 ans	C	
1. 2. Organisation interne			
1.2.1. Personnel			

Archives de France

Dossiers administratifs	3 ans à compter du départ à la retraite	D (2)	(2) Voir la circulaire AD 95-1 du 27 janvier 1995 sur le tri et la conservation des dossiers de personnel. Le dossier de carrière des agents est géré par l'administration centrale du ministère de l'intérieur. Le dossier administratif de la direction régionale ou départementale des RG n'est qu'un doublon de ce dossier de carrière et suit l'agent dans ses affectations successives
1.2.2. Budget			
Documents relatifs au budget	5 ans	D	
Pièces comptables relatives à la gestion des crédits d'investissement	10 ans	D	
Pièces comptables relatives à la gestion des crédits de fonctionnement	5 ans	D	
1.2.3. Equipement			
Matériel			
Fiches d'inventaire du matériel	Validité	D	
Inventaire des matériels	Validité	D	
Matériel des transmissions : fiches d'inventaire	Validité	D	
Véhicules : carnet de bord	Validité	D	
Carburant : répertoire de comptabilité	5 ans	D	
Armement			
Répertoire des armes	5 ans à compter de la clôture du répertoire	D	Le répertoire est rédigé par type d'armes.
Carnet de tir	Validité	D	
2. FONCTIONS DE POLICE DE RENSEIGNEMENT			
2. 1. Documents de synthèse			
Messages de synthèse régionale :			
Ces synthèses sont adressées quotidiennement par les directions régionales des RG à la direction centrale. Elles sont réalisées à partir des éléments transmis par les directions départementales des RG			
- chronos	5 ans	C	
- registres	clôture du registre (1)	C	(1) Les registres permettent de retrouver les synthèses. Ils doivent, dans la mesure du possible, être versés aux archives départementales en même temps que celles-ci et, en tout état de cause, dès leur clôture.

Archives de France

Données transmises par les directions départementales :			
- chronos	5 ans	C	
- registres	clôture du registre (2)	C	(2) Les registres permettent de retrouver les notes comportant les données transmises par les directions départementales. Ils doivent, dans la mesure du possible, être versés aux archives départementales en même temps que celles-ci et, en tout état de cause, dès leur clôture.
Notes d'informations :			
Ces notes contiennent des informations de caractère général. Elles sont généralement adressées au cabinet du préfet, à la direction régionale (lorsqu'elles émanent de directions départementales) et à la direction centrale.			
- chronos	10 ans	C	
- registres	clôture du registre (1)	C	(1) Les registres permettent de retrouver les notes d'informations. Ils doivent, dans la mesure du possible, être versés aux archives départementales en même temps que celles-ci et, en tout état de cause, dès leur clôture.
Notes confidentielles :			
Ces notes contiennent des informations sensibles			
- chronos	50 ans (2)	C	(2) Les notes contenues dans ces chronos alimentent des dossiers individuels de personnalités dont la DUA est de 50 ans.
- registres	clôture du registre (3)	C	(3) Les registres permettent de retrouver les notes confidentielles. Ils doivent, dans la mesure du possible, être versés aux archives départementales en même temps que celles-ci et, en tout état de cause, dès leur clôture.
Notes à l'attention du préfet :			
Ces notes ont le préfet pour seul destinataire			
- chronos	10 ans	C	
- registres	clôture du registre (1)	C	(1) Les registres permettent de retrouver les notes à l'attention du préfet. Ils doivent, dans la mesure du possible, être versés aux archives départementales en même temps que celles-ci et, en tout état de cause, dès leur clôture.
2. 2. Dossiers individuels			

Archives de France

Fichier permettant l'accès aux dossiers individuels	identique à celle des dossiers individuels (2)	C	(2) Lors du versement des dossiers individuels aux archives départementales, on s'attachera à joindre les fiches permettant l'accès aux dossiers versés.
Dossiers individuels : personnalités Ces dossiers peuvent concerner des hommes politiques, des fonctionnaires, des personnalités du monde culturel, économique, syndical, ou associatif, ainsi que des personnes ayant attiré l'attention dans les domaines suivants : sectes, terrorisme et mouvances extrémistes, régionalisme, délinquance financière, communautés étrangères surveillées, etc.	50 ans à compter de l'ouverture du dossier (3)	C	(3) Toutefois, lorsque ces dossiers ne sont plus alimentés depuis 15 ans, les directions régionales et départementales des RG peuvent procéder à leur versement anticipé aux archives départementales
Dossiers individuels : enquêtes :			
Contrairement aux dossiers de personnalités, les dossiers d'enquête ne couvrent pas l'ensemble de la vie d'un individu, mais concernent uniquement une circonstance précise (candidature à un concours, demande d'asile, demande d'obtention d'une décoration, etc) Leur contenu informatif est donc moins riche que celui des dossiers individuels. Depuis 1994, les enquêtes ne donnent plus lieu à l'ouverture d'un dossier individuel sur support papier, sauf lorsqu'elles sont défavorables			
- candidats aux concours administratifs	10 ans à compter de la date de l'enquête	T (4)	(4) Conserver les enquêtes défavorables.
- demandes de nouvelle affectation après un congé parental ou une mise en disponibilité	10 ans à compter de la date de l'enquête	T (1)	(1) Conserver les enquêtes défavorables.
Ces enquêtes concernent les seuls fonctionnaires de police.			
- décorations	10 ans à compter de la date de l'enquête	T (2)	(2) Conserver les enquêtes défavorables.
- détention d'armes	10 ans à compter de la date de l'enquête	T (3)	(3) Conserver les enquêtes défavorables.

Ces enquêtes ne sont plus pratiquées.			
- étrangers Ces enquêtes sont menées sur requête des préfectures ou des sous-préfectures et concernent les demandes d'asile, de naturalisation, de sauf-conduit et de visas longs et courts séjours	50 ans à compter de la date de l'enquête	T (4)	(4) Conserver les enquêtes défavorables Sur le traitement des dossiers relatifs à la naturalisation et aux étrangers conservés en préfecture, voir la circulaire NOR/INT/A/94/00198/C - AD 94-7 du 28 juillet 1994 sur le tri et la conservation des documents liés à la nationalité, produits dans les préfectures et les sous-préfectures
- individus appartenant au monde des courses et jeux Il s'agit des bailleurs, des locataires, des propriétaires et des entraîneurs de chevaux, des responsables de points PMU, des employés de casinos, des joueurs exclus, etc. Le secteur des courses et jeux constitue une compétence propre des directions régionales et départementales des RG en matière de police administrative	50 ans à compter de la date de l'enquête	C	
2. 3. Dossiers collectifs			
Dossiers collectifs :			
Les dossiers collectifs regroupent l'ensemble des informations relatives à un thème particulier traité par les renseignements généraux. Les DUA indiquées ci-dessous courent non pas à compter de l'ouverture ou de la clôture du dossier (car la plupart des dossiers ne sont pas clos à ce jour), mais de la date des documents contenus dans les dossiers. Elles couvrent la période durant laquelle les documents contenus dans le dossier du groupe concerné ont une valeur opérationnelle. Cette valeur une fois perdue, les documents sont versés aux archives départementales.			
- vie politique	20 ans (1)	C (2)	(1) Pour les dossiers relatifs à la violence politique, la DUA sera de 50 ans. (2) Les services d'archives départementales peuvent cependant éliminer, au sein de ces dossiers, les documents faisant état des résultats électoraux, sous réserve que ceux-ci soient par ailleurs versés par la préfecture ou les collectivités territoriales
- vie sociale	20 ans	C	
- vie économique	20 ans	C	
- presse et médias	20 ans	C	

Archives de France

- faits de société	20 ans	C (1)	(1) Pour les dossiers relatifs aux villes et banlieues, la DUA sera de 50 ans Il en sera de même pour les dossiers relatifs aux sectes
- dossiers d'actualité	20 ans	C	
- communautés étrangères	50 ans	C	
- vie religieuse	50 ans	C	
- courses et jeux	50 ans	C	
2. 4. Dossiers correspondant à un ressort géographique			
Dossier départemental :			
Le dossier départemental constitue la synthèse des informations collectées par les services des renseignements généraux concernant le département dont ils ont la charge Il est tenu à la disposition du préfet et régulièrement actualisé.			
- notices des personnalités	Validité	Sans objet (1)	(1) Conserver les exemplaires se trouvant au cabinet du préfet.
- dossiers thématiques	Validité	Sans objet (2)	(2) Conserver les exemplaires se trouvant au cabinet du préfet
Les thèmes sont les mêmes que ceux des dossiers collectifs			
Dossiers communaux	10 ans	C	
Ces dossiers dressent la synthèse des informations collectées pour une commune donnée. Ils ne sont pas systématiquement tenus			

ANNEXE 13 : LETTRE DU PRÉFET DE POLICE DE PARIS SUR LA MISE EN CONFORMITÉ DES FICHIERS



Paris, le 23 DEC. 2008

08 0 4 8 8 3 7

Le Préfet de Police

à

Madame le Ministre de l'Intérieur, de l'Outre mer et des Collectivités Territoriales

Objet : Mise en conformité des fichiers mis en œuvre par la Préfecture de Police.

Au lendemain de la remise du rapport du groupe de contrôle des fichiers de police et de gendarmerie présidé par M. Alain BAUER et suite à vos instructions, je souhaite vous rendre compte des travaux engagés par la Préfecture de Police pour mettre en conformité tous les traitements de données à caractère personnel qu'elle utilise.

Ne relèvent pas, dès lors, de cette réflexion spécifique les applications nationales que les services de la Préfecture de Police utilisent, en particulier celles accessibles par le système de circulation hiérarchisée des enregistrements opérationnels de la police sécurisés (CHEOPS), ainsi que les fichiers automatisés relatifs aux empreintes digitales (FAED) et génétiques (FNAEG) ou aux interdits de stade (FNIS).

1. RECENSEMENT DES FICHIERS EXISTANTS

Un inventaire exhaustif de l'ensemble des traitements administratifs et de police a tout d'abord été réalisé. Sur les 150 fichiers ainsi recensés, une grande majorité concourt à la gestion administrative des services et peuvent dès lors être aisément regroupés dans des catégories génériques.

Un travail en ce sens a donc été entrepris, qui devrait aboutir à des déclarations regroupées et, en raison de leur faible sensibilité, simplifiées.

Une autre grande catégorie concerne des traitements qui, développés et exploités localement, contribuent à des missions exercées sur l'ensemble du territoire, répondent à des finalités identiques, portent sur des catégories de données équivalentes et ont les mêmes destinataires.

REPUBLIQUE FRANÇAISE

Liberté Egalité Fraternité

PRÉFECTURE DE POLICE

9, Boulevard du Palais - 75195 PARIS RP - Tél. : 01 53 71 53 71 / 01 53 73 53 73

Facilitez vos démarches administratives - Avant de vous déplacer, téléphonez au : 08 36 67 22 22 (1,99 F la minute)

.../...

Il s'agit, par exemple, des fichiers liés à l'activité judiciaire des services comme ceux relatifs au contrôle judiciaire, aux assignations à résidence, aux mises sous écrou ou les registres de garde à vue, ou relevant de la police administrative, comme les traitements mis en œuvre au titre de la police des étrangers ou bien encore relatifs aux objets trouvés ou aux fourrières.

L'objectif est de créer, pour chaque grand domaine d'activité des services, une application nationale, afin de donner un cadre juridique approprié pour la mise en œuvre locale des traitements similaires.

Cette solution est rendue possible par les articles 23 (II) et 26 (IV) de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, qui permettent des déclarations et des autorisations uniques pour les traitements qui poursuivent des finalités identiques.

Une démarche en ce sens sera entreprise avec la DGPN, dans le cadre des travaux engagés sous l'égide de la DLPJ de mise en conformité des fichiers du ministère avec les dispositions de la loi du 6 janvier 1978 précitée dans leur rédaction issue de la loi n° 2004-801 du 6 août 2004.

2. FICHIERS A DECLARER AUPRES DE LA CNIL

Un autre chantier concerne la déclaration des applications annoncées lors des travaux du groupe de contrôle présidé par M. Alain BAUER et, au premier chef, le traitement GESTEREXT (Gestion du terrorisme et des extrémismes violents).

Créé au profit de la Direction du renseignement de la Préfecture de Police (DRPP), ce traitement comportera des données relatives aux missions de ce service relevant du domaine du renseignement intérieur, qui sont couvertes par le secret de la défense nationale. A ce titre, GESTEREXT doit, à l'instar du traitement CRISTINA de la DCRI, bénéficier du niveau protection accordé par la loi aux fichiers dits de « souveraineté » et, notamment, de la procédure de déclaration simplifiée ainsi que celle de dispense de publication et du contrôle sur place de la CNIL.

En ce qui concerne l'autre grand fichier de la DRPP, le module applicatif GEVI (Gestion des violences urbaines), il constitue le traitement utilisé par les fonctionnaires de la direction chargés du suivi des phénomènes urbains violents. Dès lors, s'inscrivant dans la mission d'information générale de la DRPP, GEVI constituera l'un des fichiers autorisés par le décret portant création de l'application EDVIRSP.

.../...

Un autre outil particulièrement utile aux services qui l'utilisent est l'application CORAIL (Cellule opérationnelle de rapprochement et d'analyse des infractions liées).

Conçu par la Direction de la police judiciaire (DPJ) de Paris, CORAIL, qui doit faire l'objet d'une procédure de déclaration auprès de la CNIL, a pour objet de diffuser aux services d'enquête les fiches relatives à des faits sériels, sous la forme d'états opérationnels triés par infractions, dans le but de faciliter les rapprochements et de permettre l'élaboration de synthèses susceptibles d'être imputées à des récidivistes notoires ayant commis des infractions graves : crime ou délit portant atteinte aux personnes punis de plus de cinq ans d'emprisonnement ou aux biens et punis de plus de sept ans d'emprisonnement.

D'autres fichiers opérationnels feront également l'objet d'une procédure de déclaration au cours de l'année 2009 et notamment les traitements :

- OCTOPUS (Outil de centralisation et de traitement opérationnel des procédures et des utilisateurs de signatures) qui, utilisé dans la lutte contre les tags sauvages, permet le recoupement, la synthèse de faits et l'identification des auteurs de ce type de dégradation ;

- LUPIN (Logiciel d'uniformisation des prélèvements et des identifications) qui, utilisé dans la lutte contre les cambriolages, permet l'inscription des données constatées sur les scènes d'infractions, afin d'effectuer des rapprochements.

3. CLASSEMENT DEFINITIF ET ARCHIVAGE DU FICHER MANUEL DES RENSEIGNEMENTS GENERAUX

Le chantier sur lequel j'ai souhaité porter une attention toute particulière est celui de l'ancien fichier manuel des renseignements généraux.

Dénommé « Archives Centrales », le fichier, qui n'est plus alimenté depuis 2001, comprend 3,5 millions de fiches cartonnées environ, réparties en trois groupes : un fichier des personnes physiques, un autre sur les personnes morales (sociétés, associations, syndicats) et le troisième sur les journaux et revues. Les fiches sont classées selon la méthode de Bertillon dite du classement phonétique.

En outre, les « Archives Centrales » détiennent 787 129 dossiers, subdivisés en dossiers individuels, de principe et de synthèse :

- les dossiers individuels se rapportent à des personnes physiques ou morales,
- les dossiers de principe sont essentiellement composés de synthèses relatives à des problèmes d'ordre général,

.../...

- les dossiers de synthèse regroupent des notices individuelles résultant d'une enquête.

Si, avec l'abandon des missions de la direction dans le domaine des activités politiques, économiques et sociales et la création de traitements automatisés performants, les « Archives Centrales » ne sont plus alimentées depuis 2001, elles pouvaient encore être consultées.

Seuls y avaient accès certains fonctionnaires de la direction habilités à cet effet, ainsi qu'à quelques fonctionnaires, spécialement autorisés par le Préfet de Police, de la DCRI, du CEA, de la DGSE (20), de la DPSD (11), de l'UCLAT et de la brigade criminelle de la DPJ de Paris (2).

A compter du début du mois de janvier prochain, je soustrairai ce fonds à la gestion de la direction du renseignement pour le placer sous statut d'archives, qui dès lors ne seront consultables que par dérogation spéciale délivrée par une autorité hiérarchique de rang élevé, selon une procédure garantissant une traçabilité exhaustive.

Au regard de son volume, j'ai fixé aux services un délai de trois ans pour procéder méthodiquement au reversement définitif de ce fonds documentaire important au service des archives historiques de la Préfecture de Police, en vertu des règles applicables à la Préfecture de Police.

L'opération consistera à séparer les documents dépourvus d'intérêt administratif ou historique et destinés à la destruction de ceux qui présentent ces caractères et doivent être conservés, en vertu de la loi sur les archives nationales. Vos instructions visant à attendre les conclusions de la mission nationale d'appui que vous avez confiée la directrice des Archives de France avant de procéder à toute destruction seront respectées.

Afin de conduire cette opération, j'ai décidé de désigner un comité de pilotage et d'affecter exclusivement à cette tâche sept fonctionnaires de police, trois en service et quatre réservistes. Le comité de pilotage se mettra en relation avec la mission nationale d'appui.

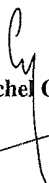
* *
*

Tels sont les principaux chantiers que la Préfecture de Police a ouvert pour mettre en conformité ses fichiers conformément à vos instructions.

Soyez assurée que ces efforts se poursuivront, en particulier pour mettre en œuvre les recommandations que vous aurez retenues du rapport de M. Alain BAUER.

.../...

Je demeure à votre disposition pour toutes autres précisions que vous souhaiteriez obtenir sur ce sujet de préoccupation prioritaire.


Michel GAUDIN

ANNEXE 14 : RÉPONSES AU QUESTIONNAIRE DES RAPPORTEURS SUR LES FICHIERS DE LA PRÉFECTURE DE POLICE DE PARIS

CORAIL (Cellule opérationnelle de rapprochements et d'analyse des infractions liées)

Date de création

En phase d'expérimentation

Base juridique

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

Article 21-1 de la loi du 18 mars 2003 pour la sécurité intérieure

Article D. 3 du code de procédure pénale

Objet du fichier

Le fichier dénommé « Cellule opérationnelle de rapprochements et d'analyse des infractions liées » a pour objet de diffuser aux services d'enquête les fiches relatives à des faits sériels, sous la forme d'états opérationnels triés par infractions, dans le but de faciliter les rapprochements et permettre l'élaboration de synthèses susceptibles d'être imputées à des récidivistes notoires ayant commis des infractions graves visées à l'article 21-1 de la loi du 18 mars 2003 pour la sécurité intérieure : crime ou délit portant atteinte aux personnes punis de plus de cinq ans d'emprisonnement ou portant atteinte aux biens et punis de plus de sept ans d'emprisonnement.

L'application permet à une cellule régionale multi directionnelle de mutualiser les renseignements relatifs à la délinquance et à la criminalité, susceptibles d'être exploités à des fins de rapprochements par les unités d'investigations de l'une ou l'autre des directions.

Type de fichier

Traitement automatisé

Service gestionnaire du fichier

État-major de la DRPJ, 36 Quai des Orfèvres PARIS 1^{er}

Nature des informations enregistrées

Les informations enregistrées et diffusées sont :

- les données issues des télégrammes d'information diffusés par le RESCOM (signalement des faits commis ou élucidés) ;

- les données issues des mains courantes d'informations ;
- les données d'affaires ou de synthèse correspondant à un résumé des faits ou de la procédure (dates, lieux, nombre d'auteurs, résumé de l'affaire, référence, service saisi, etc.) ;
- des données photographiques (photographie de suspect, portrait-robot, photographie d'objet) ;
- les données de garde à vue (identité de la personne, nature de l'infraction, nom de l'OPJ, etc.).

Ces données se présentent sous forme de fiches se rapportant à des faits, sous formes d'états opérationnels regroupant des faits de même nature ou commis dans la même zone géographique, ou encore sous forme de synthèses opérationnelles rassemblant des faits présentant des similitudes de mode opératoire.

Le nombre annuel de fiches se limite à environ 4500 pour la DPJ de Paris (faits sériels graves), variable en fonction de l'évolution du volume des infractions. Le nombre de synthèses annuelles varie entre 50 et 60. Le nombre de circulaires régionales de recherche pour identification est estimé entre 150 et 300.

Modalités de consultation et destinataires des informations

Les agents et officiers de police judiciaire individuellement désignés et spécialement habilités spécialement habilités des services de police judiciaire situés dans le ressort des DRPJ de Paris et de Versailles sont seuls autorisés à accéder aux informations.

Les fonctionnaires habilités ouvrent une session avec mot de passe. Des profils d'habilitation définissent pour chaque utilisateur les fonctions autorisées ou les catégories d'informations accessibles. Les données de connexion sont enregistrées dans un historique. Toutes les actions sur l'application sont tracées à la seconde.

- Date et heure de connexion.
- Identifiant de l'utilisateur.
- Référence des données du fichier auquel il a été accédé. (document, fiche, état, synthèse)
- Type de l'action effectuée. (Création, modification, mise à jour, lecture)

Modalités d'exercice du droit d'accès aux informations

Le fichier est soumis au droit d'accès et de rectification garanti à chaque citoyen par les articles 39 à 41 de la loi de 1978.

Concrètement, dès réception d'une demande de droit d'accès, l'application permet d'imprimer sous la forme d'une lettre type, une copie claire, référencée de l'ensemble des données concernant le requérant.

Si la recherche nominative est négative, l'application permet l'impression immédiate d'une lettre type, référencée qui précisera les dates, heure, étendue et domaine de la recherche.

Les droits d'accès concernent également les personnes morales, pour lesquelles, les requérants, en plus de la photocopie d'une pièce d'identité, devront produire un extrait Kbis.

Durée de conservation

— Les fiches et les états opérationnels sont conservés pour une durée maximum de trois ans à compter des faits. Pour les synthèses, les données sont conservées trois ans à compter de la date du fait le plus récent.

— Les synthèses élucidées concernant des faits, crimes ou délits « imputés aux personnes mises en cause dans des affaires similaires » (récidivistes) sont conservées jusqu'au terme de la période incluant la possibilité d'une « récidive légale » de l'auteur condamné.

— Les circulaires régionales de recherche pour identification sont conservées cinq ans.

— Conformément à l'article 8 de la « Charte d'accueil et droits des victimes », il est immédiatement donné droit aux demandes des victimes d'effacer leurs coordonnées dans les fiches lorsque l'auteur des faits a été définitivement condamné.

Procédures d'apurement :

L'apurement des données est automatisé, à l'exception des synthèses imputées à des malfaiteurs identifiés, qui sont supprimées manuellement au terme de la période de récidive légale de l'auteur condamné.

États des procédures de déclaration auprès de la CNIL

CORAIL, actuellement en phase d'expérimentation au sein des DRPJ de Paris et de Versailles, sera généralisé en 2009 à l'ensemble de services territoriaux d'investigations de police judiciaire et de sécurité publique. Le dossier de déclaration du traitement à la CNIL est actuellement en cours d'élaboration.

LUPIN (Logiciel d'uniformisation des prélèvements et des identifications)
--

Date de création

Décembre 2008

Base juridique

- Code pénal, notamment ses articles 311-1 et suivants ;
- Code de procédure pénale, notamment son article R. 15-20 ;
- Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 26 ;
- Loi n° 2003-239 du 18 mars 2003 modifiée pour la sécurité intérieure ;
- Arrêté du 6 juin 2006 modifié portant règlement général d'emploi de la police nationale, notamment son article 2121-7 ;

Objet du fichier

Le fichier dénommé « Logiciel d'uniformisation des prélèvements et des identifications » a pour objet de faciliter la répression des vols par l'enregistrement des données constatées et prélevées par les fonctionnaires des antennes locales de police technique sur les scènes où ces délits ont été commis, afin de permettre l'identification des auteurs notamment grâce à l'établissement de liens entre les individus, les événements ou les infractions pouvant mettre en évidence un caractère sériel.

Il pourra également être utilisé pour faciliter la répression des autres délits présentant un caractère sériel et passibles d'au moins trois ans d'emprisonnement.

Type de fichier

Traitement informatisé

Service gestionnaire du fichier

Service d'investigation transversale de la direction de la police urbaine de proximité (DPUP) de la préfecture de police.

Nature des informations enregistrées

Identité de la victime (nom, prénom, sexe, date de naissance, profession, nationalité, numéro de téléphone, mël, adresse) ;

Véhicule de la victime s'il est le lieu de l'infraction (marque, modèle, numéro d'immatriculation).

Identité de l'auteur de l'infraction (nom, prénom, date de naissance, données papillaires ou génétiques)

Date et contenu de la première identification de l'auteur de l'infraction ;

Identité des deux premiers fonctionnaires intervenant sur le lieu d'une infraction (nom)

Identité de la personne effectuant la saisie (numéro de matricule, contenu de la connexion)

Modalités de consultation et destinataires des informations

Les fonctionnaires des antennes locales de police technique ainsi que les officiers et agents de police judiciaire des services d'enquête de la DPUP individuellement désignés et spécialement habilités par le préfet de police sont, dans la limite du besoin d'en connaître, autorisés à accéder aux informations.

Peuvent être destinataires des données contenues dans l'application, dans la limite du besoin d'en connaître, les officiers et agents de police judiciaire des autres services de la police et de la gendarmerie nationales, individuellement désignés et spécialement habilités pour les recherches relatives aux infractions relevant du traitement.

Toutes les actions sur l'application sont tracées. Le fichier est interconnecté avec aucun autre fichier.

Modalités d'exercice du droit d'accès aux informations

Le fichier est soumis au droit d'accès et de rectification garanti à chaque citoyen par les articles 39 à 41 de la loi de 1978. Ce droit s'exerce, comme pour presque tous les fichiers de police, par l'intermédiaire de la CNIL. Concrètement, un document est remis aux victimes les informant de leurs droits. Les fonctionnaires effectuant la saisie et les fonctionnaires intervenant sont avisés oralement.

Durée de conservation

Durée proposée : 5 ans

Procédures d'apurement

Les données contenues dans le fichier seront détruites automatiquement à l'issue du délai de conservation.

États des procédures de déclaration auprès de la CNIL

En cours de déclaration

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

Date de création

2008

Base juridique

- code pénal notamment l'article 322-1 ;
- code de procédure pénale, notamment son article R. 15-30 ;
- loi n° 2003-239 du 18 mars 2003 modifiée pour la sécurité intérieure, notamment son article 21 ;
- décret n° 2003-932 du 1 octobre 2003 portant création d'un service de police déconcentré chargé de la sécurité des personnes et des biens sur les réseaux de transport en commun de voyageurs par voie ferrée de la région d'Île-de-France et modifiant le code de procédure pénale (partie réglementaire : Décrets en Conseil d'État) ;
- arrêté du 6 juin 2006 modifié portant règlement général d'emploi de la police nationale, notamment son article 2123-1.

Objet du fichier

Le fichier dénommé « outil de centralisation et de traitement opérationnel des procédures et des utilisateurs de signatures » a pour objet de faciliter la prévention et la répression des inscriptions, signes ou dessins tracés, sans autorisation préalable, sur les façades, les véhicules, les voies publiques ou le mobilier urbain.

Type de fichier

Traitement automatisé

Service gestionnaire du fichier

Brigade des réseaux ferrés de la sous-direction de la police régionale des transports de la direction police urbaine de proximité.

Nature des informations enregistrées

- informations ayant trait à l'état civil et à la profession ;
- adresses physiques, numéros de téléphone et adresses électroniques ;
- signalement et photographies ;

- titres d'identité ;
- déplacements dans les réseaux de transport et antécédents judiciaires ;
- motif de l'enregistrement des données ;
- données relatives à l'environnement de l'individu, notamment aux personnes entretenant ou ayant entretenu des relations directes et non fortuites avec lui.

Sont également enregistrées les informations non nominatives qui concernent les faits répondant à l'objet du fichier, les lieux, dates de l'infraction et modes opératoires ainsi que les informations et images relatives aux objets, y compris celles qui sont indirectement nominatives.

Modalités de consultation et destinataires des informations

Les agents et officiers de police judiciaire de la Brigade des réseaux ferrés de la sous-direction de la police régionale des transports individuellement désignés et spécialement habilités par le préfet de police sont autorisés à accéder aux informations.

Peuvent également être destinataires de ces données, dans la limite du besoin d'en connaître, les agents et officiers de police judiciaire des autres services de la police et de la gendarmerie nationales, individuellement désignés et spécialement habilités pour les recherches relatives aux infractions commises en matière de tag, ainsi que les magistrats du parquet et de l'instruction.

Toutes les actions sur l'application sont tracées. Le fichier est interconnecté avec aucun autre fichier.

Modalités d'exercice du droit d'accès aux informations

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

Durée de conservation

Durée proposée : 10 ans

Procédures d'apurement

Les données contenues dans le fichier seront détruites automatiquement à l'issue du délai de conservation.

États des procédures de déclaration auprès de la CNIL

En cours de déclaration

GEVI (Gestion des violences urbaines)

Date de création

1996

Base juridique

Décret n° 91-1051 du 14 octobre 1991 relatif aux fichiers gérés par les services des renseignements généraux

Projet de décret portant création de l'application concernant l'exploitation documentaire et la valorisation de l'information relative à la sécurité publique (EDVIRSP).

Objet du fichier

Conçu en 1996, l'application dénommée « gestion des violences urbaines » a pour fondement juridique le décret n° 91-1051 du 14 octobre 1991 relatif aux fichiers gérés par les services des renseignements généraux. Sa conformité avec ce texte a été reconnue par la CNIL le 19 novembre 1996.

Il constituera l'un des fichiers autorisés par le décret portant création de l'application concernant l'exploitation documentaire et la valorisation de l'information relative à la sécurité publique (EDVIRSP) actuellement en cours d'adoption.

GEVI constitue un traitement automatisé comprenant des données sur des individus majeurs ou des personnes morales susceptibles d'être impliqués dans des actions de violences urbaines ou de violences sur les terrains de sport pouvant porter atteinte à l'ordre public et aux institutions.

Son mode d'exploitation permet, à partir de recherches élémentaires (un ou plusieurs champs), d'effectuer des rapprochements et d'établir des liens entre des individus, des groupes, des événements et des faits.

Conformément au décret du 14 octobre 1991, aucun mineur n'était jusqu'ici enregistré dans le fichier ce qui constitue un lourd handicap pour l'efficacité de l'outil, un grand nombre d'acteurs de violences urbaines ne pouvant ainsi pas être pris en compte. Dès que le cadre juridique relatif à EDVIRSP aura été déterminé, des mineurs pourront faire l'objet d'une instruction, dans le respect des conditions restrictives décidées par le ministre.

Type de fichier

Traitement informatisé

Service gestionnaire du fichier

Pôle phénomènes urbains violents de la DRPP

Nature des informations enregistrées

Les données suivantes sont enregistrées :

Personnes physiques : état civil, surnoms, signalement, véhicules, relations, adresse, activités professionnelles et autres documents.

Personnes morales : enregistrement (sociétés ou associations), sièges sociaux, établissements secondaires, bureaux, dirigeants, activités.

Modalités de consultation et destinataires des informations

Le fichier, qui n'est interconnecté avec aucune autre application, est exclusivement alimenté par les fonctionnaires chargés du suivi des phénomènes urbains violents et spécialement habilités par le préfet de police. Ils sont d'ailleurs les seuls à pouvoir le consulter. À l'avenir, les fonctionnaires spécialement habilités des services départementaux d'information générale de la région d'Ile-de-France pourraient éventuellement contribuer à l'alimentation et consulter l'application au titre des missions d'animation et de coordination de la DRPP dans ce domaine.

Dans la pratique, pour pouvoir alimenter ou consulter la base, les fonctionnaires doivent s'identifier à l'aide de leur matricule et d'un mot de passe, qui leur a été attribué à l'issue de leur habilitation.

En ce qui concerne la traçabilité, un journal des actions enregistre les consultations, les créations, les modifications ainsi que les suppressions de fiches.

Modalités d'exercice du droit d'accès aux informations :

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

Durée de conservation :

GEVI étant un fichier de renseignement, aucune durée de conservation fixe n'est prévue. Les données ne sont conservées qu'en fonction des finalités (très strictement délimitées) du fichier et donc, pour l'essentiel, de l'intérêt qu'elles présentent au regard des phénomènes urbains violents.

La règle applicable est donc le principe général énoncé par l'article 6 de la loi n° 78-17 du 6 janvier 1978 : une donnée ne peut être conservée que pour autant qu'elle réponde à la finalité pour laquelle elle a été collectée et traitée.

Procédures d'apurement :

Sera fixé par le décret EDVIRSP.

États des procédures de déclaration auprès de la CNIL

En attente de la parution du décret EDVIRSP.

GESTEREXT (Gestion du terrorisme et des extrémismes à potentialité violente)

Date de création

En cours de création (GESTEREXT remplacera l'application GESTER, créée en 1996)

Base juridique

- code pénal, notamment son article 413-9 ;
- article 26 (I à III) de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique aux fichiers et aux libertés ;
- décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifié par le décret n° 2007-451 du 25 mars 2007 notamment son article 16 ;
- décret n° 2007-914 du 15 mai 2007 modifié pris pour l'application du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;
- décret n° 2008-609 du 27 juin 2008 relatif aux missions et à l'organisation de la direction centrale du renseignement intérieur, notamment le dernier alinéa de l'article 2 ;
- arrêté du 27 juin 2008 relatif à la direction du renseignement de la préfecture de police et modifiant l'arrêté du 6 juin 2006 portant règlement général d'emploi de la police nationale.

Objet du fichier :

La réforme du renseignement intérieur intervenue le 1^{er} juillet 2008 a conduit à une nouvelle organisation dans ce domaine, formalisée par le décret n° 2008-609 du 27 juin 2008 relatif aux missions et à l'organisation de la direction centrale du renseignement intérieur (DCRI).

Le dernier alinéa de l'article 2 de ce texte dispose que « le service chargé, sous l'autorité du préfet de police, de missions de renseignement intérieur concourt à l'activité de la direction centrale du renseignement intérieur ».

Sur ce fondement, Mme le ministre de l'Intérieur, de l'outre-mer et des collectivités territoriales a chargé, par un arrêté en date du 27 juin 2008 pris sur proposition du préfet de police et publié au *Journal officiel* de la République française du 1^{er} juillet 2008, la direction du renseignement de la préfecture de police (DRPP) de missions de renseignement intérieur, en en fixant le contenu ainsi que les conditions dans lesquelles elles doivent s'exercer.

Le traitement dénommé GSTEREXT constituera un outil à la disposition des fonctionnaires de la DRPP chargés d'exercer les missions de renseignement intérieur confiées à ce service à l'instar du traitement dénommé CRISTINA pour les fonctionnaires de la direction centrale du renseignement intérieur (DCRI). A ce titre, il enregistra des données sur des personnes et des faits relatifs au terrorisme ainsi qu'à des mouvements subversifs violents et phénomènes de société précurseurs de menaces pour la sécurité nationale.

Ces données, ainsi que le traitement lui-même, sont couverts par le secret de la défense nationale.

Type de fichier

Traitement informatisé

Service gestionnaire du fichier :

Service chargé de la lutte contre le terrorisme et les extrémismes à potentialité violente de la Direction du renseignement de la préfecture de police.

Nature des informations enregistrées :

Les informations enregistrées permettent de répondre aux finalités fixées à GSTEREXT.

GSTEREXT est soumis au régime juridique des fichiers dits « de souveraineté », défini par l'article 26 (III) de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. L'acte réglementaire est donc dispensé de publication.

De plus, GSTEREXT poursuit une finalité intéressant la sûreté de l'État et la sécurité nationale. En vertu du dernier alinéa du I de l'article 30 de la loi du 6 janvier 1978, l'acte réglementaire peut bénéficier d'une déclaration simplifiée telle qu'elle est définie par l'article 16 du décret 2005-1309 du 20 octobre 2005.

Modalités de consultation et destinataires des informations

Les fonctionnaires du service chargé de la lutte contre le terrorisme et les extrémismes à potentialité violente de la DRPP habilités par le préfet de police seront seuls autorisés, dans la limite du besoin d'en connaître, à accéder aux informations contenues dans le traitement.

Toutefois, la DRPP concourant à l'activité de la DCRI pour la prévention des actes de terrorisme et des extrémismes à potentialité violente, les fonctionnaires de la DCRI

intervenant dans ces domaines pourront être rendus destinataires des informations contenues dans GESTEREXT, dans la limite du besoin d'en connaître.

Modalités d'exercice du droit d'accès aux informations :

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

Durée de conservation :

GESTEREXT étant un fichier de renseignement, aucune durée de conservation fixe n'est prévue. Les données ne sont conservées qu'en fonction des finalités (très strictement délimitées) du fichier et donc, pour l'essentiel, de l'intérêt qu'elles présentent au regard de la sûreté de l'État et la sécurité nationale

Procédures d'apurement :

L'apurement est assuré par le service informatique de la DRPP s'il y a lieu.

États des procédures de déclaration auprès de la CNIL

En cours de déclaration auprès de la CNIL.

GESI (Gestion des étrangers en situation irrégulière)
--

Date de création

En cours de création

Base juridique

Code pénal

Code de procédure pénale

Code de l'entrée et du séjour des étrangers et du droit d'asile

Loi n° 2003-239 du 18 mars 2003 modifiée pour la sécurité intérieure

Décret du 29 mars 1993 portant création d'un système informatisé de gestion des dossiers des ressortissants étrangers en France (AGDREF)

Arrêté du 6 juin 2006 modifié portant règlement général d'emploi de la police nationale, notamment son article 2121-9

Objet du fichier :

L'application dénommée « Gestion des étrangers en situation irrégulière » a pour objet d'assurer une gestion des dossiers en temps réel, de l'interpellation jusqu'à la reconduite, des étrangers en situation irrégulière interpellés par les services de la préfecture de police.

Le traitement administratif et judiciaire des étrangers en situation irrégulière concerne en effet plusieurs services de la préfecture de police : sous-direction chargée de la lutte contre l'immigration irrégulière et le travail illégal des étrangers de la direction du renseignement (DRPP), services territoriaux de la direction de la police urbaine de proximité (DPUP), 8^{ème} Bureau de la direction de la police générale, service en charge des escortes et de la rétention de la direction de l'ordre public et de la circulation.

L'ensemble des données transmises par les différents intervenants est centralisé au niveau du pôle de compétence, service dépendant de la DRPP, chargé de la coordination du dispositif de traitement des dossiers.

Le pôle de compétence alimente le fichier dans le but de mémoriser l'identité des mis en cause, d'assurer le suivi de leur dossier administratif et judiciaire et de fournir des données statistiques.

Type de fichier

Traitement informatisé

Service gestionnaire du fichier :

Sous-direction chargée de la lutte contre l'immigration irrégulière et le travail illégal des étrangers de la direction du renseignement de la préfecture de police.

Nature des informations enregistrées :

- Nom, prénom, date et lieu de naissance, nationalité, sexe.
- Numéro de dossier étranger ; numéro du dossier AGDREF (gestion informatisée des dossiers de ressortissants étrangers en France).
- Domicile d'assignation à résidence.
- Coordonnées du vol de retour du reconduit.
- Service interpellateur.
- Nature de l'infraction ayant motivé l'interpellation ; passage au fichier des personnes recherchées ; passage au fichier de l'identité judiciaire ; décision du parquet ; décision administrative relative à la reconduite à la frontière, l'expulsion et au placement en rétention ; décision du juge des libertés et de la détention ; recours ; mise en exécution d'une décision judiciaire d'interdiction du territoire ; contentieux administratif.

Modalités de consultation et destinataires des informations

Seront autorisés à accéder aux données contenues dans GESI, les officiers et agents de police judiciaire concourant à la lutte contre l'immigration irrégulière et le travail illégal des étrangers de la DRPP, de la DPUP et de la DOPC, ainsi que les agents du 8^{ème} Bureau de la direction de la police générale individuellement désignés et spécialement habilités par le préfet de police.

Toutes les actions sur l'application seront tracées.

Le fichier sera interconnecté avec aucun autre fichier.

Modalités d'exercice du droit d'accès aux informations :

Le fichier est soumis au droit d'accès et de rectification garanti à chaque citoyen par les articles 39 à 41 de la loi de 1978. Concrètement la personne est avisée oralement de sa présence dans le traitement et peut accéder aux données le concernant par simple

demande formulée auprès de la sous-direction chargée de la lutte contre l'immigration irrégulière et le travail illégal des étrangers.

Durée de conservation :

Durée proposée : 2 ans

Procédures d'épurement :

Effacement des données à caractère personnel au bout de 2 ans.

Conservation des données statistiques.

États des procédures de déclaration auprès de la CNIL :

En cours de déclaration.

ANNEXE 15 : ARRÊTÉ DU PRÉFET DE POLICE DE PARIS RELATIF À L'ARCHIVAGE DU FICHIER MANUEL DES RENSEIGNEMENTS GÉNÉRAUX



Arrêté n° 2009-00038

relatif au versement au service des archives et du musée des données contenues
dans un fichier de la direction du renseignement régi par le décret n° 91-1051
du 14 octobre 1991

Le préfet de police,

Vu le code du patrimoine, notamment ses articles L. 212-3 et L. 212-4 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux
fichiers et aux libertés ;

Vu le décret n° 68-15 du 5 janvier 1968 relatif aux archives de la préfecture de
police ;

Vu le décret n° 91-1051 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 modifié par le
décret n° 2008-631 du 27 juin 2008 ;

Vu l'arrêté n° 2008-00427 du 26 juin 2008 relatif à l'organisation de la préfecture
de police ;

Vu la lettre circulaire NOR : INT/K/08/30129/5 du 18 décembre 2008 du ministre de
l'intérieur, de l'outre-mer et des collectivités territoriales relative à la mission
« archives des renseignements généraux » ;

Sur proposition du préfet, directeur du cabinet ;

Arrête :

Art. 1^{er}. - Les données contenues dans le fichier de la direction du renseignement
dénommé « Archives Centrales » et régi par le décret du 14 octobre 1991 susvisé
sont versées en dépôt au service des archives et du musée en vue de les soumettre
aux opérations organisées par les articles L. 212-3 et L. 212-4 du code du patrimoine.
.../...

REPUBLIQUE FRANÇAISE
Liberté Egalité Fraternité

A ce titre, les locaux contenant les données mentionnées à l'alinéa précédent sont affectés au service des archives et du musée.

Art. 2. - Pendant une période de trois ans à compter de la date d'entrée en vigueur du présent arrêté, les demandes de consultation des données mentionnées à l'article 1^{er} sont autorisées après avis conforme du directeur du renseignement.

Durant cette période, les fonctionnaires et réservistes de la direction du renseignement chargés de procéder aux opérations mentionnées à l'article 1^{er} sont mis à disposition du service des archives et du musée.

Art. 3. - Le directeur du renseignement et le chef du service des archives et du musée sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté qui sera publié au recueil des actes administratifs de la préfecture de police.

Fait à Paris, le 14 JAN. 2009

Le Préfet de Police



Michel GAUDIN