Collection des rapports officiels

Rapport au ministre de l'Intérieur, de l'Outre-Mer, des Collectivités territoriales et de l'Immigration

Fichiers de police et de gendarmerie en France

Une nouvelle étape vers une nécessaire transparence

RAPPORT D'ACTIVITÉ 2009-2011 DU GROUPE DE TRAVAIL SUR L'AMÉLIORATION DU CONTRÔLE ET DE L'ORGANISATION DES FICHIERS DE POLICE ET DE GENDARMERIE

ALAIN BAUER
PRÉSIDENT DU GROUPE DE TRAVAIL

CHRISTOPHE SOULLEZ
RAPPORTEUR

Rapports officiels

Rapport au ministre de l'Intérieur

ISBN 978-2-11-008847-5
DF : 5RO28570
www.ladocumentationfrancaise.fr
Paris, 2011

Photos de couverture :
Premier ministre
service de la photographie
Diffuseur :
La Documentation française
Sculpteur : Marielle Polska
et photo goodshoot

Sommaire

Avant-propos

Il y a maintenant plus de cinq ans, dans un souci de transparence et d'ouverture, le groupe de travail sur les fichiers de police et de gendarmerie était mis en place par Nicolas Sarkozy, alors ministre d'État, ministre de l'Intérieur et de l'Aménagement du territoire.

Depuis 2006, les membres du groupe de travail se sont régulièrement réunis afin d'échanger et de débattre, parfois sur l'utilité des fichiers de police et de gendarmerie – dont chacun pour autant s'accorde à reconnaître l'intérêt dans la prévention et la lutte contre la criminalité – mais essentiellement sur les conditions de mise en œuvre de ceux-ci.

Les débats ont été riches et occasionnellement animés. Mais le dialogue qui s'est instauré entre l'administration et les représentants de la société civile, et notamment les associations, a démontré qu'il était possible de progresser sur des sujets sensibles sans que cela ne se termine systématiquement en polémiques, parfois stériles.

La démarche du groupe de travail vient en complément, et non en concurrence, des missions légales dévolues à la Commission nationale de l'informatique et des libertés. Le groupe a d'ailleurs eu le plaisir de constater des échanges utiles avec l'Autorité indépendante selon le principe signalé par celle-ci de rôle « d'audit externe ». Le groupe se veut proactif. Il s'agit avant tout de permettre au ministre de l'Intérieur de présenter ses projets de création de traitements de données, d'en expliquer les finalités et l'intérêt, et de pouvoir les amender à partir des recommandations des membres du groupe.

C'est notamment la démarche qui a prévalu à l'occasion des débats sur le projet de loi de sécurité et de performance de la sécurité intérieure et sur les modalités de mise en œuvre des traitements sériels.

Mais il s'agit également, pour le ministère de l'Intérieur, de faire œuvre de transparence. Ainsi, depuis 2006, un important travail de recensement des fichiers a été réalisé. Il a permis de découvrir de nouveaux traitements et surtout d'être à l'origine d'une vaste procédure de régularisation des traitements utilisés dans les services de police et les unités de gendarmerie.

Les travaux du groupe, mais également ceux de la mission parlementaire Batho-Bénisti, les travaux de la CNIL ou du Médiateur de

la République, ainsi que l'engagement des deux directions générales de la police et de la gendarmerie et de la préfecture de police, ont amorcé un cercle vertueux contribuant à la création et au maintien d'un juste équilibre entre respect des libertés publiques et nécessité d'amélioration des outils à disposition des services de police et des unités de gendarmerie pour lutter contre la criminalité et protéger les victimes.

Le rapport d'activités 2009/2011 démontre que les réflexions du groupe ont été nombreuses et que, dans le même temps, le ministère de l'Intérieur a pris en compte une grande partie des recommandations émises.

À titre personnel, je tiens à remercier le ministre de l'Intérieur, les directions générales de la police et de la gendarmerie nationales, la direction des libertés publiques et des affaires juridiques, la préfecture de police, la direction des affaires criminelles et des grâces et l'ensemble des membres du groupe de contrôle pour leur participation, leur contribution et leur ouverture au dialogue.

Le 15 juin 2011, le directeur de cabinet du ministre de l'Intérieur indiquait au président du groupe de contrôle les éléments suivants :

«*À la suite de vos dernières interventions concernant le maintien de la mention « origines géographiques » dans le décret GIPASP, faisant suite à vos préoccupations exprimées dès 2009 pour le décret PASP, il me paraît utile de vous préciser que le ministère de l'Intérieur, de l'Outre-mer, des Collectivités territoriales et de l'Immigration confirme totalement les termes de la circulaire adressée aux préfets le 18 octobre 2009 [...] Il m'apparaît néanmoins que ce dispositif, qui avait permis de lever certaines de vos préoccupations, doit faire l'objet d'une correction afin d'éviter toute interprétation contraire à la volonté de l'exécutif et aux interprétations des juridictions et autorités administratives constitutionnelles.*

Aussi, ai-je le plaisir de vous informer que j'ai demandé à mes services d'entamer les procédures visant à la modification des décrets PASP et GIPASP afin de sortir la mention « origines géographiques » des données sensibles et de ne permettre que l'enregistrement de données factuelles strictement limitées à l'origine géographique, au lieu de naissance, à la nationalité ou à la dénomination commune de la bande selon ses propres critères».

Réuni le 12 juillet 2011, les membres du groupe ont pris acte de cette importante évolution et salué la décision du ministère de l'Intérieur mettant fin aux interrogations sur la nature de la mention « origines géographiques » dans les dispositifs adoptés précédemment.

Alain Bauer
Professeur de criminologie au CNAM
Président du groupe de travail sur le contrôle
des fichiers de police et de gendarmerie

Rappel historique

En 2006, Nicolas Sarkozy, alors ministre d'État, ministre de l'Intérieur et de l'Aménagement du territoire, met en place un groupe de travail sur les fichiers de la police et de la gendarmerie nationales. Ce groupe [1], dont l'activité s'est étalée de juin 2006 à décembre 2006, a permis de recenser une grande partie des fichiers existants et d'émettre un certain nombre de recommandations [2] sur l'amélioration du contrôle des traitements automatisés de données utilisés dans le cadre des enquêtes administratives telles que prévues par l'article 17-1 modifié de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité.

Ces recommandations avaient, à l'époque, été acceptées par le ministère de l'Intérieur, tout autant soucieux de garantir les libertés, que de doter les services de l'État de moyens lui permettant d'assurer ses missions de protection des personnes, des biens et de la sûreté de l'État. Un grand nombre de ces préconisations ont, depuis, été mises en œuvre.

En septembre 2008, réactivé par décision de la ministre de l'Intérieur, de l'Outre-mer et des Collectivités territoriales après l'émotion créée dans l'opinion publique par la présentation du fichier exploitation documentaire et valorisation de l'information générale (EDVIGE), le groupe de contrôle des fichiers de police et de gendarmerie, élargi à de nouveaux membres issus du secteur associatif [3], s'était notamment attaché à compléter ce recensement en y ajoutant divers traitements et en étudiant les nouveaux développements prévus. Un deuxième rapport avait alors été rendu public en décembre 2008 [4].

En septembre 2009, sur demande du ministre de l'Intérieur, de l'Outre-mer et des Collectivités territoriales, le groupe de travail s'est de nouveau réuni afin d'examiner notamment les deux projets de décret portant

1 Voir composition en annexe 1.
2 Voir *Fichiers de police et de gendarmerie : comment améliorer leur contrôle et leur gestion ?*, La Documentation française, novembre 2006.
3 Voir composition en annexe 2.
4 Voir *Mieux contrôler les fichiers de police pour protéger les libertés*, La Documentation française, décembre 2008.

création des traitements automatisés de données à caractère personnel relatifs à la prévention des atteintes à la sécurité publique (PASP) et aux enquêtes administratives liées à la sécurité publique (EASP), fichiers devant se substituer au fichier des renseignements généraux (FRG) et aux projets EDVIGE puis EDVRISP.

Le 20 octobre 2009, l'arrêté officiel portant création d'un groupe de travail permanent sur l'amélioration du contrôle et de l'organisation des bases de données de police est publié, répondant ainsi à l'une des recommandations du groupe de travail 2008. Les nominations des membres sont intervenues après les élections professionnelles au sein de la police nationale (arrêté du 14 avril 2010) [1].

Par un courrier du 14 décembre 2010, le directeur du cabinet du ministre de l'Intérieur a rappelé aux directions générales de la police et de la gendarmerie nationales, à la préfecture de police, à la direction des libertés publiques et des affaires juridiques et au secrétariat général à l'immigration que le groupe de travail devait être saisi de tout projet de création ou de modification de fichiers avant même leur transmission à la CNIL et au Conseil d'État.

1 Voir annexe 3.

Synthèse des recommandations du groupe

Avertissement

Le groupe de travail a notamment pour mission d'émettre des recommandations sur tous les projets de création ou de modification de traitements mis en œuvre par la police ou la gendarmerie nationales, ce avant même que le ministère ne transmette ces projets à la CNIL dans les conditions prévues par la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004. Ainsi, la CNIL précise, qu'afin de ne pas préjuger de son avis, son représentant au sein du groupe s'abstient systématiquement lors des décisions finales du groupe.

1. Sur les traitements **PASP**, le groupe de contrôle a recommandé [1] :

• De remplacer le mot « comportement » par le mot « activité ».

• De réfléchir à un dispositif d'enregistrement des informations dans le domaine institutionnel économique et social et contribuant à l'exercice des missions des représentants de l'État en matière de prévention des troubles à l'ordre public ou de gestion des manifestations culturelles, récréatives ou sportives.

• De créer un magistrat référent chargé de vérifier l'effacement des données pour les mineurs.

Cette préconisation a été mise en œuvre.

1 Séance du 23 septembre 2009.

• De réintégrer le recueil d'informations fiscales.

• De supprimer la notion « origines géographiques »

Le 15 juin 2011, le directeur de cabinet du ministre de l'Intérieur indiquait au président du groupe de contrôle les éléments suivants :

« À la suite de vos dernières interventions concernant le maintien de la mention « origines géographiques » dans le décret GIPASP, faisant suite à vos préoccupations exprimées dès 2009 pour le décret PASP, il me paraît utile de vous préciser que le ministère de l'Intérieur, de l'Outre-mer, des Collectivités territoriales et de l'Immigration confirme totalement les termes de la circulaire adressée aux préfets le 18 octobre 2009 [...] Il m'apparaît néanmoins que ce dispositif, qui avait permis de lever certaines de vos préoccupations, doit faire l'objet d'une correction afin d'éviter toute interprétation contraire à la volonté de l'exécutif et aux interprétations des juridictions et autorités administratives constitutionnelles.

Aussi ai-je le plaisir de vous informer que j'ai demandé à mes services d'entamer les procédures visant à la modification des décrets PASP et GIPASP afin de sortir la mention « origines géographiques » des données sensibles et de ne permettre que l'enregistrement de données factuelles strictement limitées à l'origine géographique, au lieu de naissance, à la nationalité ou à la dénomination commune de la bande selon ses propres critères ».

---

2. Sur le traitement **EASP**, le groupe de contrôle a recommandé [1] de réfléchir à la prise en compte des enquêtes administratives réalisées dans le cadre des procédures de naturalisation ou de demandes de titre de séjour.

Cette préconisation a été mise en œuvre.

---

3. Sur la **mutualisation des fichiers de police et de gendarmerie**, le groupe de contrôle a recommandé [2] :

• La mise en place d'une réflexion sur l'éventuel fichier de gestion des bracelets électroniques et des conditions d'accessibilité permanente des fonctionnaires de la police nationale et des militaires de la gendarmerie aux fichiers gérés par l'Administration pénitentiaire.

• L'étude de la mutualisation éventuelle des systèmes CORAIL, ANACRIM-NG, LUPIN et EASP.

1 Séance du 23 septembre 2009.
2 Séance du 13 octobre 2009.

• L'étude comparative entre les systèmes ARDOISE (aujourd'hui LRPPN) et ICARE (aujourd'hui LRPGN).

Cette préconisation a été mise en œuvre.

4. Sur les différents traitements examinés :

• **Système d'analyse des liens de la violence associée aux crimes (SALVAC)** : Les membres du groupe de travail n'ont pas émis de remarques concernant ce traitement qui a été régularisé à la suite du premier rapport [1].

• **Plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS)** : Les membres du groupe de travail n'ont pas émis pas de remarques concernant ce traitement [2].

• **Fichier des personnes recherchées (FPR – modification)** : Les membres du groupe de travail n'ont pas émis de remarques concernant ce traitement [3].

• **Fichier des courses et jeux** : Les membres du groupe de travail n'ont pas émis de remarques concernant ce traitement [4].

• **Base de données de sécurité publique (BDSP)** : Les membres du groupe de travail n'ont pas émis de remarques concernant ce traitement [5].

• **PULSAR** : Les membres du groupe de travail n'ont pas émis de remarques concernant ce traitement [6].

• **Logiciel de rédaction de la gendarmerie nationale (LRPGN)** : Les membres du groupe de travail n'ont pas émis de remarques concernant ce traitement [7].

• **Logiciel de rédaction de la police nationale (LRPPN)** : Les membres du groupe de travail n'ont pas émis de remarques concernant ce traitement [8].

• **Traitement des procédures judiciaires (TPJ)** : Les membres du groupe de travail n'ont pas émis de remarques concernant ce traitement [9].

• **Traitement de diffusion et de partage de l'information opérationnelle des unités de recherches de la gendarmerie nationale** : Les membres du

1 Séance du 10 novembre 2009.
2 Séance du 17 février 2010.
3 Séance du 22 juin 2010.
4 Séance du 16 décembre 2010.
5 Séance du 6 septembre 2010.
6 Séance du 16 décembre 2010.
7 Séance du 16 décembre 2010.
8 Séance du 6 septembre 2010.
9 Séance du 20 juin 2011.

groupe de travail n'ont pas émis de remarques concernant ce traitement hormis la demande de suppression de la mention « origine géographique » (art. 3)[1].

Cette préconisation a été prise en compte (voir supra).

• **Fichier automatisé des empreintes digitales (FAED – modification)** : Les membres du groupe de travail n'ont pas émis de remarques concernant ce traitement[2].

• **Fichier national des interdits d'acquisition et de détention d'armes (FINADIA)**[3] : Les membres du groupe de travail n'ont pas émis de remarques concernant ce traitement

• **Gestion des étrangers en situation irrégulière (GESI)** : Les membres du groupe de travail n'ont pas émis de remarques concernant ce traitement hormis SOS Racisme qui ne souhaite pas approuver ce projet[4].

• **Exécution des services commandés pour la réalisation des transfèrements et extractions (ESCORTE)** : Les membres du groupe de travail n'ont pas émis de remarques concernant ce traitement.

5. Sur le dossier **« MENS »**, le groupe de travail des fichiers de police et de gendarmerie a recommandé au ministre de l'Intérieur, de l'Outre-mer et des Collectivités territoriales de[5] :

• Procéder à la mise en conformité des bases de travail non déclarées et non conformes à la législation du 6 janvier 1978 sur l'informatique et les libertés qui ne l'auraient pas encore été à ce jour, ce qui implique la suppression des éléments irréguliers et la conception de nouvelles bases de données conformes aux règles juridiques issues de la législation actuelle ainsi que, si nécessaire, de la LOPPSI lorsque celle-ci aura été promulguée.

Cette préconisation a été mise en œuvre.

• S'assurer de la suppression effective de la mention « MENS » de tous les documents encore utilisés au sein des unités et des services centraux de la gendarmerie nationale, comme s'y est engagé le directeur général de la gendarmerie nationale, et déclarer conformément à la législation tous les outils d'analyse et de rapprochement nécessaires à la lutte contre la délinquance itinérante à partir de données personnelles.

Cette préconisation a été mise en œuvre.

1 Séance du 20 juin 2011.
2 Séance du 16 décembre 2010.
3 Séance du 16 décembre 2010.
4 Séance du 20 juin 2011.
5 Séance du 18 octobre 2010.

• Rappeler, par une circulaire générale, à l'ensemble des services de la police et de la gendarmerie nationale la législation en vigueur en matière de création de traitements de données à caractère personnel.

Cette préconisation a été mise en œuvre.

• Se rapprocher dans les meilleurs délais de la CNIL en vue de la mise en œuvre de ces mesures.

D'une manière générale, le groupe de travail sur l'amélioration du contrôle et de l'organisation des fichiers de police et de gendarmerie a recommandé au ministre de l'Intérieur, de l'Outre-mer et des Collectivités territoriales de :

• Faire procéder au recensement de toutes les bases de travail, notamment judiciaires, extensions de fichiers déclarés, mais qui, en tant que telles, n'auraient pas fait l'objet d'une déclaration spécifique

Cette préconisation a été mise en œuvre et est toujours en cours.

• Procéder, dans les meilleurs délais et dès l'instant où ses bases répondent à un réel besoin opérationnel à partir de faits ou d'éléments sériels, à la déclaration de ces bases de travail selon la législation afférente.

Cette préconisation a été mise en œuvre.

Par ailleurs, le groupe de travail sur l'amélioration du contrôle et de l'organisation des fichiers de police et de gendarmerie rappelle :

• Qu'il souhaite que soit engagée avant la fin 2010 la destruction physique et informatique des fichiers FAR et FPNE tel que cela a été acté lors de la réunion du groupe de travail du 6 septembre 2010 (destruction totale sauf pour 4 brigades pour le FAR et pour 1 lettre pour le FPNE suivant les recommandations des Archives nationales) [1].

Cette préconisation a été mise en œuvre.

• Que la mention « origines géographiques » soit supprimée du fichier Prévention des atteintes à la sécurité publique (PASP) tel que cela a été recommandé lors des réunions du 10 novembre 2009 et 22 juin 2010.

Cette préconisation a été prise en compte (voir supra).

6. Le groupe de travail a recommandé la mise en place d'un programme prévisionnel de contrôle des fichiers tenus par les polices municipales [2].

7. Le groupe de travail a recommandé la mise en place, pour les fichiers sensibles, d'un dispositif d'alarme pour les consultations anormales [3].

1 Destruction effective. Voir ci-après.
2 Séances des 10 novembre 2009, 22 juin 2010 et du 16 décembre 2010.
3 Séances du 6 septembre 2010 et du 20 juin 2011.

Chapitre 1

Les fichiers PASP et EASP

La genèse

La réorganisation des services de renseignement du ministère de l'Intérieur, intervenue le 1er juillet 2008, a entraîné la création d'un service de renseignement intérieur civil unique[1], la Direction centrale du renseignement intérieur (DCRI), chargé des missions de l'ancienne direction de la surveillance du territoire et d'une partie de celles de l'ancienne direction centrale des renseignements généraux. La DCRI a été dotée d'un nouveau fichier (CRISTINA).

Une nouvelle sous-direction de l'information générale, reprenant une partie des missions des anciens renseignements généraux, a été créée au sein de la Direction centrale de la sécurité publique. Elle a repris les missions de renseignement liées aux violences urbaines, aux dérives sectaires, au radicalisme religieux ou encore à l'information générale du gouvernement. Un nouveau fichier, reprenant une très grande partie des informations contenues dans l'ancien fichier des renseignements généraux (FRG) sorti la clandestinité en 1991, a donc dû être mis en place.

Faisant suite à une première version – EDVIGE[2] – qui avait suscité la polémique en septembre 2008, un autre traitement, « Exploitation documentaire et la valorisation de l'information relative à la sécurité publique » (EDVRISP) avait été envisagé fin 2008. Il était destiné à collecter, conserver et traiter les données concernant les personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique et les personnes faisant l'objet d'enquêtes administratives afin de déterminer si leur comportement n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées compte tenu de leur nature.

1 Il existe trois services militaires de renseignements : la Direction générale de la sécurité extérieure (DGSE) qui dépend du ministère de la Défense, la Direction du renseignement militaire (DRM) qui est rattaché au chef d'état-major des armées et la Direction de la protection et de la sécurité de la défense (DPSD) qui dépend du cabinet du ministre de la Défense. La gendarmerie nationale, pour sa part, « contribue à la mission de renseignement et d'information des autorités publiques, à la lutte contre le terrorisme, ainsi qu'à la protection des populations. Elle participe à la défense de la patrie et des intérêts supérieurs de la nation, notamment au contrôle et à la sécurité des armements nucléaires » (article 1 de la loi nº 2009-971 du 3 août 2009).
2 Délibération CNIL nº 2008-174 du 16 juin 2008.

Contrairement à son prédécesseur, ce traitement supprimait la possibilité de centraliser les informations relatives à des personnes exerçant un mandat ou jouant un rôle institutionnel, économique, social ou religieux significatif. Les données concernant la santé et les orientations sexuelles avaient également été supprimées du projet.

Les projets PASP et EASP

Après la transmission à la CNIL et au Conseil d'État du projet de décret portant création d'EDVRISP, le gouvernement a décidé, en août 2009, de proposer deux nouveaux traitements reprenant les finalités d'EDVRISP. L'une des principales nouveautés issue de ces décrets est la création de deux fichiers, au lieu d'un fichier unique, l'un consacré à la prévention des atteintes à la sécurité publique et l'autre aux enquêtes administratives. Les deux finalités du fichier EDVIGE ou de l'ex-FRG sont donc désormais distinctes ce qui a contribué à clarifier et à rendre le dispositif plus lisible pour l'opinion.

La deuxième nouveauté importante est la création d'une durée de conservation des données pour les majeurs qui est de 10 ans. Cette limite de conservation des données n'était ni présente dans le décret FRG ni dans les projets EDVIGE et EDVIRSP.

Enfin, ces deux projets consacrent la disparation du « fichier des personnalités » et donc de la centralisation des informations sur 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 ».

Le fichier PASP[1] est destiné à recueillir, conserver et analyser les informations qui concernent des personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique. Ce traitement a notamment pour finalité de recueillir, de conserver et d'analyser les informations qui concernent les personnes susceptibles d'être impliquées dans des actions de violence collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives.

Le fichier utilisé pour les personnes faisant l'objet d'enquêtes administratives visant à déterminer si leur comportement n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées compte tenu de leur nature (en application des dispositions du premier alinéa de l'article 17-1 de la loi du 21 janvier 1995), est distinct du fichier « PASP » (et donc de l'ex-fichier des renseignements généraux) et a été créé par le décret n° 2009-

1 Délibération CNIL n° 2009-355 du 11 juin 2009.

1250 du 16 octobre 2009 : enquêtes administratives liées à la sécurité publique (EASP)[1]. Il devrait être complété par un nouveau décret permettant aussi la réalisation, par les fonctionnaires de police chargés du renseignement, des enquêtes administratives en vue de l'instruction de dossiers de demande d'acquisition de la nationalité française et des demandes de titres de séjour. Les données peuvent être conservées pendant une durée maximale de cinq ans à compter de leur enregistrement. Les données ne peuvent concerner des mineurs que s'ils sont âgés de seize ans au moins et ont fait l'objet d'une enquête administrative. Les consultations du traitement automatisé font l'objet d'un enregistrement comprenant l'identifiant du consultant, la date, l'heure et l'objet de la consultation. Ces informations sont conservées pendant un délai de cinq ans.

Un projet de décret modifiant PASP et EASP permettant aussi la réalisation, par les fonctionnaires de police chargés du renseignement, des enquêtes administratives en vue de l'instruction de dossiers de demande d'acquisition de la nationalité française et des demandes de titres de séjour a été transmis au Conseil d'État.

Les recommandations du groupe de travail

Le groupe de travail sur l'amélioration du contrôle et de l'organisation des fichiers de police et de gendarmerie a été réactivé en septembre 2009 afin d'examiner notamment ces deux nouveaux projets de décret.

Toutefois, lors de sa séance du 23 septembre 2009, si les projets ont pu être présentés et si les membres du groupe ont pu émettre un certain nombre de recommandations lors de sa séance du 23 septembre 2009, il est apparu que les projets de décret, qui avaient déjà été présentés à la CNIL et au Conseil d'État, devaient faire l'objet d'une publication rapide afin que les fonctionnaires de la sous-direction de l'information générale puissent travailler en toute légalité suite à la disparition, au 31 décembre 2009, du FRG. C'est pourquoi le cabinet du ministre de l'Intérieur avait indiqué que certaines propositions du groupe de travail feraient l'objet de décrets modificatifs ultérieurs.

Dans sa séance du 23 septembre, les membres du groupe de contrôle ont pris acte, avec satisfaction, que la demande visant à distinguer les finalités des traitements avait été prise en compte. Ainsi, au lieu d'un fichier unique portant tant sur la prévention des atteintes à la sécurité

1 Délibération CNIL n° 2009-356 du 11 juin 2009.

publique que sur les enquêtes administratives, et qui pouvait porter à confusion en mélangeant des finalités différentes, il a été proposé, comme l'avait demandé une majorité des membres du groupe de contrôle en 2008, la création de deux fichiers distincts.

PASP

Sur l'économie du texte portant sur PASP, plusieurs membres du groupe de contrôle ont souhaité faire part de leurs observations qui ont fait l'objet, en réunion, de réponse du cabinet du ministre de l'Intérieur.

1. Dans son article 1er, le texte évoque le « comportement individuel ou collectif ». Or, dans le reste du projet, il est toujours fait mention du mot « activité » qui est, par ailleurs, plus précis puisque portant sur des actes et non sur des attitudes. Les membres du groupe de contrôle proposent de remplacer le mot « comportement » par le mot « activité ».

Le ministère de l'Intérieur accepte cette proposition.

2. Il est fait remarquer que ce projet ne tient pas compte de la nécessité de recueillir les informations dans le domaine institutionnel, économique et social et contribuant à l'exercice des missions des représentants de l'État en matière de prévention des troubles à l'ordre public ou de gestion des manifestations culturelles, récréatives ou sportives. Il est rappelé que, lors de ses réunions précédentes, le groupe de contrôle avait proposé que les données pouvaient être recueillies :

2° Lorsqu'elles concernent des groupes, mouvements ou organisations dont l'activité peut faire l'objet de la mission de renseignement et d'information du gouvernement, et des représentants de l'État dans les collectivités territoriales, en ce qui concerne le domaine institutionnel, économique et social ainsi que dans tous les domaines susceptibles d'intéresser l'ordre public notamment les phénomènes de violence.

Le ministère de l'Intérieur est en effet conscient de cette absence et indique que cette question fera l'objet d'un décret ultérieur. À la date de publication du présent rapport d'activités cette problématique n'a pas encore été prise en compte.

3. Il est fait observer par certains membres que la nouvelle disposition visant à la fixation d'une durée de conservation des données pour les majeurs (art. 4), dans un fichier de renseignements, peut limiter l'intérêt d'un tel fichier de police administrative et la capacité opérationnelle des services de police, d'autant que cette durée de conservation semble être courte au regard des finalités du fichier.

Le ministère de l'Intérieur prend acte des observations des membres du groupe mais n'envisage pas une modification de cet article considérant que celui-ci apportait des garanties supplémentaires.

4. Alain Bauer relève qu'une des principales recommandations du groupe de contrôle portant sur la création d'un magistrat référent, de l'ordre administratif, chargé de vérifier l'effacement des données pour les mineurs n'a pas été prise en compte. Le cabinet du ministre de l'Intérieur indique que cette proposition, qui a reçu l'accord du ministre, fera l'objet d'un décret ultérieur.

Le texte créant le magistrat référent pour les inscriptions des mineurs dans les fichiers a été publié au Journal Officiel du 14 décembre 2010.

---

5. Certains membres du groupe de contrôle s'étonnent de la formulation du 8° de l'article 2 portant sur le recueil d'informations relatives aux « agissements susceptibles de recevoir une qualification pénale » et non plus aux « antécédents judiciaires ». Le directeur des Libertés publiques et des Affaires juridiques indique que cette nouvelle formulation répond de manière plus précise aux finalités du fichier qui est, non pas un fichier d'antécédents judiciaires, mais un fichier de renseignements. Aussi, il est important que les informations enregistrées ne concernent pas exclusivement des faits ayant fait l'objet d'une mise en cause, et donc d'une procédure, ou de poursuites. Par ailleurs, l'enregistrement d'informations portant sur des antécédents judiciaires serait prohibé par le Code de procédure pénale.

6. Il est fait observer que la suppression du recueil d'informations fiscales et du seul enregistrement de données patrimoniales peut entraîner certaines difficultés : ainsi, comment évaluer si une personne a un train de vie supérieur à ses revenus s'il n'est pas possible de confronter le patrimoine et les revenus déclarés ?

Pour certains membres du groupe, les informations fiscales sont inclues dans ce qui relève du domaine patrimonial.

Le ministère de l'Intérieur demande la réalisation d'une étude visant à définir exactement la nature exacte de ce qui est qualifié d'informations patrimoniales. À la date de publication du présent rapport d'activités cette question n'a pas encore fait l'objet de développements.

---

7. Certains membres du groupe de contrôle relèvent que, tel que libellé, le projet de décret ne permettrait pas aux fonctionnaires de la SDIG de recueillir et d'exploiter des données relatives au phénomène sectaire et interdirait ainsi de suivre les sectes puisque cette finalité n'est pas prévue dans le texte.

Le ministère de l'Intérieur répond que les activités religieuses intègrent les dérives sectaires.

---

8. Par ailleurs, suite à la publication du décret portant création du système PASP, dans sa séance du 10 novembre 2009, le groupe de travail a indiqué que la disposition du texte sur « les origines géographiques » mériterait d'être précisée.

La DGPN précise que, dès l'adoption du texte, une circulaire a été envoyée aux préfets précisant les caractéristiques des informations pouvant être enregistrées dans ce cadre. Elle indique également que la dérogation à l'article 8 a été insérée suite à la modification de la loi de 1978, en 2004, et ce afin d'être en conformité avec ce texte qui prévoit notamment l'interdiction d'enregistrer des données sensibles même de manière incidente. Or l'enregistrement d'une donnée telle que le nom de la bande « black guérilla armée » peut faire apparaître, de manière incidente, une information sur l'origine ethnique de ses membres.

Concernant l'enregistrement de données sur « l'origine géographique », Alain Bauer a indiqué que si ces informations concernaient le lieu d'origine des membres des bandes (nom du quartier par exemple), comme l'a indiqué le ministère de l'Intérieur, l'enregistrement de telles données n'a pas à être régi par les dispositions relatives aux données sensibles. Afin de lever toute ambiguïté sur l'interprétation de cet article du décret, et en cohérence avec les directives adressées aux Préfets par le ministère de l'Intérieur, le groupe de travail recommande que les informations sur « l'origine géographique » soient exclues de l'article 3 du décret portant sur les données sensibles.

Le 15 juin 2011, le directeur de cabinet du ministre de l'Intérieur indiquait au président du groupe de contrôle les éléments suivants :

« *À la suite de vos dernières interventions concernant le maintien de la mention « origines géographiques » dans le décret GIPASP, faisant suite à vos préoccupations exprimées dès 2009 pour le décret PASP, il me paraît utile de vous préciser que le ministère de l'Intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration confirme totalement les termes de la circulaire adressée aux préfets le 18 octobre 2009 [...] Il m'apparaît néanmoins que ce dispositif, qui avait permis de lever certaines de vos préoccupations, doit faire l'objet d'une correction afin d'éviter toute interprétation contraire à la volonté de l'exécutif et aux interprétations des juridictions et autorités administratives constitutionnelles.*

Aussi ai-je le plaisir de vous informer que j'ai demandé à mes services d'entamer les procédures visant à la modification des décrets PASP et GIPASP afin de sortir la mention « origines géographiques » des données sensibles et de ne permettre que l'enregistrement de données factuelles strictement limitées à l'origine géographique, au lieu de naissance, à la nationalité ou à la dénomination commune de la bande selon ses propres critères ».

EASP

Sur le projet portant création d'EASP, deux observations ont été portées à la connaissance du ministre de l'Intérieur :

1. Le mot « comportement » est utilisé dans l'article 2. Par parallélisme des formes avec le projet de décret « PASP » le groupe de travail propose d'utiliser le mot « activité ».

Le ministère de l'Intérieur fait valoir que le terme « comportement » est celui dont il est fait référence dans la loi du 21 janvier 1995.

2. Il est fait remarquer que, dans les finalités du traitement, il n'est pas fait mention des enquêtes administratives réalisées dans le cadre des procédures de naturalisation ou de demande de titres de séjour ce qui représentent une part importante des enquêtes administratives réalisées par les fonctionnaires des SDIG au profit des préfets notamment.

Le ministère de l'Intérieur indique que cette question fera l'objet d'un décret ultérieur. Dans sa séance du 20 janvier 2011, le groupe de travail a pu examiner les projets modificatifs des décrets PASP et EASP en vue de permettre la réalisation des enquêtes administratives portant sur la délivrance de titres de séjour et les demandes de naturalisation. Il n'a été émis aucune objection.

Chapitre 2

La mutualisation des fichiers de police et de gendarmerie

La séance du 13 octobre 2009 a été consacrée à l'examen des différents fichiers de police et de gendarmerie et à leur possible mutualisation lorsque celle-ci n'existe pas encore (*cf. liste en annexe 8*).

La question de l'éventuel fichier sur la gestion des bracelets électroniques et des conditions d'accessibilité permanente des fonctionnaires de la police nationale et des militaires de la gendarmerie aux fichiers gérés par l'Administration pénitentiaire est soulevée. Il est demandé qu'un point puisse être effectué entre les directions générales de la police et de la gendarmerie nationales et la direction de l'administration pénitentiaire.

À la date de publication du présent rapport d'activités, cette question n'a pas encore été débattue.

À l'issue de l'examen des différents fichiers, le groupe de travail suggère qu'une réflexion soit engagée sur la mutualisation possible des traitements suivants notamment, pour certains d'entre eux, en vue de l'adoption d'un texte législatif sur les logiciels de rapprochement judiciaire, comme **CORAIL**, **ANACRIM-NG,** ou **LUPIN** *(La liste n'est pas exhaustive)*.

Le cadre législatif des logiciels de rapprochements judiciaires (art. 14) a pu être fixé dans le cadre de l'examen de la loi d'orientation et de performance de la sécurité intérieure, promulguée le 14 mars 2011. Il permettra de procéder à la mutualisation de certains traitements.

Il a été demandé une étude comparative sur les différences et ressemblances entre les logiciels **ARDOISE** (aujourd'hui dénommée LRPPN) et **ICARE** (aujourd'hui dénommée LRPGN) en vue de savoir si, à moyen terme, une mutualisation des applications bureautiques ne serait pas envisageable.

Une mission commune IGPN/IGGN sur les deux logiciels de rédaction de procédure, et à laquelle était associé, comme observateur, le groupe de travail par l'intermédiaire de Christophe Soullez, Rapporteur, a été lancée en décembre 2010. Un premier rapport a été remis mi-janvier 2010. Suite à ce dernier, une nouvelle mission a été confiée à l'Inspection Générale de l'Administration (IGA) en janvier 2011. Son rapport a été rendu fin mars 2011.
Concernant le ***fichier sur les enquêtes administratives liées à la sécurité publique (EASP),*** *et dès lors que les gendarmes*

sont conduits à réaliser ce type d'enquêtes, il est demandé une réflexion sur la possibilité de mutualisation de ce traitement.
À la date de publication du présent rapport d'activités, cette question n'a pas encore été débattue.

Chapitre 3

Les traitements examinés

Système d'analyse des liens de la violence associée aux crimes (SALVAC)

SALVAC, qui avait été mis en place en 2005 sans cadre légal, se fondait sur l'article 30 de la loi du 12 décembre 2005 relative au traitement de la récidive des infractions pénales. Il a fait l'objet d'une autorisation par le décret n° 2009-786 du 23 juin 2009 suite à la délibération CNIL n° 2009-042 du 29 janvier 2009.

La finalité du traitement consiste à opérer des rapprochements entre les procédures judiciaires afin d'identifier et poursuivre les auteurs de crimes ou délits commis « en série », dans le domaine de la criminalité violente (meurtre, assassinat, acte de torture et de barbarie, viol, agression sexuelle, atteinte sexuelle sur mineur, etc.). L'alimentation et les consultations sont effectuées par 15 policiers et gendarmes de l'office central pour la répression des violences aux personnes (OCRVP), spécialement habilités et individuellement désignés. Au 1er février 2010, SALVAC contenait 9 421 dossiers. SALVAC a permis de résoudre 17 affaires sérielles portant sur 120 victimes.

Les membres du groupe de contrôle n'émettent pas de remarques concernant ce traitement qui a été régularisé à la suite du premier rapport.

Plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS)

Créé par un arrêté du 16 juin 2009, Pharos est tout d'abord un site internet permettant aux utilisateurs et acteurs d'internet, et notam-

ment aux internautes, fournisseurs d'accès et services de veille étatiques, de signaler, sans préjudice du respect dû aux correspondances privées, à l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication des sites ou des contenus contraires aux lois et règlements diffusés sur internet. Il inclut également un traitement automatisé de données à caractère personnel mis en œuvre par l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication et destiné à traiter les signalements transmis par les utilisateurs et acteurs d'internet. Pharos a pour finalités de recueillir, de manière centralisée, l'ensemble des signalements, d'effectuer des rapprochements entre eux et de les orienter vers les services enquêteurs compétents en vue de leur exploitation.

Les informations enregistrées sont les nom et prénom de l'auteur du signalement, son adresse, son numéro de téléphone et son adresse de messagerie électronique et l'identité du ou des agents ayant traité le signalement. Les données à caractère personnel mentionnées sont conservées deux ans à compter de leur enregistrement. L'adresse IP de l'auteur du signalement est conservée deux ans à compter de son enregistrement.

Les membres du groupe de contrôle n'émettent pas de remarques concernant ce traitement.

Modification du fichier des personnes recherchées (FPR)

Le fichier des personnes recherchées (FPR), créé par arrêté du 15 mai 1996 (modifié en 2005), répertorie, au plan national, toutes les personnes faisant l'objet de recherches par l'autorité judiciaire, les services de police, de gendarmerie et des douanes, les administrations ou les autorités militaires dans le cadre de leurs compétences légales.

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

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

Un nouveau décret a été publié le 30 mai 2010 (*décret n° 2010-569*). Les conditions d'inscription au FPR ont été élargies à certaines mesures

administratives relatives à la police des étrangers (interdiction d'entrée sur le territoire national).

De même peuvent désormais êtres inscrites au fichier les ressortissants d'un État non membre de l'Union européenne faisant l'objet d'une mesure restrictive de voyage, interdisant l'entrée sur le territoire ou le transit par le territoire, adoptée par l'Union européenne ou une autre organisation internationale et légalement applicable en France.

Le décret précise également que les services préfectoraux peuvent directement alimenter le fichier sur certaines mesures administratives dont ils sont à l'origine : fiches E (étrangers), G (permis de conduire) et TP (opposition à délivrance de passeport). Enfin, dans un souci d'amélioration de la sécurité routière et de lutte contre la fraude et la conduite avec un permis invalidé, il a rendu nécessaire d'inscrire dans le FPR les personnes faisant l'objet de recherches en vue de la notification de mesures administratives concernant leur permis de conduire et celles faisant l'objet d'une mesure administrative visant au retrait d'un permis de conduire obtenu indûment.

Une nouvelle modification devrait intervenir courant 2011 : la possibilité, sous le contrôle des services de police, de rendre les agents de police municipale destinataires de certaines informations utiles à l'accomplissement de leurs missions.

Au 1er novembre 2010, les services de police et unités de gendarmerie ont effectué plus de 51 millions de consultations depuis le 1er janvier 2010 lesquelles ont permis 75 896 découvertes.

Les membres du groupe de contrôle n'émettent pas de remarques concernant ce traitement.

Le fichier des courses et jeux

Créé par arrêté du 8 novembre 2010, ce traitement est l'héritier du traitement qui était géré par le service « courses et jeux » de la Direction centrale des renseignements généraux disparu, et transféré à la Direction centrale de la police judiciaire, suite à la réforme des services de renseignement en 2010. Il a pour finalité d'assurer la surveillance de la régularité et de la sincérité des jeux, des courses et des paris par la conservation des données recueillies notamment à l'occasion des enquêtes administratives d'agrément et d'autorisation de jeux ou relatives aux personnes faisant l'objet d'une mesure d'interdiction ou d'exclusion des salles de jeux ou des champs de courses.

Les membres du groupe de contrôle n'émettent pas de remarques concernant ce traitement.

Base de données de sécurité publique (BDSP – EX ATHENA)

Devant notamment remplacer le système Aramis ainsi que le FAR, la gendarmerie nationale a créé son traitement de données lié au renseignement de proximité à travers quatre modules relatifs aux traitements « ordre public ». Le module GISPAP est une proche copie du fichier PASP de la Police Nationale. Le module Gestion des évènements d'ampleur (GEA) permettra de recueillir des informations sur le déroulement des événements majeurs et les conduites à tenir. Le module Gestion des sollicitations et des interventions (GSI) et le module Sécurisation des interventions et demandes particulières de protection (SIDPP) sont destinés à apporter des réponses adaptées aux sollicitations des usagers et de conduire l'engagement des personnels et des moyens de la gendarmerie dans les meilleures conditions de sécurité. Ainsi, pour exemple, si lors d'une intervention une brigade est face à une personne en possession d'une arme, celle-ci pourra être inscrite en base afin que, dans le cas d'une nouvelle intervention, l'équipage soit averti de cet élément. L'inscription dans ce fichier ne pourra être réalisée qu'*a posteriori* d'une première intervention et non *a priori.* Enfin, le module Sécurisation des interventions et demandes particulières de protection (SIDPP) a aussi pour finalité de collecter des données destinées à prévenir les risques encourus par des personnes vulnérables ou sollicitant une demande de protection (tranquillité vacances, tranquillité seniors,...).

Les membres du groupe de contrôle n'émettent pas de remarques concernant ce traitement.

Trois décrets en Conseil d'État ont été signés et publiés le 29 mars 2011.

PULSAR [1]

En 2011, le traitement PULSAR [2], évolution de l'application Bureautique Brigade 2000, a été déployé dans les brigades de gendarmerie. Cette application permet aux unités territoriales de la gendarmerie nationale de gérer sur le plan administratif le service et les registres (courrier et procès-verbaux), les amendes forfaitaires, ainsi que de générer les messages

1 Délibérations CNIL nº 2010-117 et 118 du 6 mai 2010.
2 Voir le rapport *Mieux contrôler les fichiers de police pour protéger les libertés*, La Documentation française, juin 2009, p. 86.

d'information statistique relatifs à la délinquance et les bulletins d'analyse des accidents relatifs à l'accidentalité.

Quatre modules ont été créés par arrêté : 1) gestion des amendes forfaitaires et des consignations dénommé « Gestion des amendes forfaitaires des unités élémentaires de la gendarmerie départementale et des gendarmeries spécialisés » (arrêté du 2 décembre 2010) 2) gestion des messages d'information statistique et des bulletins d'analyse des accidents des unités élémentaires de la gendarmerie départementale et des gendarmeries spécialisées, dénommé « gestion des MIS et des BAA » (arrêté du 2 décembre 2010) 3) gestion des courriers et des procédures dans les unités élémentaires de la gendarmerie départementale et des gendarmeries spécialisées, dénommé « gestion du registre des unités » (déclaré sur le fondement de l'article 23 de la loi « informatique et libertés ») 4) gestion du service dans les unités élémentaires de la gendarmerie départementale et des gendarmeries spécialisées, dénommé « gestion du service des unités » (déclaré sur le fondement de l'article 23 de la loi « informatique et libertés »).

Les membres du groupe de contrôle n'émettent pas de remarques concernant ce traitement.

LRPPN [1]

La police nationale devrait utiliser, en 2011, le "Logiciel de rédaction des procédures de la police nationale, V2" (ex-ARDOISE) destiné à uniformiser la rédaction de procédures et à alimenter notamment le futur Traitement des Procédures Judiciaires (TPJ – ex-ARIANE), qui remplacera à la fois le STIC de la police nationale et le JUDEX de la gendarmerie nationale. Plus qu'un simple logiciel d'assistance à la rédaction des procédures LRPPN est le cœur du nouveau système d'information de la police nationale.

LRPPN constituera donc, dans sa version définitive qui interviendra au terme des améliorations techniques successives (LRPPN V3), un support technique unique de l'activité procédurale de l'ensemble des services de la police nationale dans l'exercice de leurs missions de police judiciaire et administrative et l'outil d'alimentation des traitements nationaux de documentation criminelle (traitement des procédures judiciaires, fichiers des objets et véhicules signalés).

LRPPN V2, version provisoire, permet la collecte et l'archivage des informations recueillies par les services chargés de l'établissement des

1 Délibération CNIL n° 2008-379 du 6 novembre 2008.

procédures diligentées dans le cadre de leurs missions de police judiciaire. Les données enregistrées sont donc issues des procès-verbaux, comptes rendus d'enquêtes et rapports administratifs ou judiciaires. Il faudra toutefois attendre la version 3 pour que le LRPPN puisse alimenter d'autres traitements dont TPJ, le système du ministère de la Justice Cassiopée ; ou le module statistiques (état 4001 et statistiques opérationnelles). Après une expérimentation de plusieurs mois en 2010, le décret autorisant le déploiement de LRPPN V2 a été publié le 29 janvier 2011 (*décret nº 2011-110*). La version 3 devra faire l'objet d'une nouvelle autorisation. Elle serait déployée courant 2011.

Les membres du groupe de contrôle n'émettent pas de remarques concernant ce traitement.

LRPGN

Le logiciel « Logiciel de rédaction des procédures de la gendarmerie nationale » (LRPGN – ex-*Icare*[1]) est destiné à assister les militaires de la gendarmerie dans la rédaction de leurs procès-verbaux. Cet outil participe, par ailleurs, à la remontée d'informations en alimentant les bases de données opérationnelles (Judex puis, lorsqu'il sera mis en en service, TPJ) et est aussi en mesure d'échanger avec le logiciel Cassiopée du ministère de la Justice et des libertés.

La création de cet outil informatique a été validée par la commission nationale de l'informatique et des libertés (CNIL) le 6 mai 2010[2]. Le Conseil d'État a rendu son avis le 13 juillet 2010 en proposant des modifications qui ont été reprises par le gouvernement. LRPGN avait déjà été examiné par le groupe de travail en 2008 lorsqu'il portait le nom d'Icare. LRPGN a été autorisé par le décret nº 2011-111 du 27 janvier 2011.

Les membres du groupe de contrôle n'émettent pas de remarques concernant ce traitement.

1 Voir le rapport *Mieux contrôler les fichiers de police pour protéger les libertés*, La Documentation française, juin 2009, p. 24. Notons que depuis juin 2010, la DGGN a prêté une version du logiciel Icare afin qu'il soit testé par le SNDJ.
2 Délibération CNIL nº 2010-119 du 6 mai 2010.

Traitement des procédures judiciaires (TPJ – ex-ARIANE)

Début 2005, la gendarmerie et la police nationales, qui sont depuis le 1er janvier 2009 placées sous la tutelle unique du ministère de l'Intérieur, confrontées à la nécessité de moderniser leurs systèmes respectifs JUDEX et STIC, se sont associées pour réaliser un nouveau fichier commun d'antécédents judiciaires : traitement des procédures judiciaires (TPJ – ex-ARIANE).

Cette coopération opérationnelle et technique s'inscrit dans le sens de la loi d'orientation et de programmation pour la sécurité intérieure d'août 2002 (LOPSI) qui prescrivait le rapprochement des grands fichiers informatisés des deux forces.

Outre les avantages attendus en termes de rationalisation des moyens techniques et financiers nécessaires à sa réalisation, le nouveau système permettra l'accès pour tout gendarme ou policier à l'ensemble des informations relatives aux enquêtes judiciaires quel que soit le service ou l'unité à l'origine de leur enregistrement. Un dossier de déclaration a été transmis à la CNIL. La mise en œuvre opérationnelle devrait intervenir au second semestre 2011.

Les informations contenues dans TPJ respecteront les mêmes règles que les applications STIC et JUDEX actuelles. Deux nouvelles catégories de données seront intégrées au système : les morts suspectes et les disparitions inquiétantes (art. 74 et 74-1 du Code de procédure pénale).

Les règles actuelles valables pour STIC et JUDEX seront appliquées pour TPJ et ouvertes, sous certaines conditions aux services de la Douane judiciaire. Il est également prévu d'organiser l'accès direct effectif, déjà prévu par le législateur, au profit des parquets au titre du contrôle de la régularité du fichier. TPJ sera alimenté par LRPPN et LRPGN. Il permettra de regrouper l'ensemble des procédures judiciaires en vue de leur transmission automatique, et de leur mise à jour, au système Cassiopée du ministère de la Justice.

Les membres du groupe de contrôle n'émettent pas de remarques concernant ce traitement.

Traitements de diffusion et de partage de l'information opérationnelle des unités de recherches de la gendarmerie nationale

Un décret devrait être pris en 2011 ou 2012[1] afin de couvrir, notamment, l'ensemble des traitements locaux des unités de recherche de la gendarmerie (11 % des unités).

Ces traitements ont pour finalité de faciliter la diffusion et le partage d'informations opérationnelles, détenues par différents services ou unités judiciaires de la gendarmerie nationale, sur les enquêtes en cours ou les individus qui en font l'objet ainsi que l'activité judiciaire de ces unités, en vue d'une meilleure coordination de leurs investigations.

Ces traitements stockent des documents officiels, à l'exception des pièces de procédure, émis ou reçus par des services ou unités de gendarmerie et qui sont relatifs à des phénomènes de délinquance ou criminalité. Ils peuvent contenir des données notamment sur les personnes à l'encontre desquelles il existe des raisons plausibles de soupçonner qu'elles aient pu participer, comme auteurs ou complices, à la commission d'un crime, d'un délit ou d'une contravention (l'enregistrement des données concernant ces personnes peut intervenir, le cas échéant, après leur condamnation pour un crime ou délit) ou faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort ou de blessures, prévue par l'article 74 du Code de procédure pénale, ou d'une enquête ou d'une instruction pour recherche des causes d'une disparition inquiétante ou suspecte, prévue par les articles 74-1 et 80-4 du même code.

Des durées de conservation de 3 à 20 ans sont prévues. Les mineurs peuvent y être enregistrés. Les traitements ne font l'objet d'aucune interconnexion, aucun rapprochement ni aucune forme de mise en relation avec d'autres traitements ou fichiers. Ils ne peuvent être utilisés à des fins d'enquête administrative.

Les membres du groupe de contrôle n'émettent pas de remarques concernant ce traitement hormis la demande de la suppression de la mention « origine géographique » (art. 3). La DGGN confirme qu'elle supprimera cette mention.

Le 15 juin 2011, le directeur de cabinet du ministre de l'Intérieur indiquait au président du groupe de contrôle les éléments suivants :

« *À la suite de vos dernières interventions concernant le maintien de la mention « origines géographiques » dans le*

1 La DGGN a proposé à la DGPN de s'associer.

décret GIPASP, faisant suite à vos préoccupations exprimées dès 2009 pour le décret PASP, il me paraît utile de vous préciser que le ministère de l'Intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration confirme totalement les termes de la circulaire adressée aux préfets le 18 octobre 2009 [...] Il m'apparaît néanmoins que ce dispositif, qui avait permis de lever certaines de vos préoccupations, doit faire l'objet d'une correction afin d'éviter toute interprétation contraire à la volonté de l'exécutif et aux interprétations des juridictions et autorités administratives constitutionnelles.

Aussi, ai-je le plaisir de vous informer que j'ai demandé à mes services d'entamer les procédures visant à la modification des décrets PASP et GIPASP afin de sortir la mention « origines géographiques » des données sensibles et de ne permettre que l'enregistrement de données factuelles strictement limitées à l'origine géographique, au lieu de naissance, à la nationalité ou à la dénomination commune de la bande selon ses propres critères ».

Modification du fichier automatisé des empreintes digitales

Il s'agit d'une modification du FAED en vue de le mettre en conformité avec les dispositions du traité de Prüm.

Extraits du rapport au Premier ministre « Le Traité de Prüm, signé par l'Allemagne, l'Autriche, la Belgique, l'Espagne, la France, le Luxembourg et les Pays-Bas, le 27 mai 2005, et dont la ratification a été autorisée par la loi du 1er août 2007, vise à approfondir la coopération transfrontalière notamment dans les domaines du terrorisme, de la criminalité organisée et de l'immigration illégale.

Il prévoit notamment des échanges d'informations en matière d'empreintes dactyloscopiques, en instituant un mécanisme de consultations automatisées et réciproques entre les bases de données des États signataires. Le décret du 8 avril 1987, relatif au fichier automatisé des empreintes digitales (FAED) a été modifié en conséquence par le décret 2011-157 du 7 février 2011 [1].

1 Délibération CNIL no 2010-194 du 20 mai 2010.

D'autre part, le décret relatif au FAED ainsi modifié permet également l'application d'une disposition de la loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, entrée en vigueur le 1er octobre 2004. Celle-ci a en effet prévu, à l'article 28-1 du Code de procédure pénale, la faculté pour les agents de la douane judiciaire de recourir aux opérations de signalisation en vue de l'alimentation et de la consultation du FAED, telles que prévues par l'article 55-1 du même Code.

L'article premier du projet de décret ajoute les services des douanes exerçant des missions de police judiciaire à la liste des services pouvant recourir au traitement.

De même, l'article 2, ajoute les services des douanes judiciaires à la liste des services pouvant demander des opérations d'identification.

Après un article 3 décalant l'actuel article 9-1 du décret (qui devient l'article 9-3), l'article 4 introduit des articles 9-1 et 9-2 dont l'objet est de permettre les échanges d'informations avec des services de police étrangers sur le fondement du traité de Prüm ainsi que, le cas échéant, en vertu d'actes pris en application du traité sur l'Union européenne ou d'engagements internationaux ultérieurs. Ces dispositions ont été rédigées sur le modèle de celles ayant récemment modifié le Code de procédure pénale à propos du fichier national automatisé des empreintes génétiques (FNAEG)». Le décret modifiant le FAED a été publié au journal officiel du 9 février 2011.

Les membres du groupe de contrôle n'émettent pas de remarques concernant ce traitement.

Fichier national des interdits d'acquisition et de détention d'armes (FINADIA) [1]

Ce traitement a été créé par l'article L. 2336-6 du Code de la défense et a pour finalité la mise en œuvre et le suivi, au niveau national, des interdictions d'acquisition et de détention des armes en application du IV de l'article L. 2336-4 du Code de la défense.

Ce traitement ne comporte pas de données sensibles.

Les catégories de données à caractère personnel enregistrées dans ce fichier sont : état civil ; domicile ; profession ; catégorie ou type d'arme et de munition dont l'acquisition et la détention sont interdites ; date de l'inter-

1 Délibération CNIL nº 2010-455 du 9 décembre 2010.

diction ; fondement de l'interdiction ; date de levée de l'interdiction. La durée de conservation est de 20 ans à compter de la date de levée de l'interdiction.

Ce traitement est techniquement intégré dans l'application de gestion du répertoire informatisé des propriétaires et possesseurs d'armes (AGRIPPA) qui permet aux services de police d'avoir accès aux données relatives aux propriétaires d'armes lorsqu'elles sont soumises à déclaration ou autorisation. L'ouverture de l'accès à AGRIPPA étant effective depuis janvier 2010, il a été décidé d'abandonner dans les services de police le recours aux fichiers locaux d'armes qui n'étaient pas déclarés.

Les membres du groupe de contrôle n'émettent pas de remarques concernant ce traitement qui a été publié au Journal Officiel du 7 avril 2011.

Gestion des étrangers en situation irrégulière (GESI)

Ce fichier, géré par la préfecture de police, n'est pas un traitement d'ordre administratif mais un fichier de police judiciaire utilisé par les services de police pour assurer la gestion des dossiers en temps réel des 13 000 étrangers en situation irrégulière interpellés annuellement à Paris et dans les départements de la petite couronne, territoires sur lesquels la Direction centrale de la police aux frontières n'est pas compétente.

Compte tenu de la complexité des procédures mises en œuvre dans ce domaine spécialisé et du nombre des services de police concernés, GESI constitue un outil contribuant à rendre plus efficaces et rigoureuses les interventions des services de police en la matière, notamment s'agissant du respect des droits reconnus aux personnes interpellées lors des différentes étapes de la procédure (droit de se faire assister par un conseil, un interprète, examiner par un médecin, etc.).

Les membres du groupe de contrôle n'émettent pas de remarques concernant ce traitement hormis SOS Racisme qui ne souhaite pas approuver ce projet.

Exécution des services commandés pour la réalisation des transfèrements et extractions (ESCORTE)

Ce traitement a pour finalité la gestion des opérations de transfèrement ou d'extraction des personnes détenues. Il permet le suivi administratif et comptable de ces missions.

Examiné par la CNIL qui a rendu son avis le 25 novembre 2010[1] puis par le Conseil d'État, ce texte a été mis en point d'information du groupe de contrôle en mars 2011.

Fichier de la fraude documentaire et d'usurpation d'identité

Cadre juridique

Loi du 6 janvier 1978, article 26.

Finalités

Le traitement a pour finalités :
– de permettre l'enregistrement et la conservation des dossiers de fraude matérielle et d'usurpation d'identité par la section fraude documentaire du bureau de la nationalité et des titres d'identité et de voyage (BNTIV) en vue d'établir, le cas échéant, la réalité d'une fraude et d'en identifier la victime. Cette instruction permet de déterminer les suites à donner quant à l'opportunité d'une inscription dans le fichier des personnes recherchées (sous forme de « fiches TP » de retrait de document d'identité et/ou d'opposition à délivrance de titres) ;
– de permettre de renseigner, dans le cadre de leurs attributions légales et pour les besoins exclusifs de l'accomplissement de leurs missions, les personnels chargés des missions de recherche et de contrôle de l'identité des personnes, de vérification du respect des conditions de délivrance, de validité et d'authenticité des titres d'identité et de voyage au sein des préfectures et des postes consulaires ainsi que des services de la police et de la gendarmerie nationales

1 Délibération CNIL nº 2010-426 du 25 novembre 2010.

Lieu de mise en œuvre

Locaux du bureau de la nationalité et des titres d'identité et de voyage, DLPAJ.

Données à caractère personnel et informations pouvant figurer dans le traitement

• Dans le tableau de pilotage commun des dossiers :
– 1° l'identité mise en cause : nom, prénom, date et lieu de naissance, sexe ;
– 2° les références du dossier : autorité de saisine, dates de saisine, de clôture et dernière évolution, s'il a été rouvert, initiales du rédacteur le traitant, numéro du dossier ;
– 3° l'état du dossier : dates de la décision administrative, de l'inscription dans le FPR, du classement sans suite, nombre d'appels reçus suite au signalement dans le FPR et date du dernier appel ;
– 4° la nature du dossier : type de fraude (en distinguant usurpation, fraude matérielle et tentatives pour chaque) et caractéristiques de la fraude (nombre de personnes impliquées types de documents frauduleux utilisés *cf*. justificatifs d'état civil, de nationalité, de domicile litigieux et déclaration de perte/vol de titres).

• Dans les dossiers informatiques individualisés enregistrés sur le réseau sécurisé du ministère (avec accès restreint) :
– 1° la fiche de décision, synthèse du travail d'instruction réalisé par le rédacteur de la section fraude documentaire ;
– 2° la dernière version du tableau des titres demandés et/ou délivrés supportant un trombinoscope (sans dispositif de reconnaissance faciale) ;
– 3° le courrier de saisine initiale de la section fraude documentaire : par une préfecture, un poste consulaire, un particulier ;
– 4° les courriers émanant du bureau de la nationalité, des titres d'identité et de voyage : consultation, réponse à l'autorité de saisine, décision ayant donné lieu à l'inscription dans le FPR ;
– 5° les éléments officiels d'identification de la victime (exemple : jugement, procès-verbal d'audition de proches, compte rendu de production de pièces probantes) ;
– 6° les éléments relatifs à un éventuel contentieux administratif.

Durée de conservation

Les données à caractère personnel enregistrées dans le fichier sont conservées douze ans à compter de leur enregistrement (les titres sont valables 10 ans et peuvent être renouvelés pendant deux ans à compter de leur expiration sans qu'il soit à nouveau nécessaire de prouver son identité).

Cette durée est augmentée de cinq années, lorsque les données sont relatives à un titre obtenu frauduleusement et qui n'a pas pu être retiré à son détenteur par l'administration.

Accès au traitement

Les agents de la direction des libertés publiques et des affaires juridiques (section fraude documentaire et encadrement du BNTIV) peuvent avoir accès aux données.

Peuvent avoir communication des données en raison de leurs attributions légales : les services des préfectures ou des postes consulaires chargés de la délivrance des titres d'identité et de voyage ; les OPJ et APJ dans le cadre d'une procédure judiciaire ;et les magistrats ayant à connaître de l'affaire.

Information des personnes

En vertu du IV de l'article 32 et au 3e alinéa de l'article 38 de la loi informatique et libertés, les droits d'information et d'opposition ne sont pas applicables au présent traitement.

Droit d'accès

Conformément aux dispositions de l'article 40 de la loi informatique et libertés, le droit d'accès et de rectification s'exerce directement auprès du service gestionnaire du traitement (DLPAJ-BNTIV).

Interconnexions

Aucune interconnexion avec un autre traitement n'est prévue.

Les membres du groupe de contrôle n'émettent pas de remarques concernant ce traitement.

Chapitre 4

La polémique sur le «fichier MENS»

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

Le fichier de suivi des titres de circulation délivrés aux personnes sans domicile ni résidence fixe (FSDRF) a pour finalité le suivi des titres de circulation délivrés aux personnes circulant en France sans domicile ni résidence fixes, soumises aux dispositions de la loi nº 69-3 du 3 janvier 1969. Il a été créé par l'arrêté interministériel du 22 mars 1994 modifié par l'arrêté du 28 février 2005. Ce fichier a été déclaré à la CNIL qui a rendu un avis le 2 mars 1993 (nº 93-018)

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

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

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

Dans le cadre de sa démarche qualité, la gendarmerie nationale a finalement choisi de confier en mars 2011 l'administration de ce fichier administratif à une unité administrative (centre technique de la gendarmerie nationale).

Ce fichier a été recensé dans le cadre des travaux du groupe de travail sur les fichiers de police (rapports de janvier 2007 et de juin 2009) et du rapport parlementaire d'information nº 1548 de Delphine Batho et Jacques Alain Bénisti.

La mention « minorités ethniques non sédentaires » (MENS)

L'acronyme « minorités ethniques non sédentarisées » est usité au sein de la gendarmerie nationale depuis une étude sur la criminalité en date du 25 mai 1992 qui a fait l'objet d'une note, à diffusion restreinte, du bureau de la police judiciaire de la sous-direction Organisation Emploi. Cette note a été abrogée du mémorial de la gendarmerie dès fin 2010.

La gendarmerie nationale considère qu'elle n'a pas la paternité de ces appellations et qu'elle n'est pas la seule à faire usage de ce terme.

En gendarmerie, ce vocable a été utilisé pour faciliter le classement et l'échange d'informations et non pas pour constituer des fichiers d'étrangers ou de catégorie de citoyens.

Rappel des faits

Dans son édition du 8 octobre 2010, le quotidien *Le Monde* titrait « La gendarmerie utilise un fichier illégal qui vise les Roms et les gens du voyage ». Il mentionnait que la « gendarmerie avait constitué un fichier ethnique, baptisé « MENS », détenu par l'Office central de lutte contre la délinquance itinérante (OCLDI). Deux avocats défendant les principales associations des gens du voyage ont déposé plainte auprès du procureur de la République pour constitution de fichier non déclaré et conservation de « données à caractère personnel qui font apparaître les origines raciales et ethniques ».

Dans la même édition, le journal faisait état d'un document de présentation des missions de l'OCLDI (présentation *powerpoint*) mentionnant « une généalogie des familles tziganes ». Une autre page du même document recensait « les groupes à risques : gens du voyage (manouches, gitans) ; les équipes des cités ; les délinquants itinérants en provenance des pays de l'est (Roms),... ». Le même document indiquait également « un état numérique des interpellations de Roms (étrangers) par la gendarmerie de 2000 à 2004 ».

Par ailleurs, le quotidien *Le Monde* affirmait que « l'existence du fichier MENS était prouvée par nombre de documents internes à la gendarmerie. Ainsi, l'OCLDI, dans une fiche de travail sur les vols avec violences aurait annexé en pièce jointe un tableau *excel* « recensant des dossiers en cours, consultation fichier MENS, schéma relationnel ». Dans une autre note, selon *Le Monde*, la gendarmerie aurait écrit « l'environnement généalogique effectué par l'OCLDI à partir des procédures et des renseignements recueillies ainsi que la consultation de notre base documentaire de données (fichier MENS) permet d'indiquer que certains individus suspectés appar-

tiennent à la communauté française des gens du voyage... ». Dans un autre document, à destination d'un procureur de la République, il était fait état de la « consultation du fichier MENS ».

Sur le blog du journaliste du quotidien *Le Monde,* Franck Johannes[1] figurent notamment les diapositives de la présentation *power-point* résumant les missions de l'OCLDI et sur lesquels figurent les mentions « *généalogie des familles tsiganes* » ou encore un tableau sur l'état numérique des interpellations de Roms (étrangers) effectuées par la gendarmerie. Par ailleurs, il reproduit des fac-similés d'une note interne à la gendarmerie nationale mentionnant « consultation fichiers MENS », d'une fiche de travail de l'OCLDI indiquant « consultation et recoupements à partir du fichier MENS de l'OCLDI » ou encore d'une note adressée à un procureur de la République sur laquelle figure « Consultation des fichiers SDRF sur les titres de circulation et fichier MENS (OCLDI) sur les liens de famille (généalogie), environnements patrimoniaux des personnes précitées. »

Dans un communiqué du 7 octobre 2010, le cabinet du ministre de l'Intérieur, de l'Outre-mer et des Collectivités territoriales précisait qu'il n'avait pas connaissance d'un tel fichier et que le fichier généalogique, alors détenu par l'OCLDI, avait été supprimé le 13 décembre 2007, conformément aux obligations de la loi. Il précisait également qu'une note de la gendarmerie nationale, en date du 25 mai 1992, faisait référence à la notion de « minorités ethniques non sédentarisées ». Enfin, il indiquait que, dès qu'il a eu connaissance de ces différentes informations et dans un souci de totale transparence, le ministère de l'Intérieur – qui rappelle que la gendarmerie nationale ne lui a été rattachée qu'à compter de la loi du 3 août 2009 – a demandé au groupe de contrôle et de l'organisation des bases de données de la police et de la gendarmerie, présidé par Alain Bauer, de procéder à un contrôle des éléments recueillis dans les bases de données de la gendarmerie nationale.

La Commission nationale de l'Informatique et des libertés (CNIL), autorité compétente pour mener le contrôle d'une base de données personnelles, a débuté vendredi 8 octobre ses contrôles dans les locaux de la gendarmerie nationale. Les opérations de contrôle sur place et sur pièce ont permis de conclure à l'existence d'une base de données mise en œuvre par l'office au regard de sa mission de renseignement et de coordination prévue par son décret de création. **Ils ont également permis de conclure que l'OCLDI ne disposait pas de fichier à caractère ethnique.**

La CNIL et le Groupe de contrôle ont échangé durant cette période.

Le mercredi 13 octobre, le général Mignaux a été auditionné avec Laurent Touvet, directeur des libertés publiques et des affaires juridiques par la commission des Lois de l'Assemblée nationale.

1 http ://libertes.blog.lemonde.fr/2010/10/07/le-fichier-des-roms-du-ministere-de-linterieur/

Selon la Direction générale de la gendarmerie nationale

L'OLCDI ne possède plus de fichier de généalogie. Une base de donnée, intitulée « généatic », avait été créée en 2000 pour faciliter le travail de la cellule interministérielle chargée de la lutter contre la délinquance itinérante (CILDI prédécesseur de l'OCLDI). Le responsable de la cellule avait acheté un logiciel de généalogie pour constituer des schémas généalogiques et des présentations des environnements des délinquants. En 2006, l'amélioration de la remontée de l'information judiciaire par le traitement JUDEX a rendu cet outil inutile et qui apparaissait par ailleurs juridiquement difficile à régulariser. La gendarmerie a alors décidé de supprimer cette base de données par une note en date du 13 décembre 2007, en raison de sa non-conformité avec la loi informatique et libertés du 6 janvier 1978.

À l'OCLDI, les informations nécessaires à l'office sont enregistrées dans une base de données temporaire de travail appelé « base OCLDI », hébergé sur un serveur du STRJD depuis décembre 2007. Seule une quinzaine d'analystes, au regard des quelque 200 000 enquêteurs de police et de gendarmerie, sont en capacité d'effectuer des requêtes dans cette base de données afin de satisfaire tant aux demandes des enquêteurs de terrain que des magistrats.

Cette base de données conserve une trace des demandes adressées par les unités, ce qui permet notamment le rapprochement de faits identiques et d'alerter les services d'enquête territoriaux. Elle fournit également des éléments statistiques pour définir des plans de lutte contre les phénomènes de délinquance itinérante qui évoluent sans cesse.

Cette base de données comprend l'ensemble des informations relevant des domaines de compétences de l'OCLDI, informations transmises par les unités de gendarmerie, les divers services partenaires (police nationale, administration fiscale, douane) et recueillies dans le cadre de procédure judiciaire.

Ces données sont issues des différentes bases judiciaires et des messages opérationnels transmis par les unités ou administrations.

Lors de la constitution de cette base documentaire, la gendarmerie s'est interrogée sur le statut juridique de ces données qui ne constituent pas un fichier d'antécédents contrairement aux applications STIC et JUDEX, mais participent de la prévention et recherche d'infractions pénales.

Les délais pris dans l'adoption de la LOPPSI depuis 2007 expliquent la situation actuelle d'une base de données au statut juridique imprécis.

Conclusions du rapport définitif de la CNIL après les contrôles effectués auprès de la gendarmerie nationale dans le cadre du fichier « MENS »

CNIL.

A l'attention de Monsieur le Premier Ministre

CONCLUSIONS DEFINITIVES DES CONTROLES EFFECTUES LES 8, 12 ET 14 OCTOBRE 2010 AUPRES DE L'OCLDI ET DU STRJD DE LA GENDARMERIE NATIONALE

Le 14 octobre 2010, je vous ai adressé les conclusions du rapport préliminaire des contrôles effectués par mes services dans le cadre de l'instruction d'une plainte relative à l'existence supposée d'un fichier dénommé « MENS » détenu par la gendarmerie nationale.

Ces conclusions peuvent, aujourd'hui, être complétées par les constatations effectuées lors d'un contrôle complémentaire qui s'est déroulé le 14 octobre dernier au service technique de recherches judiciaires et de documentation (STRJD) et de l'analyse des différents documents copiés à l'occasion des contrôles menés par notre Commission, dont les derniers ont été reçus du STRJD le 9 novembre 2010.

I. Les traitements mis en œuvre au sein de l'office central de lutte contre la délinquance itinérante (OCLDI)

1. Comme le relevaient nos conclusions préliminaires, l'OCLDI met en œuvre une base documentaire ayant pour finalité la collecte, l'enregistrement, l'organisation, la conservation, la consultation, la communication par transmission et le rapprochement d'informations relatives aux personnes impliquées dans la délinquance itinérante. Cette base documentaire contient des données à caractère personnel, lesquelles ne laissent pas apparaître l'origine ethnique des personnes qui y figurent. Les investigations complémentaires réalisées ne remettent pas en cause cette affirmation.

L'examen complet des données contenues dans cette base n'a pas, non plus, révélé la présence de données excessives.

Pour autant, aucune durée de conservation des données n'a été définie, en méconnaissance de la loi du 6 janvier 1978 modifiée.

Notre Commission souhaite également rappeler que ce traitement n'a pas fait l'objet des formalités préalables prévues par la loi. Compte tenu des constats effectués lors du contrôle, ce traitement, qui a pour objet la prévention et la recherche d'infractions pénales, doit, conformément aux dispositions de l'article 26-I 2° de la loi « informatique et libertés », être autorisé par arrêté du ministre de l'intérieur, pris après avis motivé et publié de notre Commission.

Commission Nationale de l'Informatique et des Libertés
8 rue Vivienne CS 30223 75083 PARIS Cedex 02 - Tél: 01 53 73 22 22 - Fax: 01 53 73 22 00 - www.cnil.fr
RÉPUBLIQUE FRANÇAISE

2. Les contrôles réalisés n'ont pas conduit à constater l'existence d'une base relative à la généalogie de certaines catégories de personnes particulièrement connues de la gendarmerie nationale.

3. Ces contrôles ont mis à jour les pratiques suivantes :

L'OCLDI utilise, dans le cadre de la coopération policière internationale, un outil d'échange de messages dénommé « CONTINEO » qui contient des données à caractère personnel. Il permet d'enregistrer les documents relatifs aux échanges s'inscrivant dans le cadre de la coopération policière internationale qui peuvent faire référence aux nom et prénom d'un délinquant itinérant et a donc pour objet de faciliter la constatation des infractions commises par les délinquants itinérants.

Ce traitement n'a pas fait l'objet des formalités préalables prévues par la loi auprès de notre Commission.

Ce traitement relève ainsi, en première analyse, des dispositions de l'article 26 I. 2° de la loi « informatique et libertés » et doit, à ce titre, faire l'objet d'un arrêté du ministre de l'intérieur, pris après avis motivé et publié de notre Commission qui devra, en outre, mentionner le transfert de données lié à la coopération policière internationale.

Comme nous l'avons relevé dans nos conclusions préliminaires, l'OCLDI utilise également le logiciel ANACRIM, lequel n'a pas non plus été déclaré à ce jour auprès de notre Commission. Il relève également des formalités prévues à l'article 26 I. 2° de la loi « informatique et libertés », à savoir un arrêté du ministre de l'intérieur, pris après avis motivé et publié de notre Commission.

II. Le traitement du « renseignement » relatif aux « gens du voyage » au sein de la gendarmerie nationale

Notre rapport préliminaire concluait que la fonction de « renseignement » de la gendarmerie nationale ignore largement la loi « informatique et libertés ». Les investigations complémentaires effectuées tant auprès de l'OCLDI que du STRJD confirment cette première conclusion.

En effet, le STRJD et l'OCLDI sont destinataires de données à caractère personnel relatives aux « gens du voyage », qui leur sont transmises, le plus souvent par message électronique, par les unités territoriales (comptes rendus de contrôles d'identités effectués dans les campements, rapports adressés à la suite de la commission d'une infraction et/ou de l'interpellation d'un ou plusieurs membres de la communauté des « gens du voyage »).

Cette transmission d'informations ne s'inscrit pas dans un cadre garantissant le respect des dispositions légales relatives à la protection des données à caractère personnel.

Ainsi, la nature des informations transmises est laissée à l'appréciation des unités locales.

Elles communiquent, la plupart du temps, les nom, prénom, date et lieu de naissance, numéro de carnet de circulation, commune de rattachement, lieu du contrôle, date de l'installation et du départ éventuel ou prévu du campement, immatriculation des véhicules et nom de leurs propriétaires, photographies éventuellement prises à l'occasion de ces contrôles, etc.

Cette liberté d'appréciation les conduit également à communiquer des données non pertinentes (précédentes condamnations) voire susceptibles de révéler les origines ethniques des personnes concernées (présence ponctuelle des mentions « MENS », « roms », « tzigane » ou encore « gitan »).

De plus, les destinataires finaux de ces messages au sein de l'OCLDI, mais surtout du STRJD, peuvent, librement, décider de les détruire ou de les conserver.

Lorsque ces messages sont conservés par leurs destinataires, la Commission considère que cette centralisation de données doit s'analyser comme un seul et même traitement ayant pour finalité le recueil de renseignements susceptible de fonder un travail de rapprochement criminel sur les « gens du voyage ».

Le traitement ainsi mis en œuvre n'a par ailleurs fait l'objet d'aucune des formalités prévues par la loi.

La direction générale de la gendarmerie nationale nous a, certes, déclaré, le 27 septembre dernier - soit avant les contrôles effectués - sa future « base de donnée de sécurité publique ». Toutefois, le dossier de formalités laisse apparaître que ce traitement sera mis en œuvre par la section du système des opérations et du renseignement dans un cadre purement administratif, et ne concerne donc pas le traitement dont la mise en œuvre a été constatée lors des contrôles effectués.

Les formalités à accomplir relèveraient, a priori, de l'article 26-II de la loi « informatique et libertés » (décret en Conseil d'État pris après avis motivé et publié de la Commission), dès lors que sont traitées des données à caractère personnel qui font apparaître, directement ou indirectement, les origines ethniques des personnes.

Si toutefois la gendarmerie nationale supprimait de ce traitement des données qui font apparaître, directement ou indirectement les origines ethniques des personnes, elle pourrait procéder par arrêté du ministre de l'intérieur pris après avis motivé et publié de notre Commission en application de l'article 26-I 2° de la loi « informatique et libertés ».

Les contrôles ont également permis de constater l'absence de durée de conservation des données traitées et il conviendra, par conséquent, qu'elle soit définie à l'occasion de l'accomplissement des formalités préalables.

III. L'accès de l'OCLDI et du STJRD au SDRF

La CNIL a constaté la possibilité, offerte à l'OCLDI et au STRJD, de consulter, en accès libre, le fichier de suivi des titres de circulation délivrés aux personnes sans domicile ni résidence fixe (SDRF).

Or, ce fichier a une finalité purement administrative. Les personnels de la gendarmerie nationale ne sont destinataires des informations qui y sont contenues que dans le cadre de cette finalité.

Le fichier SDRF ne saurait donc être consulté par les services à vocation judiciaire que sont l'OCLDI, office central de police judiciaire, et le STRJD, service technique de recherches judiciaires et de documentation, que dans l'hypothèse où ces derniers justifient d'une demande expresse de l'autorité judiciaire. Par conséquent, cette consultation du SDRF par l'OCLDI et le STRJD, peut être considérée comme constituant un détournement de finalité.

IV. Conclusions

1. Lors des contrôles menés auprès de l'OCLDI et du STRJD, et l'exploitation des documents et pièces copiés à cette occasion, notre Commission n'a pas constaté l'existence d'un fichier structuré et pérenne regroupant des données à caractère personnel de nature ethnique visant, en particulier, les « gens du voyage ».

2. Notre Commission a constaté une méconnaissance des obligations issues de la loi du 6 janvier 1978, modifiée le 6 août 2004, lors du traitement par la gendarmerie nationale de données concernant cette catégorie de population dans le cadre de ses activités de renseignement. Il lui appartient donc de définir un cadre précis à cette mission de renseignement, judiciaire ou administratif, permettant de déterminer notamment la nature des données qui peuvent être traitées, leur condition de traitement et leur durée de conservation en procédant aux formalités préalables requises par la loi.

Ce travail, engagé en ce qui concerne le renseignement administratif, devra être poursuivi et approfondi afin que les pratiques observées actuellement par la gendarmerie en matière de renseignement à vocation judiciaire respectent les principes posés par la loi, notamment en termes de proportionnalité des données et de durée de conservation.

Alex TÜRK
Président de la CNIL

Alex Türk

Le 25 NOV. 2010

Les recommandations du groupe de travail

Le groupe de travail sur l'amélioration du contrôle et de l'organisation des fichiers de police et de gendarmerie qui s'est réuni le 18 octobre 2010 constate :

• Que le fichier de suivi des titres de circulation délivrés aux personnes sans domicile ni résidence fixe (FSDRF), fichier de nature exclusivement administrative, a été régulièrement déclaré et créé par l'arrêté du 22 mars 1994 (modifié par l'arrêté du 28 février 2005).

• Que la mention « Minorités ethniques non sédentarisées » (MENS) existe depuis une circulaire à diffusion restreinte du 24 mai 1992 (circulaire nº 1400 DEF/GEND/OE/PJ/DR) ayant pour objet « Étude sur la criminalité au sein de certaines minorités ethniques non sédentarisées », circulaire désormais supprimée dès le 22 octobre, par une note du DGGN prohibant définitivement l'appellation MENS.

• Qu'il n'existe pas de fichier « Minorités ethniques non sédentarisées » (MENS) en tant que tel.

• Qu'il existe en revanche, au sein de l'OCLDI, une base documentaire, pour laquelle le contrôle de la CNIL a permis de préciser qu'il s'agissait bien d'un traitement de données à caractère personnel n'ayant pas été déclaré, mais ne comprenant aucune donnée relative aux origines ethniques des personnes.

• Que de même, il n'existe au sein du STRJD aucun fichier structuré regroupant des données à caractère personnel relatives aux « Roms » et organisé autour de cette notion, mais des remontées d'informations constituant un traitement de données personnelles, certaines informations enregistrées utilisant l'acronyme MENS n'ayant pas été déclarées.

• Que des dossiers, ne constituant pas un traitement automatisé, portant la mention « fichiers MENS » ont bien été identifiés dans les serveurs de l'OCLDI.

• Que ce traitement a été constitué dans le cadre d'une base de travail liée à des enquêtes ou des analyses justifiées par les missions et les compétences de l'OCLDI mais ne respectant pas la législation en vigueur durant cette période et notamment l'obligation de déclaration d'un tel dispositif au regard des dispositions de la loi de 1978.

• Que diverses bases de travail, notamment judiciaires, n'ont pas été systématiquement déclarées par certains services centraux par ignorance des obligations légales s'imposant pour la constitution d'un sous-fichier ou d'une base de travail alors même que les finalités mentionnées lors de la création du fichier « source » ne couvraient ces développements.

• Que des présentations publiques faites par des représentants de l'OCLDI montrent que des éléments d'analyse utilisant l'outil « généalogie » du fichier concerné entre 2000 et 2007 n'ont pas respecté la législation.

• Que le ministère de l'Intérieur, de l'Outre-mer et des Collectivités territoriales indique, dans son communiqué du 7 octobre, que le fichier dénommé GENEATIC, alors détenu par l'OCLDI (faisant suite à la CILDI), avait été supprimé en décembre 2007 alors même que ce traitement n'avait pas fait l'objet d'un recensement lors des travaux du groupe de travail de l'année 2006.

Le groupe de travail des fichiers de police et de gendarmerie recommande donc au ministre de l'Intérieur, de l'Outre-mer et des Collectivités territoriales de :

• Procéder à la mise en conformité des bases de travail non déclarées et non conformes à la législation du 6 janvier 1978 sur l'informatique et les libertés qui ne l'auraient pas encore été à ce jour, ce qui implique la suppression des éléments irréguliers et la conception de nouvelles bases de données conformes aux règles juridiques issues de la législation actuelle ainsi que, si nécessaire, de la LOPPSI lorsque celle-ci aura été promulguée.

Cette préconisation a été mise en œuvre et est toujours en cours.

• S'assurer de la suppression effective de la mention « MENS » de tous les documents encore utilisés au sein des unités et des services centraux de la gendarmerie nationale, comme s'y est engagé le directeur général de la gendarmerie nationale, et déclarer conformément à la législation tous les outils d'analyse et de rapprochement nécessaires à la lutte contre la délinquance itinérante à partir de données personnelles.

Cette préconisation a été mise en œuvre.

• Rappeler, par une circulaire générale, à l'ensemble des services de la police et de la gendarmerie nationale la législation en vigueur en matière de création de traitements de données à caractère personnel.

Cette préconisation a été mise en œuvre.

• Se rapprocher dans les meilleurs délais de la CNIL en vue de la mise en œuvre de ces mesures.

D'une manière générale, le groupe de travail sur l'amélioration du contrôle et de l'organisation des fichiers de police et de gendarmerie recommande au ministre de l'Intérieur, de l'outre-mer et des collectivités territoriales de :

• Faire procéder au recensement de toutes les bases de travail, notamment judiciaires, extensions de fichiers déclarés, mais qui, en tant que telles, n'auraient pas fait l'objet d'une déclaration spécifique.

Cette préconisation a été mise en œuvre.

• Procéder, dans les meilleurs délais et dès l'instant où ses bases répondent à un réel besoin opérationnel à partir de faits ou d'éléments sériels, à la déclaration de ces bases de travail selon la législation afférente.

Cette préconisation a été mise en œuvre.

Par ailleurs, le groupe de travail sur l'amélioration du contrôle et de l'organisation des fichiers de police et de gendarmerie rappelle :

• Qu'il souhaite que soit engagée avant la fin 2010 la destruction physique et informatique des fichiers FAR et FPNE tel que cela a été acté lors de la réunion du groupe de travail le 6 septembre 2010 (destruction totale sauf pour 4 brigades pour le FAR et pour 1 lettre pour le FPNE suivant les recommandations des Archives Nationales)[1].

Cette préconisation a été mise en œuvre.

• Que la mention « origines géographiques » soit supprimée du fichier Prévention des Atteintes à la Sécurité Publique (PASP) tel que cela a été recommandé lors des réunions du 10 novembre 2009 et 22 juin 2010.

Cette préconisation a été prise en compte (voir supra).

1 Destruction effective. Voir ci-après.

Chapitre 5

Les suites réservées aux recommandations 2008 du groupe de travail

1. Institutionnaliser le groupe de contrôle sur les fichiers de police et de gendarmerie

Les récents débats suscités par la création du fichier EDVIGE ont montré à quel point la question des fichiers de police et de gendarmerie, de leur contrôle et de leur modernisation était particulièrement sensible, notamment au regard de leurs conséquences sur les libertés individuelles et collectives. En 2006, déjà, lors de la mise en place du premier groupe de travail sur l'amélioration du contrôle de l'utilisation des fichiers STIC et JUDEX dans le cadre des enquêtes administratives, les questions inhérentes au développement de ces fichiers avaient été soulevées et avaient fait l'objet d'échanges passionnés.

La prévention et la répression des crimes et délits nécessitent des outils adaptés et modernes permettant à la police et à la gendarmerie de lutter plus efficacement contre la criminalité et le terrorisme. Toutefois, de tels systèmes ne peuvent être créés et utilisés que dans un cadre strictement défini par la loi et la réglementation et pour une finalité conforme aux principes de proportionnalité et de garantie des libertés individuelles et collectives. Par ailleurs, il est indispensable que la mise en œuvre de tels dispositifs soit comprise et acceptée par l'opinion publique et que tout fichier de police ou de gendarmerie nouvellement créé ou modernisé de façon substantielle fasse l'objet d'une présentation et d'une concertation préalable.

Le groupe de contrôle recommande l'institutionnalisation de ses réunions et propose qu'il puisse se réunir, une fois par trimestre, en vue d'analyser les suites réservées aux préconisations de son rapport et toute évolution substantielle liée à la création ou au développement des fichiers de police et de gendarmerie.

Il souhaite également que le CNIL puisse assurer l'ensemble des prérogatives qui lui sont dévolues par la loi et les textes réglementaires sachant que le groupe de contrôle n'a pas vocation à examiner, ni les conditions de mise en œuvre du droit d'accès, ni les fiches individuelles enregistrées dans les traitements automatisés de données nominatives. Il exerce de ce fait une mission technique différente et complémentaire.

L'arrêté du 20 octobre 2009 porte création d'un groupe de travail sur l'amélioration du contrôle et de l'organisation des bases de données de police (et de gendarmerie).

2. Fournir à la population une information pédagogique sur ces fichiers

En vue de lutter contre les idées fausses et de « renforcer l'acceptabilité des fichiers au sein de la population », une campagne d'information pédagogique visant le grand public, en particulier les jeunes, doit être envisagée. La création d'un site Internet dédié, à l'instar du site Cyberbudget réalisé par le ministère du budget sur un domaine pourtant plus austère, semble à cet égard intéressante.

Ce site pourrait mettre à disposition :
– des animations ou infographies illustrant l'utilité concrète des fichiers de police et/ou de renseignement et les garanties offertes pour la protection des libertés ;
– un jeu de simulation permettant de prendre virtuellement les commandes d'un fichier de police pour mener une enquête (tout en en subissant les contraintes juridiques) ;
– des éléments de comparaison internationale permettant de relativiser la situation française pour les principaux fichiers de police et/ou de renseignement.

Le groupe de contrôle recommande la réalisation d'une campagne d'information sur les fichiers de police et de gendarmerie et la création d'un site internet public visant à mieux expliquer l'utilité et les conditions d'utilisation de tels dispositifs. En accord avec la CNIL, il souhaite également qu'en cas de création d'un tel site une information sur le droit des personnes à l'égard de ces fichiers soit clairement mentionnée.

La mise en œuvre de cette recommandation relève du ministère de l'Intérieur.

La DGPN a mis en ligne sur son intranet des informations et de la documentation relatives aux fichiers de police mais celles-ci ne sont accessibles qu'à ses seuls services.

3. Définir les modalités de destruction, d'archivage et de transfert des fichiers

La création, le développement ou la modernisation de nouvelles bases de données ou applications bureautiques entraînent automatiquement l'abandon de fichiers plus anciens. C'est pourquoi, dans ce cadre, il est nécessaire de fixer les modalités de destruction, d'archivage ou de transfert des informations contenues dans les fichiers devant faire l'objet d'un abandon.

Le groupe de contrôle recommande la mise en place d'un groupe de travail, placé sous la responsabilité de la Direction des archives nationales, et chargé de proposer le cadre légal et pérenne des modalités de destruction d'archivage et de transfert des données enregistrées dans des fichiers de police et de gendarmerie devenus obsolètes.

Le ministère de l'Intérieur a demandé au ministère de la Culture de lui désigner un expert chargé de cette mission. La chef de l'inspection générale des archives de France ayant été désignée pour conduire cette mission, le ministre de l'Intérieur lui a adressée le 4 décembre 2008 une lettre de mission en ce sens.

Par lettre du 4 décembre 2008, le ministre de l'intérieur a confié à l'Inspection générale des archives de France, la mission de définir les « règles de tri, d'archivage et d'exploitation des données ». Suite à ce rapport, la Direction des libertés publiques et des affaires juridiques a indiqué que seuls les trois fichiers de la gendarmerie nationale concernés (FAR, FPNE et le fichier de la batellerie) avaient fait l'objet d'une étude. Pour le fichier de la batellerie, compte tenu de son intérêt historique, il sera conservé dans sa totalité et transmis aux Archives de France au printemps 2011. Pour les fichiers FAR et FPNE, considérant l'opportunité de conserver des « témoins » des méthodes de travail de la gendarmerie, il a été proposé, pour le FPNE de garder un échantillon de toutes les fiches commençant par la lettre « B » de l'alphabet (tirée au sort). Les opérations de destructions du FPNE sont toujours en cours et s'achèveront en juin 2011. Pour le FAR, il a été proposé de conserver les fiches de quatre brigades territoriales comme éléments de témoignage des méthodes de travail des gendarmes (COLMAR, LUNEL, GUJAN-MAESTRAS et PLOERMEL). Toutes les autres fiches (près de 60 millions) ont été détruites au 3 mars 2011.

Concernant les anciennes fiches du fichier des renseignements généraux, un premier tri, achevé, a été effectué afin de les répartir entre les trois directions et services qui ont repris les compétences de l'ancienne DCRG : la Direction centrale du renseignement intérieur, le service central des courses et jeux de la DCPJ et la sous-direction de l'information générale de la DCSP. Concernant cette dernière sous-direction, toutes les anciennes fiches des services centraux qui n'entrent pas dans le cadre défini par les décrets du 16 octobre 2009 ont été d'ores et déjà versées aux archives nationales conformément à la réglementation en matière d'archives ; quant aux services territoriaux, ce tri est en cours et un tiers environ des anciennes fiches qui n'entrent plus dans le cadre réglementaire actuel ont été versées aux archives nationales au 1er avril 2011.

4. Intégrer la démarche qualité

Au cours des années, la CNIL a affiné ses pratiques et exigé le bénéfice d'une vision plus précise du fonctionnement des traitements soumis à son avis au point d'accompagner ses avis de recommandations très précises quant à leur utilisation opérationnelle. Les textes réglementaires visant à garantir le respect de telles recommandations portant création des fichiers sont encore perfectibles.

Face à des exigences de plus en plus précises du fonctionnement des traitements soumis à la validation de la CNIL, il apparaît nécessaire d'instaurer une démarche qualité qui, assortie aux exigences juridiques, permet un maillage plus fin de normes d'administration et d'utilisation des fichiers. Cette démarche bénéficierait également à la performance opérationnelle par l'élaboration d'un schéma directeur clarifiant l'architecture des flux d'informations propres à la police et à la gendarmerie nationales ainsi que les flux mutualisés entre ces institutions.

Le groupe de contrôle recommande l'instauration d'une démarche qualité visant à définir plus précisément les modalités d'usage des fichiers de police et de gendarmerie.

Voir la partie spécifique du présent rapport d'activités.

5. Désigner un expert « informatique et libertés » au sein des services de police et de gendarmerie

La nécessité de toujours veiller à l'équilibre entre protection des libertés, respect de la législation et nécessité de doter les services de la police nationale et les unités de la gendarmerie nationale de systèmes d'aide à l'enquête adaptés et modernes impliquent une meilleure prise en compte de l'environnement technologique et réglementaire.

Des personnels ressources, spécialisés sur les questions « informatique et libertés », pourraient être mis en place au sein des services opérationnels de la police et de la gendarmerie. Ces experts auraient d'abord pour mission de diffuser une « culture informatique et libertés » dans les services opérationnels, qui manquent souvent de connaissances dans ce domaine alors même que le fichier est un des outils de travail fondamentaux des policiers et des gendarmes. Mieux au fait des contraintes juridiques mais aussi de leur raison d'être et de leur intérêt pour eux-mêmes, les services de police et les unités de gendarmerie seraient mieux à même de les prendre en compte dès l'expression d'un besoin opérationnel, alors qu'actuellement le droit des fichiers constitue davantage une contrainte exogène et assez abstraite, que le service a parfois tendance à ne prendre en compte qu'au dernier moment. Dès lors, le risque de voir se constituer des fichiers « sauvages » serait fortement réduit, de même que le risque de se rendre compte trop tard qu'un traitement ne répond pas aux contraintes liées au droit des fichiers (dossier de consultation, traçabilité, exercice du droit d'accès, etc.).

Au titre de cette mission, les experts, spécialement formés à la législation sur les fichiers, seront notamment chargés :
– de former les services opérationnels par des actions de formation ponctuelles ;
– de conseiller les services opérationnels quant à l'opportunité de déployer au niveau local des projets de fichier et quant au cadre juridique et à l'architecture les plus adaptés ;
– d'assister les services lors de l'élaboration du dossier de déclaration ;
– d'être les interlocuteurs, au sein de leur service, de l'administration centrale qui disposera ainsi de relais plus efficaces ;
– de permettre des échanges d'expériences entre services.

L'action de ces experts permettra de mieux identifier les petits fichiers mis en œuvre localement (comme ceux constitués par les DDSP sur les fourrières, les débits de boissons, les objets volés ou les procurations de vote) et ainsi de les déclarer de manière cohérente et ordonnée à la CNIL.

Ces experts devront avoir une position hiérarchique suffisamment élevée pour avoir l'autorité nécessaire au sein de leurs services (par exemple : un commissaire ou un commandant dans chaque DDSP et un officier dans chaque groupement de gendarmerie), le cabinet du DGPN et du DGGN restant bien entendu le seul interlocuteur de la DLPAJ et celui de la préfecture de police pour les fichiers qu'elle met en œuvre.

Le groupe de contrôle recommande au ministère de l'Intérieur de désigner au sein de chaque service opérationnel de police et de gendarmerie un expert « informatique et libertés ». Il recommande que les missions de ces experts soient précisées par une circulaire commune du DGPN et du DGGN. En accord avec les recommandations de la CNIL, il conviendra de clarifier le rôle de ces experts et contrôleurs par rapport à celui des correspondants à la protection des données à caractère personnel, tels que définis à l'article 22 de la loi du 6 janvier 1978, et dont le groupe propose la création au sein des directions générales de la police et de la gendarmerie.

La Direction générale de la gendarmerie nationale a mis en place, depuis le mois d'octobre 2008, une mission permanente de suivi des systèmes d'information (MPSSI) pilotée par le magistrat délégué auprès du DGGN, épaulé par un référent national « informatique et libertés ». Cette structure anime un réseau de correspondants fonctionnels et techniques placés au sein des services et sous-directions (22 référents centraux « informatique et libertés » et 31 référents territoriaux, ces derniers ayant été désignés fin 2010). Ce dispositif répond à l'organisation de la gendarmerie dans le domaine des fichiers qui repose sur une forte centralisation permettant un contrôle permanent des applications installées sur les postes de chaque militaire. Par ailleurs, aucun traitement ne peut être développé au niveau local sans une validation par l'administration centrale.

Quant à la Direction générale de la police nationale, elle a mis en place un vaste réseau de conseillers « informatique et libertés » (CIL). Depuis novembre 2010, ce sont plus de 180 CIL qui ont été désignés dans les services centraux et territoriaux de la police nationale.

Ces CIL recevront une formation spécifique en droit des fichiers au cours des 2e et 3e trimestres 2011. Leur rôle a été précisé lors d'une journée d'information en présence du Directeur général de la police nationale, du Président du groupe de travail sur l'amélioration du contrôle des fichiers de police et de gendarmerie et de l'ensemble des directeurs centraux de la police nationale.

Les objectifs sont : de mieux identifier les petits fichiers mis en œuvre localement et ainsi de les déclarer de manière cohérente et ordonnée à la CNIL ; de conseiller les services opérationnels quant aux moyens, à l'opportunité et au cadre juridique du déploiement des projets de fichiers, au niveau local ou au niveau central ; d'assister les services lors de l'élaboration d'un dossier de déclaration et de permettre des échanges d'expériences entre les services.

---

6. Recourir systématiquement aux déclarations-cadres pour faciliter l'action des services de police et de gendarmerie et améliorer la cohérence des outils opérationnels

Dans le cadre du recensement des fichiers de police engagé par la DGPN au titre de leur mise en conformité avec les dispositions introduites en 2004 dans la loi du 6 janvier 1978, il a été constaté que de nombreux services de police locaux mettaient en œuvre les mêmes catégories de fichiers (fourrières, objets trouvés, etc.). Bien que poursuivant une finalité identique, ces traitements ne suivent pas toujours la même architecture technique ni par conséquent les mêmes règles de sécurité des données.

Ces initiatives dispersées ont trois autres inconvénients majeurs :
– elles multiplient le risque de voir se constituer des fichiers « sauvages » ;
– elles entraînent une forte déperdition de moyens, chaque service travaillant à mettre en place son propre système ;
– elles ne profitent pas aux autres services parce qu'elles ne peuvent pas être révélées pour être généralisées lorsqu'elles le méritent.

Le groupe de contrôle propose donc au ministère de l'Intérieur de recourir systématiquement aux procédures de « déclarations-cadres » prévues par la loi « informatique et libertés » aux termes du IV de l'article 26 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés qui permet au gestionnaire du traitement de déclarer sur la base d'une déclaration unique des fichiers répondant aux mêmes finalités, portant sur les mêmes catégories de données et ayant les mêmes destinataires.

Cette modalité de déclaration unique des traitements à la CNIL permettra d'améliorer le respect des exigences légales et de réduire d'autant les pratiques clandestines. Elle favorisera également la mise en œuvre d'architectures techniques uniformisées, offrant ainsi les mêmes garanties.

En lien avec la Direction des libertés publiques et des affaires juridiques, la Direction générale de la gendarmerie nationale adhère progressivement aux projets de déclarations-cadres établis par la police nationale, à l'exemple du suivi des contrôles judiciaires, du suivi des assignés à résidence, du suivi des permissions de sortir, du suivi des débits de boisson...

Indépendamment des présents projets de déclarations-cadres et outre les déclarations en cours ou en projets déjà mentionnées dans le présent rapport (supra ou infra), la DGGN réfléchit aussi aux thématiques suivantes (déclarations-cadres ou uniques) : bases criminalistiques départementales, procès-verbal électronique (sécurité routière), application de stockage des procédures clôturées (ASPC), bandes violentes, homicides non résolus, identification des victimes de catastrophes, fraude documentaire, escroqueries, etc.

À la suite du recensement national des fichiers existant au sein des services de police engagés par le cabinet du Directeur général de la police nationale dès l'été 2008, et conformément à la recommandation nº 6, plusieurs projets de déclarations-cadres permettant de régulariser par blocs les fichiers mis en œuvre dans les services et ayant une même finalité ont été préparés. Certains de ses projets ont déjà été présentés à la CNIL, d'autres le seront prochainement. Ces projets concernent notamment : la gestion des véhicules immobilisés et des fourrières ; les procurations de vote ; les débits de boissons, le contrôle de l'accès aux locaux par le recours à des moyens biométriques, les contrôles judiciaires, les assignations à résidence, les permissions de sortir ou encore la gestion des « appels à témoins ».

7. Définir des référentiels communs

Afin d'éviter les descriptions subjectives, les fichiers de police judiciaire susceptibles d'enregistrer des informations relatives au signalement des personnes pourraient être soumis à un thésaurus fermé, inspiré des recommandations faites à propos du STIC-Canonge par le précédent groupe de travail sur les fichiers. D'autres thésaurus pourraient être créés afin de mieux encadrer la saisie d'informations relatives à la nature des infractions commises.

Le groupe de contrôle recommande au ministère de l'Intérieur d'engager une réflexion sur la possibilité d'intégrer des référentiels communs dans chaque catégorie de fichiers. Ces référentiels permettraient ainsi, sur le plan technique, de normaliser des champs de données afin de les rendre plus conformes aux principes définis par la loi de 1978 en matière de collecte de données.

Cette réflexion devra notamment être à la charge des attributions du groupe de contrôle institutionnalisé (recommandation nº 1) afin de ne pas multiplier les instances de réflexion, de garantir la présence de tous les partenaires institutionnels concernés, et de préserver la cohérence du dispositif d'ensemble de contrôle.

Les traitements les plus récents disposent de thésaurus communs (thésaurus des qualifications pénales rendant un profil génétique éligible pour le FNAEG par exemple).

S'agissant du FAED, la mise à jour des référentiels était conditionnée au développement du projet Métamorpho, dont le financement n'est pas encore assuré ; néanmoins les référentiels existants, qui ont

vocation à l'administration dossier par dossier ne présentent pas un caractère sensible

L'architecture de ces fichiers de nouvelle génération repose également sur la mutualisation des outils de la police et de la gendarmerie nationales. C'est le cas dans le projet de mise en place du système Traitement des procédures judiciaires (TPJ – Ex-Ariane), qui se substituera au STIC de la police et au JUDEX de la gendarmerie au cours des années 2011/2012.

Au-delà, il est utile d'étendre les thésaurus communs aux différents traitements nationaux de la police et de la gendarmerie. En effet, il est souhaitable que ces traitements (TPJ, FNAEG, FAED, etc.) puissent disposer de thésaurus communs mis à jour régulièrement par un service à vocation transversale. Il pourrait notamment s'agir des thésaurus des services, des thésaurus des communes de naissance ou des infractions. Une réflexion a été lancée à ce sujet dans le cadre de la modernisation de l'architecture du portail CHEOPS.

Dans le cadre des travaux de conception du traitement des objets et véhicules signalés ou volés, les référentiels concernant la description des objets et véhicules ont été établis en commun par les deux forces de police, sur la base des besoins connus du futur système d'information Schengen, ainsi que sur l'existant de traitements tels que le STIC, le FOS, le JUDEX et le FVV.

Ces référentiels mettant en œuvre une nomenclature d'objets ont été repris dans le cadre du projet TPJ et, dans un souci de cohérence, les thésaurus qui seront utilisés par LRPPN, traitement de rédaction et de gestion des procédures, ont été mis à jour pour intégrer ces évolutions. Pour ce qui concerne la description des personnes physiques, les recommandations du groupe de travail ont été prises en compte.

De ce fait, il existe désormais une cohérence totale des référentiels depuis le traitement source LRPPN jusqu'aux futures bases nationales mutualisées de recherches TPJ et FOVES.

La gendarmerie nationale, qui a participé à cette réflexion, a aussi fait évoluer les référentiels utilisés au niveau du traitement de rédaction de procédures LRPGN (ex-ICARE).

Toujours concernant la gendarmerie nationale, on peut également noter que la normalisation des libellés d'infractions est réalisée à partir du Code NATINF justice au sein des traitements de procédure, ces travaux étant réalisés dans le cadre de la conception des futurs échanges entre les fichiers LRPGN et CASSIOPEE.

8. Intégrer systématiquement un module de contrôle interne des données

Si chacun reconnaît l'utilité et la nécessité de disposer d'outils informatiques performants, il convient d'en contrôler l'usage de la manière la plus efficiente afin de limiter, de prévenir et éventuellement réprimer les utilisations contraires aux règles déontologiques et aux finalités.

Le groupe de contrôle recommande de développer les possibilités de contrôles au sein de chaque service.

Il conviendrait ainsi de renforcer le pouvoir de contrôle des chefs de service sur la volumétrie et la nature des consultations effectuées par chacun des fonctionnaires qu'il a habilité. Un tel dispositif aurait automatiquement un effet dissuasif en faisant apparaître les consultations « de curiosité » et permettrait de mettre en place des contrôles aléatoires sur les liens existants entre des recherches sur les fichiers de procédure et une enquête en cours.

Le groupe de contrôle demande qu'une réflexion soit engagée sur la possibilité de mettre en œuvre des traitements systématiquement dotés :
– d'un dispositif de pilotage interne donnant des indications d'ordre quantitatif sur les consultations effectuées sur une période donnée par chacun des fonctionnaires du service habilité, avec un dispositif d'alerte sur des variations significatives du total moyen habituel ;
– d'une visualisation, à partir du nom des fonctionnaires habilités, du patronyme des individus mis en cause ayant fait l'objet d'une consultation de fichier par chacun d'eux.

Ce module devrait obligatoirement être intégré dans les architectures techniques des fichiers dès leur phase de conception. Dès lors, l'ensemble des fichiers de police seraient constitués du même bloc de sécurisation des données (traçabilité des connexions, contrôle des habilitations, contrôle des accès aux traitements et ce nouveau module de visibilité interne).

La DGGN réalise le contrôle de l'accès aux données grâce aux fonctionnalités offertes par son dispositif d'authentification (WEB-SSO).

Ce dispositif technique permet un établissement automatique des droits d'accès sur la base d'un référentiel défini et régulièrement mis à jour par l'administration centrale et dont la mise à jour est directement opérée à partir de la base des ressources humaines de la gendarmerie (cf. recommandation n° 4 : intégrer la démarche qualité). L'état des habilitations est, à cet effet, totalement transparent et susceptible de contrôle à tout instant.

Par ailleurs, le contenu des traces fait l'objet d'une normalisation selon des critères de cohérence que la DGGN impose lors du

développement de toute nouvelle application. À cette standardisation technique s'est adjointe une réforme des modalités d'utilisation des traces dissociant clairement :
1. l'administration technique ;
2. l'exploitation fonctionnelle ;
3. le contrôle.

Enfin, le contrôle de l'utilisation des fichiers par les personnels de la gendarmerie est exercé par l'IGGN qui s'est dotée en 2009 d'un bureau spécialement dédié à cette mission. Ce bureau s'appuie sur un logiciel d'analyse quantitative des connexions aux fichiers opérationnels ou sensibles. Ce logiciel permet de mettre en exergue, fichier par fichier, les unités ou les militaires dont le comportement est anormal au regard des normes quantitatives de consultation des fichiers propres à leur profil d'utilisateur dans un laps de temps donné. Il autorise la production de rapports d'analyse détaillés. L'IGGN peut, en tant que de besoin, extraire les traces de connexions des militaires identifiés et vérifier, en liaison avec leur hiérarchie de contact, si les consultations opérées ont un lien avec l'activité professionnelle des intéressés.

Pour la DGPN, les traitements automatisés tels que le FAED et le FNAEG disposent déjà d'un dispositif de traçabilité qui permet, à partir de l'enregistrement d'un opérateur habilité, de connaître le volume des consultations réalisé et les patronymes consultés. Toutefois, ce contrôle ne peut être opéré actuellement que par l'intermédiaire de la Direction des systèmes d'information et de communication. L'accès à la traçabilité par le gestionnaire de ces deux fichiers est prévu dans les évolutions fonctionnelles à venir. Cet accès pourrait utilement être accordé aux chefs de service pour les personnels sur lesquels ils ont autorité.

En ce qui concerne le portail d'accès CHEOPS, qui commande l'accès à un certain nombre de fichiers de police et a été fortement modernisé depuis janvier 2011, les chefs de service ont accès au trafic des utilisateurs locaux, de sorte qu'ils peuvent savoir si un fonctionnaire a un accès excessif à certains fichiers de police, mais pas au contenu des consultations.

9. Améliorer la gestion des habilitations

Le groupe de contrôle recommande que le contrôle des habilitations des fonctionnaires soit amélioré.

À cette fin, le système de gestion des habilitations mis en œuvre par la police nationale dans le cadre du portail d'accès CHEOPS devrait faire l'objet d'évolutions techniques destinées à mieux prendre en compte les évolutions de carrière de chaque fonctionnaire. Ainsi, en cas de mutation, de changement d'affectation ou de départ à la retraite, les droits d'accès de la personne devront être automatiquement revus ou supprimés.

Cette recommandation permettra de lutter plus efficacement contre les consultations indues de fichiers mais aussi d'éliminer tout risque de consultation indue de fichiers à partir d'un matricule qui aurait été créé frauduleusement par un fonctionnaire mal intentionné. Sur ce second point, le groupe de travail propose qu'une réflexion soit engagée sur les possibilités techniques d'interrogation automatique du fichier de gestion du personnel de la police nationale de l'authenticité des matricules utilisés par le portail CHEOPS.

Si le FNAEG est accessible par le portail d'accès CHEOPS, ce n'est pas le cas pour le FAED. Pour ce fichier, les habilitations sont délivrées par la Direction d'application du FAED à la demande expresse des chefs de service. Le passage sous CHEOPS est envisagé dans les années à venir. Pour les deux traitements, les mots de passe sont renouvelés régulièrement.

D'autre part, le portail CHEOPS modernisé permettra l'automatisation des liaisons entre les centres de gestion des personnels, chargés de suivre la carrière des policiers, et les responsables des accès sécurisés des traitements. De la sorte, il ne sera plus possible d'utiliser les codes d'accès d'un agent qui ne serait plus en poste.

En outre, la DGPN va déployer progressivement à compter du second semestre 2011 une nouvelle carte professionnelle permettant notamment l'accès aux fichiers de police en fonction des droits de chaque agent (*cf. recommandation n° 10*).

10. Recourir à terme à la biométrie pour améliorer le contrôle de l'accès aux traitements

Le groupe de contrôle recommande l'utilisation, à terme, de systèmes de contrôle d'accès aux traitements par la voie biométrique (empreinte digitale du fonctionnaire, par exemple) afin de renforcer le dispositif de sécurisation et de traçabilité de l'accès aux fichiers.

Le recours à ces outils permettra en effet de mettre fin aux « prêts » de mot de passe entre fonctionnaires de police ainsi qu'aux consultations de fichiers par un agent non habilité qui aurait indûment disposé ou conservé le mot de passe.

En outre, l'identification par l'empreinte digitale devrait davantage responsabiliser le fonctionnaire dans la mesure où ce dernier serait personnellement impliqué dans le processus d'authentification.

Eu égard aux coûts induits par la mise en œuvre d'un tel dispositif, le recours à la biométrie doit être subordonné à une évaluation financière et serait sans doute réservé, au moins au début, aux traitements les plus sensibles.

À compter du premier trimestre 2011, les militaires de la gendarmerie nationale bénéficieront d'un système d'authentification encore plus performant et innovant pour leur accès aux fichiers, sous la forme d'une carte professionnelle à puce (doublée d'un code personnel). Ce document sécurisé élèvera ainsi le seuil de fiabilité de l'authentification.

Une expérimentation relative à l'utilisation de la biométrie a été confiée à la DGPN par le ministre de l'Intérieur.

11. Renforcer très nettement le rôle de contrôle et d'audit des services d'inspection

Le groupe de contrôle suggère le renforcement des missions de l'IGPN, de l'IGS et de l'IGGN en matière de contrôle des fichiers.

Ces services pourraient ainsi multiplier les contrôles ciblés sur l'utilisation des fichiers, notamment au regard de la déontologie et des règles fixées par la loi « informatique et libertés ». Les textes réglementaires

concernant les missions respectives de ces services devront être modifiés en conséquence.

En outre, le groupe de travail recommande un suivi effectif des recommandations émises par l'Inspection générale de la police nationale (IGPN), l'Inspection générale des services (IGS) ou l'Inspection générale de la gendarmerie nationale (IGGN). Les services concernés devront se conformer aux éventuelles observations dans le délai qui aura été fixé par le rapport d'audit.

Un guide d'audit portant sur l'informatique et les libertés pourrait être élaboré à l'usage des inspections mais aussi, à titre pédagogique et pour favoriser l'« auto-contrôle », à l'usage des experts « informatique et liberté » (*cf. proposition n° 5*). Une « cotation », un « label » ou une procédure interne de certification pourrait également être institué et faire l'objet d'une certaine publicité une fois l'audit effectué.

Il conviendra de préciser l'articulation entre ces missions d'inspection « institutionnalisées » et les possibilités de contrôle d'ores et déjà dévolues à la CNIL. Le périmètre d'action de ces missions d'inspection sera utilement limité aux services et unités dans lesquels des dysfonctionnements ont été effectivement constatés afin d'en déterminer les causes en termes d'organisation du service et d'agissements des personnels.

En complément de la MPSSI évoquée au point n° 5, deux bureaux spécifiques ont été créés au cours de l'année 2009 au sein de l'inspection de la gendarmerie nationale (IGGN) :

– le bureau du contrôle de la sécurité des systèmes d'information (BSSI) en charge du contrôle de la sécurité des infrastructures et de la centralisation des traces de connexion ;

– le bureau de contrôle et d'évaluation des fichiers (BCEF) chargé de veiller à la conformité des applications utilisées au sein de la gendarmerie nationale et de la régularité de l'utilisation qui en est faite par les militaires.

Outre le traçage des connexions des utilisateurs de certains fichiers opérationnels sensibles, une partie importante de l'activité du BCEF consiste à sensibiliser et contrôler les unités de niveau départemental et régional. Le bureau s'appuie à cet effet sur un questionnaire d'auto-évaluation qui permet d'identifier des vulnérabilités et de sensibiliser les commandants d'unité concernés à la problématique des fichiers. Sur la base de l'analyse de ces questionnaires et dans le cadre des directives permanentes du DGGN, le BCEF procède à des visites sur place débouchant sur des recommandations et, ultérieurement, des contrôles. Une trentaine d'unités a ainsi été visitée par le BCEF depuis juin 2010.

Parallèlement, afin d'intégrer la logique de contrôle dans Athén@/BDSP, une section du système des opérations et du renseignement (SSOR) a été créée à l'été 2009, au sein de la Direction des opérations

et de l'emploi de la DGGN ; elle a notamment en charge le contrôle de contenu du système Athén@/BDSP, en lien avec l'IGGN (contrôle de l'activité des utilisateurs par extraction de traces fonctionnelles relatives à une activité considérée comme anormale).

Jusqu'en 2009, les contrôles et audits des fichiers de police organisés par l'Inspection générale de la police nationale (IGPN) portaient d'une manière très large sur la sécurité des systèmes d'information. Depuis avril 2009, ces contrôles visent plus spécifiquement les traitements de données utilisés par la police nationale.

En 2008, six contrôles ont été réalisés au sein des DDSP.

À partir de l'année 2009, par un plan annuel national de contrôles, l'IGPN a pour objectif de réaliser une vingtaine d'audits de l'utilisation par les services territoriaux de police des traitements de données personnelles.

Les conclusions de ces audits sont systématiquement adressées aux directions concernées qui en assurent le suivi.

12. Créer un contrôleur interne au sein de la DGPN, de la PP et de la DGGN spécialisé dans la protection des données

La désignation d'une personnalité qualifiée, chargée de la surveillance et du fonctionnement de chaque traitement, pourrait être proposée. Il s'agirait d'un interlocuteur spécialisé en matière de protection de données à caractère personnel, tant pour le responsable et les utilisateurs des traitements, que pour la CNIL. La désignation de ce type de correspondant garantirait ainsi la transparence de la consultation de ces données.

La mise en place d'un tel correspondant a déjà été entreprise au niveau européen. Au sein d'Europol, comme d'Eurojust, un membre du personnel est en effet spécialement désigné pour assurer la protection des données.

Le groupe de contrôle recommande que, la fonction de correspondant informatique et libertés introduite en août 2004 avec la réforme de la loi informatique et libertés (article 22 III de la loi informatique et libertés et titre III du décret du 20 octobre 2005) pour les traitements les plus courants soit étendue à la mise en place d'un correspondant à la protection des données

au sein des directions générales de la police et de la gendarmerie nationales ainsi qu'au sein des services de la préfecture de police de Paris.

Au sein de la Direction générale de la gendarmerie nationale, un correspondant fonctionnel responsable de l'application a été désigné pour chaque traitement. Ces responsables sont particulièrement sensibilisés aux normes de protection des données et leur action est coordonnée par le magistrat délégué auprès du DGGN dans le cadre des travaux de la mission permanente de suivi des systèmes d'information (MPSSI), lequel s'est adjoint un référent national informatique et liberté (cf. recommandations 4 et 5). De plus, les deux bureaux précédemment mentionnés de l'IGGN agissent aussi dans ce domaine. Enfin, il faut noter l'existence du bureau de la sécurité et de la veille au sein du Service des technologies et des systèmes d'information de la sécurité intérieure (STSI2 ; service conjoint gendarmerie-police placé sous la responsabilité de la DGGN). La DGGN souhaite cependant que son système hiérarchique soit préservé (même réflexion concernant les CIL).

Pour la Direction générale de la police nationale, si cette recommandation vise à étendre aux services de police et de gendarmerie le « correspondant à la protection des données à caractère personnel » de l'article 22 de la loi du 6 janvier 1978, elle paraît peu adaptée aux services de l'État. Institué par le législateur en 2004, ce correspondant exerce ses missions et saisit la CNIL « d'une manière indépendante », en dehors de toute instruction de sa hiérarchie, et il n'est compétent que pour les traitements soumis à une simple déclaration, ce qui n'est presque jamais le cas des fichiers de police.

Pour ces deux raisons, le correspondant à la protection des données n'a pas sa place dans une organisation hiérarchisée mettant en œuvre des règles propres de protection des données personnelles, sous le contrôle direct de la CNIL : ce dispositif, instauré pour mieux encadrer la prolifération de fichiers dans une multitude d'organismes privés, ne saurait être élargi à une structure d'État telle que la police nationale.

L'organisation adoptée par les pouvoirs publics (et détaillée par les circulaires du Premier ministre des 12 mars 1983 et 29 juin 2007) repose sur un réseau constitué par le commissaire du gouvernement auprès de la CNIL et ses correspondants ministériels, eux-mêmes chargés de veiller au respect du droit des fichiers dans l'ensemble des services de leur ministère.

Ces correspondants sont ainsi chargés en particulier de « veiller à la protection de la vie privée dans les traitements automatisés », comme le font les correspondants à la protection des données dans le secteur privé ou les collectivités locales.

Ainsi, dans son rapport sur le projet de loi de 2004 modifiant la loi de 1978, le sénateur Türk indiquait à propos des correspondants à la protection des données que «leur mise en place doit permettre à la CNIL de disposer d'un réseau de correspondants, ainsi que cela existe déjà dans le secteur public».

Toutefois, la recommandation 5 poursuit le même objectif : améliorer la diffusion, la compréhension et le respect du droit des fichiers au sein des services de police.

13. Désigner un magistrat en charge du contrôle des fichiers d'antécédents judiciaires

L'article 6 du projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure modifie l'article 21 de la loi nº 2003-239 du 18 mars 2003 relatif aux fichiers d'antécédents judiciaires et introduit la désignation d'un magistrat chargé du contrôle de ces fichiers.

Un tel magistrat serait destiné à assurer, parallèlement aux parquets qui continueront à assumer la mise à jour quotidienne au fil de l'eau des fichiers, un contrôle en profondeur des traitements, notamment grâce à un accès direct aux données.

Le groupe de contrôle recommande donc la création de la fonction de magistrat chargé du contrôle des fichiers d'antécédents judiciaires.

En tout état de cause, il importerait de clarifier l'articulation de l'action dudit magistrat avec celle de la CNIL, même s'il est souhaitable que les magistrats soient plus étroitement associés au suivi des fichiers d'antécédents judiciaires, en particulier s'agissant de leur mise à jour.

La loi d'orientation et de programmation pour la performance de la sécurité intérieure (LOPPSI), du 14 mars 2011, a prévu, dans son article 11, la création de ce magistrat chargé de suivre la mise en œuvre et la mise à jour des traitements automatisés de données à caractère personnel pour les fichiers d'antécédents judiciaires (art. 230-9 du Code de procédure pénale).

Ses attributions et les conditions d'exercice de sa mission seront détaillées et précisées très prochainement, dans le cadre des décrets d'application de la LOPPSI, en cours de rédaction.

14. Renforcer le contrôle des fichiers des polices municipales

Le groupe de travail a constaté que les textes qui encadrent la création et le fonctionnement des polices municipales restent très restrictifs en ce qui concerne le contrôle de ces services de police par une autorité extérieure. Ainsi, depuis la mise en application de ces dispositions, les services de contrôle de l'État (IGA, IGPN, IGGN) n'ont été saisis qu'une seule fois. D'autre part, les services de police municipale sont susceptibles de créer des fichiers avec pour seule contrainte de respecter le droit commun en la matière.

Le groupe de contrôle recommande que les contrôles sur le fonctionnement des services de police municipale soient plus nombreux et ciblés notamment d'une part sur la recherche des fichiers qui pourraient avoir été créés, sur l'étude de leur conformité avec les prescriptions de la loi, sur leur alimentation, sur leur utilisation et sur leur éventuelle extension, et d'autre part sur le traitement des informations contenues dans les traitements de données à caractère personnel et transmises par les forces de sécurité [1].

Au besoin, le groupe de travail recommande une modification de la loi du 15 avril 1999 en vue de préciser les modalités des contrôles pouvant intervenir.

Cette recommandation a fait l'objet de plusieurs rappels lors des différentes séances du groupe de travail. Une circulaire du ministre de l'Intérieur du 15 décembre 2010 a rappelé à l'ensemble des Préfets qu'un arrêté cadre du 14 avril 2009 avait été signé et que celui-ci déterminait précisément quelles catégories de communes pouvaient créer des traitements de données à caractère personnel, les finalités poursuivies par ces traitements, les catégories de données et d'informations pouvant être recueillies ainsi que la durée de conservation.

1 Séance du groupe de travail du 20 janvier 2011.

15. Renforcer la formation des fonctionnaires de police et des militaires de la gendarmerie

Le groupe de contrôle suggère la mise en place d'un module d'enseignement spécifique relatif aux droits et à l'utilisation des fichiers dès la formation initiale.

À cette occasion, les élèves et les stagiaires devront bénéficier d'un enseignement particulier sur les règles relatives aux principaux fichiers ainsi qu'aux différentes sanctions encourues en cas de détournement de finalité. Le groupe de travail estime en effet essentiel que le fichier, avec toutes les contraintes que notre droit y associe, soit regardé comme un des outils de travail fondamentaux du policier et du gendarme et soit traité comme tel, au même titre que, par exemple, l'arme de service ; de même que celle-ci fait l'objet d'un enseignement détaillé (notion de légitime défense, etc.), il est indispensable que le droit des fichiers soit largement diffusé dans toute formation dispensée aux policiers et aux gendarmes.

Un module d'enseignement destiné aux fonctionnaires ou aux militaires de la gendarmerie déjà en activité pourrait faire partie du catalogue des formations prévues dans le cadre du droit individuel à la formation continue.

---

*En gendarmerie, des espaces pédagogiques «fichiers» existent depuis plus de deux ans sur **l'intranet gendarmerie**. Et la **circulaire interne** (mémorial gendarmerie) portant sur l'application de la loi susvisée a été refondue afin de renforcer certains éléments de langage.*

Un séminaire d'approfondissement au profit des commandements de groupements de gendarmerie départementale et spécialisée, de sections de recherches et offices centraux a en outre été organisé début février 2011.

*Enfin, toute mise en place d'un fichier en gendarmerie est obligatoirement précédée d'une **triple formation (juridique, éthique, technique)** : formation initiale, formation continue, formation des formateurs, formation des utilisateurs, didacticiels... Il faut au surplus préciser que certains postes nécessitent obligatoirement une formation plus poussée en matière de fichiers ou traitements informatisés, à l'image des militaires affectés en BDRIJ (5 semaines au centre national de formation à la police judiciaire de Fontainebleau), des techniciens des systèmes d'information et de communication (formation de base de 10 mois), ou encore des analystes criminels qui disposent désormais d'une formation universitaire diplômante de type DU voire master dans le cadre d'un partenariat gendarmerie-Université de Troyes (mise en exergue par l'Union européenne dans le cadre du 5e cycle d'évaluations*

mutuelles relatives à la lutte contre la délinquance économique et financière – rapport France d'avril 2010).

En ce qui concerne plus spécifiquement le système Athén@/BDSP, la formation a été intégrée au marché afin de développer les outils d'auto-formation et principalement d'assurer celle de 300 formateurs experts au niveau national. Ces experts formeront à leur tour un formateur relais par unité utilisatrice du système. La formation TPJ, en gendarmerie, devrait adopter le même schéma.

La DGPN a entrepris d'élaborer des outils pédagogiques destinés à renforcer la formation initiale et continue sur le droit des fichiers de police. Ce renforcement est effectif depuis 2010 pour les trois corps de la police nationale.

16. Renforcer la formation des agents administratifs chargés de l'alimentation des fichiers

L'alimentation de certains traitements (le STIC, par exemple) requiert un niveau de connaissance élevé en droit et en procédure pénale. Ces fichiers comportent en effet des informations relatives à la qualification judiciaire des infractions, qu'il est d'autant plus important de savoir exploiter sans commettre d'erreur que celles-ci peuvent avoir de lourdes conséquences du point de vue des libertés publiques.

Afin de remédier à cette difficulté, le groupe de contrôle recommande que ces agents bénéficient d'une formation juridique adaptée et régulièrement entretenue. Cet effort de formation permettra d'améliorer les conditions d'alimentation des fichiers et de réduire le risque de saisies erronées.

Le groupe de contrôle souhaite que les administrations centrales se rapprochent des autorités administratives indépendantes afin de garantir la pluralité et l'efficacité des formations dispensées.

Le plan national d'enrichissement (PNE) du STIC mis en œuvre depuis décembre 2004 est accompagné d'une formation juridique des agents concernés, laquelle est régulièrement entretenue par les administrateurs régionaux. Ces derniers sont réunis chaque année par la direction d'application pour être informés notamment des dernières évolutions juridiques et doctrinales.

Cette action, complétée par la direction des ressources et des compétences bénéficiera du travail d'actualisation et de renforcement de l'enseignement du droit des fichiers (cf. recommandation 15).

17. Définir dans la loi du 6 janvier 1978 un régime d'expérimentation

Certains traitements complexes ou de grande ampleur nécessitent de longues procédures d'expérimentation et d'évaluation qui sont nécessaires à leur mise au point et à leur bon fonctionnement opérationnel. Dans ce cas, les services de police sont confrontés à une difficulté : au moment de passer de la procédure de « vérification d'aptitude » (VA), qui peut donner lieu jusqu'au dernier moment à de nombreux aménagements techniques, à celle de « vérification de service régulier » (VSR), ils sont juridiquement tenus de présenter un dossier de déclaration déjà totalement abouti puisque la VSR suppose un emploi dans des conditions réelles par des services opérationnels (généralement, dans un nombre réduit de services sélectionnés en fonction de critères donnés). Cette contrainte pose deux problèmes majeurs :
– l'élaboration du dossier de déclaration puis la procédure réglementaire (examen du projet par la CNIL puis, bien souvent, examen par le Conseil d'État) imposent en toute rigueur de suspendre le projet et par conséquent de surseoir à la phase de VSR pendant une période qui peut largement dépasser un an ;
– l'élaboration d'un dossier de déclaration alors que la VSR n'a pas eu lieu oblige le gestionnaire du traitement à fournir des informations susceptibles de ne pas correspondre à la version définitive du traitement, celle qui résulte précisément de l'expérience acquise pendant la phase de VSR.

Au plan opérationnel, surseoir à la VSR est d'autant plus difficile que cela peut entraîner une lourde charge financière, du fait par exemple des équipes d'ingénieurs qui ne peuvent plus travailler sur le projet ou des contrats passés avec les entreprises prestataires. La DGPN est d'ailleurs confrontée actuellement à ces difficultés avec LRPPN et le FAED (dans le cadre de son adaptation aux dispositions du traité de Prüm).

Pour ces raisons, la procédure de déclaration ne peut bien souvent être entreprise qu'à l'issue de la VSR, celle-ci n'étant dès lors couverte par aucun cadre juridique.

Le groupe de contrôle recommande que, pour les fichiers relevant de l'article 26 de la loi (ceux intéressant la sûreté de l'État, la défense ou la sécurité publique et ceux ayant pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté), la loi du 6 janvier 1978 soit modifiée

pour reconnaître une phase d'expérimentation permettant de ne produire dans un premier temps qu'une déclaration simplifiée.

Cette procédure d'expérimentation ne pourrait excéder une année et ne devrait préjuger en rien de décision finale de la CNIL.

Le contenu de la déclaration simplifiée serait défini par décret en Conseil d'État, comme dans le cadre du dernier alinéa du I de l'article 30 de la loi (procédure utilisée récemment pour les fichiers CRISTINA et EDVIRSP) ; le même décret préciserait les critères permettant de bénéficier de ce régime d'expérimentation (par exemple les finalités du traitement ou sa complexité technique). Pendant les douze mois de cette période légale d'expérimentation, la CNIL disposerait naturellement de tous les pouvoirs de contrôle qui lui confie l'article 44 de la loi, notamment pour s'assurer que le champ de l'expérimentation est respecté.

La reconnaissance de cette procédure d'expérimentation, étroitement contrôlée par la CNIL, aurait le grand avantage de concilier les exigences du droit des fichiers et les contraintes techniques inséparables d'un projet informatique de grande ampleur. Elle mettrait également fin à une situation trop fréquente, mais parfois inévitable, de mise en place d'un traitement sans aucun cadre juridique (cas d'Ardoise).

Le régime expérimental des fichiers a été introduit la proposition de loi Batho-Bénisti par amendement adopté par la commission des lois de l'Assemblée nationale sur la proposition du DGPN. Le régime expérimental des fichiers de police a été repris dans la proposition de loi dite « Warsmann » de simplification et d'amélioration de la qualité du droit avait d'être supprimé, en même temps que l'ensemble des dispositions sur les fichiers de police, par le Sénat puis par la commission mixte paritaire.

Le texte issu de la CMP ne comprend plus ses dispositions, écartées en seconde lecture par le Sénat.

---

18. Renforcer la CNIL dans son rôle de conseil

Instance de contrôle, la CNIL s'est également vu reconnaître un rôle de conseil du gouvernement et, d'ailleurs, de tout gestionnaire de traitement afin que, par une relation de partenariat et un rôle pédagogique clairement assumé, les contraintes liées au droit des fichiers, trop souvent perçues comme exogènes et difficiles à mettre en œuvre, puissent être mieux intégrées et mieux comprises par les acteurs. Il paraît d'ailleurs évident que toute mission de contrôle est plus

efficace lorsqu'elle s'accompagne d'une démarche active d'assistance, de pédagogie et d'incitation que lorsqu'elle se réduit à une censure.

Le groupe de contrôle propose que la Commission nationale de l'informatique et des libertés voit renforcer son rôle de conseil des services et directions administratives chargées de mettre en œuvre des traitements automatisés de données à caractère personnel. Ce rôle ne pouvant, bien entendu, préjuger des délibérations ultérieures de la CNIL.

En intégrant et en donnant un cadre légal au régime d'expérimentation, la proposition de loi Warsmann précitée visait également à faire assurer par la CNIL un suivi en amont des projets de création de traitements.

19. Simplifier la transmission des suites judiciaires dans le cadre du traitement en temps réel

Le groupe de contrôle suggère que soit examinée, en concertation avec la police et la gendarmerie nationale et le ministère de la Justice, la possibilité de simplifier la transmission des suites judiciaires dans le cadre du traitement en temps réel.

Il pourrait être ainsi étudié la possibilité de transmission des suites judiciaires, au niveau régional, par voie de courrier électronique (avec accusé de réception) sur une boîte électronique fonctionnelle dédiée et dans le respect du Code de procédure pénale.

L'instruction de classement sans suite des parquets pour insuffisances de charges pourrait, selon des modalités à définir, être immédiatement prise en compte par les services enquêteurs sans qu'il soit besoin de leur transmettre une fiche navette. Par ailleurs, une réflexion pourrait être menée sur le moment opportun de l'inscription de la personne mise en cause au STIC ou au JUDEX : différer l'inscription au moment où la responsabilité de la personne est véritablement bien établie peut être de nature à éviter le maintien de mentions erronées.

Parmi les pistes de travail examinées depuis 2009 dans le cadre de travaux interministériels, seules deux ont pu aboutir à un consensus :
– l'expérimentation de l'accès à JUDEX, toujours en cours sur les ressorts cours d'appel de Douai et d'Amiens ;
– les échanges inter-applicatifs entre CASSIOPEE (déployé sur quasiment toute la France – hors l'Île-de-France) – et TPJ, expérimenté depuis le 1er avril 2011 sur le ressort de la cour d'appel de Poitiers, pour la seule partie « DGGN » du futur TPJ.

20. Étendre les cas de mise à jour des fichiers STIC et JUDEX

Le groupe de contrôle suggère d'élargir la liste des cas justifiant une mise à jour des fichiers STIC et JUDEX aux décisions alternatives aux poursuites, telles que les rappels à la loi et la composition pénale, qui ne font actuellement pas l'objet d'une mention au STIC ou au JUDEX.

Une ligne additionnelle devra apparaître sur l'écran indiquant « décision alternative aux poursuites » en cas de consultation pour une enquête administrative.

Ainsi que le groupe de travail l'avait déjà souligné en novembre 2006, l'autorité administrative n'est pleinement en mesure d'effectuer une prise en compte proportionnée des faits que pour autant qu'elle a connaissance des suites judiciaires qui leur ont été réservées.

L'article 11 de la LOPPSI a complété les garanties en ce sens : désormais, toutes les décisions de classement sans suite, quel qu'en soit le motif, doivent faire l'objet d'une mention dans le traitement et, d'autre part, ces décisions favorables ne seront pas consultables dans le module consacré aux enquêtes administratives des fichiers d'antécédents.

Par ailleurs, la gendarmerie nationale a été mandatée par le ministre de l'Intérieur pour étudier la question du portrait-robot numérique (projet SOSIE). Les recommandations sur la notion de signalement et la notion d'équilibre entre la nécessité de l'identification des personnes recherchées et le principe de non-discrimination ont ainsi été prises en compte dans le cahier des charges finalisé en juillet dernier.

21. Garantir dans certains cas une procédure contradictoire

Selon le premier alinéa de l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 modifiée d'orientation et de programmation relative à la sécurité, certaines décisions administratives de recrutement, d'affectation, d'autorisation, d'agrément ou d'habilitation peuvent faire l'objet d'enquêtes administratives donnant lieu à consultation des fichiers de police STIC et JUDEX.

Dans le cadre de cette procédure, il est souhaitable de garantir effectivement que la personne faisant l'objet d'une telle enquête soit, préalablement à une décision défavorable :
– informée qu'une décision défavorable est envisagée et de ses motifs ;
– invitée à formuler ses observations écrites ;
– entendue, si elle le demande.

En effet, le principe des droits de la défense implique qu'une « mesure individuelle d'une certaine gravité, reposant sur l'appréciation d'une situation personnelle, ne peut être prise par l'administration, sans entendre au préalable la personne qui est susceptible d'être lésée dans ses intérêts moraux et matériels par cette mesure ». [CE, sect., 9 mai 1980, Sté des établissements Cruse fils et frères : Rec. CE 1980, p. 217, concl. B. Genevois].

Le groupe de contrôle propose la mise en place d'un groupe de réflexion, composé de la CNIL, de la DGPN, de la DGGN, de la DLPAJ et du Médiateur de la République, visant à proposer de nouvelles garanties aux personnes faisant l'objet d'une enquête administrative au titre de la loi du 21 janvier 1995.

En août 2010, suite à la recommandation nº 21 du groupe de travail, visant à « garantir le respect d'une phase contradictoire lors des procédures d'enquêtes administratives », et à la fin de non-recevoir du ministère de l'Intérieur concernant la mise en place d'une telle mesure, le Médiateur de la République a initié une réunion à la Médiature avec la participation de la CNIL et de la HALDE afin de « déterminer avec précision, au regard de la pratique des services compétents en matière d'enquêtes administratives, les raisons qui permettraient de conclure à l'absence de nécessité de mettre en place une telle phase contradictoire ».

En septembre 2010, la Médiature de la République a organisé une réunion afin d'échanger sur cette proposition. Suite à cette rencontre, le Médiateur de la République a adressé une nouvelle proposition au ministre de l'Intérieur tendant à modifier la circulaire du 24 février 2009 relative à l'entrée en vigueur de la carte professionnelle des salariés participant aux activités privées de sécurité définies à l'article 1er de la loi du 12 juillet 1983. Il est proposé qu'en cas d'existence d'éléments susceptibles d'entraîner une décision défavorable, la personne faisant l'objet de l'enquête devra désormais être informée des motifs susceptibles de motiver la décision et de la possibilité qui lui est offerte de faire valoir ses observations écrites avant la date prévue pour la prise de décision. La DGPN et la DGGN précisent que, dans le cas où cette mesure serait adoptée, il serait opportun de demander une étude d'impact à la DMAT car la charge de telles procédures peut peser sur l'activité des services préfectoraux.

Le groupe de travail a souligné l'intérêt de cette nouvelle proposition équilibrée et a souhaité qu'une attention particulière puisse lui être portée.

---

22. Créer une voie de recours contre certaines décisions du procureur de la République

Pour le Médiateur de la République, l'article 21-III de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure prévoit que « le traitement des informations nominatives est opéré sous le contrôle du procureur de la République compétent qui peut demander qu'elles soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire ».

« La rectification pour requalification judiciaire est de droit lorsque la personne concernée la demande ». En revanche, en cas de « décision de relaxe ou d'acquittement devenue définitive, les données personnelles concernant les personnes mises en cause sont effacées sauf si le procureur de la République en prescrit le maintien pour des raisons liées à la finalité du fichier, auquel cas elle fait l'objet d'une mention ».

Le législateur a ainsi confié en cette matière au procureur de la République un pouvoir décisionnel, qu'il exerce selon son appréciation, qui s'impose au responsable du traitement et fait grief à la personne mise en cause.

Or, lorsque cette décision intervient, elle n'est pas notifiée à la personne mise en cause et n'est pas susceptible de recours. Pourtant, cette décision est susceptible d'avoir pour conséquence un refus d'embauche, d'agrément ou un licenciement, alors même que la personne a été relaxée ou acquittée.

En vue d'assurer « un meilleur équilibre entre l'efficacité de la protection des personnes et l'attention de tous les instants que requiert la protection des libertés* », la proposition suivante est par conséquent formulée :

En cas de décision de relaxe ou d'acquittement devenue définitive, la prescription du procureur de la République tendant au maintien des mentions relatives aux données personnelles concernant la personne mise en cause, devra désormais lui être notifiée et sera susceptible d'un recours devant le procureur général.

Le ministère de la Justice, observe pour sa part, que la demande de mise à jour des fichiers STIC ou JUDEX, selon les conditions précisées par le III de l'article 21 de la loi du 18 mars 2003 pour la sécurité intérieure, peut être adressée directement auprès du procureur de la République. Cette saisine peut alors être considérée comme une modalité d'exercice du droit d'accès indirect sui generis puisque la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés précise en son article 41 qu'une telle demande est adressée au gestionnaire du fichier *via* la Commission nationale de l'informatique et des libertés.

C'est donc afin d'améliorer la procédure d'instruction de telles demandes qu'il a été prévu, par les actes réglementaires portant création de

ces fichiers, qu'elles puissent être adressées directement au procureur de la République.

Son contrôle, opéré à l'occasion de l'exercice du droit d'accès indirect, quelles qu'en soient ses modalités, a pour objet de déterminer si les mentions figurant dans les fichiers STIC ou JUDEX, si elles existent, répondent lors de la demande aux conditions légales pouvant conduire à leur effacement ou à leur rectification.

Par ailleurs, la loi du 18 mars 2003 doit s'articuler avec la loi du 6 janvier 1978 ainsi que l'a rappelé le Conseil Constitutionnel dans sa décision n° 2003-467 DC du 13 mars 2003. Ainsi, il appartient au seul responsable du traitement en application de la loi du 6 janvier 1978 précitée de prendre ou non la décision d'effacement ou de rectification dans le cadre du droit d'accès indirect, crée par la loi du 18 mars 2003 et ce même lorsqu'il est tenu de suivre la position prise par le procureur de la République.

Il s'ensuit que les conclusions du magistrat sur le mérite de certaines données à être rectifiées ou à être effacées ne sont adressées qu'au responsable du traitement, celui-ci demeurant la seule autorité compétente à l'exclusion de toute autre, pour prendre ou non la décision d'effacement ou de rectification et la notifier au requérant.

Elles peuvent être cependant portées à la connaissance du requérant à simple titre de mesure d'information attestant du contrôle opéré par le magistrat sur les mentions enregistrées au STIC ou au JUDEX. Il s'ensuit que cette information, ne faisant pas grief au demandeur, est insusceptible de recours quelle qu'en soit sa nature.

On relèvera qu'une analyse similaire a été retenue par le Conseil d'État, s'agissant du fichier des renseignements généraux. Ainsi la Haute assemblée à jugé que « la lettre réponse de la CNIL doit être regardée comme informant le demandeur qu'une décision de refus de communication lui est opposée et qu'à défaut dans le texte de la lettre de précisions faisant apparaître que la demande de l'intéressé aurait été soumise à la [CNIL], le refus de communication s'analyse, eu égard aux dispositions précitées [...] du décret, en une décision du ministre de l'Intérieur et de la sécurité publique s'opposant à la communication au requérant des informations le concernant » (*CE, 23 juin 1993, M. Ruwayha*).

Ainsi, la circonstance que les prescriptions du magistrat ne puissent pas faire l'objet d'un recours ne prive en aucun cas l'intéressé de la possibilité de contester la décision finale prise par le responsable du traitement. L'accès au juge protégé par 6 de l'article de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales est donc garanti. Au surplus, l'instauration d'un recours contre les prescriptions du magistrat serait de nature à allonger le délai de traitement des demandes d'accès indirect et n'iraient donc pas dans le sens de l'intérêt des citoyens.

Cette recommandation, proposée par le Médiateur de la République, avait déjà été présentée lors des précédents travaux du groupe de travail de 2006. Elle n'avait pas fait l'objet d'un consensus et avait été rejetée par le ministère de la Justice.

En tout état de cause, le groupe de contrôle recommande la mise en place d'une procédure de notification à l'intéressé par le service gestionnaire du fichier dès lors que la décision de maintien de son inscription dans les fichiers d'antécédents judiciaires serait prise sur prescription du parquet.

La loi d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011 a prévu, dans son article 11, que, dans le cas d'une décision de relaxe ou d'acquittement pour laquelle le procureur déciderait malgré tout le maintien des données personnes dans les fichiers, il devra en aviser la personne concernée (art. 230-8 du Code de procédure pénale)

23. Sur la notion de signalement

À l'occasion de l'examen des suites réservées à la recommandation du groupe de travail de 2006 sur l'évolution de l'application « Canonge », et notamment des éléments sur les caractéristiques physiques des personnes recherchées, un débat a eu lieu sur les éléments les plus pertinents devant faciliter l'identification d'un individu suspecté d'avoir perpétré une infraction.

Les échanges ont notamment porté sur deux exigences, parfois contradictoires, et qui ont d'ailleurs fait l'objet de plusieurs contributions des membres du groupe de contrôle :
– la nécessité, pour les services de police et de gendarmerie, de disposer d'un dispositif permettant d'orienter leurs recherches lorsqu'ils sont sur les traces d'un présumé délinquant, en enquête de flagrance, en enquête préliminaire ou lors d'une instruction ;
– la nécessité de ne pas stigmatiser telle ou telle catégorie de la population en fonction de son origine ;
– le refus de toute classification ethno-raciale suivant les recommandations des Autorités administratives indépendantes et de toute utilisation des données en vue de la constitution d'un outil statistique basé sur ces données ;
– la définition d'un outil de détermination de ce que sont les « critères physiques objectifs » retenus.

Ce dispositif doit permettre d'écarter tel ou tel individu du champ d'investigation en fonction de plusieurs critères dont les caractéristiques physiques de la personne. Il doit contribuer à limiter le champ de recherche des enquêteurs et leur faciliter l'identification des mis en cause.

La question qui a fait l'objet de débats concerne la manière de caractériser une personne : doit-on utiliser l'appartenance vraie ou supposée à une origine ethno-raciale ou doit-on plutôt se servir d'une gamme chromatique telle que proposée par le milieu associatif notamment ?

L'opposition entre les partisans de l'utilisation d'une typologie telle que définis dans le thésaurus du fichier « Canonge » issu des discussions du groupe de travail de 2006 et les tenants de l'utilisation d'une solution nouvelle tournant le dos à la précédente et prônant l'utilisation d'une gamme chromatique adaptée (milieu associatif et Conférence des bâtonniers) a révélé les difficultés à trouver un dispositif équilibré entre la nécessité de l'identification des personnes recherchées et le principe de non-discrimination.

De plus, les partisans des deux solutions opposées n'ont pas considéré qu'une expérimentation concomitante des deux dispositifs fût possible en l'état.

C'est pourquoi la majorité du groupe de contrôle préconise, dans l'ensemble des fichiers sur les personnes recherchées de la police et de la gendarmerie nationales, et faisant référence à l'apparence :
– l'usage du terme « apparence » qui devra se substituer au mot « signalement » ;
– l'utilisation corrigée de la classification adoptée par le groupe de travail de 2006 :
1. type caucasien
2. type méditerranéen
3. type moyen-oriental
4. type maghrébin
5. type asiatique/eurasien
6. type amérindien
7. type indo-pakistanais
8. type métis-mulâtre
9. type africain/antillais
10. type polynésien
11. type mélanésien (dont canaque)
– en tout état de cause, la suppression du type gitan dans la typologie définie actuellement et le reclassement du stock sont recommandés.

Par ailleurs, et eu égard aux échanges sur cette problématique, le groupe de contrôle souhaite la poursuite de cette réflexion et la possibilité de poursuivre le débat dans le cadre de l'institutionnalisation éventuelle de son existence.

Suite aux réflexions menées à l'occasion de l'examen des projets TPJ et LRPPN, la démarche de sélection des thèmes inscrits dans les thésaurus (nomenclatures) des traitements a été retenue, afin d'éviter d'avoir des traitements avec des champs libres de données à remplir, mais plutôt un choix parmi un nombre limité d'items. Ce choix permet en outre une rationalisation des recherches menées par les services de police.

L'usage du terme « apparence » et la classification adoptée par le groupe de travail en 2006 ont été mis en œuvre dans le traitement CANONGE en décembre 2008.

Cette classification est en cours s'agissant du fichier des personnes recherchées et devrait être effective d'ici fin 2011.

Par ailleurs, la DGGN a été mandatée pour expérimenter un dispositif de portrait-robot informatisé (projet SOSIE).

---

25. Sur la révélation des infractions sérielles par des applications informatiques

Le groupe de travail relève que les fichiers relatifs à la révélation d'infractions sérielles (AJDRCDS, CORAIL[1], etc.) peuvent avoir une capacité de traitement des informations très large due à la possibilité importante des croisements et rapprochements qu'ils peuvent opérer.

Si le groupe de travail reconnaît l'utilité de ces applications visant à révéler une criminalité qui n'a pas pu et qui n'aurait pas pu être découverte par les dispositifs traditionnels existants, il émet des réserves sur l'idée qu'une telle capacité puisse être mise en œuvre pour l'ensemble des crimes, délits et contraventions.

Le groupe de contrôle recommande que les applications visant à révéler une criminalité inconnue par l'analyse de la sérialité soient limitées aux infractions les plus graves :

• Celles présentant un niveau de gravité qui les rendent particulièrement insupportables à la société telles que les atteintes aux personnes (homicides, agressions à caractère sexuel, coups et blessures délictuels ou criminels), les atteintes aux biens graves, le trafic de stupéfiants et la cyber-criminalité concernant les faits visés précédemment.

• Celles qui sont punies au moins de 5 années d'emprisonnement pour les atteintes aux personnes et de 7 années d'emprisonnement pour les atteintes aux biens.

Il préconise également qu'un magistrat de l'ordre judiciaire, disposant d'une compétence nationale, soit nommé et dédié au contrôle des ces applications.

La loi d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011 a prévu l'encadrement juridique des fichiers d'analyse sérielle et de rapprochement judiciaire. Il a été créé un magistrat, chargé de contrôler la mise en œuvre des logiciels de rapprochement judiciaire et de s'assurer de la mise à jour des données, désigné. Par ailleurs, la demande du groupe de travail visant à prendre comme seuil de peine pour les infractions pouvant faire l'objet des traitements d'analyse sérielle la durée de cinq années a été prise en compte (art. 230.12 du Code de procédure pénale).

1 Il est à noter que le projet « CORAIL » comporte une durée de conservation des données très limitées (3 années maximum).

Chapitre 6

La démarche qualité mise en œuvre par les directions générales de la police et de la gendarmerie nationales

Le plan d'action de la DGPN en matière de fichiers de police

À la suite du rapport du groupe de contrôle sur les fichiers de police de décembre 2008, la DGPN a mis en place un plan d'action ambitieux qui repose sur trois axes :
– un effort de régularisation massive des fichiers de police ;
– la mise en place d'un réseau de « conseillers informatique et libertés » (CIL) dans les services de police ;
– le renforcement des formations initiales et continues.

Régularisation des fichiers privés de cadre réglementaire

Dès l'été 2008, un vaste travail de recensement national de l'ensemble des fichiers existants au sein des services de police, préalable nécessaire à leur régularisation, avait été engagé. Il a permis d'identifier de nombreux fichiers locaux mais dont la grande majorité correspond en réalité à des fichiers identiques, en tout cas par leurs finalités. Ainsi, ce sont des centaines de commissariats qui ont chacun mis en œuvre leur fichier des procurations de vote ou leur fichier des fourrières et des immobilisations de véhicules.

En effet, les services de police ont souvent été conduits à créer – on pourrait même dire à « bricoler » – les outils opérationnels que ne leur fournissait pas toujours assez vite l'administration centrale. C'est même de cette manière que certains services, notamment judiciaires, ont pu améliorer grandement leur efficacité (c'est le cas par exemple avec CORAIL, à la préfecture de police). À côté de ces « bonnes » raisons – dans la mesure où il existerait de bonnes raisons de ne pas respecter la loi –, il faut avoir l'honnêteté de reconnaître les « mauvaises » : la réalité, aussi déplaisante soit-elle, est que les services de police ont mis trop longtemps à prendre conscience des contraintes juridiques mais aussi du niveau d'exigence des médias et de l'opinion en matière de fichiers.

Pour assainir la situation, une première vague de régularisations a été entreprise en partenariat avec la CNIL. Il a ainsi été décidé de recourir à des « déclarations-cadres », qui permettent de mettre en conformité avec

la loi un grand nombre de traitements ayant des caractéristiques identiques. Dans ce cas, la procédure est simple : le ministère de l'Intérieur porte à la connaissance de la CNIL, de manière globale, une catégorie des fichiers (avec les caractéristiques techniques détaillées de cette catégorie) et chacun des fichiers locaux qui s'y rattachent est de ce fait régularisé (sous réserve, en général, d'un engagement de conformité par chaque service concerné).
À titre d'exemple, le dossier de déclaration des fichiers relatifs aux « fourrières et immobilisations » a été transmis à la CNIL le 19 novembre 2010. Le ministère de l'Intérieur a également transmis à la CNIL un projet de déclaration-cadre destiné aux traitements permettant le recours à la biométrie pour le contrôle des accès aux locaux et, éventuellement, la gestion et le contrôle du temps de travail.

Les dossiers de déclaration des traitements relatifs au contrôle judiciaire, aux assignations à résidence, aux permissions de sortir ou encore aux débits de boissons, qui sont en cours d'achèvement, devraient également être transmis prochainement à la CNIL.

D'autre part, la CNIL a dispensé le ministère de déclarer les registres de procuration de vote.

Dans d'autres cas, les fichiers locaux devront tout simplement être supprimés, notamment parce qu'un traitement national en assure les fonctions. C'est le cas notamment de la plupart des fichiers relatifs à la gestion du personnel, qui n'ont pas lieu d'être dès lors qu'il existe Dialogue et Géopol.

Au terme de cette démarche, qui prendra nécessairement plusieurs années, la police nationale aura régularisé (ou supprimé) la grande majorité des fichiers irréguliers. Mais pour que de tels fichiers ne réapparaissent pas, il faut aussi, de manière encore plus ambitieuse, remettre les services de police à niveau en matière de droit des fichiers pour que celui-ci soit mieux pris en compte par les services au quotidien.

C'est l'objet des deux autres axes d'action.

Création d'un réseau territorial de « conseillers informatique et libertés » (CIL)

Mis en place par la circulaire du DGPN du 3 novembre 2010, le réseau des CIL comprend dans les services territoriaux plus de 180 personnes qui sont notamment chargées, en lien avec leur « CIL central » :
– de mieux identifier les fichiers mis en œuvre localement et, si besoin, de les signaler pour qu'ils puissent être déclarés de manière cohérente et ordonnée à la CNIL ;
– de conseiller les services opérationnels quant à l'opportunité de déployer, au niveau local ou au niveau central, des projets de fichiers et quant au cadre juridique et à l'architecture les plus adaptés ;
– d'assister les services lors de l'élaboration d'un dossier de déclaration ;
– d'être les interlocuteurs, au sein des services territoriaux, de l'administration centrale qui disposera ainsi de relais efficaces.

Plus largement, il s'agit de diffuser au sein des services opérationnels une « culture informatique et libertés » qui leur fait actuellement défaut. L'ensemble des CIL ont bénéficié le 9 février d'une journée de formation ouverte par le directeur général de la police nationale, en présence du président du groupe de contrôle des fichiers de police ; ils bénéficieront ensuite, au cours de cette année, de formations assurées à l'échelon régional.

Enfin, la formation initiale a été renforcée à tous les niveaux de recrutement et, au titre de la formation continue, des formations régionales sont en cours d'élaboration avec la DRCPN.

Enfin, la DGPN s'est dotée d'une capacité juridique et opérationnelle sans précédent en matière de fichiers de police grâce à la constitution d'une équipe spécialisée, placée au cabinet du directeur général. Cette équipe est chargée, en lien avec les services opérationnels, de l'élaboration complète des dossiers de déclaration des fichiers auprès de la CNIL, du conseil aux services opérationnels et de la conception et de la mise en œuvre du programme de régularisation et de formation détaillé dans le présent plan d'actions.

Renforcement des formations

La formation initiale a été renforcée à tous les niveaux de recrutement : au-delà des règles d'utilisation des fichiers, sont désormais abordés les grands principes de la loi de 1978 et les obligations de déclaration.

Un manuel de droit appliqué des fichiers de police a été largement diffusé, principalement à l'intention des formateurs.

En ce qui concerne la formation continue, les outils pédagogiques sont en cours d'élaboration, notamment pour les CIL.

Le plan d'action de la DGGN en matière de fichiers de gendarmerie

Des structures de gouvernance au niveau de l'administration centrale [1]

• Depuis 2008, une **Mission permanente de suivi des systèmes d'information (MPSSI)**, à vocation principalement opérationnelle, a été placée sous la responsabilité du conseiller juridique et judiciaire (magistrat de l'ordre judiciaire) du directeur général de la gendarmerie nationale, afin d'assurer un pilotage stratégique global.

• En février 2010, un **Groupe des référents fichiers (GréFic)**, à vocation opérationnelle, réunissant **22 référents centraux** des sous-directions de la DGGN et autres organismes centraux (STRJD, *etc.*), est venu prolonger le travail de la MPSSI. Ce groupe met régulièrement à jour l'inventaire des bases centrales et identifie pour chacune d'entre elles les responsables fonctionnels et techniques. Il administre le référentiel des droits d'accès (RDA) en définissant le profil des utilisateurs, répondant ainsi aux exigences de la Commission nationale de l'informatique et des libertés (CNIL) en matière de sécurité des données.

• Un **officier supérieur**, sous l'autorité du DOE et en lien avec le cabinet DGGN, a pris ses fonctions en décembre 2010 en tant que **chargé de projet « suivi des fichiers / informatique et libertés ».** Secrétaire général de la **MPSSI** et animateur du **GréFic** précédemment mentionnés, **référent** « informatique et libertés », il assure une mission de suivi d'ensemble des différents traitements de données à caractère personnel, et de coordination générale des formations centrales impliquées dans ce domaine. Il entretient des relations avec les partenaires ministériels (**DGPN, DLPAJ**...) et siège au groupe de travail sur l'amélioration du contrôle et de l'organisation des bases de données de gendarmerie et police.

Des relais déconcentrés dans les régions et formations assimilées

Le dispositif vient enfin d'être parachevé au 1er janvier 2011, en application des recommandations du rapport du groupe de contrôle présidé par Alain Bauer, par la désignation de **référents « informatique et libertés » au sein des régions** et organismes assimilés. Au nombre de **31** (parfois relayés

1 Exemple de décisions récentes de pilotage : dès le 22 octobre 2010, par note, le DGGN prohibait l'appellation MENS ; la gendarmerie nationale a par ailleurs choisi de confier en mars 2011 l'administration du fichier administratif SDRF à une unité administrative (centre technique de la gendarmerie nationale) et non plus au STRJD, unité judiciaire.

par des référents auxiliaires), conseillers des commandants de région ou de formation assimilée, ils sont des relais d'information efficaces entre la DGGN et les unités.

Leur rôle est notamment de veiller à ce que les éventuels projets de fichiers locaux satisfassent à la loi et au règlement d'une part, et ne créent pas de doublon avec un traitement central existant d'autre part. Un mémento « informatique et libertés » et un *Que sais-je ?* leur ont été distribués début février 2011.

Un travail mené de front avec la police nationale

En effet, le **Service des technologies et des systèmes d'information de la sécurité intérieure [ST (SI) 2]** est actif depuis septembre 2010. Service commun gendarmerie-police, placé au sein de la Direction générale de la gendarmerie nationale, il a vocation à assurer la conception et la réalisation des systèmes d'information et de communication de la gendarmerie et de la police nationales. Il permettra donc de développer des convergences et synergies nouvelles en matière de traitements automatisés de données.

Le respect de l'éthique et de la déontologie

Un Bureau du contrôle et de l'évaluation des fichiers (BCEF) a été créé au sein de l'Inspection générale de la gendarmerie nationale (IGGN) dès 2009. Il veille à l'utilisation conforme des bases de données et procède, à ce titre, à des contrôles d'initiative ou à la demande. Il s'appuie, en tant que de besoin, sur le bureau du contrôle de la sécurité des systèmes d'information (BCSSI) de l'IGGN.

L'IGGN peut en outre s'appuyer sur un dispositif logiciel de **traçabilité des connexions** aux fichiers opérationnels ou sensibles. Ce logiciel permet, fichier par fichier, d'identifier soit des unités, soit des militaires au comportement anormal au regard des normes habituellement constatées et de leurs profils, sur des périodes considérées. Il autorise en outre l'édiction de rapports d'analyse de ces traces.

De surcroît, l'IGGN a diffusé des questionnaires d'auto-évaluation aux unités de niveau départemental ou régional afin de déceler des incompréhensions ou faiblesses.

Une formation adéquate

Des espaces pédagogiques « fichiers » existent depuis plus de deux ans sur **l'intranet gendarmerie**. Et la **circulaire interne** (mémorial gendarmerie) portant sur l'application de la loi susvisée a été refondue afin de renforcer certains éléments de langage.

Un **séminaire d'approfondissement** au profit des commandements de groupements de gendarmerie départementale et spécialisée, de sections de recherches et offices centraux a en outre été organisé début février 2011.

Enfin, toute mise en place d'un fichier en gendarmerie est obligatoirement précédée d'une **triple formation (juridique, éthique, technique)** : formation initiale, formation continue, formation des formateurs, formation des utilisateurs, didacticiels... Il faut au surplus préciser que certains postes nécessitent obligatoirement une formation plus poussée en matière de fichiers, à l'image des militaires affectés en BDRIJ (5 semaines au centre national de formation à la police judiciaire de Fontainebleau) ou les analystes criminels qui disposent désormais d'une formation universitaire diplômante de type DU voire master dans le cadre d'un partenariat gendarmerie-Université de Troyes (mise en exergue par l'Union européenne dans le cadre du 5° cycle d'évaluations mutuelles relatives à la lutte contre la délinquance économique et financière – rapport France d'avril 2010).

Chapitre 7

Les contributions des membres du groupe

La contribution de SOS Racisme

Dans le cadre de la commission de contrôle des fichiers de police, nous avons à connaître des projets de décrets ou d'arrêtés créant ou modifiant des fichiers de gestion de l'activité policière : renseignement, enquêtes administratives ou judiciaires.

La discussion n'est pas toujours aisée et nous devons faire preuve d'une grande vigilance s'agissant de la mention de données révélant directement ou indirectement l'origine ethnique des individus dans une part importante des projets qui nous sont soumis.

Au-delà de la mention de ces données, nous avons constaté que la finalité de certains fichiers n'était pas souvent strictement définie. À titre d'exemple un fichier de police judiciaire peut être amené à se muer en un fichier administratif.

Par ailleurs, bien souvent le préambule de l'acte créateur du fichier concerné mentionne régulièrement la possibilité d'établir des études statistiques qui, selon notre analyse, peuvent emporter certaines dérives (ex : fichier GESI).

Enfin, la question de la mutualisation et de l'interconnexion des fichiers existant pose un grave problème au regard de la protection des données personnelles.

La collecte de l'origine ethnique sous couvert de l'origine géographique

Fichiers PASP / GISPAP

Nous avons engagé deux recours en annulation à l'encontre des décrets mettant en œuvre les fichiers PASP et GISPAP. La procédure est en cours et porte principalement sur la possibilité dans le cadre d'atteinte potentielle à la sureté de l'État d'enregistrer des données relatives à « l'origine géographique ». Le ministère de l'Intérieur estime qu'il s'agirait uniquement de données objectives telles que le lieu de résidence. Pour autant, aux termes d'une circulaire adressée aux préfets, l'origine géographique pourrait également s'entendre comme le lieu de naissance, et donc de provenance. Les

différentes versions données quant à la signification de cette notion laisse penser qu'elle serait susceptible de révéler, à tout le moins de façon indirecte, l'origine ethnique des personnes concernées.

Bien qu'une procédure soit toujours en cours, les services du ministère de l'Intérieur ont déjà commencé à utiliser cette nomenclature que nous considérons comme étant illicite.

Par ailleurs, les récentes modifications des décrets PASP et GISPAP – qui n'ont pas porté sur la notion «d'origine géographique» contrairement aux recommandations de la commission – ont permis d'élargir la finalité première du fichier initialement destiné à la protection de la sûreté de l'État. En effet, les agents peuvent se servir de cette base pour la réalisation d'enquête administrative dans le cadre de l'acquisition de la nationalité française. Il y a donc là un détournement certain de la finalité première du fichier.

Fichiers de travail de la gendarmerie nationale

On retrouve la mention de l'origine géographique dans le décret récemment promulgué portant sur les fichiers de travail de police judiciaire des unités de recherches de la gendarmerie nationale. La DGGN s'était engagée à supprimer cette mention. Une fois encore les recommandations de la commission n'ont pas été prises en compte.

La création de fichiers clandestins : vers un profilage ethnique de la délinquance

Au-delà de Mens...

La circulaire du 5 août 2010 concernant les démantèlements de campements illicites de Roms.

Étaient annexés à cette circulaire des modèles de synthèses – distinguant les campements d'une part des Roms et d'autre part, ceux des Gens du voyage – devant être transmises aux services du ministère de l'Intérieur. Nous considérons que pour renseigner ces tableaux, a nécessairement été mis en place en amont un système de fichage ethnique des occupants Roms des camps démantelés.

Nous avons donc saisi la CNIL en parallèle du recours en annulation que nous avons engagé à l'encontre de la circulaire devant le Conseil d'État.

La haute juridiction a considéré que le texte était bien entaché d'une illégalité. De son côté, la CNIL n'a pas donné de suite favorable à notre demande au motif que ces données ne se rapportaient pas à des données personnelles. Nous avons contesté cette analyse rappelant que la notion de données personnelles renvoie à la possibilité d'identifier directement ou indi-

rectement les personnes concernées par l'enregistrement, ce qui peut être le cas en l'espèce.

Les fichiers du Val de Marne

La préfecture de police de Paris a enjoint ses services de comptabiliser le nombre de personnes interpelées dès lors qu'elles étaient originaires des « pays de l'Est ». La Direction de la sécurité de proximité de l'agglomération parisienne et l'état-major de la police judiciaire ont ensuite transmis ces consignes à la DTSP du Val de Marne et ce système a été mis en place dans 17 commissariats.

Si les données renseignées sont *a priori* basées sur des éléments objectifs, tels que la nationalité, mentionnés dans les registres du commissariat, il n'en demeure pas moins que le regroupement réalisé sous le vocable « pays de l'Est » apparaît illicite, car n'étant pas une catégorie juridiquement définie.

Ces deux instruments, qui n'ont pas fait l'objet de la procédure préalable d'avis de la part de la CNIL et du Conseil d'État, risquent de conduire à la commission de pratiques illégales telles que le contrôle d'identité au faciès.

Le risque de détournement des finalités de certains fichiers

Le fichier GESI, qui prévoit la gestion en temps réel des étrangers en situation irrégulière appartient à la catégorie des fichiers de police judiciaire. Ce fichier intervient en complément du fichier administratif de gestion de dossiers d'étrangers AGDREF. Au-delà de la finalité d'améliorer la gestion des procédures d'expulsion, le décret instaurant le fichier GESI prévoit la possibilité de procéder à « *l'exploitation des données contenues à des fins de recherches statistiques* ». Nous estimons que cette possibilité peut mener à des dérives détournant le fichier de sa finalité première.

Les risques de l'utilisation d'une identification des personnes signalées basée sur des types prédéfinis

Dans le cadre des signalements des individus, le fichier CANONGE prévoyait une classification basée sur des types prédéfinis. Cette classification est reprise dans les fichiers TPJ et LRPN. À notre sens, cette classification est contraire aux principes de protection des données personnelles. Dans cette mesure nous proposons que soit simplement fait une description physique de la personne signalée, sans qu'il soit nécessaire de se baser sur une base chromatique.

Les recommandations de SOS Racisme

• Assurer un inventaire et une transparence réelle sur les fichiers de police par le biais d'un audit externe.

• Supprimer toutes catégories révélant l'appartenance ethnique directe ou indirecte et notamment la notion « origine géographique ».

• Conditionner la création de nouveaux fichiers à une approbation législative.

• Mettre en place une communication annuelle du ministre de l'Intérieur sur la création et le fonctionnement des fichiers de police.

La contribution de la LICRA

La LICRA a accueilli favorablement le souhait exprimé par le ministre de l'Intérieur à l'automne 2009 de pérenniser et d'institutionnaliser le groupe de travail sur les fichiers de police et de gendarmerie et s'est réjoui de la volonté ainsi affirmée de transparence, de rationalisation et de régularisation de ses fichiers.

À ce titre, la LICRA a participé assidument aux travaux de ce groupe.

La LICRA ne peut qu'être satisfaite de la mise en place de référents locaux « informatiques et libertés » pour la Gendarmerie et de conseillers « informatiques et libertés » pour la Police nationale. Il est ainsi démontré qu'au-delà du travail de recensement effectué, le Ministère souhaite veiller et parer à toute éventualité de création de fichiers non déclarés.

Néanmoins, la LICRA continue de déplorer que des points de polémiques, ayant justement conduit à justifier l'existence de ce groupe de travail, n'aient pas été résolus.

Malgré les polémiques sur les fichiers CRISTINA, EDVIGE, EDVIRSP, le ministère persiste et signe sur l'origine géographique

Dès octobre 2009, dans un courrier adressé au ministre de l'Intérieur M. Brice Hortefeux, la LICRA avait fait part de ses interrogations et fortes réserves quant à la mention, au titre des données sensibles, des « origines géographiques ».

En effet :
– soit c'est une information sensible, à savoir à caractère personnel (art. 8 loi informatique et liberté de 1978) : la LICRA demande à ce que le contenu et la finalité de ce type d'information soit précisée ;
– soit ce n'est pas une information sensible parce que cela concerne l'adresse des personnes fichées (quartiers, villes) : la LICRA demande à ce que cette mention sur l'origine géographique apparaisse dans une autre disposition du Décret (sans le fondement de l'article 8 de la loi de 1978).

La LICRA avait alors pris acte des engagements exprimés par le ministère devant le groupe de travail sur les fichiers d'adresser une circulaire aux préfets rappelant qu'aucune donnée relative aux origines raciales ou ethniques des personnes ne devait y figurer.

Par la suite, les représentants du ministère s'étaient engagés, toujours, devant les membres du groupe de travail sur les fichiers, à ce que la mention relative aux origines géographiques soit supprimée dans le prochain fichier PASP.

Aujourd'hui, la LICRA note que décret du 29 mars 2011 sur le fichier PASP reprend encore la mention relative aux origines géographiques au titre des informations dites « sensibles » (article 3 décret n° 2011-340 du 29 mars 2011).

La LICRA ne peut que réitérer sa plus grande réserve sur le maintien de cette donnée dans les fichiers de renseignements et demande à ce que ces données soient supprimées.

La LICRA demande par ailleurs qu'un bilan des données figurant au titre des origines géographiques dans les actuels fichiers PASP soit présenté au groupe de travail pour évaluer leur sensibilité ou le respect de la circulaire.

Des extractions par nationalité qui doivent être limitées et justifiées

La tendance à l' « ethnicisation » dans l'interprétation des phénomènes de délinquance ne peut qu'inquiéter la LICRA. Outre leur caractère illicite, cela ne peut que desservir les objectifs de prévention et de lutte contre la délinquance.

À cet égard, les fichiers de police et de gendarmerie sont un outil à utiliser avec la plus grande vigilance car la création de nouveaux fichiers ou les extractions malveillantes ou maladroites de certaines informations dans les fichiers existants sont aisées.

Il en est ainsi de la nationalité, laquelle n'est pas une mention « sensible » au sens de la loi de 1978 dite informatique et liberté mais qui peut facilement être instrumentalisée.

La LICRA demande ainsi à ce que les fichiers de police ou de gendarmerie n'utilisent la mention de la nationalité que pour des motifs justifiés et explicités.

La LICRA demande à ce que les référents ou conseillers « informatiques et libertés » reçoivent une formation et une sensibilisation nécessaire pour mettre fin aux erreurs qui ont pu être déplorées en ce sens en 2010, telle cette note rédigée par un commandant de la brigade de gendarmerie de Hochfeden appelant à signaler le comportement suspect d'individus étrangers et particulièrement des personnes originaires des pays de l'Est et des Balkans ou telle que le listing des interpellés Roumains qui semblent avoir été mis en place par la Direction de la sécurité de proximité de l'agglomération parisienne (DSPAP), notamment dans le Val de Marne.

La mise en place d'un groupe de réflexion sur la classification par « apparence » sur la base de type ethno-racial du CANONGE

La LICRA fait partie des opposants à l'utilisation de la typologie Canonge afin d'identifier les personnes recherchées, y compris sur la base de l'« apparence » (types caucasien, méditerranéen, moyen-oriental, maghrébin, asiatique/eurasien, amérindien, indo-pakistanais, métis-mulâtre, africain/antillais, polynésien, mélanésien).

La LICRA appelle à la mise en place d'un groupe de réflexion *ad hoc* afin de faire avancer ce débat en particulier et réfléchir à des référencements plus objectifs permettant l'identification des personnes recherchées, tels que ceux relatifs à la gamme chromatique.

La contribution de la HALDE

La HALDE a participé depuis 2008 au groupe de travail sur les fichiers de police et a concouru à la réflexion collective à travers plusieurs contributions écrites.

En premier lieu, concernant les fichiers de police voués à remplacer les fichiers des renseignements généraux, la HALDE s'est réjouie de l'existence de deux outils distincts qu'elle avait appelée de ses vœux, l'un relatif à la prévention des atteintes à la sécurité publique, l'autre aux enquêtes administratives, a lieu et place d'un fichier unique tel EDVIGE ou EDVIRSP, évitant ainsi la possibilité d'interconnexion de fait.

Toutefois, elle s'est notamment inquiétée du fait que des **données liées à « l'origine géographique »** puissent être recensées. En effet, dans la mesure où cette mention est classée, dans le décret, au paragraphe sur les données sensibles, la notion d'origine ne semble pas seulement d'ordre « géographique » mais semble davantage viser à remplacer la très contestée référence aux origines raciales ou ethniques. À défaut de précision, **la**

haute autorité avait réitéré ses recommandations tendant ce que ne puissent plus apparaître l'origine ethnique des personnes fichées, la notion de « signes physiques particuliers et objectifs » étant suffisante pour parvenir aux buts poursuivis par le traitement automatisé.

La circulaire du 18 octobre 2009 du ministre de l'Intérieur précise les termes de l'article 3 du décret en indiquant que *« le présent traitement ne pourra en aucun cas comporter de données relatives aux origines raciales et ethniques ».* Le ministre explique dans cette même circulaire que *« les données relatives à l'origine géographique des personnes se limitent à l'indication de leur provenance, l'appartenance à un même quartier ou le partage d'un même lieu de naissance [pouvant], par exemple, jouer un rôle déterminant. »*

Si ces indications paraissent claires, elles ne semblent néanmoins pas pouvoir, à elles seules, permettre d'exclure tout risque lié au recensement, sur ce fondement, de données relatives à l'origine dite ethnique. À ce titre, on peut, en effet, s'interroger sur la raison pour laquelle les données liées à l'origine géographique sont considérées dans le décret comme des données sensibles si elles consistent exclusivement à recenser des informations sur le lieu de naissance ou de résidence.

En second lieu, le Collège de la haute autorité a, comme d'autres membres du groupe, donné un avis défavorable à la classification proposée dans la rubrique « signalement » du fichier STIC-Canonge. Outre les six rubriques principales qui peuvent être renseignées (état civil, sexe, âge, taille, surnom et alias, fait historique, signalement, pilosité, yeux, cheveux ; signes particuliers, photos anthropométriques), une partie « signalement » comporte un filtre sur le « type », lequel distingue 12 types différents : Blanc (caucasien), Méditerranéen, Gitan, Moyen-Oriental, Nord africain Maghrébin, Asiatique Eurasien, Amérindien, Indien (Inde), Métis-Mulâtre, Noir, Polynésien, Mélanésien-canaque.

Les risques de généralisation de l'utilisation de tels « types » dans le travail quotidien des services de police ont conduit la haute autorité à se prononcer sur l'avis sollicité par le groupe de travail.

En matière de fichiers de police, la haute autorité a déjà eu à se prononcer, dans la délibération 2008-233 du 20 octobre 2008, aux termes de laquelle le Collège a recommandé d'exclure de la dérogation prévue à l'article 2 du projet de décret les données liées à l'origine ethnique des personnes fichées. Il a précisé que la notion de « signes physiques particuliers et objectifs » était suffisante pour parvenir aux buts poursuivis par le traitement automatisé.

En l'espèce, la question qui se pose est celle de la définition des « signes physiques particuliers et objectifs ». Or, à l'occasion de sa première réunion en 2006, le groupe de travail sur les fichiers avait préconisé une nouvelle déclinaison : type européen (nordique, caucasien, méditerranéen), type africain/antillais, type métis, type maghrébin, type moyen-oriental, type asiatique, type indo-pakistanais, type latino-américain, type polynésien.

À ce jour, et au vu des éléments échangés au sein du groupe de travail, les services de police n'ont pas mis en œuvre cette nouvelle liste et ce,

pour des problèmes techniques (difficulté à requalifier le stock des données par ces nouveaux types).

Pour la HALDE, la typologie ainsi proposée, comme celle qui existe déjà, fait donc davantage référence à l'origine dite « ethnique » des personnes qu'à leurs caractéristiques physiques objectives. 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.

Ce sont pour ces raisons qu'elle a donné un avis défavorable à une telle classification.

Annexes

Annexe 1

Composition du groupe de travail sur les fichiers de police et de gendarmerie (juin 2006-décembre 2006)

Alain Bauer, président du conseil d'orientation de l'Observatoire national de la délinquance, président du groupe de travail

Michel Gaudin, directeur général de la police nationale

Général Guy Parayre, directeur général de la gendarmerie nationale

Martine Monteil, directeur central de la police judiciaire

Pierre Bousquet de Florian, directeur central de la surveillance du territoire

Joël Bouchite, directeur central des renseignements généraux

Philippe Laureau, directeur central de la sécurité publique

Jacques Lamotte, directeur de l'Inspection générale de la police nationale

Général Edmond Buchheit, inspecteur de la gendarmerie nationale

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

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

Stéphane Fratacci, directeur des libertés publiques et des affaires juridiques

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

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

Alex Türk, président de la CNIL, représenté par François Giquel, vice-président

Jean-Paul Delevoye, Médiateur de la République, représenté par Serge Petit

Pierre Truche, président de la CNDS, représenté par Jean Bonnard

Bruno Thouzellier, Union syndicale des magistrats

Bruno Beschizza, Synergie Officiers

Joaquim Masanet, UNSA Police

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

Maître Franck Natali, avocat, président de la conférence des bâtonniers

Frédéric Ploquin, journaliste, *Marianne*

Maître Henri Leclerc, sollicité, n'a pu participer aux travaux.

Christophe Soullez, criminologue, chef du département OND, rapporteur du groupe de travail

Annexe 2

Composition du groupe de travail sur les fichiers de police et de gendarmerie (septembre-décembre 2008)

Président : M. Alain Bauer, Criminologue, président du conseil d'orientation de l'OND

Secrétaire général : M. André-Michel Ventre, inspecteur général de la police nationale

Rapporteur : M. Christophe Soullez, criminologue, chef du département OND, INHES

– M. le directeur général de la police nationale (Frédéric Péchenard)

– M. le directeur général de la gendarmerie nationale (Général Roland Gilles)

– Monsieur le préfet de police (Michel Gaudin)

– M. le directeur des libertés publiques et des affaires juridiques (Laurent Touvet)

– M. le directeur des affaires criminelles et des grâces (Jean-Marie Huet)

– M. le président de la CNIL (Alex Türk) représenté par Jean-Marie Cotteret

– M. le président de la HALDE (Louis Schweitzer)

– M. le président de la CNCDH (Joël Thoraval)

– M. le médiateur de la République (Jean-Paul Delevoye) représenté par Luc Charrié

– M. le secrétaire général de Synergie Police (Bruno Beschizza)

– M. le secrétaire général de l'UNSA Police (Henri Martini)

– Mme le secrétaire général du SCPN (Sylvie Feucher)

– M. le président de l'Union syndicale des magistrats (Christophe Regnard)

– Mme la présidente du Syndicat de la magistrature (Emmanuelle Perreux)[1]

1 Le Syndicat de la magistrature a souhaité quitter le groupe de travail le 17 novembre 2008.

– M. le président du Conseil national des barreaux (Paul-Albert IWEINS)

– M. le président de la Conférence des bâtonniers (Pascal EYDOUX)

– M. le bâtonnier de Paris (Christian CHARRIÈRE-BOURNAZEL)

– M. le président de la LICRA (Patrick GAUBERT)

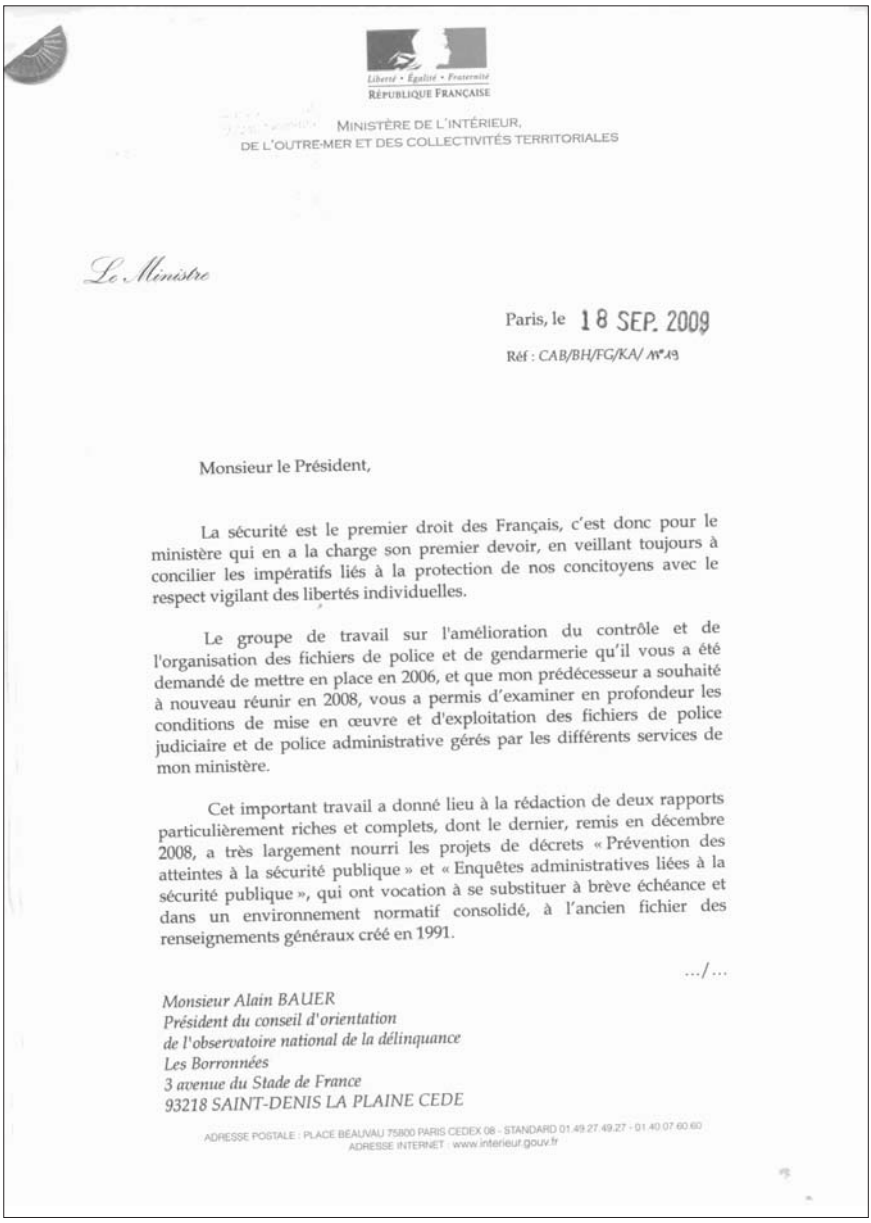
– M. le président de SOS Racisme (Dominique SOPO)

– M. le président de SOS Homophobie (Jacques LIZE)

– M. Jean-Marc LECLERC, journaliste, *Le Figaro*

Annexe 3

Lettre de mission [1]



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INTÉRIEUR,
DE L'OUTRE-MER ET DES COLLECTIVITÉS TERRITORIALES

Le Ministre

Paris, le 18 SEP. 2009

Réf : CAB/BH/FG/KA/ N°49

Monsieur le Président,

La sécurité est le premier droit des Français, c'est donc pour le ministère qui en a la charge son premier devoir, en veillant toujours à concilier les impératifs liés à la protection de nos concitoyens avec le respect vigilant des libertés individuelles.

Le groupe de travail sur l'amélioration du contrôle et de l'organisation des fichiers de police et de gendarmerie qu'il vous a été demandé de mettre en place en 2006, et que mon prédécesseur a souhaité à nouveau réunir en 2008, vous a permis d'examiner en profondeur les conditions de mise en œuvre et d'exploitation des fichiers de police judiciaire et de police administrative gérés par les différents services de mon ministère.

Cet important travail a donné lieu à la rédaction de deux rapports particulièrement riches et complets, dont le dernier, remis en décembre 2008, a très largement nourri les projets de décrets « Prévention des atteintes à la sécurité publique » et « Enquêtes administratives liées à la sécurité publique », qui ont vocation à se substituer à brève échéance et dans un environnement normatif consolidé, à l'ancien fichier des renseignements généraux créé en 1991.

.../...

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

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

1 18 septembre 2009, Brice Hortefeux, ministre de l'Intérieur, de l'Outre-mer et des Collectivités territoriales réactivant le groupe de travail sur les fichiers

Compte-tenu de la qualité des travaux conduits sous votre autorité, de l'expérience acquise par le groupe de travail en matière de traitements automatisés de police et de gendarmerie, et de l'attention de tous les instants que requiert la protection des libertés, je souhaite pérenniser ce groupe de travail.

A cet effet, vous voudrez bien trouver ci-joint un projet d'arrêté par lequel il est créé auprès du ministre de l'intérieur, de l'outre-mer et des collectivités locales une telle structure, dont l'objet est précisé à l'article 2 :

« Le groupe de travail exprime au ministre de l'intérieur des orientations et recommandations sur les conditions générales de création et d'utilisation des fichiers de police et de gendarmerie et sur la cohérence d'ensemble du développement de ces fichiers au regard des évolutions technologiques et des contraintes opérationnelles. Il assure à intervalles réguliers un recensement de ces fichiers. Il peut être saisi par le ministre de toute question relative à ce domaine. »

Naturellement, vous pourrez compter sur l'appui constant de mes services pour faciliter la conduite de cette mission, dont je vous saurais gré de bien vouloir me rendre compte à intervalles réguliers, et autant de fois que vous l'estimerez nécessaires au regard notamment de la sensibilité de cette question dans l'opinion.

Je vous prie de croire, Monsieur le Président, à l'assurance de mes sentiments les meilleurs.

Brice HORTEFEUX

Arrêté du 20 octobre 2009 portant création d'un groupe de travail sur l'amélioration du contrôle et de l'organisation des bases de données de police

NOR : IOCD0922534A

Le ministre de l'Intérieur, de l'Outre-mer et des Collectivités territoriales,

Vu la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,

Arrête :

Article 1

Il est créé auprès du ministre de l'Intérieur, de l'Outre-mer et des Collectivités territoriales un groupe de travail relatif aux bases de données de la police et de la gendarmerie.

Article 2

Le groupe de travail adresse au ministre de l'Intérieur des orientations et recommandations sur les conditions générales de création et d'utilisation des fichiers de police et de gendarmerie et sur la cohérence d'ensemble du développement de ces fichiers au regard des évolutions technologiques et des contraintes opérationnelles. Il assure à intervalles réguliers un recensement de ces fichiers.

Il peut être saisi par le ministre de toute question relative à ce domaine.

Article 3

Le groupe de travail comprend vingt-cinq membres, désignés pour quatre ans :

a) Cinq représentants du ministère de l'Intérieur :

– le secrétaire général du ministère de l'Intérieur ;
– le directeur général de la police nationale ;
– le directeur général de la gendarmerie nationale ;
– le préfet de police ;
– le directeur des libertés publiques et des affaires juridiques ;

b) Un magistrat désigné par le ministre de la Justice ;
c) Un représentant de la Commission nationale de l'informatique et des libertés ;
d) Un représentant de la Haute autorité de lutte contre les discriminations et pour l'égalité ;
e) Un représentant de la Commission nationale consultative des droits de l'homme ;
f) Un représentant du Médiateur de la République ;
g) Trois représentants des syndicats de police ;
h) Deux représentants des syndicats de magistrats ;
i) Un représentant du Conseil national des barreaux ;
j) Un représentant de la Conférence des bâtonniers ;
k) Un représentant du bâtonnier de Paris ;
l) Quatre représentants des associations de lutte contre les discriminations ;
m) Trois personnalités qualifiées désignées par le ministre de l'Intérieur ;
n) Le président du groupe de travail est nommé par le ministre de l'Intérieur parmi les membres de la commission.

Article 4

Le groupe de travail se réunit, à l'initiative de son président ou sur demande du ministre de l'Intérieur, au moins une fois par an. En cas d'empêchement, chacun des membres peut se faire représenter.

Il fait parvenir au ministre de l'Intérieur un relevé des conclusions de chacune de ses réunions.

Son secrétariat est assuré par les services du ministre de l'Intérieur.

Article 5

Les membres du groupe de travail exercent leurs fonctions à titre gratuit.

Ils peuvent bénéficier du remboursement de leurs frais de déplacement et de séjour dans les conditions prévues par la réglementation applicable aux fonctionnaires de l'État.

Article 6

Le secrétaire général du ministère de l'Intérieur, le directeur général de la police nationale, le directeur général de la gendarmerie nationale, le préfet de police et le directeur des libertés publiques et des affaires juridiques sont chargés, chacun en ce qui le concerne, de l'exécution du présent arrêté, qui sera publié au *Journal officiel de la République française*.

Fait à Paris, le 20 octobre 2009.

Brice Hortefeux

Annexe 5

Composition du travail sur l'amélioration du contrôle et de l'organisation des fichiers de police et de gendarmerie (arrêté du 15 avril 2010)

Décrets, arrêtés, circulaires

MESURES NOMINATIVES

MINISTÈRE DE L'INTÉRIEUR, DE L'OUTRE-MER ET DES COLLECTIVITÉS TERRITORIALES

Arrêté du 15 avril 2010 désignant les membres du groupe de travail sur l'amélioration du contrôle et de l'organisation des bases de données de police créé par arrêté du 20 octobre 2009

NOR : *IOCD1008176A*

Par arrêté du ministre de l'intérieur, de l'outre-mer et des collectivités territoriales en date du 15 avril 2010, sont désignés membres du groupe de travail sur l'amélioration du contrôle et de l'organisation des bases de données de police créé par arrêté du 20 octobre 2009 :

a) Représentant le ministère de l'intérieur :

M. Comet (Henri-Michel), secrétaire général du ministère de l'intérieur ;
M. Péchenard (Frédéric), directeur général de la police nationale ;
M. le général Mignaux (Jacques), directeur général de la gendarmerie nationale ;
M. Gaudin (Michel), préfet de police de Paris ;
M. Touvet (Laurent), directeur des libertés publiques et des affaires juridiques ;

b) Mme Caillibotte (Maryvonne), directrice des affaires criminelles et des grâces ;

c) M. Türk (Alex), président de la Commission nationale de l'informatique et des libertés ;

d) M. Dubourdieu (Marc), directeur général de la Haute Autorité de lutte contre les discriminations et pour l'égalité ;

e) M. Repiquet (Yves), président de la Commission nationale consultative des droits de l'homme ;

f) M. Delevoye (Jean-Paul), Médiateur de la République ;

g) M. Beauvois (Roger), président de la Commission nationale de déontologie de la sécurité ;

h) Représentant les syndicats de police :

Mme Feucher (Sylvie), secrétaire générale du Syndicat national des commissaires de police ;
M. Boisteaux (Olivier), secrétaire général du Syndicat indépendant des commissaires de police ;
M. Comte (Nicolas), secrétaire général de l'Union SGP - Unité police FO ;
M. Ribeiro (Patrice), secrétaire général adjoint de Synergie police ;
M. Achispon (Dominique), secrétaire général du Syndicat national des officiers de police ;
M. Delage (Jean-Claude), secrétaire général d'Alliance ;

i) Représentant les syndicats de magistrats :

M. Régnard (Christophe), président de l'Union syndicale des magistrats ;
M. Bonduelle (Matthieu), secrétaire général du Syndicat de la magistrature ;

j) M. Wickers (Thierry), président du Conseil national des barreaux ;

k) M. Pouchelon (Alain), président de la Conférence des bâtonniers ;

l) M. Castelain (Jean), bâtonnier de Paris ;

m) Représentant les associations de lutte contre les discriminations :

M. Jakubowicz (Alain), président de la Ligue internationale contre le racisme et l'antisémitisme ;
M. Sopo (Dominique), président de SOS racisme ;
M. Lozès (Patrick), président du Conseil représentatif des associations noires ;
M. Poisson (Guillaume), président de SOS homophobie ;

n) Personnalités qualifiées désignées par le ministre de l'intérieur :

M. Bauer (Alain), professeur de criminologie au Conservatoire national des arts et métiers, président du groupe de travail ;

M. Ventre (André-Michel), directeur de l'Institut national des hautes études de la sécurité, secrétaire général du groupe de travail ;

M. Soullez (Christophe), chef du département observatoire national de la délinquance à l'Institut national des hautes études de la sécurité, rapporteur du groupe de travail ;

M. Leclerc (Jean-Marc), journaliste, *Le Figaro*.

Décret nº 2009-1249 du 16 octobre 2009 portant création d'un traitement de données à caractère personnel relatif à la prévention des atteintes à la sécurité publique

JORF nº 0242 du 18 octobre 2009

Décret

NOR : IOCD0918274D

Le Premier ministre,

Sur le rapport du ministre de l'Intérieur, de l'Outre-mer et des Collectivités territoriales,

Vu le Code de procédure pénale, notamment son article 777-3 ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment le II de son article 26 ;

Vu la loi nº 95-73 du 21 janvier 1995 modifiée d'orientation et de programmation relative à la sécurité, notamment son article 17-1 ;

Vu le décret nº 2007-914 du 15 mai 2007 modifié pris pour l'application du I de l'article 30 de la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 11 juin 2009 ;

Le Conseil d'État (section de l'intérieur) entendu,

Décrète :

Article 1

Le ministre de l'Intérieur est autorisé à mettre en œuvre un traitement de données à caractère personnel, intitulé « Prévention des atteintes à la sécurité publique », ayant pour finalité de recueillir, de conserver et d'analyser les informations qui concernent des personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique.

Ce traitement a notamment pour finalité de recueillir, de conserver et d'analyser les informations qui concernent les personnes susceptibles d'être impliquées dans des actions de violence collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives.

Article 2

Peuvent être enregistrées dans le traitement, dans le respect des dispositions de l'article 6 de la loi du 6 janvier 1978 susvisée et dans la stricte mesure où elles sont nécessaires à la poursuite de la finalité mentionnée à l'article 1er, les catégories de données à caractère personnel suivantes :
1° Motif de l'enregistrement ;
2° Informations ayant trait à l'état civil, à la nationalité et à la profession, adresses physiques, numéros de téléphone et adresses électroniques ;
3° Signes physiques particuliers et objectifs, photographies ;
4° Titres d'identité ;
5° Immatriculation des véhicules ;
6° Informations patrimoniales ;
7° Activités publiques, comportement et déplacements ;
8° Agissements susceptibles de recevoir une qualification pénale ;
9° Personnes entretenant ou ayant entretenu des relations directes et non fortuites avec l'intéressé.

Le traitement ne comporte pas de dispositif de reconnaissance faciale à partir de la photographie.

Article 3

L'interdiction prévue au I de l'article 8 de la loi du 6 janvier 1978 s'applique au présent traitement.

Par dérogation, sont autorisés, pour les seules fins et dans le strict respect des conditions définies au présent décret, la collecte, la conservation et le traitement de données concernant les personnes mentionnées à l'article 1er et relatives :
– à des signes physiques particuliers et objectifs comme éléments de signalement des personnes ;
– à l'origine géographique ;
– à des activités politiques, philosophiques, religieuses ou syndicales.

Il est interdit de sélectionner dans le traitement une catégorie particulière de personnes à partir de ces seules données.

Article 4

Les données mentionnées aux articles 2 et 3 ne peuvent être conservées plus de dix ans après l'intervention du dernier événement de nature à faire apparaître un risque d'atteinte à la sécurité publique ayant donné lieu à un enregistrement.

Article 5

Les données mentionnées aux articles 2 et 3 ne peuvent concerner des mineurs que s'ils sont âgés d'au moins treize ans et sont au nombre des personnes mentionnées à l'article 1er. Ces données ne peuvent alors être conservées plus de trois ans après l'intervention du dernier événement de nature à faire apparaître un risque d'atteinte à la sécurité publique ayant donné lieu à un enregistrement.

Article 6

Dans la limite du besoin d'en connaître, y compris pour des enquêtes administratives prévues par le premier alinéa de l'article 17-1 de la loi du 21 janvier 1995 susvisée, sont autorisés à accéder aux données mentionnées aux articles 2 et 3 :
1° Les fonctionnaires relevant de la sous-direction de l'information générale de la Direction centrale de la sécurité publique, individuellement désignés et spécialement habilités par le directeur central de la sécurité publique ;
2° Les fonctionnaires des directions départementales de la sécurité publique affectés dans les services d'information générale, individuellement désignés et spécialement habilités par le directeur départemental ;
3° Les fonctionnaires de la préfecture de police affectés dans les services chargés du renseignement, individuellement désignés et spécialement habilités par le préfet de police.

Les fonctionnaires des groupes spécialisés dans la lutte contre les violences urbaines ou les phénomènes de bandes, individuellement désignés et spécialement habilités par le directeur départemental de la sécurité publique ou par le préfet de police, sont autorisés à accéder aux données mentionnées aux articles 2 et 3 relevant de la finalité mentionnée au deuxième alinéa de l'article 1er.

En outre, peut-être destinataire des données mentionnées aux articles 2 et 3, dans la limite du besoin d'en connaître, tout autre agent d'un service de la police nationale ou de la gendarmerie nationale, sur demande expresse précisant l'identité du demandeur, l'objet et les motifs de la consultation. Les demandes sont agréées par les responsables des services mentionnés aux 1° à 3°.

Article 7

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

Sont conservées pendant le même délai les demandes mentionnées au dernier alinéa de l'article 6.

Article 8

Le traitement ne fait l'objet d'aucune interconnexion, aucun rapprochement ni aucune forme de mise en relation avec d'autres traitements ou fichiers.

Article 9

Conformément aux dispositions de l'article 41 de la loi du 6 janvier 1978 susvisée, le droit d'accès aux données s'exerce auprès de la Commission nationale de l'informatique et des libertés.

Le droit d'information prévu au I de l'article 32 et le droit d'opposition prévu à l'article 38 de la même loi ne s'appliquent pas au présent traitement.

Article 10

Le traitement mis en œuvre en application du présent décret est soumis au contrôle de la Commission nationale de l'informatique et des libertés dans les conditions prévues à l'article 44 de la loi du 6 janvier 1978 susvisée.

En outre, le directeur général de la police nationale présente chaque année à la Commission nationale de l'informatique et des libertés un rapport sur ses activités de vérification, de mise à jour et d'effacement des données enregistrées dans le traitement, notamment celles relatives aux mineurs mentionnés à l'article 5. Ce rapport annuel indique également les procédures suivies par les services gestionnaires pour que les données enregistrées soient en permanence exactes, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées.

Article 11

À l'article 1er du décret du 15 mai 2007 susvisé, il est rétabli un dixième alinéa ainsi rédigé :

« 9. Décret portant création de l'application relative à la prévention des atteintes à la sécurité publique. »

Article 12

Le présent décret est applicable sur tout le territoire de la République.

Article 13

Le ministre de l'Intérieur, de l'Outre-mer et des Collectivités territoriales est chargé de l'exécution du présent décret, qui sera publié au *Journal officiel de la République française*.

Fait à Paris, le 16 octobre 2009.

Décret nº 2009-1250 du 16 octobre 2009 portant création d'un traitement automatisé de données à caractère personnel relatif aux enquêtes administratives liées à la sécurité publique

JORF nº 0242 du 18 octobre 2009

NOR : IOCD0918264D

Le Premier ministre,

Sur le rapport du ministre de l'Intérieur, de l'Outre-mer et des Collectivités territoriales,

Vu le Code de procédure pénale, notamment son article 777-3 ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment le II de son article 26 ;

Vu la loi nº 95-73 du 21 janvier 1995 modifiée d'orientation et de programmation relative à la sécurité, notamment son article 17-1 ;

Vu l'avis de la Commission nationale de l'informatique et des libertés en date du 11 juin 2009 ;

Le Conseil d'État (section de l'intérieur) entendu,

Décrète :

Article 1

Le ministre de l'Intérieur (direction centrale de la sécurité publique et préfecture de police) est autorisé à mettre en œuvre un traitement automatisé de données à caractère personnel, dénommé « Enquêtes administratives liées à la sécurité publique », ayant pour finalité de faciliter la réalisation d'enquêtes administratives en application des dispositions du premier alinéa de l'article 17-1 de la loi du 21 janvier 1995 susvisée par la conservation des données issues de précédentes enquêtes relatives à la même personne.

Article 2

Peuvent être enregistrées dans le traitement, dans le respect des dispositions de l'article 6 de la loi du 6 janvier 1978 susvisée, les catégories de données à caractère personnel suivantes, recueillies dans le cadre d'enquêtes administratives :
1° Motif de l'enquête ;
2° Informations ayant trait à l'état civil, à la nationalité et à la profession, adresses physiques, numéros de téléphone et adresses électroniques ;
3° Photographies ;
4° Titres d'identité.

Est également conservé le rapport de l'enquête administrative, contenant les éléments permettant de déterminer si le comportement de la personne concernée n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées, compte tenu de leur nature.

Le traitement ne permet des recherches automatisées qu'à partir des données mentionnées aux 1° et 2°.

Article 3

L'interdiction prévue au I de l'article 8 de la loi du 6 janvier 1978 susvisée s'applique au présent traitement.

Toutefois, l'enregistrement de données, contenues dans un rapport d'enquête, relatives à un comportement incompatible avec l'exercice des fonctions ou des missions envisagées est autorisé alors même que ce comportement aurait une motivation politique, religieuse, philosophique ou syndicale.

Article 4

Les données peuvent être conservées pendant une durée maximale de cinq ans à compter de leur enregistrement.

Article 5

Les données mentionnées aux articles 2 et 3 ne peuvent concerner des mineurs que s'ils sont âgés de seize ans au moins et ont fait l'objet d'une enquête administrative mentionnée à l'article 1er.

Article 6

Dans la limite du besoin d'en connaître, en vue de la réalisation d'enquêtes administratives, sont autorisés à accéder aux données mentionnées aux articles 2 et 3 :

1° Les fonctionnaires relevant de la sous-direction de l'information générale de la Direction centrale de la sécurité publique, individuelle-

ment désignés et spécialement habilités par le directeur central de la sécurité publique ;

2° Les fonctionnaires affectés dans les services d'information générale des directions départementales de la sécurité publique, individuellement désignés et spécialement habilités par le directeur départemental ;

3° Les fonctionnaires affectés dans les services de la préfecture de police chargés du renseignement, individuellement désignés et spécialement habilités par le préfet de police.

En outre, peut-être destinataire des données mentionnées aux articles 2 et 3, dans la limite du besoin d'en connaître, tout agent d'un service de la police nationale ou de la gendarmerie nationale chargé d'une enquête administrative, sur demande expresse précisant l'identité du demandeur, l'objet et les motifs de la consultation. Les demandes sont agréées par les responsables des services mentionnés aux 1° à 3°.

Article 7

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

Sont conservées pendant le même délai les demandes mentionnées au dernier alinéa de l'article 6.

Article 8

Le traitement ne fait l'objet d'aucune interconnexion, aucun rapprochement ni aucune forme de mise en relation avec d'autres traitements ou fichiers.

Article 9

Conformément aux dispositions prévues à l'article 41 de la loi du 6 janvier 1978 susvisée, le droit d'accès aux données s'exerce auprès de la Commission nationale de l'informatique et des libertés.

Les personnes faisant l'objet d'une enquête administrative sont informées que celle-ci peut donner lieu à une insertion dans le traitement prévu par le présent décret.

Le droit d'opposition prévu à l'article 38 de la même loi ne s'applique pas au présent traitement.

Article 10

Le traitement mis en œuvre en application du présent décret est soumis au contrôle de la Commission nationale de l'informatique et des

libertés dans les conditions prévues à l'article 44 de la loi du 6 janvier 1978 susvisée.

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

Article 11

Le présent décret est applicable sur tout le territoire de la République.

Article 12

Le ministre de l'Intérieur, de l'Outre-mer et des Collectivités territoriales est chargé de l'exécution du présent décret, qui sera publié au *Journal officiel de la République française*.

Fait à Paris, le 16 octobre 2009

Annexe 8

Liste des traitements automatisés et « mutualisables »

propositions initiales de la DGPN, DGGN et PP (13 octobre 2009)

Nom	Service gestionnaire	Finalité	Utilisateurs	Mutualisable
ANACRIM	Gendarmerie	Confronter divers éléments d'investigation figurant en procédure afin de caractériser certaines relations au sein d'une enquête déterminée comportant un ou plusieurs faits	Gendarmerie Police Douanes	Fait
Application de gestion du répertoire informatisé des propriétaires et possesseurs d'armes (AGRIPPA)	DMAT, et à court terme DLPAJ	Enregistrer et suivre les autorisations et récépissés de déclaration relatifs aux matériels de guerre ainsi qu'aux armes et munitions des 4e, 5e et 7e catégories	Police Gendarmerie	Fait
Application de rapprochements, d'identification et d'analyse pour les enquêteurs (ARI@NE) – désormais TPJ	Police Gendarmerie	Faciliter la constatation des infractions, le rassemblement des preuves et la recherche des auteurs + statistiques Permettra une plus grande efficacité dans le cadre des enquêtes impliquant des malfaiteurs récidivistes	Police Gendarmerie	Fait (mise en service en 2011)
ANACRIM-NG ATRT pour fin 2011	Gendarmerie	Confronter divers éléments d'investigation figurant en procédure afin de caractériser certaines relations au sein d'une enquête déterminée comportant un ou plusieurs faits	Gendarmerie	Oui En attente de LOPPSI
ARAMIS	Gendarmerie	Informer les autorités hiérarchiques des événements en cours et de leur évolution	Gendarmerie	Supprimé avec l'arrivée de BDSP/Athéna
Athen@ / BDSP	Gendarmerie	– Améliorer l'accueil du public et la relation aux usagers – Aider et sécuriser les interventions – Optimiser le traitement du renseignement d'ordre public et de défense	Gendarmerie	Non Mutualisation non envisagée car liée au mode de fonctionnement propre d'une institution. – GEA (gestion des événements d'ampleur) : fournir aux autorités les informations nécessaires à la prise de décision lors d'un événement d'ordre public. La finalité est statistique et ne comporte pas de données nominatives (pas de décret donc). – GSI (gestion des sollicitations et des interventions) : apporter une réponse adaptée aux sollicitations des usagers (par l'appel 17 notamment) et assurer l'engagement des militaires et des moyens de la gendarmerie dans les meilleures conditions d'efficacité. – GIPASP (gestion de l'information et prévention des atteintes à la sécurité publique) : recueillir, conserver et analyser les informations concernant des personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique. – SIDPP (sécurisation des interventions et demandes particulières de protection) : collecter des données destinées à une gestion des interventions des forces de gendarmerie adaptée soit aux personnes dont la dangerosité a été constatée lors d'une précédente intervention, soit aux personnes se trouvant dans une situation de vulnérabilité particulière (tranquillité seniors, tranquillité vacances,...). Le module RENS est l'outil de la gendarmerie correspondant à sa mission de renseignement telle que rappelée dans la loi du 3 août 2009.

Nom	Service gestionnaire	Finalité	Utilisateurs	Mutualisable
Bureautique brigade 2000 (BB 2000)	Gendarmerie	Au niveau local, gestion du service et des registres, partage des informations sur les lieux et personnes particuliers de la circonscription	Gendarmerie	Prochainement supprimé avec l'arrivée de Pulsar
Cellule opérationnelle de rapprochement et d'analyse des infractions liées (CORAIL)	Police	– Mutualisation des diffusions d'informations opérationnelles auprès des enquêteurs (télégrammes via le réseau de commandement (RESCOM), circulaires d'information et de recherche diffusées par la police judiciaire.) – Gestion des GAV – Établissement de synthèses d'affaires	Police	Oui
Centralisation du renseignement intérieur pour la sécurité du territoire et les intérêts nationaux (CRISTINA)	Police	Lutte contre les activités susceptibles de constituer une atteinte aux intérêts fondamentaux de la Nation	Police	Non (domaine de compétence de la DCRI aux termes du décret du 27 juin 2008 relatif aux missions et à l'organisation de la DCRI)
Enquêtes administratives liées à la sécurité publique (EALSP)	Police	Réalisation des enquêtes administratives	Police	Oui
Exécution des services commandés pour la réalisation des transfèrements et extractions (ESCORTE)	Gendarmerie	Gestion des opérations de transfèrements	Gendarmerie	Oui, éventuellement avec l'administration pénitentiaire lors de la reprise des missions de transfèrements
Fichier alphabétique de renseignements de la gendarmerie nationale (FAR)	Gendarmerie	Connaître de manière approfondie la population résidente, en particulier sur sa dangerosité	Gendarmerie	Supprimé
Fichier automatisé des empreintes digitales (FAED)	Police Gendarmerie	– Identifier les auteurs de crimes ou délits grâce aux traces digitales ou palmaires – Détecter les usurpations d'identité et les identités multiples	Police Gendarmerie	Fait
Fichier d'information Schengen (SIS)	Police	Recensement : – des personnes recherchées, sous surveillance ou indésirables – des véhicules ou objets recherchés	Police Gendarmerie	Fait
Fichier de gestion du service central de préservation des prélèvements biologiques (SCPPB)	Gendarmerie	Assurer la gestion des prélèvements biologiques recueillis sur certaines scènes de crime ou de délit, ou lors de découvertes de cadavres non identifiés voire lors de disparitions de personnes	Gendarmerie	Ce fichier est géré par la Gendarmerie nationale et regroupe l'ensemble des scellés (police et gendarmerie).

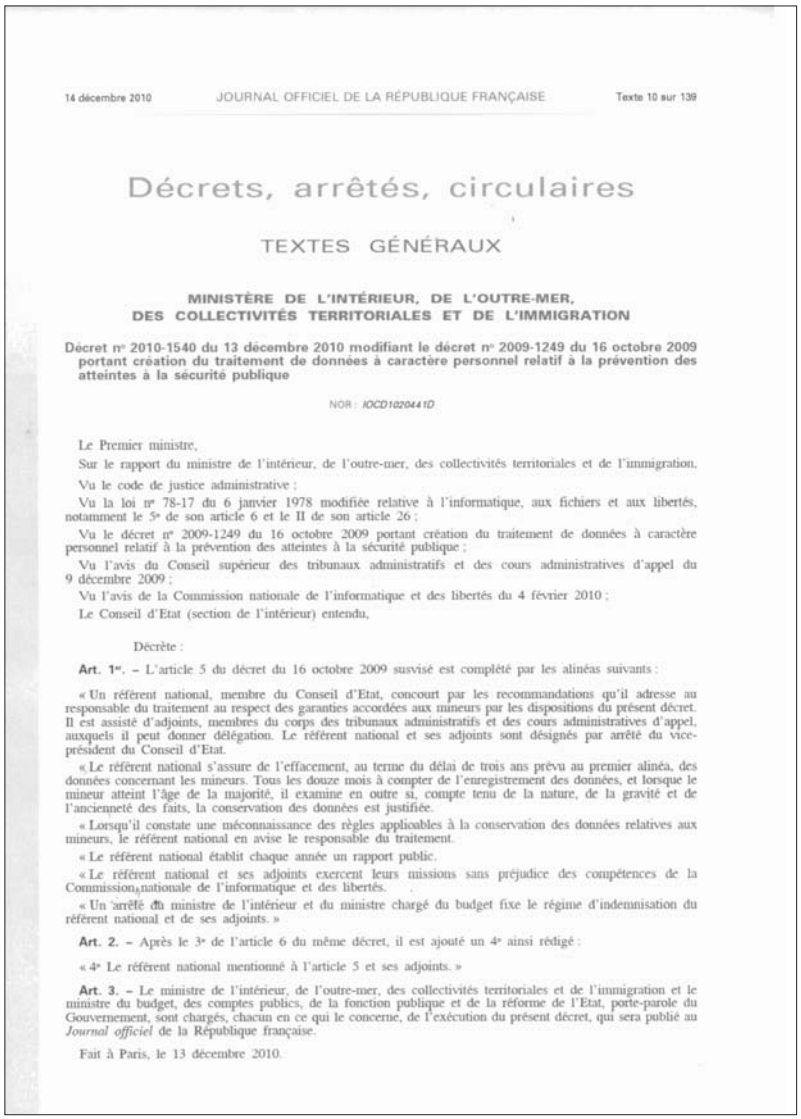
Nom	Service gestionnaire	Finalité	Utilisateurs	Mutualisable
Fichier de la batellerie	Gendarmerie	Assurer le suivi des mariniers, des compagnies fluviales et des bateaux affectés au transport fluvial de marchandises	Gendarmerie	Neutralisé. En cours d'archivage historique au SHGN.
Fichier de suivi des personnes faisant l'objet d'une rétention administrative	Gendarmerie	Assurer le suivi des personnes faisant l'objet d'une décision de rétention	Gendarmerie	Neutralisé Le MIOMCTI à la responsabilité du nouveau fichier ELOI
Fichier de suivi des titres de circulation délivrés aux personnes sans domicile ni résidence fixe (SDRF)	Gendarmerie	Assurer le suivi des titres de circulation délivrés aux personnes circulant en France sans domicile ni résidence fixe	Gendarmerie	Fait
Fichier de travail de la police judiciaire (FTPJ)	Police	Collecter des informations sur les délinquants spécialisés	Police	Prochainement supprimé
Fichier des brigades spécialisées (FBS)	Police	Collecter des informations sur les délinquants spécialisés et favoriser la coopération des services	Police	Oui, dans sa version rénovée (2011)
Fichier des objets et véhicules signalés (FOVES)	Police Gendarmerie	Fusion des fichiers FVV et FOS	Police Gendarmerie	Fait
Fichier des objets signalés (FOS)	Gendarmerie	Vérifier si un objet précisément identifié est signalé volé	Gendarmerie	Supprimé avec l'arrivée du FOVES
Fichier des passagers aériens (FPA)	Police	Améliorer le contrôle aux frontières, lutter contre l'immigration clandestine et les actes de terrorisme	Police	Sans objet. N.B. Directive PNR en cours de négociation au sein de l'UE depuis février 2011
Fichier des personnes nées à l'étranger (FPNE)	Gendarmerie	Collationner les renseignements relatifs aux personnes nées hors de France	Gendarmerie	Neutralisé, en cours de destruction.
Fichier des personnes recherchées (FPR)	Police Gendarmerie	Répertorier au niveau national les personnes faisant l'objet de recherches judiciaires, et administratives	Police Gendarmerie	Fait
Fichier des véhicules volés (FVV)	Police Gendarmerie	Faciliter les recherches de véhicules, bateaux et aéronefs signalés volés ou mis sous surveillance	Police Gendarmerie	Fait
Fichier judiciaire national automatisé des auteurs d'infractions sexuelles (FIJAIS)	Ministère de la Justice	Prévenir la récidive des auteurs d'infractions sexuelles ou violentes et faciliter l'identification des auteurs de ces infractions	Police Gendarmerie	Fait
Fichier national automatisé des empreintes génétiques (FNAEG)	Police Gendarmerie	Faciliter la recherche des auteurs d'infractions et des personnes disparues	Police Gendarmerie	Fait
Fichier national des interdictions de stade (FNIS)	Police	Prévenir et lutter contre les violences lors de manifestations sportives	Police	Fait

Nom	Service gestionnaire	Finalité	Utilisateurs	Mutualisable
Fichier national des permis de conduire (FNPC)	DLAPJ	Enregistrer et gérer les informations relatives aux permis de conduire	Police Gendarmerie	Fait
Fichier national du faux monnayage (FNFM)	Police Gendarmerie	Recenser les affaires relatives au faux monnayage commises sur le territoire national	Police Gendarmerie	Fait
Fichier national transfrontières (FNT)	Police	– Améliorer le contrôle aux frontières et la lutte contre l'immigration clandestine – Prévenir et réprimer les actes de terrorisme	Police	Fait, (accès prévu dans l'arrêté de création du traitement)
Fichier relatif à la carte nationale d'identité	DLPAJ	– Limiter les risques de contrefaçon et de falsification – Mettre en œuvre les procédures de délivrance ou renouvellement – Permettre au titulaire d'une carte d'identité de justifier de son identité – Faciliter l'action des policiers et gendarmes lors du franchissement des frontières	Police Gendarmerie	Fait
Fichier relatif aux passeports (DELPHINE et TES)	DLPAJ	– Mettre en œuvre les procédures d'établissement, de délivrance, de renouvellement et de retrait des passeports – Prévenir et détecter leur falsification ou contrefaçon	Police Gendarmerie	Fait
Gestion du terrorisme et des extrémismes à potentialité violente (GESTEREX)	Police (PP)	– Prévenir les actes de terrorisme – Surveiller les individus, groupes, organisations et phénomènes de société susceptibles de porter atteinte à la sûreté nationale	Police	Non, (domaine de compétence de la DCRI aux termes du décret du 27 juin 2008 relatif aux missions et à l'organisation de la DCRI, qui prévoit par ailleurs la contribution de la PP)
Gestion des violences (GEVI)	Police (PP)	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	Police (PP)	Prochainement supprimé
iC@RE/LRPGN	Gendarmerie	– Rédiger les procès-verbaux et rapports – Faciliter et optimiser les tâches des personnels – Alimenter le FVV et JUDEX	Gendarmerie	Mutualisation possible avec toute administration travaillant sous Open Source (Linux, Open Office) Actuellement mutualisation en cours avec DGDDI
Lecture automatisée des plaques d'immatriculation (LAPI)	Ministère de l'Intérieur, de la Défense et du Budget	Prévenir et réprimer certains types d'infractions : – en matière de terrorisme – criminelles ou relatives à la criminalité organisée – vols ou recels de véhicules volés – contrebande, importation ou exportation en bande organisée – opérations financières définies à l'article 415 du code des douanes	Police Gendarmerie	Fait

Nom	Service gestionnaire	Finalité	Utilisateurs	Mutualisable
Logiciel d'uniformisation des prélèvements et d'identification (LUPIN)	Police (PP)	Lutter contre les cambriolages en procédant à des rapprochements à partir des données de police technique et scientifique	Police (PP)	Oui
Logiciel de rédaction de procédures (LRP)	Police	Rédiger les procès-verbaux et les rapports administratifs ou judiciaires	Police	Prochainement supprimé
Main courante informatisée (MCI)	Police	Gérer l'emploi des effectifs, les événements et les déclarations des usagers	Police	Non
Outil de centralisation et de traitement opérationnel des procédures et des utilisateurs de signatures (OCTOPUS)	Police (PP)	Rechercher les auteurs de « tags »	Police	Oui
Prévention des atteintes à la sécurité publique (PASP)	Police	Collecter, conserver et traiter les données concernant des personnes dont le comportement individuel ou collectif indique qu'elles peuvent être responsables d'atteintes à la sécurité publique	Police	Non, (la mutualisation des bases de données liées aux missions de renseignement n'est pas envisagée)
PULS@R	Gendarmerie	Gérer le service et les registres ainsi que les amendes forfaitaires Générer les messages d'information statistique et les bulletins d'analyse des accidents	Gendarmerie	Mutualisation non envisagée car liée au mode de fonctionnement et d'organisation du service très spécifique à la gendarmerie. Système qui permet également de mesurer l'activité des unités.
Système d'analyse et de liens de la violence associée au crime (SALVAC)	Police	Identifier les auteurs de crimes ou délits commis en série, dans le domaine de la criminalité violente	Police Gendarmerie (fichier uniquement utilisé par les personnels de l'OCRVP)	Fait
Système de traitement des images des véhicules volés (STIVV)	Gendarmerie	Exploiter à des fins judiciaires les photographies prises par les radars automatisés de certains véhicules (volés, mis sous surveillance, etc.)	Gendarmerie	Prochainement supprimé. FOVES et LAPI pourraient ouvrir d'autres perspectives
Système de traitement des infractions constatées (STIC)	Police	Faciliter la constatation des infractions, le rassemblement des preuves et la recherche des auteurs + statistiques	Gendarmerie	Prochainement supprimé
Système judiciaire de documentation et d'exploitation (JUDEX)	Gendarmerie	Faciliter la constatation des infractions, le rassemblement des preuves et la recherche des auteurs	Gendarmerie	Prochainement supprimé avec l'arrivée de TPJ/Ariane
Traitement de données « préplainte en ligne » (PPL)	Police Gendarmerie	Permettre à la victime ou son représentant de faire une déclaration en ligne, pour certaines infractions, et d'obtenir un rendez-vous pour la signature de la plainte.	Police Gendarmerie	Fait

Annexe 9

Décret nº 2010-1540 portant création du magistrat référent pour les mineurs dans le cadre du fichier PASP



14 décembre 2010 JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE Texte 10 sur 139

Décrets, arrêtés, circulaires

TEXTES GÉNÉRAUX

MINISTÈRE DE L'INTÉRIEUR, DE L'OUTRE-MER, DES COLLECTIVITÉS TERRITORIALES ET DE L'IMMIGRATION

Décret nº 2010-1540 du 13 décembre 2010 modifiant le décret nº 2009-1249 du 16 octobre 2009 portant création du traitement de données à caractère personnel relatif à la prévention des atteintes à la sécurité publique

NOR : *IOCD1020441D*

Le Premier ministre,

Sur le rapport du ministre de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration,

Vu le code de justice administrative ;

Vu la loi nº 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment le 5º de son article 6 et le II de son article 26 ;

Vu le décret nº 2009-1249 du 16 octobre 2009 portant création du traitement de données à caractère personnel relatif à la prévention des atteintes à la sécurité publique ;

Vu l'avis du Conseil supérieur des tribunaux administratifs et des cours administratives d'appel du 9 décembre 2009 ;

Vu l'avis de la Commission nationale de l'informatique et des libertés du 4 février 2010 ;

Le Conseil d'Etat (section de l'intérieur) entendu,

Décrète :

Art. 1er. – L'article 5 du décret du 16 octobre 2009 susvisé est complété par les alinéas suivants :

« Un référent national, membre du Conseil d'Etat, concourt par les recommandations qu'il adresse au responsable du traitement au respect des garanties accordées aux mineurs par les dispositions du présent décret. Il est assisté d'adjoints, membres du corps des tribunaux administratifs et des cours administratives d'appel, auxquels il peut donner délégation. Le référent national et ses adjoints sont désignés par arrêté du vice-président du Conseil d'Etat.

« Le référent national s'assure de l'effacement, au terme du délai de trois ans prévu au premier alinéa, des données concernant les mineurs. Tous les douze mois à compter de l'enregistrement des données, et lorsque le mineur atteint l'âge de la majorité, il examine en outre si, compte tenu de la nature, de la gravité et de l'ancienneté des faits, la conservation des données est justifiée.

« Lorsqu'il constate une méconnaissance des règles applicables à la conservation des données relatives aux mineurs, le référent national en avise le responsable du traitement.

« Le référent national établit chaque année un rapport public.

« Le référent national et ses adjoints exercent leurs missions sans préjudice des compétences de la Commission nationale de l'informatique et des libertés.

« Un arrêté du ministre de l'intérieur et du ministre chargé du budget fixe le régime d'indemnisation du référent national et de ses adjoints. »

Art. 2. – Après le 3º de l'article 6 du même décret, il est ajouté un 4º ainsi rédigé :

« 4º Le référent national mentionné à l'article 5 et ses adjoints. »

Art. 3. – Le ministre de l'intérieur, de l'outre-mer, des collectivités territoriales et de l'immigration et le ministre du budget, des comptes publics, de la fonction publique et de la réforme de l'Etat, porte-parole du Gouvernement, sont chargés, chacun en ce qui le concerne, de l'exécution du présent décret, qui sera publié au *Journal officiel* de la République française.

Fait à Paris, le 13 décembre 2010.

Table des matières