N° 4113

___

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

TREIZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 21 décembre 2011.

RAPPORT D'INFORMATION

DÉPOSÉ

en application de l'article 145-8 du Règlement

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

sur la mise en oeuvre des conclusions de la mission d'information sur les **fichiers de police**

ET PRÉSENTÉ

PAR Mme DELPHINE BATHO et M. JACQUES ALAIN BÉNISTI

Députés.

___

SOMMAIRE

Pages

INTRODUCTION

La mission d'information sur les fichiers de police a été créée le 24 septembre 2008 par la commission des Lois de l'Assemblée nationale, dans le contexte des débats sur le fichier de renseignement « EDVIGE » [(1)] qui avaient souligné combien le domaine des fichiers de police restait trop peu connu et propice à de réelles inquiétudes des citoyens sur le respect des libertés publiques et la protection de leurs données personnelles. Elle a conduit à la formulation, en mars 2009 [(2)], de cinquante-sept recommandations visant à assurer tant la performance des traitements de données à caractère personnel utilisés par les forces de l'ordre qu'une meilleure protection des droits et libertés des citoyens. Ces recommandations figuraient dans un rapport, qui constituait la première étude réalisée par le Parlement en la matière et que vos rapporteurs avaient présenté à la commission des Lois le 24 mars 2009.

Vos rapporteurs avaient alors constaté l'inadaptation du cadre juridique relatif aux fichiers de police. Ambigu, complexe, faisant insuffisamment intervenir la représentation nationale et les citoyens, suscitant de vives tensions entre le ministère de l'Intérieur et la CNIL, les ambiguïtés du cadre juridique de création des fichiers de police avait conduit à leur multiplication, souvent dans l'illégalité. Ce constat avait conduit vos rapporteurs à proposer une refonte complète de la procédure de création des fichiers de police.

Par ailleurs, plusieurs éléments concourraient à rendre ces fichiers peu performants : pour le STIC, le fichier d'antécédents judiciaires de la police nationale, l'inexactitude des données remettait en cause sa fiabilité ; pour le fichier des empreintes génétiques, le FNAEG, la montée en puissance de la police technique et scientifique conduisait à une crise de croissance ; pour d'autres, comme le fichier alphabétique de renseignements, leur illégalité comme leur obsolescence technique devaient conduire à leur destruction. À l'inverse, de nouveaux fichiers, performants et utiles comme CORAIL ou LUPIN, étaient utilisés en dehors de tout cadre juridique.

Enfin, les droits et libertés étaient, aux yeux de vos rapporteurs, insuffisamment protégés. Le droit d'accès indirect s'exerçait difficilement, les délais de rectification des données erronées étaient bien trop longs au regard des conséquences qu'une inscription pouvait avoir, notamment pour l'accès à certains emplois. Le contrôle de l'utilisation des fichiers était trop faible pour permettre une lutte efficace contre de possibles consultations abusives. Les diverses carences constatées par vos rapporteurs avaient donné lieu à autant de recommandations.

---

(1) Exploitation documentaire et valorisation de l'information générale.

(2) Rapport d'information n° 1548 déposé en application de l'article 145 du Règlement par la commission des Lois constitutionnelles, de la législation et de l'administration générale de la République sur les fichiers de police par Mme Delphine Batho et M. Jacques Alain Bénisti, députés.

*

Au cours des mois écoulés depuis la publication du précédent rapport, l'actualité est venue, à plusieurs reprises, confirmer les conclusions de vos rapporteurs. L'utilisation de fiches illégalement tirées du STIC, les soupçons portés sur l'existence passée de fichiers ethniques au sein de la gendarmerie nationale ou, plus récemment, le possible commerce de fiches par des fonctionnaires de la police nationale, illustrent l'utilisation controversée qui peut être faite des fichiers de police.

Lors de l'audition du général Jacques Mignaux, directeur général de la gendarmerie nationale, relative aux fichiers détenus par la gendarmerie nationale à la suite de la publication d'informations relatives à l'existence d'un fichier « MENS », par la commission des Lois le 13 octobre 2010, votre rapporteure a proposé la poursuite de la mission au titre de l'article 145-8 du Règlement de l'Assemblée nationale, proposition accueillie favorablement par le président Jean-Luc Warsmann.

Au cours de sa réunion du mardi 19 octobre 2010, la commission des Lois a ainsi décidé de poursuivre et d'approfondir ses travaux sur les fichiers de police, en confiant à vos rapporteurs, en application de l'article 145-8 introduit dans notre Règlement par la résolution du 27 mai 2009 [(1)], une nouvelle mission portant, cette fois-ci, sur le suivi des cinquante-sept recommandations.

En 2009, 58 fichiers de police et à usage de police avaient été recensés par la mission d'information. Depuis la publication du précédent rapport, certains fichiers ont été supprimés ou gelés, comme le fichier alphabétique de renseignements ou le fichier des renseignements généraux, ou sont sur le point de l'être, comme le fichier des objets signalés, le fichier des voitures volées, les fichiers d'antécédents judiciaires de la police et de la gendarmerie, la main courante informatisée de la gendarmerie nationale, le logiciel de rédaction des procédures (LRP) de la police nationale, ou le fichier de gestion des violences urbaines.

Leur suppression n'entraîne cependant pas la diminution du nombre global de fichiers. Ils ont vocation à être remplacés, dans un avenir proche, par des outils plus performants. De nouveaux fichiers sont ainsi créés : le logiciel de rédaction des procédures de police nationale (LRPPN), le traitement des antécédents judiciaires (TAJ), la base de données de sécurité publique de la gendarmerie nationale (BDSP), les traitements relatifs à la prévention des atteintes à la sécurité publique (PASP) et aux enquêtes administratives (EASP), la nouvelle main courante informatisée (NMCI).

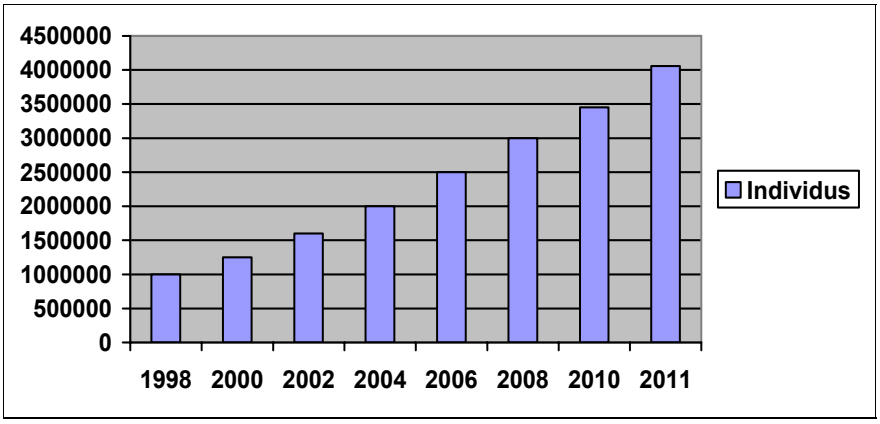
Sur les 58 fichiers recensés en 2009, 48 étaient utilisés et 23 étaient dépourvus de base légale. Fin 2011, vos rapporteurs recensaient 80 fichiers [(2)],

(1) Résolution n° 292 du 27 mai 2009.
(2) Cf. Annexe n° 2.

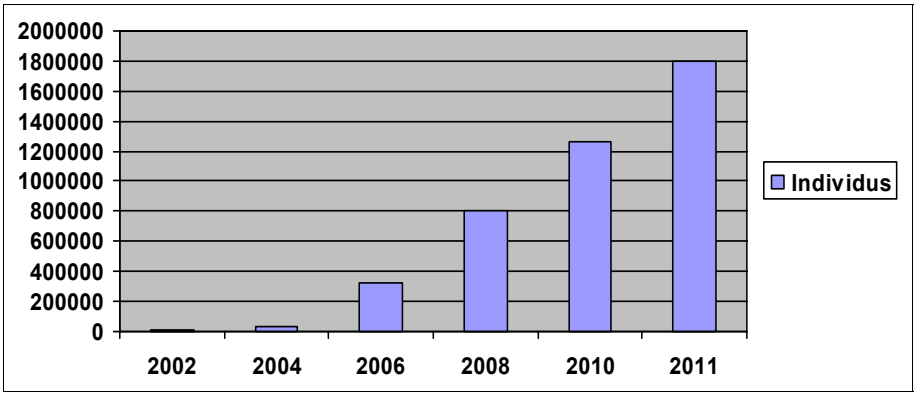
dont 62 étaient effectivement utilisés. L'augmentation du nombre de fichiers utilisés par rapport à 2009 est principalement imputable à la découverte de fichiers qui existaient déjà à cette date, mais dont l'existence n'avait pas été portée à la connaissance de la mission d'information, malgré ses demandes. Parmi les fichiers actuellement utilisés, 28 n'ont fait l'objet ni d'une déclaration à la CNIL, ni d'un texte législatif ou réglementaire, soit 45 % des fichiers utilisés. Toutefois, outre le fait que le ministère de l'Intérieur a procédé à la régularisation d'une quinzaine de fichiers depuis cette date, une vingtaine fait actuellement l'objet de projets de texte réglementaire. Enfin, des accords cadres sont en cours de rédaction qui devraient assurer la régularisation de l'ensemble des fichiers locaux ayant une finalité identique, notamment en matière d'assignation à résidence, de fourrière ou encore de contrôle des détenus.

L'évolution constatée dans le précédent rapport de la mission, qui avait trait à la croissance continue du nombre de personnes inscrites dans des fichiers de police, persiste aujourd'hui. Le fichier des antécédents judiciaires de la police nationale, le STIC, a poursuivi sa croissance de façon régulière. Alors qu'il comportait, en 2009, 3,96 millions de fiches de personnes mises en cause et 28 millions de fiches relatives à des victimes d'infraction, il recensait, au 1er novembre 2011, 6,5 millions de mis en cause et 38 millions de victimes. L'accroissement très important du fichier des empreintes génétiques (FNAEG), qui est passé de 806 356 profils génétiques en 2008 à 1,79 million en novembre 2011, est particulièrement révélateur de cette tendance de fond. Le fichier des empreintes digitales (FAED), qui comportait moins de trois millions d'empreintes fin 2008, en comptait 4,06 millions au 1er novembre 2011. La progression du nombre de citoyens inscrit dans les fichiers d'identification est donc significative. Il en va de même, dans une moindre mesure, pour le fichier des auteurs d'agressions sexuelles et violentes, qui a connu une progression de 27 % depuis 2008.

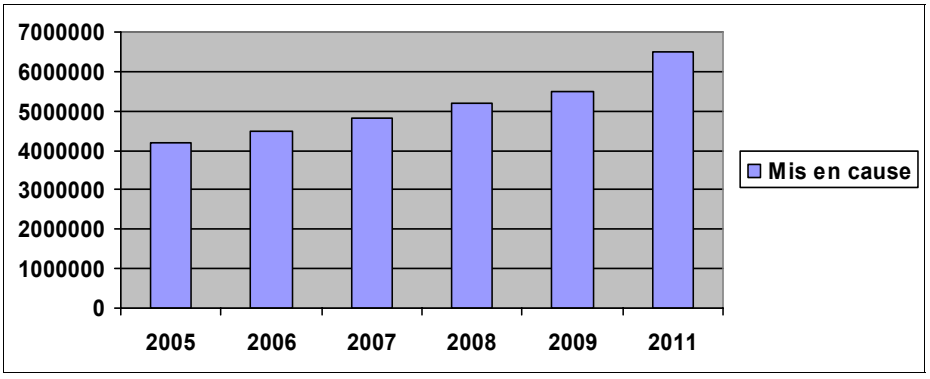
FICHIER AUTOMATISÉ DES EMPREINTES DIGITALES (FAED)



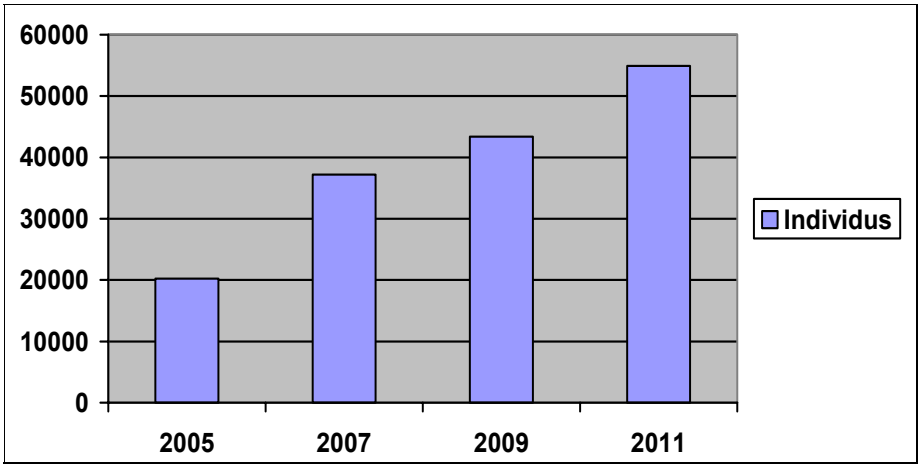
FICHIER NATIONAL AUTOMATISÉ DES EMPREINTES GÉNÉTIQUES (FNAEG)



SYSTÈME DE TRAITEMENT DES INFRACTIONS CONSTATÉES (STIC)



FICHIER JUDICIAIRE AUTOMATISÉ DES AUTEURS D'INFRACTIONS SEXUELLES OU VIOLENTES (FIJAISV)



Un mouvement inverse s'observe dans le domaine de l'information générale de sécurité publique. La destruction du fichier alphabétique de renseignement (FAR) de la gendarmerie nationale a conduit à la diminution de la volumétrie du fichier destiné à le remplacer, la base de données de sécurité publique (BDSP). En effet, le module de prévention des atteintes à l'ordre public comportera un nombre de fiches sans commune mesure avec l'ancien FAR. De même, un nombre très réduit de fiches issues du fichier des renseignements généraux est aujourd'hui repris par le nouveau fichier de prévention des atteintes à la sécurité publique (PASP).

*

Le présent rapport dresse donc le bilan de la mise en œuvre des recommandations formulées par vos rapporteurs en mars 2009. Plutôt que de reprendre une à une ces recommandations, qui figurent en annexe du présent rapport [(1)], vos rapporteurs ont préféré privilégier une présentation dynamique de la mise en œuvre des cinquante-sept propositions.

La première partie de ce rapport est consacrée au suivi des recommandations relatives au cadre juridique entourant les fichiers de police. En effet, vos rapporteurs avaient formulé de nombreuses recommandations qui entendaient refondre entièrement la procédure de création et de destruction des fichiers de police et renforcer les prérogatives du Parlement en la matière. Vos rapporteurs avaient également souhaité qu'un cadre législatif soit donné aux fichiers de rapprochement utilisés par les forces de l'ordre dans le domaine de la petite et moyenne délinquance sérielle. Hormis la représentation pluraliste du

(1) Cf. Annexe n° 1.

Parlement parmi les membres de la CNIL issus de l'Assemblée nationale et du Sénat, aucune des recommandations formulées par vos rapporteurs n'a pu aboutir. (Partie I)

Vos rapporteurs ont souhaité aborder la question de la protection des droits et libertés, tant au plan juridique que pratique. En matière de fichiers d'antécédents judiciaires, le droit d'accès indirect et de rectification s'exerce toujours difficilement, tandis que le droit à l'information des personnes inscrites et à l'équité est toujours inexistant. Par ailleurs, l'encadrement proposé par vos rapporteurs en ce qui concerne les fichiers de renseignement n'a été que partiellement pris en compte. Des progrès ont en revanche été accomplis pour les mineurs, qui bénéficient aujourd'hui d'un véritable droit à l'oubli. Enfin, la question des données sensibles demeure une préoccupation essentielle de vos rapporteurs. (Partie II)

Vos rapporteurs ont néanmoins observé qu'une culture « Informatique et libertés » dans la gestion et l'utilisation des fichiers de police se développe peu à peu. Dans ce domaine, des progrès ont été accomplis : la formation des utilisateurs est plus poussée ; l'enregistrement des données, étape cruciale, est plus encadré ; si les fichiers comportent encore un certain nombre de données erronées, leur mise à jour est aujourd'hui plus rapide ; enfin, l'accès aux fichiers et leur utilisation fait l'objet de procédures de contrôle plus poussées. (Partie III)

La modernisation de certains fichiers de police se révèle plutôt concluante, tandis que l'évolution de leur gouvernance permettra, à terme, d'aboutir à un processus performant de création et de développement des fichiers. Néanmoins, l'environnement technique et l'infrastructure des réseaux ne semblent pas avoir bénéficié des mêmes évolutions, et un important chemin reste à parcourir. (Partie IV)

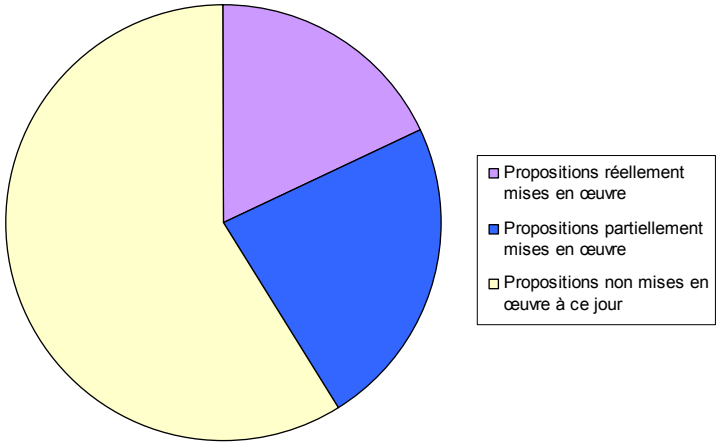
Enfin, vos rapporteurs ont également souhaité établir un état des lieux des fichiers qui concernent la lutte contre la récidive des infractions à caractère sexuel. Plusieurs événements dramatiques intervenus en 2010 et en 2011 ont convaincu vos rapporteurs d'examiner plus avant les fichiers de police concourant à la lutte contre la délinquance sexuelle à caractère sériel. En effet, dans plusieurs de ces affaires, des failles ont été révélées, que l'auteur présumé des faits soit en défaut de justification d'adresse au regard du fichier des délinquants sexuels ou violents (FIJAISV), qu'il soit déclaré sous une mauvaise adresse, que son inscription au fichier des personnes recherchées ait été retardée, ou qu'il ait tout simplement échappé à l'inscription au FIJAISV du fait des règles de droit existantes. (Partie V)

*

Au final, plus de trente mois après la publication du rapport de la mission d'information, le bilan en matière de suivi des recommandations fait apparaître

que, si 59 % des soixante et une recommandations [1] n'ont pas été mises en œuvre, 41 % d'entre elles l'ont été : 18 % des recommandations ont été intégralement suivies d'effet et 23 % d'entre elles ont été partiellement mises en œuvre (cf. graphique ci-dessous).

SUIVI DES RECOMMANDATIONS DU RAPPORT DE MARS 2009



Tout d'abord, **11 recommandations ont bel et bien été mises en œuvre**, conformément aux vœux de vos rapporteurs. Des failles juridiques ont ainsi été comblées, notamment en matière de prélèvement biologique. Des contractuels ont été recrutés afin de faire diminuer le stock de données en souffrance devant être intégrées dans différents fichiers de police. Les délais de réponse aux demandes d'effacement et de rectification ont également été réduits conformément aux recommandations émises par vos rapporteurs. La sécurisation des données a également progressé, ce dont vos rapporteurs se félicitent. Vos rapporteurs, pleinement conscients des difficultés tant juridiques que pratiques que certaines de leurs recommandations comportent, se félicitent de la mise en œuvre rapide de certaines d'entre elles.

Par ailleurs, **14 recommandations font l'objet d'une mise en œuvre partielle**, soit que les moyens employés aient été différents de ceux suggérés par vos rapporteurs, soit que l'évolution, bien qu'elle ait été amorcée, ne soit pas tout à fait accomplie. Par exemple, le développement de formations adéquates pour les personnels, s'il a été entrepris, n'est pas complet. De même, si la mise en place de systèmes d'alerte en temps réel, visant à repérer les consultations abusives de fichiers, a débuté au sein de la gendarmerie nationale, elle n'est pas encore achevée. Une évolution des mentalités semble cependant être à l'œuvre, qui

(1) En tenant compte des quatre recommandations faisant l'objet de points de vue divergents de la part de vos rapporteurs, le nombre total de recommandations est porté à 61.

permet d'espérer que de nouvelles recommandations seront bientôt mises en œuvre dans leur intégralité.

Enfin, parmi les **36 recommandations pour l'instant non suivies d'effet**, une part importante concerne la refonte du cadre législatif suggérée dans le rapport de 2009. Dans ce domaine, seules quelques rares avancées ont pu être enregistrées. L'une d'entre elles concerne la représentation pluraliste des parlementaires membres de la Commission nationale de l'informatique et des libertés (CNIL). En ce qui concerne la protection des droits et libertés, vos rapporteurs constatent que la plupart des recommandations ont été repoussées. Par ailleurs, les fichiers d'information générale et d'enquêtes administratives n'ont pas fait l'objet d'un encadrement aussi poussé que ce qui avait été souhaité par vos rapporteurs. Une part importante des recommandations émises en 2009 reste à mettre en œuvre, et vos rapporteurs ne peuvent que réitérer leurs propositions afin de mieux protéger les droits et libertés des citoyens mais aussi d'améliorer les outils utilisés par les policiers et gendarmes.

De façon générale, vos rapporteurs ont pu constater, au cours de leurs auditions et déplacements, qu'une culture « Informatique et libertés » commençait à se développer en France. Les acteurs, policiers et gendarmes, ont été sensibilisés à la question des fichiers. Vos rapporteurs se félicitent de ces changements culturels comme de la prise de conscience qui a fait suite à la publication de leur précédent rapport qui s'intitulait « Fichiers de police : les défis de la République ». Des décisions ont bel et bien été prises et des améliorations substantielles ont été apportées dans la gestion des fichiers. Vos rapporteurs appellent à la poursuite de ces efforts, tant sur le plan des garanties juridiques à apporter quant à la protection des données personnelles que sur celui de la modernisation technique des fichiers utilisés quotidiennement par nos forces de sécurité.

*

* *

PREMIÈRE PARTIE : LE CADRE JURIDIQUE DES FICHIERS DE POLICE : LA RÉVOLUTION N'A PAS EU LIEU

Assis sur des bases juridiques fluctuantes voire inexistantes, les fichiers de police étaient soumis à un processus de création empirique incompatible avec le respect des droits et des libertés. Tel était le constat dressé par vos rapporteurs en 2009. Pour y remédier, des propositions ambitieuses avaient été formulées, qui devaient conduire à modifier profondément le régime juridique issu de la loi n° 78-17 du 6 janvier 1978 relative aux fichiers, à l'informatique et aux libertés.

Le Parlement notamment devait retrouver toute sa place dans un domaine longtemps laissé aux mains du pouvoir exécutif. La création comme la destruction, la définition des finalités et des modalités des fichiers de police devaient devenir une compétence exclusive du Parlement, mieux informé grâce à la transmission de l'avis de la CNIL et à la réalisation d'études d'impact. Pour mettre un terme, à l'avenir, aux polémiques entourant la création de traitements de données personnelles, dont le fichier EDVIGE avait notamment fait les frais, un débat démocratique réel devait s'instaurer au travers d'une procédure rénovée de création des fichiers de police.

Force est de constater aujourd'hui que la révolution juridique n'a pas eu lieu. Le cadre juridique entourant les fichiers de police est toujours porteur d'ambiguïtés qui sont susceptibles de porter atteinte aux droits et libertés de chacun. Une seule proposition formulée par vos rapporteurs apparaît aujourd'hui dans la loi, qui concerne la représentation de l'opposition parlementaire au sein de la CNIL. Si vos rapporteurs se réjouissent de cette avancée, ils ne peuvent que déplorer l'inertie législative en matière de fichiers de police.

Par ailleurs, vos rapporteurs avaient également pour ambition de faciliter les relations entre la CNIL et le ministère de l'Intérieur, en proposant l'instauration d'un dialogue formalisé et d'une procédure de mise en application progressive des fichiers de police nouvellement créés par le législateur. Si les relations entre la CNIL et le ministère de l'Intérieur se sont effectivement améliorées, ce progrès n'est cependant pas imputable à une quelconque évolution juridique.

Au-delà, vos rapporteurs ont procédé à un nouveau recensement des fichiers de police existants, ce qui leur a permis d'évaluer le chemin parcouru, en matière de légalité des fichiers de police, depuis 2009.

A. UN QUASI *STATU QUO* LÉGISLATIF

Si quelques progrès ont été accomplis, notamment en ce qui concerne la représentation pluraliste du Parlement au sein de la CNIL, l'ambiguïté du cadre juridique issu de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et

aux libertés, soulignée en mars 2009, n'a pas été résolue, en dépit d'une proposition de loi déposée en ce sens par vos rapporteurs.

1. La représentation pluraliste du Parlement au sein de la CNIL

Vos rapporteurs avaient souhaité, en mars 2009, que les députés et sénateurs membres de la CNIL soient choisis de manière à assurer une représentation pluraliste des opinions politiques. En effet, eu égard aux prérogatives de cette commission en matière de fichiers de police et de libertés publiques, il importait que l'opposition parlementaire y soit représentée.

Vos rapporteurs avaient donc suggéré de modifier l'article 13 de la loi du 6 janvier 1978 relatif à la composition de la CNIL, afin que les deux députés et les deux sénateurs, membres de l'autorité de contrôle, soient désignés respectivement par l'Assemblée nationale et par le Sénat *« de manière à assurer une représentation pluraliste* » (**Recommandation n° 1**).

Cette recommandation a été mise en œuvre par l'adoption de l'article 54 de la loi n° 2011-525 du 17 mai 2011 de simplification et d'amélioration de la qualité du droit. Le premier alinéa de l'article 13 de la loi « Informatique et Libertés » dispose désormais que les deux députés et les deux sénateurs membres de la CNIL sont « *désignés respectivement par l'Assemblée nationale et par le Sénat de manière à assurer une représentation pluraliste* ». Il convient de noter que l'exigence de pluralisme s'apprécie au vu de l'ensemble des membres désignés au sein de la CNIL par les deux assemblées [(1)]. Cette évolution figurait déjà dans la proposition de loi n° 1659 déposée par vos rapporteurs, adoptée le 16 juin 2009 à l'unanimité par la commission des Lois de l'Assemblée nationale. Elle doit entrer en application dès que de nouvelles nominations seront rendues nécessaires. Pour les députés membres de la CNIL, cette disposition s'appliquera donc dès 2012. Pour les sénateurs membres de la CNIL, la nomination prochaine, par le Sénat, d'un nouveau parlementaire en remplacement de M. Alex Türk, devra répondre à cette règle, de même que celle du remplaçant de M. Claude Domeizel, en 2014.

2. La refonte complète de la procédure juridique entourant les fichiers de police : des recommandations repoussées

a) La création des fichiers de police confiée au législateur

Vos rapporteurs avaient souligné, en mars 2009, **l'ambiguïté du cadre juridique entourant les fichiers de police, notamment leur création**. En effet, sur le fondement de l'article 26 de la loi « Informatique et libertés », les fichiers de police peuvent être créés par arrêté ou décret en Conseil d'État, mais aussi par le biais d'une habilitation législative ponctuelle donnée par le Parlement au Gouvernement. La diversité des bases normatives envisageables ne concourait pas

(1) Rapport n° 2095 fait au nom de la commission des Lois constitutionnelles, de la législation et de l'administration générale de la République sur la proposition de loi de M. Jean-Luc Warsmann n° 1890 de simplification et d'amélioration de la qualité du droit par M. Etienne Blanc.

à l'établissement d'un cadre juridique clair garantissant la légalité de l'ensemble des fichiers de police.

Ces deux régimes ont d'ailleurs été utilisés de façon variable dans le temps par le pouvoir exécutif. En mars 2009, après la vive émotion suscitée par le fichier EDVIGE, créé par voie réglementaire [(1)], c'est le régime de l'habilitation législative qui semblait devoir prévaloir. Pourtant, il apparaît que c'est le régime réglementaire qui a été le plus couramment utilisé. **C'est d'ailleurs par la voie réglementaire qu'ont été créés les fichiers les plus récents** : le fichier de prévention des atteintes à la sécurité publique [(2)], le fichier des enquêtes administratives liées à la sécurité publique [(3)], la base de données de sécurité publique [(4)], le logiciel de rédaction des procédures de la police nationale [(5)]…

Or, la création d'un fichier par la voie réglementaire n'offre pas les mêmes garanties, en termes de débat public, que l'autorisation de la loi. Aussi vos rapporteurs avaient-ils proposé **que le législateur dispose d'une compétence exclusive en la matière, afin qu'un débat public puisse avoir lieu sur l'opportunité d'une telle création.**

Cela les avait conduit à recommander la modification de l'article 26 de la loi du 6 janvier 1978, afin que les fichiers ou toute catégorie de fichiers intéressant la sécurité publique et ceux qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ne puissent être autorisés que par la loi **(Recommandation n° 2)**.

Afin que l'autorisation du législateur prenne tout son sens, **vos rapporteurs avaient également proposé que chaque loi autorisant la création d'un fichier comporte de façon obligatoire certains éléments essentiels à l'établissement d'un véritable cadre juridique**, comme l'identité du responsable du traitement, la finalité et la dénomination du traitement ainsi que la description générale de ses fonctions, le service chargé de la mise en œuvre, le service auprès duquel s'exerce le droit d'accès, direct ou indirect, les catégories de données à caractère personnel enregistrées, leur origine et les catégories de personnes concernées par le traitement, les catégories de personnes qui ont accès aux informations enregistrées, les destinataires de ces informations, les rapprochements et

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

(2) Décret n° 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.

(3) Décret n° 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.

(4) Décrets n° 2011-340 du 29 mars 2011 portant création d'un traitement de données à caractère personnel relatif à la gestion de l'information et la prévention des atteintes à la sécurité publique, n° 2011-341 du 29 mars 2011 portant création d'un traitement de données à caractère personnel intitulé « gestion des sollicitations et des interventions » et n° 2011-342 du 29 mars 2011 portant création d'un traitement de données à caractère personnel relatif à la sécurisation des interventions et demandes particulières de protection.

(5) Décret n° 2011-110 du 27 janvier 2011 portant création d'un traitement automatisé de données à caractère personnel dénommé LRPPN 2.

interconnexions, et enfin, la durée de conservation des données **(Recommandation n° 3)**.

Ces dispositions avaient fait l'objet d'une traduction juridique, par le dépôt de la proposition de loi n° 1659 relative aux fichiers de police, cosignée par vos rapporteurs et enregistrée à la présidence de l'Assemblée nationale le 7 mai 2009. L'article 5 de cette proposition de loi est l'exacte transposition des recommandations rappelées ci-dessus.

Article 5 de la proposition de loi n° 1659 relative aux fichiers de police

« *I. – L'article 26 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est ainsi rédigé :*

« Art. 26. – I. – Sont autorisés par la loi les traitements ou catégories de traitements de données à caractère personnel mis en œuvre pour le compte de l'État et :

« 1° Qui intéressent la sécurité publique ;

« 2° Ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.

« Les catégories de traitements de données à caractère personnel sont constituées par les traitements qui répondent à une même finalité, portent sur de mêmes catégories de données et ont les mêmes catégories de destinataires.

« L'avis de la Commission nationale de l'informatique et des libertés mentionné au a du 4° de l'article 11 sur tout projet de loi autorisant la création d'un tel traitement ou d'une telle catégorie de traitements de données est transmis au Parlement simultanément au dépôt du projet de loi.

« II. – La loi autorisant un traitement ou une catégorie de traitements de données mentionnés au I prévoit :

« – leurs finalités ;

« – les services responsables ;

« – la nature des données à caractère personnel prévues au I de l'article 8 dont la collecte, la conservation et le traitement sont autorisés, dès lors que la finalité du traitement l'exige ;

« – l'origine de ces données et les catégories de personnes concernées ;

« – la durée de conservation des informations traitées ;

« – les destinataires ou catégories de destinataires des informations enregistrées ;

« – la nature du droit d'accès des personnes figurant dans les traitements de données aux informations qui les concernent ;

« – les interconnexions autorisées avec d'autres traitements de données.

« III. – Sont autorisés par décret en Conseil d'État du ou des ministres compétents, après avis motivé et publié de la commission, les traitements de données à caractère personnel mis en œuvre pour le compte de l'État et qui intéressent la sûreté de l'État ou la défense.

« Ces traitements peuvent être dispensés, par décret en Conseil d'État, de la publication de l'acte réglementaire qui les autorise. Pour ces traitements :

« – est publié en même temps que le décret autorisant la dispense de la publication de l'acte, le sens de l'avis émis par la commission ;

« – l'acte réglementaire est transmis à la délégation parlementaire au renseignement.

« IV. – Les modalités d'application des dispositions mentionnées au I sont fixées par arrêté du ou des ministres compétents. Si les traitements portent sur des données mentionnées au I de l'article 8, ces modalités sont fixées par décret en Conseil d'État.

« La commission publie un avis motivé sur tout projet d'acte réglementaire pris par le ou les ministres concernés en application d'une loi autorisant un traitement ou une catégorie de traitements de données conformément au I.

« V. – Un protocole d'accord entre la commission et le ou les ministres concernés détermine les modalités selon lesquelles les demandes d'avis sur les éléments d'information énumérés à l'article 30 sont adressées à la commission lors des principales étapes de la création d'un traitement de données préalablement à la publication de l'acte réglementaire prévu au III ou au IV. »

II. – Le protocole d'accord mentionné dans le dernier alinéa du I est conclu dans un délai d'un an à compter de la publication de la présente loi. »

Toutefois, **cette proposition de loi, bien qu'adoptée à l'unanimité de la commission des Lois le 16 juin 2009, a ensuite été repoussée par l'Assemblée nationale** le 24 novembre 2009, au motif qu'il était préférable d'insérer des

dispositions relatives aux fichiers de police, par voie d'amendement, au sein de la proposition de loi n° 1890 de simplification et d'amélioration de la qualité du droit, susceptible d'aboutir plus rapidement. Votre rapporteure déplore le fait qu'un autre véhicule législatif ait, à l'époque, été préféré. Ce d'autant plus que les dispositions introduites au sein de la proposition de loi de simplification et d'amélioration de la qualité du droit précitée, au demeurant très éloignées des recommandations ci-dessus, n'ont pas connu un sort plus favorable.

Votre rapporteur est quant à lui favorable à la proposition de loi déposée au Sénat, par M. Yves Détraigne et de Mme Anne-Marie Escoffier, visant à mieux garantir le droit à la vie privée à l'heure du numérique [(1)], telle qu'elle a été amendée par la commission des Lois du Sénat. Son article 4 énonce douze catégories de fichiers pour lesquelles le pouvoir réglementaire peut autoriser la mise en œuvre de traitement de données. Votre rapporteur estime qu'il est préférable d'introduire directement dans la loi du 6 janvier 1978 précitée les catégories de fichiers susceptibles de donner lieu à la création, par le pouvoir réglementaire, de traitements de données à caractère personnel. Il est en effet apparu que la faible normativité de la proposition initiale, qui entendait lier le législateur pour l'avenir, était susceptible de conduire à une censure constitutionnelle.

Votre rapporteure estime au contraire que l'adoption d'une telle proposition constituerait un recul considérable par rapport aux recommandations du rapport de la mission d'information. En termes strictement juridiques, le dispositif n'introduit aucun changement substantiel par rapport à la situation actuelle, sauf dans l'hypothèse où le pouvoir réglementaire souhaiterait la création d'un fichier de police n'entrant pas dans les catégories ainsi définies. En revanche, **un tel dispositif conférerait au pouvoir exécutif un véritable blanc-seing législatif** en matière de fichiers de police. Ce dernier pourrait ainsi créer librement, ou presque, des fichiers de police, tout en se prévalant d'une autorisation législative. Votre rapporteure déplore enfin le fait que, si des catégories de fichiers sont définies dans la loi, le régime de chacun d'entre eux ne l'est pas nécessairement.

b) L'autorisation expresse du législateur pour la collecte de données sensibles

Par ailleurs, afin de rendre le dispositif parfaitement cohérent, vos rapporteurs avaient proposé, en mars 2009, que le **législateur autorise expressément la collecte des données sensibles définies par l'article 8 de la loi du 6 janvier 1978 (Recommandation n° 10)**. Aujourd'hui, le droit n'exige qu'un simple décret en Conseil d'État pris après avis de la CNIL pour autoriser les services de police à collecter et traiter des données dites sensibles. Ce garde-fou semblait insuffisamment protecteur des droits et libertés des individus. Ainsi, dans le cadre du dispositif envisagé, il reviendrait au législateur d'indiquer, lors de la

(1) Proposition de loi, adoptée par le Sénat, visant à mieux garantir le droit à la vie privée à l'heure du numérique, n° 2387, déposée le 24 mars 2010 et renvoyé à la commission des Lois constitutionnelles, de la législation et de l'administration générale de la république de l'Assemblée nationale.

création du fichier par la loi, s'il autorise ou non la collecte des données sensibles, ainsi que les conditions dans lesquelles celle-ci peut s'effectuer.

Cette proposition a connu une traduction législative à l'article 1er de la proposition de loi relative aux fichiers de police [(1)], déposée par vos rapporteurs. En effet, celui-ci visait à modifier le IV de l'article 8 de la loi du 6 janvier 1978 de la façon suivante : « *IV. De même, ne sont pas soumis à l'interdiction prévue au I les traitements, automatisés ou non, justifiés par l'intérêt public et autorisés dans les conditions prévues au I ou au III de l'article 26.* ». Bien qu'elle ait été adoptée sans modification par la commission des Lois, cette proposition n'a pu être mise en œuvre par la suite.

c) Des fichiers strictement nécessaires

Afin de ne conserver que les fichiers strictement nécessaires, **vos rapporteurs avaient proposé qu'une évaluation des traitements créés soit systématiquement réalisée à moyen terme**, de sorte à ne conserver que les fichiers de police dont l'utilité est avérée. Dans l'optique de vos rapporteurs, les projets de loi autorisant la création de fichiers de police devaient prévoir une clause de rendez-vous dans le temps, afin que le Parlement opère à moyen et long terme une évaluation du fichier considéré. Au terme de cette évaluation, qui devait faire l'objet d'un débat en séance publique, le Parlement pouvait décider de mettre fin, par la loi, au fichier concerné, si la finalité qui avait initialement présidé à sa création n'était plus démontrée (**Recommandation n° 6**). Cette proposition n'a pas été mise en œuvre.

De la même façon, vos rapporteurs avaient recommandé que le Parlement soit également à l'origine de la destruction des fichiers de police devenus obsolètes ou inutiles. En effet, comme on a pu le constater avec le remplacement du fichier des renseignements généraux par EDVIGE, la destruction d'un fichier de police, parce qu'elle implique généralement son remplacement par un outil jugé plus performant, nécessite qu'un débat démocratique ait lieu. En conséquence, ils avaient proposé de compléter l'article 26 de la loi du 6 janvier 1978, afin que seule la loi puisse mettre fin à l'existence des fichiers intéressant la sécurité publique et ceux qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté (**Recommandation n° 57**). **Cette proposition n'a pas été mise en œuvre.**

3. Les prérogatives du Parlement n'ont pas été renforcées

Compte tenu de la **présence d'informations relevant du secret de la défense nationale dans les traitements intéressant la sûreté de l'État et la défense nationale**, vos rapporteurs n'avaient pas souhaité modifier le régime juridique auquel obéissait leur création. La proposition de loi qui a fait suite au

(1) Cf. Annexe n° 3.

rapport prévoyait d'ailleurs que ces traitements seraient toujours créés par la voie réglementaire, par décret pris en Conseil d'État après avis de la CNIL. De même, la proposition de loi déposée par vos rapporteurs n'était pas revenue sur la dispense de publication au *Journal Officiel* dont bénéficient ces actes.

Toutefois, afin d'assurer un **contrôle démocratique minimal** sur ces actes réglementaires, vos rapporteurs avaient recommandé la transmission systématique à la délégation parlementaire au renseignement mise en place par la loi n° 2007-1443 du 9 octobre 2007 portant création de cette délégation de l'ensemble des textes relatifs à la mise en place de traitements automatisés de données à caractère personnel par les services de renseignement, lorsque les textes portant création des fichiers intéressant la sûreté de l'État et la défense ne sont pas publiés au *Journal Officiel* (**Recommandation n° 44**).

Cette recommandation avait été traduite en des termes juridiques par les articles 5 et 13 de la proposition de loi de vos rapporteurs. Toutefois, le rejet de la proposition par l'Assemblée nationale n'a pas permis à cette recommandation d'aboutir. On constatera néanmoins que **l'article 4 de la proposition de loi sénatoriale visant à mieux garantir la vie privée à l'heure numérique**, telle qu'elle a été adoptée par le Sénat le 23 mars 2010, reprend cette recommandation, en prévoyant que les traitements intéressant la sûreté de l'État et la défense nationale dispensés de publicité par décret en Conseil d'État sont « *portés à la connaissance de la délégation parlementaire au renseignement et de la Commission nationale de l'informatique et des libertés* ».

Vos rapporteurs avaient également proposé, afin que le Parlement soit parfaitement informé, que **l'avis consultatif de la CNIL sur tout projet de loi tendant à la création d'un fichier de police soit rendu public et transmis au Parlement simultanément au dépôt du projet de loi (Recommandation n° 4)**. Dans le même but, tout projet ou proposition de loi tendant à la création d'un fichier de police devait être accompagné d'une étude d'impact appréciant le volume du fichier considéré ainsi que sa finalité, au regard de l'ensemble des fichiers d'ores et déjà existants (**Recommandation n° 5**).

L'article 5 de la proposition de loi relative aux fichiers de police cosignée par vos rapporteurs visait à mettre en œuvre la recommandation n° 4 (cf. *supra*), mais n'a pu aboutir. La recommandation n° 5 n'a pas été mise en œuvre.

B. L'AMÉLIORATION DES RELATIONS ENTRE LA CNIL ET LE MINISTÈRE DE L'INTÉRIEUR

En application de l'article 26 de la loi « Informatique et Libertés », la CNIL s'assure que le traitement informatique envisagé par le texte réglementaire qui lui est soumis est conforme aux dispositions de la loi du 6 janvier 1978. Cet avis, bien qu'il ne lie pas le pouvoir réglementaire, constitue une étape majeure dans la création des fichiers de police, qui peut dès lors être à l'origine de

désaccords entre la CNIL et le ministère de l'Intérieur. Vos rapporteurs avaient souhaité amorcer par le droit la résolution de ces conflits.

1. Les prémices d'un réel dialogue entre les deux institutions, en l'absence de modifications législatives

Vos rapporteurs avaient constaté, en 2009, qu'une **forte incompréhension** régnait entre les deux institutions. La CNIL tenait insuffisamment compte des besoins opérationnels des forces de l'ordre et se montrait, aux dires de la police nationale, par trop suspicieuse. À l'inverse, la CNIL regrettait de ne pas être associée plus en amont aux développements de nouveaux fichiers de police. Vos rapporteurs avaient proposé, **afin d'instaurer un dialogue minimal entre les deux institutions, que le rapport annuel de la CNIL bénéficie d'une procédure contradictoire**, à l'image du rapport de la Cour des comptes (**Recommandation n° 7**). Au-delà, vos rapporteurs avaient préconisé l'adoption d'une procédure identique pour l'ensemble des traitements de données à caractère personnel (**Recommandation n° 8**).

Ces recommandations faisaient l'objet de l'article 2 de la proposition de loi relative aux fichiers de police déposée par vos rapporteurs. En effet, cet article visait à modifier le dernier alinéa de l'article 11 de la loi du 6 janvier 1978 de la façon suivante : « *Préalablement à la présentation de son rapport annuel, la commission fait connaître aux ministres concernés et aux organismes qui mettent en œuvre des traitements de données à caractère personnel pour le compte de l'État les observations provisoires sur lesquelles elle estime nécessaire de susciter leurs remarques* ». Cette proposition n'a cependant pas abouti.

Si les directions générales de la police et de la gendarmerie nationales se sont déclarées favorables à une telle proposition [(1)], **la CNIL a émis certaines réserves** [(2)]. Même si elle est *a priori* favorable à toute proposition permettant d'améliorer les conditions du dialogue avec le ministère de l'Intérieur, elle a estimé que l'instauration d'**une telle procédure pourrait alourdir considérablement les conditions d'élaboration du rapport public annuel**. Ses représentants ont d'ailleurs précisé que **cette logique juridictionnelle empruntée à la Cour des comptes** ne correspondait pas à la vocation première de la CNIL ; au surplus, aucune autorité administrative indépendante n'est aujourd'hui soumise à de telles obligations.

Malgré l'absence d'avancée législative, **des progrès significatifs ont été accomplis** dans les relations qu'entretient le ministère de l'Intérieur avec la CNIL, d'après M. Frédéric Péchenard, directeur général de la police nationale [(3)]. La CNIL s'efforce désormais de prendre en compte les besoins opérationnels des

(1) Réponse du 7 mars 2011 des directions générales de la police et de la gendarmerie nationales au questionnaire de suivi des recommandations.

(2) Éléments de réponse au questionnaire adressé à M. Alex Türk en vue de son audition par la mission d'information le 1er décembre 2010.

(3) Audition du 16 mars 2011 de M. Frédéric Péchenard, directeur général de la police nationale.

services **en traitant dans des délais très restreints les dossiers pour lesquels il existe une urgence particulière**, tels que la base de données de sécurité publique (BDSP) de la gendarmerie nationale [(1)]. Elle tente également de **mieux appréhender ces réalités opérationnelles** en ayant recours à des auditions et des démonstrations des traitements utilisés, et en intégrant parmi son personnel des gendarmes et d'anciens gendarmes [(2)].

Le ministère de l'Intérieur s'est quant à lui engagé dans un **processus de régularisation qui contribue à l'amélioration des rapports avec la CNIL**. Cette tendance s'observe au sein de la police comme de la gendarmerie, mais aussi au sein de la préfecture de police de Paris. S'il existe encore des fichiers illégaux du fait de l'absence de déclaration, la plupart d'entre eux font l'objet d'une procédure de régularisation ou, *a minima*, d'échanges informels [(3)]. Cependant, la mise en place de véritables contacts reste difficile, notamment en raison du rôle de filtre joué par la direction des libertés publiques et des affaires juridiques du ministère de l'Intérieur (DLPAJ) [(4)], qui, lorsqu'elle est saisie de projets de fichiers, les remet en forme sur le plan juridique, avant de les présenter à la CNIL. Le constat était identique en 2009.

2. Vers un régime d'expérimentation des fichiers de police en étroite collaboration avec la CNIL ?

La CNIL déplorait également, en 2009, que les déclarations qui lui parvenaient portaient souvent sur des fichiers d'ores et déjà opérationnels sur un plan technique, limitant ainsi grandement la marge de manœuvre des services de police chargés du développement du traitement en cas de demande de modification. Mais, comme vos rapporteurs l'avaient souligné dans leur précédent rapport, il s'agit là d'un problème consubstantiel à la loi du 6 janvier 1978, lié à l'extrême précision des annexes techniques exigées lors du dépôt des dossiers de déclaration.

Pour remédier à ce problème, vos rapporteurs avaient proposé l'instauration d'une **procédure de mise en application par étapes**, qui permettrait d'introduire une certaine souplesse dans les relations entre la CNIL et les services. Ils avaient ainsi recommandé l'introduction, dans la loi du 6 janvier 1978, d'une disposition nouvelle prévoyant que les fichiers relevant de l'article 26 (ceux intéressant la sécurité publique et ceux ayant pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté), une fois autorisés par le législateur et en amont de la publication du décret d'application de la loi, fassent l'objet, sur le plan technique, d'une procédure de mise en application par étapes, afin qu'ils puissent, à chaque étape clé de leur élaboration et lors de rendez-vous

(1) Éléments de réponse au questionnaire adressé à M. Alex Türk en vue de son audition par la mission d'information le 1er décembre 2010.
(2) Idem.
(3) Idem.
(4) Idem.

obligatoires, faire l'objet d'une validation conjointe entre la CNIL et le ministère de l'Intérieur (**Recommandation n° 9**). D'un point de vue financier, cela permettait de limiter les coûts engendrés par les modifications successives des systèmes d'information. Cette procédure reposait sur l'idée d'un dialogue entre la CNIL et les services tout au long du processus de développement du fichier, à des échéances fixées à l'avance.

Cette proposition n'a pas été mise en œuvre à ce jour. Elle figurait dans la proposition de loi déposée par vos rapporteurs. En effet, son article 5, tel qu'il a été amendé par la commission des Lois de l'Assemblée nationale, prévoyait la mise en place d'un régime d'expérimentation : « *V. – Par dérogation aux III et IV, lorsque sa mise au point nécessite une exploitation en situation réelle de fonctionnement, un traitement peut être mis en œuvre à titre expérimental pour une durée de dix-huit mois, après déclaration auprès de la commission. Un décret en Conseil d'État, pris après avis de la commission, détermine les modalités selon lesquelles la commission est informée de l'évolution technique d'un tel projet de traitement et fait part de ses recommandations au seul responsable de ce projet.* » Mais, comme il a été rappelé plus haut, cette proposition n'a pas abouti.

Toutefois, la proposition de loi sénatoriale précitée visant à mieux garantir la vie privée à l'heure du numérique prévoit l'introduction d'une disposition permettant la mise en œuvre, à titre expérimental et sous le contrôle de la CNIL, de certains fichiers de police.

En effet, l'article 4 de la proposition adoptée au Sénat en première lecture le 23 mars 2010 dispose que *« lorsque la mise au point technique d'un traitement mentionné aux I ou II nécessite une exploitation en situation réelle de fonctionnement, un tel traitement peut être autorisé, à titre expérimental, pour une durée maximale de dix-huit mois, par arrêté pris après avis de la Commission nationale de l'informatique et des libertés. Cet arrêté détermine les finalités, la durée et le champ d'application de l'expérimentation. Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, détermine les modalités selon lesquelles la commission est informée de l'évolution technique d'un tel projet de traitement et fait part de ses recommandations au seul responsable de ce projet. »*

Dès lors que le législateur n'est pas à l'origine de la création du fichier considéré, ce dispositif n'est pas équivalent à celui envisagé par vos rapporteurs. En effet, alors que la recommandation de vos rapporteurs tendait à rendre possible une mise en application par étape du fichier de police créé par le législateur, la proposition sénatoriale confère une fois de plus au pouvoir réglementaire toute latitude pour créer et expérimenter un nouveau fichier. Cependant, d'après la CNIL [(1)], cette disposition permettrait de clarifier le cadre juridique actuel qui, sans interdire de telles expérimentations, ne confie aucune prérogative à la CNIL dans leur suivi.

(1) Idem.

Proposition n° 1

Modifier rapidement le cadre juridique des fichiers de police conformément aux recommandations n° 1 à 10 du précédent rapport.

C. LA LÉGALITÉ DES FICHIERS DE POLICE: UNE PRÉOCCUPATION QUI DEMEURE

Vos rapporteurs ont souhaité recenser, autant que possible, les fichiers de police existants et faire le bilan des deux années écoulées au regard de la nécessité, soulignée lors du précédent rapport de la mission, de mettre fin à l'illégalité de certains fichiers.

1. Un important processus de régularisation des nombreux fichiers de police

Une réelle prise de conscience semble être intervenue à la suite de la publication du rapport de la mission d'information, en mars 2009. Plusieurs fichiers de police utilisés au plan national par l'ensemble des forces de l'ordre ont été régularisés, d'autres le seront sous peu. Au plan local, le développement spontané des fichiers de police demeure une pratique courante, dont les directions générales de police et de la gendarmerie nationales semblent avoir pris toute la mesure, comme en témoigne cette déclaration faite à vos rapporteurs par des fonctionnaires des forces de l'ordre : « *on a développé un petit logiciel en interne* ».

En 2009, vos rapporteurs avaient recensé 58 fichiers de police, dont 48 effectivement utilisés et 10 en cours de développement. Parmi les 48 fichiers utilisés par les forces de l'ordre, 23 n'avaient fait l'objet d'aucune déclaration à la CNIL et se trouvaient donc dans l'illégalité la plus totale. Aujourd'hui, sur 80 fichiers de police recensés, 62 effectivement utilisés [(1)], 28 n'ont pas fait l'objet d'un texte législatif ou réglementaire les autorisant expressément. Ces chiffres figurent dans le tableau ci-dessous.

(1) Par rapport à 2009, 10 fichiers ont été supprimés et 8 fichiers sont en cours de développement ou de déploiement.

COMPARAISON DES RECENSEMENTS EFFECTUÉS EN 2009 ET 2011

	En mars 2009	En décembre 2011
Nombre de fichiers (toutes catégories confondues)	58	80
Nombre de fichiers de police utilisés recensés	48	62
Dont		
— Fichiers autorisés par la loi ou un texte réglementaire	35 (73 %)	34 (55 %)
— Fichiers n'ayant pas fait l'objet d'une autorisation légale ou réglementaire	13 **(27 %)**	28 **(45 %)**
▪ Mais pour lesquels un projet de texte réglementaire est en préparation		24 *(soit **86 %** des fichiers non déclarés)*
▪ Mais pour lesquels un projet de texte réglementaire est en préparation et pour lesquels la CNIL a rendu un avis		3
Nombre de fichiers de police en cours de développement	10	8
Dont		
— Fichiers autorisés par la loi ou un texte réglementaire	0	3
— Fichiers n'ayant pas fait l'objet d'une autorisation légale ou réglementaire	10	5
Nombre de fichiers supprimés par rapport à 2009		10

Alors qu'en mars 2009, seuls 27 % des fichiers effectivement utilisés étaient illégaux, à l'heure actuelle, ce chiffre est porté à 45 %. Toutefois, **il convient de ne pas tirer de ces chiffres une conclusion hâtive qui ne refléterait qu'imparfaitement la réalité**.

En effet, **de nombreux fichiers ont été régularisés** : le fichier SALVAC (cf. *infra*) d'analyse criminelle [(1)], le traitement automatisé de contrôle des données signalétiques des véhicules [(2)], les fichiers des résidents des zones sécurisées [(3)], le fichier national des interdits d'acquisition et de détention d'armes [(4)], le fichier PULSAR [(5)] de la gendarmerie nationale et le logiciel de rédaction des procédures de la gendarmerie nationale, dénommé, en 2009, ICARE [(6)].

(1) Décret n° 2009-786 du 23 juin 2009.
(2) Arrêté du 18 mai 2009 portant création d'un traitement automatisé de contrôle des données signalétiques des véhicules.
(3) Arrêté du 2 mai 2011 relatif aux traitements automatisés de données à caractère personnel dénommés « fichiers des résidents des zones sécurisées » créés à l'occasion d'un événement majeur.
(4) Décret n° 2011-374 du 5 avril 2011.
(5) Arrêtés du 2 décembre 2010.
(6) Décret n° 2011-111 du 27 janvier 2011.

De plus, un effort a été entrepris pour procéder **à la déclaration des fichiers de police, non plus *a posteriori*, mais avant ou pendant leur développement**. C'est le cas de la base de données de sécurité publique, anciennement ATHENA [(1)], des fichiers PASP et EASP remplaçant le fichier EDVIRSP [(2)], dont le développement à proprement parler n'a débuté qu'après la parution des décrets, mais aussi du logiciel de rédaction des procédures de la police nationale, anciennement connu sous le nom d'ARDOISE [(3)].

Enfin, **de nombreux projets de textes réglementaires sont en cours d'élaboration** [(4)], qui concernent les fichiers OCTOPUS, LUPIN, CORAIL, le système de traitement des images des véhicules volés, CALIOPE, GESTEREXT, la pré-plainte en ligne, le logiciel ANACRIM de rapprochement de la gendarmerie nationale, mais aussi le traitement des antécédents judiciaires (TAJ) qui doit remplacer sous peu le STIC et JUDEX, ou le fichier des objets et véhicules signalés (FOVES). Vos rapporteurs souhaiteraient que la publication de ces textes intervienne très rapidement, notamment en ce qui concerne les fichiers d'ores et déjà utilisés par les forces de l'ordre et qui correspondent à un besoin réel des services.

Proposition n° 2

Donner très rapidement une base juridique solide aux fichiers de police d'ores et déjà utilisés par les forces de l'ordre et qui correspondent à un besoin réel des services.

Les offices centraux ont fait l'objet d'une attention particulière. En effet, comme cela a été indiqué à vos rapporteurs lors d'un déplacement, « *il n'existe pas un seul office central sans base de données propre* ». C'est en effet ce qu'a révélé l'affaire du fichier MENS (cf. *infra*), ainsi que les déplacements effectués par vos rapporteurs au cours de l'année écoulée. Vos rapporteurs ont en effet pu constater, à plusieurs reprises, que **des fichiers, dont certains ont été créés grâce à un logiciel de développement appelé WINDEV, avaient été développés par de nombreux services afin d'opérer des rapprochements entre les affaires relevant de leur compétence**. Ces fichiers n'avaient pas, à l'époque, fait l'objet de déclarations auprès de la CNIL.

Prenant la mesure du problème, les directions générales de la police et de la gendarmerie nationales, ont mis au point divers textes réglementaires qui devraient bientôt faire l'objet d'un avis de la CNIL, voire d'une publication. C'est notamment le cas, pour la gendarmerie nationale, de différentes bases de données utilisées par les services des offices centraux : la base OCLDI, la base des

(1) Décrets n^os^ 2011-340, 2011-341 et 2011-342.
(2) Décrets n^os^ 2009-1249 et 2009-1250.
(3) Décret n° 2011-110 du 27 janvier 2011.
(4) Réponse du 9 août 2011 de M. Claude Guéant, ministre de l'Intérieur, à la mission d'information.

victimes non identifiées, la base de données relative aux escroqueries, celle portant sur les objets volés, la base de données relative aux atteintes aux biens et à la criminalité organisée…

Par ailleurs, une régularisation massive des fichiers de police développés au plan local et non déclarés est mise en œuvre par les directions générales. Notamment, **l'utilisation d'accords cadres, permettant la déclaration de plusieurs fichiers aux fins identiques**, constitue un outil précieux pour assurer la déclaration rapide de ces fichiers auprès de la CNIL. Ainsi, les fichiers judiciaires des brigades et sections de recherche, qui visent au partage de l'information opérationnelle par l'envoi de messages d'information, seront déclarés par ce biais, comme l'a indiqué à la mission d'information le Général Jacques Mignaux, directeur général de la gendarmerie nationale (1).

Ainsi, le ministère de l'Intérieur (2) a entrepris la **régularisation de six catégories de fichiers de police développés localement, par le biais d'actes cadres**. Ainsi, les **registres des fourrières** et des immobilisations, les fichiers relatifs au **contrôle judiciaire**, aux **assignations à résidence**, aux **permissions de sortir** et aux **appels à témoins** seront déclarés par ce biais. Les fichiers de **résidents des zones sécurisées** ont d'ores et déjà été régularisés par un arrêté du 2 mai 2011. Les répertoires locaux pour les opérations de protection des personnes âgées de plus de 65 ans devraient également faire l'objet d'un texte réglementaire de même nature.

Au total, une observation plus fine des fichiers recensés et de leur statut juridique montre que la situation, par rapport à mars 2009, s'améliore. En effet, **86 % des fichiers actuellement utilisés de façon illégale doivent faire, dans un avenir proche, l'objet d'un texte réglementaire et d'une déclaration à la CNIL**. Pour trois d'entre eux, la CNIL s'est d'ailleurs d'ores et déjà prononcée, ce qui laisse à penser que la régularisation interviendra rapidement (3).

2. L'absence de base juridique pour les fichiers de rapprochement destinés à lutter contre la délinquance sérielle

En mars 2009, deux fichiers développés par la préfecture de police étaient en cours d'expérimentation: **CORAIL, cellule opérationnelle de rapprochement et d'analyse des infractions et LUPIN, le logiciel d'uniformisation des procédures d'identification**. Ces deux fichiers avaient pour dessein de réaliser des rapprochements dans le domaine de la petite et moyenne délinquance. Ces deux fichiers, extrêmement utiles aux forces de l'ordre, ne bénéficiaient pas, en 2009, d'un cadre juridique adapté. Aussi vos rapporteurs avaient-ils proposé qu'un cadre juridique spécifique à ces fichiers soit défini par le législateur (**Recommandation n° 50**).

---

(1) Audition du 23 mars 2011du Général Jacques Mignaux, directeur général de la gendarmerie nationale.
(2) Courrier en date du 9 août 2011 du ministre de l'Intérieur (cf. annexe n° 6).
(3) C'est le cas des répertoires locaux pour les opérations de protections des personnes âgées de plus de 65 ans, du fichier ARES et de la pré-plainte en ligne.

L'article 21-1 de la loi n° 2003-239 pour la sécurité intérieure n'offrant pas un cadre juridique adapté aux nouveaux logiciels de rapprochements en matière délictuelle, l'article 19 de la proposition de loi n° 1738 relative aux fichiers de police, co-signée par vos rapporteurs, avait pour objet de définir **un cadre légal adapté aux fichiers de rapprochements en matière de petite et moyenne délinquance sérielle** (1), clairement **distinct de celui existant pour les crimes et délits les plus graves**.

Article 19 de la proposition de loi n° 1738 relative aux fichiers de police

« *Après l'article 21-1 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, il est inséré un article 21-2 ainsi rédigé :*

« Art. 21-2. – I. – Les services et les unités de la police et de la gendarmerie nationales chargés d'une mission de police judiciaire peuvent mettre en œuvre des traitements automatisés de données à caractère personnel collectées au cours des enquêtes préliminaires ou de flagrance ou des investigations exécutées sur commission rogatoire afin de faciliter la constatation des délits présentant un caractère sériel, d'en rassembler les preuves et d'en identifier les auteurs, grâce à l'établissement de liens entre les individus, les événements ou les infractions pouvant mettre en évidence ce caractère sériel :

« – par le rapprochement d'informations de police technique et scientifique recueillies sur les lieux des infractions ainsi que des modes opératoires ;

« – ou par l'établissement de rapprochements à partir des informations transmises entre officiers de police judiciaire au titre de l'article D. 3 du code de procédure pénale.

« Ces traitements peuvent concerner tout délit portant atteinte aux personnes puni de plus d'un an d'emprisonnement ou portant atteinte aux biens et puni de plus de deux ans d'emprisonnement.

« II. – Par dérogation à l'article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, sont autorisés, pour les seules fins mentionnées au I, la collecte, la conservation et le traitement par les services précités des données susceptibles de faire apparaître les signes physiques particuliers et objectifs comme éléments de signalement.

(1) *En effet, l'article 21-1 de la loi du 18 mars 2003 porte sur «* tout crime ou délit portant atteinte aux personnes punis de plus de cinq ans d'emprisonnement ou portant atteinte aux biens et punis de plus de sept ans d'emprisonnement », tandis que la proposition de loi n° 1738 relative aux fichiers de police vise « tout délit portant atteinte aux personnes puni de plus d'un an d'emprisonnement ou portant atteinte aux biens et puni de plus de deux ans d'emprisonnement *».*

« III. – Ces traitements peuvent contenir des données :

« 1° Sur les personnes de plus de treize ans à l'encontre desquelles il existe des indices graves ou concordants qu'elles aient pu participer, comme auteurs ou complices, à la commission d'une infraction mentionnée au I. L'enregistrement des données concernant ces personnes peut intervenir, le cas échéant, après leur condamnation ;

« 2° Sur les personnes victimes d'une infraction mentionnée au I, sans limitation d'âge.

« IV. – La durée de conservation des données décomptée à partir de la date de leur enregistrement dans ces traitements est au maximum de trois ans.

« V. – Les personnes mentionnées au 2° du III peuvent demander l'effacement des données les concernant enregistrées dans le traitement dès lors que l'auteur des faits a été définitivement condamné.

« VI. – Les dispositions du III de l'article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure sont applicables à ces traitements.

« VII. – Sont destinataires des données à caractère personnel mentionnées au présent article :

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

« – les magistrats du parquet et les magistrats instructeurs, pour les recherches relatives aux informations dont ils sont saisis.

« L'habilitation précise la nature des données auxquelles elle autorise l'accès.

« VIII. – Les traitements prévus au I ne font l'objet d'aucune interconnexion avec d'autres traitements ou fichiers.

« IX. – En application de l'article 26 de la loi n° 78-17 précitée, un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, fixe les modalités d'application du présent article.

« Il précise les conditions dans lesquelles :

« – les personnes mentionnées au 1° du III peuvent exercer leur droit d'accès de manière indirecte, conformément aux dispositions de l'article 41 de la loi n° 78-17 précitée ;

« – les personnes mentionnées au 2° du III peuvent exercer leur droit

d'accès directement auprès du responsable du traitement, conformément aux dispositions de l'article 39 de la loi n° 78-17 précitée.

« X. – Les dispositions de cet article sont applicables pendant trois années à compter de la publication de la présente loi. Le Gouvernement remet au Parlement un rapport sur l'application de cet article trois mois avant l'expiration du délai précité. »

Cette proposition de loi n'ayant pas pu aboutir, les services de police utilisateurs de CORAIL et LUPIN, comme les services de gendarmerie à propos d'ANACRIM, leur logiciel de rapprochement, comptaient sur la loi d'orientation et de programmation pour la performance de la sécurité intérieure pour donner une base légale à ces fichiers non déclarés à la CNIL.

En effet, l'article 14 de la loi d'orientation et de programmation pour la performance de la sécurité intérieure prévoyait la création d'un nouveau type de fichiers de police, distinct des fichiers d'analyse sérielle, intitulés « Fichiers de rapprochements ». Il s'agissait de permettre aux services de police et de gendarmerie d'effectuer des rapprochements dans le domaine de la petite et moyenne délinquance sérielle. **L'absence de seuil infractionnel ainsi que le périmètre de collecte relativement large** (enquêtes préliminaires, enquêtes de flagrance, investigations sur commission rogatoire, disparitions inquiétantes, procédure de recherche des causes de la mort), devaient permettre d'**améliorer le taux d'élucidation des faits de petite et moyenne délinquance**.

Toutefois, cette proposition s'éloignait considérablement du dispositif envisagé par vos rapporteurs. Outre que l'article 14 de la LOPPSI ne fixe aucun seuil de peine, le texte demeure **lacunaire sur le cadre juridique de ces logiciels de rapprochement judiciaire**, puisqu'il renvoie au pouvoir réglementaire l'éventuelle dérogation à l'interdiction de collecte et d'exploitation des données sensibles, la possibilité d'enregistrer des données personnelles relatives aux témoins ainsi que la question de l'âge à partir duquel une personne peut figurer dans un traitement de rapprochement judiciaire.

Par ailleurs, le Conseil constitutionnel a mis un terme aux espoirs portés par les services. En effet, dans sa décision du 10 mars 2011 relative à la loi de programmation et d'orientation pour la performance de la sécurité intérieure [(1)], il a considéré **que le législateur ne pouvait souhaiter créer de nouvelles bases de données susceptibles d'assimiler un très grand nombre de faits et d'effectuer, de façon automatique, des rapprochements de grande ampleur**. En effet, s'agissant des traitements, **les dispositions en cause présentaient une ambiguïté en ce qu'elles pouvaient se prêter à deux interprétations** : soit il s'agissait de permettre le recours à ces logiciels par des services déterminés de police judiciaire conduisant à travailler sur une série de faits et sur des données collectées dans le cadre d'une enquête déterminée ; soit il s'agissait de permettre à tous les services

(1) Décision n° 2011-625 DC du 10 mars 2011.

de police judiciaire de mettre en commun leurs informations exploitées par des logiciels de rapprochement. Le Conseil constitutionnel a écarté cette seconde interprétation, puisqu'***« il ne saurait être question de faire travailler des logiciels de rapprochement sur un grand fichier global de toutes les informations en provenance des services d'enquête*** » (1).

Le Conseil constitutionnel a en outre considéré que **l'article 14 ne faisait qu'étendre les dispositions prévues pour les fichiers d'analyse sérielle aux faits de plus faible gravité**. En effet, le rapprochement dont il est question à l'article 14, de même que les finalités de ces fichiers, se distinguent assez peu, dans le texte, des fichiers d'analyse sérielle. Il s'agit en effet d'établir des séries dans le but d'identifier leurs auteurs. Or, le Conseil constitutionnel considère **la gravité de l'infraction comme un élément déterminant de l'appréciation de la proportionnalité entre la protection de l'ordre public et le respect de la vie privée**.

Dès lors, le Conseil constitutionnel a indiqué, dans son considérant n° 71 (2), que **ces logiciels ne sauraient avoir pour effet de permettre la mise en œuvre d'un traitement général des données recueillies au cours des diverses enquêtes**. Bien au contraire, le Conseil constitutionnel considère que « *ces logiciels ne pourront conduire qu'à la mise en œuvre, autorisée (par le juge d'instruction ou le procureur), de traitements de données à caractère personnel particuliers, dans le cadre d'une enquête ou d'une procédure déterminée portant sur une série de faits et pour les seuls besoins de ces investigations* ».

En dépit de la décision du Conseil constitutionnel, le choix a été fait, par le ministère de l'Intérieur, de déclarer les fichiers LUPIN (3) et ANACRIM sur le fondement des nouveaux articles 230-20 et suivants du code de procédure pénale, relatifs aux logiciels de rapprochements judiciaires. En revanche, CORAIL serait déclaré sur le fondement de l'article 26 de la loi du 6 janvier 1978. Vos rapporteurs ne peuvent dès lors que recommander, à nouveau, la création d'un cadre législatif adapté aux fichiers CORAIL et LUPIN.

Proposition n° 3

Donner un cadre législatif adapté aux fichiers de rapprochements en matière de petite et moyenne délinquance sérielle et conforme à la décision du Conseil constitutionnel.

Au final, sur les treize recommandations relatives au cadre juridique des fichiers de police, une seule a pu être mise en œuvre, qui porte sur la représentation pluraliste du Parlement au sein de la CNIL.

(1) Commentaire aux cahiers, p. 43.
(2) Décision n° 2011-625 DC du 10 mars 2011.
(3) Réponse du 9 août 2011 de M. Claude Guéant, ministre de l'intérieur, à la mission d'information.

DEUXIÈME PARTIE : LA PROTECTION DES DROITS ET LIBERTÉS : DES PROGRÈS INSUFFISANTS

Au terme de la mission d'information conduite en 2009, vos rapporteurs avaient acquis la profonde conviction que, contrairement aux idées reçues, une meilleure protection des droits et libertés des citoyens dans l'utilisation de leurs données personnelles et une meilleure performance des fichiers de police utilisés par les policiers et gendarmes, loin d'être des objectifs contradictoires, allaient de pair. Cette conviction fondamentale demeure. Les dysfonctionnements et les inexactitudes dans la gestion des fichiers portent préjudice aux citoyens comme aux utilisateurs. C'est avec l'ambition d'améliorer tant le respect des droits et libertés, que la fiabilité et l'efficacité des fichiers que vos rapporteurs avaient, en 2009, émis un certain nombre de recommandations tendant à renforcer les droits des personnes, auteurs ou victimes, susceptibles d'être inscrites au sein de fichiers de police.

Force est de constater que peu d'entre elles ont été mises en œuvre depuis la publication du rapport de la mission d'information, en mars 2009. Certes, des vides juridiques ont été comblés, par exemple en matière de prélèvement biologique. Les délais légaux de traitement des demandes d'effacement ou de rectification des données ont été réduits, notamment pour ce qui est des fichiers d'antécédents judiciaires. Les mineurs bénéficient aujourd'hui d'un semblant de droit à l'oubli. De nouveaux fichiers, plus encadrés, ont vu le jour en matière d'atteintes à la sécurité publique et d'enquêtes administratives.

Mais d'importants motifs d'insatisfaction demeurent. Les délais de traitement des demandes d'accès indirect sont toujours trop longs, les demandes d'effacement et de rectification particulièrement urgentes ne bénéficient d'aucun traitement particulier. L'information des personnes demeure indigente et d'importantes failles juridiques aboutissent à ce que figurent dans les fichiers des données et des personnes qui ne devraient pas y être. Aujourd'hui comme hier, la protection des droits et libertés reste, pour vos rapporteurs, un impératif absolu.

A. LA PROTECTION DES DROITS DES PERSONNES INSCRITES DANS DES FICHIERS À FINALITÉ JUDICIAIRE

Les droits de personnes inscrites au sein des fichiers d'antécédents judiciaires que sont le STIC pour la police nationale, et JUDEX pour la gendarmerie nationale, n'ont connu que peu d'avancées ces deux dernières années. **Les recommandations émises par vos rapporteurs sont, à de rares exceptions près, restées lettre morte.** Seuls deux points donnent satisfaction : un vide juridique comblé en ce qui concerne les prélèvements biologiques visant à alimenter le fichier des empreintes génétiques (FNAEG), et la réduction à un mois du délai de traitement des demandes de rectification par le procureur de la République.

1. Un toilettage législatif appréciable en matière de prélèvement biologique

Un toilettage législatif significatif est intervenu dans le domaine des fichiers d'identification. Dans le cadre du précédent rapport, la mission d'information avait souhaité que soit clarifié **le cadre légal du prélèvement biologique visant à alimenter le fichier des empreintes génétiques** (FNAEG), un vide juridique étant apparu concernant les prélèvements opérés sur des personnes contre lesquelles il existait des « *raisons plausibles* » de soupçonner qu'elles avaient commis un crime ou un délit.

En effet, la nature des crimes et délits susceptibles de donner lieu à un prélèvement biologique n'était pas explicitée par l'article 706-54 du code de procédure pénale, alors même qu'une circulaire d'application renvoyait expressément aux infractions définies à l'article 706-55 du même code. Vos rapporteurs avaient donc proposé qu'à l'instar des prélèvements opérés sur les personnes condamnées ou suspectées, ce prélèvement ne soit possible que dans le cadre des infractions définies à l'article 706-55 du code (**Recommandation n°24**).

Cette recommandation a été mise en œuvre, puisque l'article 9 de la loi n° 2011-267 du 14 mars 2011 [(1)] a modifié le troisième alinéa de l'article 706-54 du code de procédure pénale comme suit : « *Les officiers de police judiciaire peuvent également, d'office ou à la demande du procureur de la République ou du juge d'instruction, faire procéder à un rapprochement de l'empreinte de toute personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis* ***l'une des infractions mentionnées à l'article 706-55*** *avec les données incluses au fichier, sans toutefois que cette empreinte puisse y être conservée* ». La divergence qui existait alors entre la lettre de la loi et son interprétation est donc résolue, conformément à la proposition de vos rapporteurs.

Cependant, en matière de prélèvement génétique, votre rapporteure déplore le fait que la loi ait été détournée de son but premier pour poursuivre les représentants syndicaux qui refusent que soit effectué sur eux un prélèvement génétique. En effet, comme l'a rappelé le jugement du tribunal correctionnel de Compiègne le 3 mai 2011, « *on ne saurait assimiler un enlèvement et séquestration opérés de façon crapuleuse dans le cadre d'opérations mafieuses et les actions qualifiées par les mêmes mots par le code pénal mais qui se sont déroulées dans le cadre d'une action syndicale certes réprimée par la cour d'appel mais s'inscrivant dans un conflit social difficile* » [(2)]. La poursuite des responsables syndicaux pour refus de se soumettre à un prélèvement génétique est ainsi jugée contraire à la loi du 6 janvier 1978 et à la nécessaire proportionnalité entre le but visé par le fichier – en l'occurrence, l'élucidation d'infractions – et les moyens d'y parvenir, à savoir le prélèvement génétique.

---

(1) Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

(2) Cf. Annexe n° 6.

2. Une amélioration modeste du droit d'accès aux fichiers d'antécédents judiciaires

Le droit d'accès et de rectification dont disposent les personnes figurant dans des fichiers d'antécédents judiciaires n'a que très peu évolué depuis 2009, les recommandations formulées par vos rapporteurs n'ayant, pour la plupart, pas été suivies.

a) Droit d'accès aux fichiers d'antécédents judiciaires : l'immobilisme

L'article 41 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, prévoit, par dérogation au droit commun, un droit d'accès indirect en matière de fichiers de police. Ainsi, les citoyens qui souhaitent savoir s'ils sont inscrits dans des fichiers d'antécédents judiciaires (STIC, JUDEX) ou de police (FPR, SALVAC, ANACRIM) doivent saisir la CNIL d'une demande spécifique. C'est alors un magistrat membre de la CNIL qui se met en relation avec le responsable du traitement en question et exerce ce droit d'accès en lieu et place de la personne [(1)].

Comme vos rapporteurs l'avaient constaté en 2009, la CNIL doit répondre à un nombre croissant de demandes d'accès et de rectification, si bien que les délais d'attente sont extrêmement longs au regard des enjeux personnels que peut revêtir une inscription dans un fichier d'antécédents judiciaires. C'est pourquoi vos rapporteurs avaient préconisé **l'embauche ponctuelle de contractuels par la CNIL**, afin de traiter le stock des recours accumulés (**Recommandation n° 41**), ainsi que l'engagement d'une **réflexion sur la création d'une redevance permettant de financer l'adaptation des moyens humains de la CNIL** au nombre croissant des recours (**Recommandation n° 43**).

Ces recommandations n'ont pas été mises en œuvre, ce qui explique l'accroissement du stock de dossiers en souffrance et la persistance d'importants délais de traitement des demandes d'accès. Ainsi, en 2010, 2 796 demandes de droit d'accès aux fichiers d'antécédents judiciaires STIC et JUDEX étaient encore en cours de traitement [(2)]. Parmi ces demandes, une centaine résulte d'ailleurs de saisines antérieures à 2007 [(3)]. De façon générale, la CNIL évalue le délai moyen de réponse à un an lorsque la personne est effectivement inscrite dans un fichier d'antécédents [(4)], soit le double du délai prévu par l'article 87-1 du décret n° 2005-1309 du 20 octobre 2005 [(5)]. Toutefois, il semble que ces délais soient en partie imputables à la complexité de certains dossiers, qui nécessitent la centralisation, par les services gestionnaires, de toutes

(1) Cf. annexe n°7.

(2) Eléments de réponse au questionnaire adressé à M. Alex Türk en vue de son audition par la mission d'information le 1er décembre 2010.

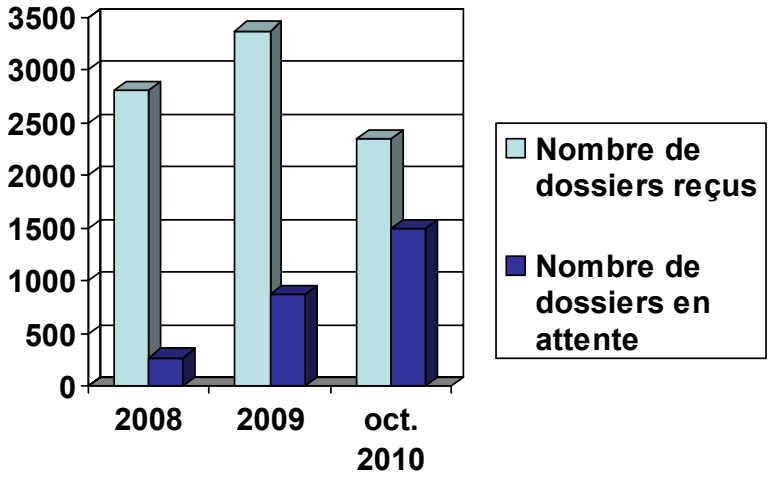
(3) Eléments de réponse au questionnaire adressé à M. Alex Türk en vue de son audition par la mission d'information le 1er décembre 2010.

(4) Cf. annexe n°7.

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

les procédures judiciaires relatives au demandeur, ainsi qu'à des difficultés récurrentes d'obtention des suites judiciaires auprès de certaines juridictions [(1)].

ÉTAT DES DEMANDES DU DROIT D'ACCÈS INDIRECT ADRESSÉES A LA CNIL POUR LES FICHIERS D'ANTÉCÉDENTS JUDICIAIRES (STIC ET JUDEX)



Source : éléments de réponse au questionnaire adressé à M. Alex Türk en vue de son audition par la mission d'information le 1er décembre 2010.

Vos rapporteurs avaient constaté en 2009 que les délais de réponse de la CNIL étaient également liés à la **lourde procédure mise en place pour les personnes victimes d'infraction pénale** figurant dans des fichiers d'antécédents judiciaires, identique à celle applicable aux personnes mises en cause. Vos rapporteurs avaient donc proposé, afin de désengorger les services de la CNIL, que les victimes bénéficient d'un droit d'accès direct aux fichiers d'antécédents judiciaires (**Recommandation n° 42**). C'était d'ailleurs l'objet de l'article 15 de la proposition de loi déposée par vos rapporteurs. Mais **cette proposition n'a pas été mise en œuvre.**

b) Le traitement en temps réel des demandes de rectification et d'effacement par les parquets : la prochaine étape ?

Une avancée notable a été réalisée en matière de demandes de mise à jour. L'instruction de ces demandes, qu'il s'agisse de demandes de rectification ou d'effacement, appartient au procureur de la République, qui enjoint ensuite aux services de police et de gendarmerie concernés de procéder à la mise à jour. Il peut

(1) Eléments de réponse au questionnaire adressé à M. Alex Türk en vue de son audition par la mission d'information le 1er décembre 2010.

être saisi, en application de l'article 87-1 du décret n° 2005-1309 du 20 octobre 2005 (1), tant par la CNIL que par des particuliers.

Vos rapporteurs avaient noté à quel point un important délai dans la mise à jour des données figurant dans les fichiers d'antécédents judiciaires pouvait être préjudiciable aux personnes. Aussi la mission avait-elle préconisé qu'**un délai d'un mois soit imposé au procureur pour traiter ces demandes (Recommandation n° 36), au lieu des trois mois** qui lui sont laissés par le décret mentionné plus haut.

L'article 15 de la proposition de loi relative aux fichiers de police, co-signée par vos rapporteurs, avait précisément pour but de traduire cette recommandation dans le droit positif. Tout en faisant figurer le délai de traitement des demandes d'effacement et de rectification par le procureur dans un texte de nature législative, cet article le ramenait à un mois seulement. Si cette proposition de loi n'a pu aboutir, **cette recommandation a cependant été mise en œuvre par l'article 11 de la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure** (2). Le nouvel article 230-8 du code de procédure pénale dispose désormais que « *le procureur de la République se prononce sur les suites qu'il convient de donner aux demandes d'effacement ou de rectification* ***dans un délai d'un mois*** ». Ce délai d'un mois fixé par le législateur constitue une garantie supplémentaire pour les personnes inscrites dans des fichiers d'antécédents judiciaires.

Parallèlement, vos rapporteurs avaient souhaité qu'**une procédure de traitement des demandes en temps réel par un magistrat référent** soit mise en place pour traiter les demandes de mise à jour présentant un niveau d'urgence particulièrement élevé (**Recommandation n° 37**).

L'article 14 de la proposition de loi relative aux fichiers de police, cosignée par vos rapporteurs, visait à transcrire cette recommandation dans le droit positif. Vos rapporteurs avaient alors souhaité confier à un magistrat référent le soin de traiter les demandes urgentes de mises à jour. Deux critères avaient été retenus pour avoir droit à ce traitement en temps réel : un risque d'inexactitude des données personnes et un préjudice immédiat et sérieux pour la personne requérant la mise à jour des fichiers d'antécédents judiciaires. Lorsque ces deux conditions sont réunies, le dispositif prévoyait que le magistrat référent pouvait ordonner sans délai la rectification des données. Toutefois, il n'a pas été donné de suite favorable à cette proposition.

Cependant, cette recommandation a été partiellement mise en œuvre par la loi du 14 mars 2011 précitée. En effet, son article 11 prévoit le contrôle d'un magistrat spécialement désigné, titulaire des mêmes prérogatives que le pro-

(1) Décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.

(2) Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

cureur de la République. **Ce magistrat référent devrait, à terme, être l'interlocuteur privilégié des particuliers demandant une rectification de données.**

Si la mise en place d'un magistrat référent en matière de fichiers d'antécédents judiciaires à l'article 230-9 du code de procédure pénale constitue un progrès, on peut néanmoins déplorer le fait que ses prérogatives et obligations se distinguent si peu de celles du procureur de la République. En effet, comme le procureur, le magistrat référent dispose d'un mois pour se prononcer sur les suites à donner à la demande. Il convient par ailleurs de noter que ce magistrat n'a pas encore été nommé, le décret nécessaire à la mise en œuvre de ce dispositif étant en cours d'élaboration par le ministère de la Justice. **Si aucun traitement en temps réel n'est donc prévu aujourd'hui, la mise en place d'un magistrat référent constitue un premier pas vers la mise en œuvre de la recommandation formulée par vos rapporteurs.**

c) L'effacement des données personnelles en cas de classement sans suite, de non lieu, de relaxe ou d'acquittement : les impératifs de la sécurité

Les décisions de relaxe ou d'acquittement doivent, en toute logique, entraîner l'effacement des données personnelles concernant la personne mise en cause. Toutefois, la loi donne au procureur la faculté d'ordonner le maintien de ces données pour des raisons liées à la finalité du fichier. Vos rapporteurs ont, sur ce sujet, des vues divergentes, ce qui avait donné lieu, en mars 2009, à **deux recommandations opposées**.

Votre rapporteur souhaitait, dans sa **recommandation n° 38**, maintenir la faculté accordée au procureur de la République de prescrire le maintien dans un fichier d'antécédent judiciaire des données personnelles concernant les personnes mises en cause en cas de décision de relaxe ou d'acquittement devenue définitive. Votre rapporteure, quant à elle, souhaitait voir supprimée la faculté accordée au procureur de la République de prescrire le maintien dans un fichier d'antécédent judiciaire des données personnelles concernant les personnes mises en cause en cas de décision de relaxe ou d'acquittement devenue définitive (**Recommandation n°38 *bis***).

Il semble que la sécurité des concitoyens ait prévalu, dans ce domaine, sur le droit à l'effacement conféré par la loi, puisque **c'est la recommandation n° 38 de votre rapporteur qui a été mise en œuvre par le législateur en 2011**. Le nouvel article 230-8 du code de procédure pénale, issu de la loi du 14 mars 2011 [(1)], dispose ainsi qu'« *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.*

(1) Idem.

Lorsque le procureur de la République prescrit le maintien des données personnelles relatives à une personne ayant bénéficié d'une décision d'acquittement ou de relaxe devenue définitive, il en avise la personne concernée. »

L'information de la personne constitue toutefois une innovation bienvenue par rapport au droit antérieur. Cette nouvelle rédaction est d'ailleurs tout à fait conforme au compromis auquel étaient parvenus vos rapporteurs dans le cadre de la proposition de loi relative aux fichiers de police, notamment son article 15.

Vos rapporteurs s'étaient en outre accordés sur **la nécessité de permettre au procureur d'ordonner l'effacement des données dans des cas alors non envisagés par la loi**. En effet, il était apparu que certaines demandes d'effacement du procureur n'étaient pas prises en compte par les services gestionnaires des fichiers, au motif qu'elles ne correspondaient pas au cadre fixé par le législateur (1). Notamment, les personnes mises en cause mais non poursuivies ne pouvaient être effacées des fichiers d'antécédents judiciaires, puisqu'elles n'avaient pas fait l'objet d'une décision de relaxe, d'acquittement ou d'un non lieu. En outre, seules les décisions de classement sans suite motivées par une insuffisance de charge étaient alors susceptibles d'entraîner l'effacement des données. Vos rapporteurs avaient donc recommandé d'**élargir le nombre de cas dans lesquels le procureur de la République peut ordonner l'effacement des données personnelles (Recommandation n° 39)**.

Cette recommandation devait être traduite dans le droit positif par l'article 15 de la proposition de loi relative aux fichiers de police de vos rapporteurs, qui entendait permettre l'effacement des données dans tous les cas de classement sans suite, non plus seulement ceux motivés par une insuffisance de charges. Cette proposition de loi n'a cependant pas pu aboutir.

Cette proposition n'a donc pas été mise en œuvre à ce jour, puisque le procureur ne peut, en application du nouvel article 230-8 du code de procédure pénale, effacer que les données relatives à des personnes relaxées ou acquittées. Il peut également ordonner l'effacement des décisions de non lieu et de classement sans suite, uniquement lorsque ces dernières sont motivées par une insuffisance de charges. Lorsque la personne inscrite au fichier n'a pas fait l'objet de poursuites et *a fortiori* d'une décision de classement pour insuffisance de charges ou d'un non lieu, le procureur ne peut en aucun cas requérir l'effacement des données la concernant.

La loi du 14 mars 2011 (2) a cependant apporté quelques précisions quant au traitement des autres décisions de classement sans suite, dans un sens plus protecteur pour les personnes inscrites. En effet, contrairement au droit antérieur,

(1) Article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure.

(2) Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

les décisions de classement sans suite non motivées par une insuffisance de charges font désormais l'objet d'une mention au fichier des antécédents judiciaires. Cela constitue une avancée certaine pour les personnes inscrites dans des fichiers d'antécédents judiciaires, puisque toute personne qui consultera les données personnelles d'un individu inscrit dans un de ces fichiers sera avisée que cet individu a bénéficié d'une mesure de classement sans suite.

Par ailleurs, la loi du 14 mars 2011 [(1)] introduit **une protection supplémentaire pour les personnes figurant dans ces fichiers**, puisque le nouvel article 230-8 du code de procédure pénale dispose que « *lorsqu'une décision fait l'objet d'une mention, les données relatives à la personne concernée ne peuvent faire l'objet d'une consultation dans le cadre des enquêtes administratives prévues à l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité.* » Ainsi, les conséquences d'une inscription dans un fichier d'antécédents judiciaires d'une personne simplement mise en cause dans une procédure pénale sont, en matière d'emploi ou d'accès à la nationalité, largement amoindries.

De façon générale, même si les recommandations de vos rapporteurs n'ont pas été suivies, plusieurs avancées ont été réalisées en matière d'inscription dans des fichiers d'antécédents judiciaires, permettant d'améliorer les droits de personnes inscrites dans des fichiers d'antécédents judiciaires. En revanche, des progrès restent à accomplir en matière de droit à l'information et d'équité dans l'utilisation de ces données personnelles.

3. Le droit à l'information et à l'équité toujours inexistant

Deux points noirs demeurent dans le droit des fichiers de police, qui n'ont connu aucune évolution législative : le droit à l'information des personnes susceptibles d'être inscrites au sein de fichiers d'antécédents judiciaires et le respect du contradictoire lorsque les informations sont utilisées dans le cadre d'un procès pénal.

a) L'information des personnes inscrites dans des fichiers d'antécédents judiciaires toujours indigente

Le précédent rapport de la mission d'information avait souhaité remédier à une **anomalie en matière d'information des personnes inscrites dans des fichiers d'antécédents judiciaires**. En effet, vos rapporteurs avaient constaté que l'inscription au STIC était presque inéluctable lorsqu'une personne est gardée à vue ou qu'elle apparaît dans un compte rendu d'enquête. Dès lors, il avait semblé souhaitable, afin que les personnes puissent faire valoir leurs droits de rectification et d'effacement, qu'elles soient informées de leur possible inscription au fichier des antécédents judiciaires de la police nationale.

---

(1) Idem.

Vos rapporteurs avaient ainsi proposé de remettre à toute personne placée en garde à vue un document d'information précisant que d'éventuelles poursuites judiciaires peuvent entraîner l'inscription dans un fichier d'antécédent judiciaire et récapitulant de manière pratique les différentes possibilités qui sont offertes aux citoyens en matière de droit d'accès, de demande de mise à jour et de rectification des données (**Recommandation n° 27**).

Cette proposition n'a pas été mise en œuvre, puisque l'obligation d'information prévue par l'article 32 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, n'est toujours pas applicable aux fichiers de police. Toutefois, les directions générales de la police et de la gendarmerie nationale ont indiqué à vos rapporteurs **que l'information des personnes était assurée par le biais d'un affichage dans tous les commissariats et unités de gendarmerie** (1). Vos rapporteurs considèrent, comme en 2009, que ce simple affichage est insuffisant et qu'il conviendrait qu'il soit complété par une information individualisée et écrite, comme le proposait la recommandation n° 27.

Une avancée limitée est toutefois intervenue à l'occasion de la réécriture de l'article 21 de la loi pour la sécurité intérieure de 2003, intégré au code de procédure pénale, à l'article 230-8. En effet, désormais, lorsque le procureur prescrit le maintien des données relatives à une personne relaxée ou acquittée, l'intéressé en est « *avisé* ». Vos rapporteurs ne peuvent que se féliciter de cette information, somme toute indispensable, de la personne inscrite dans un fichier d'antécédents judiciaires.

b) L'encadrement de l'utilisation des fichiers d'antécédents judiciaires dans le cadre d'un procès pénal : affaire à suivre

L'utilisation des antécédents judiciaires des prévenus et accusés, par le ministère public, dans le cadre d'un procès pénal, ne faisait l'objet d'aucun encadrement lorsque la mission d'information a rendu son rapport, en mars 2009. Notamment, la défense n'y avait pas accès, alors même que ces éléments pouvaient avoir un impact non négligeable sur l'opinion des juges.

Vos rapporteurs avaient alors souhaité qu'à l'instar des rapports du fichier des empreintes génétiques (FNAEG), les fiches issues des fichiers d'antécédents judiciaires soient versées au dossier, afin que la défense puisse en prendre connaissance et que la règle du contradictoire soit respectée (**Recommandation n° 33**). Cette précaution est d'autant plus nécessaire que ces fiches, notamment celles issues du STIC, ne sont guère actualisées et comportent un nombre très important d'erreurs.

Si cette mesure n'est pas encore mise en œuvre aujourd'hui, vos rapporteurs avaient recommandé son introduction dans leur proposition de loi

(1) Réponse du 7 mars 2011 des directions générales de la police et de la gendarmerie nationales au questionnaire de suivi des recommandations.

relative aux fichiers de police. En effet, son article 16 prévoyait d'introduire dans le code de procédure pénale, pour les comparutions immédiates, l'alinéa suivant : « *Si le procureur de la République envisage de faire mention d'éléments concernant le prévenu et figurant dans un traitement automatisé d'informations nominatives prévu par l'article 21 de la loi n° 2003-239 du 18 mars 2003 relative à la sécurité intérieure, ces informations doivent figurer dans le dossier mentionné à l'article 393 du présent code.* » Cette proposition de loi n'a pas abouti.

Cependant, l'introduction d'une disposition identique est envisagée par la proposition de loi, déposée au Sénat le 6 novembre 2009, visant à mieux garantir le droit à la vie privée à l'heure du numérique. Notamment, son article 4 *octies* prévoit l'introduction d'un nouvel alinéa à l'article 395 du code de procédure pénale. Toutefois, cette proposition de loi n'a pas encore été discutée à l'Assemblée nationale.

B. LA REFONTE DES FICHIERS DE RENSEIGNEMENT A LAISSÉ DE CÔTÉ CERTAINES RECOMMANDATIONS

Depuis mars 2009, vos rapporteurs ont assisté à un véritable bouleversement du paysage en matière de renseignement. Les dénominations ont changé, les contenus aussi. Le fichier de prévention des atteintes à la sécurité publique (PASP) et la base de données de sécurité publique (BDSP) ont remplacé EDVIRSP [(1)], le fichier des renseignements généraux (FRG) comme le fichier alphabétique de renseignement (FAR) ont disparu, tandis qu'un fichier distinct dédié aux enquêtes administratives (EASP) a vu le jour. Si certaines des recommandations du précédent rapport sont à l'origine de ces changements, la refonte des fichiers de renseignement a laissé de côté certaines d'entre elles, notamment en matière d'enquêtes administratives.

1. Le remplacement du fichier des renseignements généraux : après EDVIGE et EDVIRSP, le fichier PASP

a) Améliorer les outils de travail des services départementaux d'information générale : de véritables progrès

Vos rapporteurs avaient constaté, lors de leurs précédents travaux, que le gel du fichier des renseignements généraux (FRG), en l'absence d'un fichier nouveau répondant à des finalités proches, du fait de l'abandon d'EDVIGE, soulevait d'importants problèmes pour les services utilisateurs. Notamment, les personnels des services départementaux d'information générale (SDIG) se trouvaient dans l'impossibilité de conserver, sous la forme d'un traitement informatique, les données personnelles recueillies dans l'exercice de leurs fonctions. **C'est pourquoi vos rapporteurs avaient proposé que l'alimentation du FRG soit temporairement admise, en attendant l'adoption d'une loi autorisant la création d'un nouveau fichier (Recommandation n° 53).**

(1) Exploitation documentaire et valorisation de l'information relative à la sécurité publique.

Depuis le 1er juillet 2008, les personnels des SDIG se sont attelés au reclassement des fiches issues du FRG [1]. Le sort de ces fiches varie en fonction de leur contenu : la plupart sont reversées aux archives départementales, notamment lorsqu'elles comportent des données nominatives ; d'autres ont vocation à être conservées par le service et alimentent dès lors un fichier intermédiaire « Archives Information Générale » (AIG) ; certaines sont reversées à d'autres services, comme le service des courses et jeux ; enfin, les fiches restantes sont normalement détruites.

Lors d'un déplacement auprès du SDIG du Val d'Oise, vos rapporteurs ont pu constater l'ampleur de la tâche. Sur environ 16 000 fiches à reclasser, 12 000 ont d'ores et déjà été traitées. Parmi elles, moins de 200 fiches ont été reversées au fichier AIG. L'avancée des travaux de reclassement est très inégale selon les départements, certains ayant des doutes sur les fiches qu'ils peuvent conserver ou non. Tous vivent dans l'attente du fichier de prévention des atteintes à l'ordre public (cf. *infra*), qui doit reprendre les données du fichier AIG.

Malgré l'absence de fichier, l'activité des services ne s'est pas arrêtée depuis 2008, des fiches nominatives, ne pouvant pas faire l'objet d'un traitement informatique, étant toujours envoyées au préfet et au Gouvernement. Les notes produites par les services soient inexploitables du fait des données nominatives qu'elles contiennent, ce qui appauvrit considérablement le fonds documentaire des SDIG. C'est pourquoi, les services utilisent désormais de moteurs de recherche comme Google pour trouver la biographie de certaines personnes, au lieu de rechercher dans les notes déjà rédigées par les services. Face à cette situation et pour exploiter leurs archives, certains services ont préféré expurger leurs fiches de toute donnée nominative. D'autres utilisent en dehors de tout cadre juridique les modules du fichier AIG pour classer des fiches comportant des données nominatives.

Si la recommandation de vos rapporteurs n'a pas été mise en œuvre, la publication des décrets relatifs aux fichiers relatifs à la prévention des atteintes à la sécurité publique (PASP) et aux enquêtes administratives (EASP), aurait permis, d'après la direction générale de la police nationale [2], de donner un cadre juridique au traitement informatique des données nouvelles. Si l'on peut considérer que le fichier temporaire AIG utilisé par les SDIG pour traiter de nouvelles informations dispose peu ou prou d'un vernis de légalité depuis la parution des décrets relatifs aux fichiers PASP et EASP, il ne semble toutefois pas avoir fait l'objet d'une déclaration auprès de la CNIL, ce qui le rend *de facto*

(1) En effet, si aucune donnée ne peut être collectée et enregistrée depuis le 1er juillet 2008, le transfert des données vers d'autres fichiers était possible jusqu'au 31 décembre 2009, en application du décret n° 2008631.

(2) Réponse du 7 mars 2011 des directions générales de la police et de la gendarmerie nationales au questionnaire de suivi des recommandations.

illégal. **Le problème devrait être résolu par le déploiement des fichiers déclarés PASP et EASP, dans le courant de l'année 2012** [(1)]**.**

Vos rapporteurs avaient également souhaité **améliorer les outils de travail des SDIG par l'extension de fichier relatif aux bandes violentes (GEVI) utilisé par la préfecture de police de Paris (Recommandation n° 18)**.

Cette forte préoccupation des services a été entendue, puisque le fichier PASP comportera un module relatif aux bandes violentes calqué sur le fichier GEVI. Vos rapporteurs se félicitent de ce que le service de la préfecture de police de Paris utilisateur de GEVI ait été associé, en tant que direction métier, au développement du fichier PASP. Certaines fonctionnalités du traitement GEVI, comme la réalisation de sociogrammes, ont d'ailleurs été intégrées au fichier PASP [(2)]. Les SDIG seront donc bientôt dotés d'un module de traitement des informations relatives aux bandes violentes.

Vos rapporteurs avaient également souhaité, afin d'améliorer la gestion des bandes violentes et de répondre aux spécificités de cette région en matière de violences urbaines, **étendre l'application GEVI à toute l'Île de France**, en permettant l'alimentation et la consultation du fichier GEVI par les fonctionnaires spécialement habilités des services départementaux d'information générale de la région Île-de-France (**Recommandation n° 19**).

En effet, la mise en place d'un outil commun à la région Île-de-France apparaît tout à fait indispensable. À l'heure actuelle, la gestion des bandes est relativement bien coordonnée entre Paris et la petite couronne, grâce au plan « Bandes » mis en place par le Préfet de police de Paris en 2010.

(1) Le fichier PASP est actuellement en phase de vérification d'aptitude au bon fonctionnement et devrait faire l'objet d'une vérification en service régulier à partir de janvier 2012, pour un déploiement à compter d'avril 2012. Aucune date n'a pour le moment été fixée pour le déploiement du fichier EASP.

(2) Audition de Mmes Claude Jacopin et Sylvia Viteritti de la direction des systèmes d'information et de la communication (DSIC), de MM. Vincent Lafon et Antoine Delouvrier du service des technologies et des systèmes de l'information de la sécurité intérieure (ST(SI)2) et de M. Loïc Alixant, de la sous-direction de l'information générale du 31 mars 2011.

LE PLAN « BANDES » DE LA PRÉFECTURE DE POLICE DE PARIS

M. Michel Gaudin, Préfet de police de Paris, a lancé, en 2010, un plan « Bandes », sur le modèle du plan relatif aux trafics de stupéfiants. Une réunion mensuelle entre la sous-direction chargée de l'information générale de la direction du renseignement de la préfecture de police de Paris (DRPP), la police régionale des transports (PRT) et le service de l'investigation transversale (SIT), qui dépendent de la direction de la sécurité de proximité de l'agglomération parisienne (DSPAP), et les sûretés territoriales des départements de la petite couronne (92, 93 et 94) assure l'échange de données relatives aux bandes.

Une cellule de veille opérationnelle a également été mise en place et présente tous les mois les incidents qui se sont produits à Paris et dans les départements de la petite couronne (entre 30 et 40 incidents par mois). Des objectifs prioritaires, visant certaines bandes déterminées, sont définis collégialement en fonction de la récurrence des incidents et de leur gravité. Une surveillance attentive, doublée de mises sur écoute, peut alors être organisée, le but étant de démanteler le groupe via une procédure judiciaire (pour trafic de stupéfiants, violences ou détention d'armes par exemple).

Source : déplacement du 3 février 2011 à la préfecture de police de Paris.

Si le plan « Bandes » pallie l'absence d'outil informatique commun pour Paris et la petite couronne, la coordination de l'action publique avec la grande couronne demeure problématique. La faible organisation de l'échange d'information avec la grande couronne a même pu retarder l'élucidation de certaines affaires [(1)]. Toutefois, **la coopération devrait être facilitée, dès les prochains mois, par le déploiement du fichier PASP, qui comporte un module proche de GEVI**. En effet, si les SDIG des départements de la grande couronne ont naturellement vocation à en être dotés, il est également prévu d'habiliter des fonctionnaires de la DRPP et de la DSPAP de la préfecture de police à la consultation de PASP [(2)].

b) Encadrer le fichier de prévention des atteintes à la sécurité publique : des recommandations écartées

En ce qui concerne le fichier relatif aux atteintes à la sécurité publique devant remplacer le traitement EDVIGE, vos rapporteurs avaient recommandé que **sa création soit assurée par un texte de valeur législative** (**Recommandation n° 11**). En effet, il était apparu nécessaire qu'un débat public ait lieu autour du fichier EDVIRSP, qui devait succéder à EDVIGE. Sur ce fichier particulièrement, un décret pris en Conseil d'État après avis de la CNIL semblait insuffisant au regard des enjeux.

(1) Déplacement du 3 février 2011 à la Préfecture de police de Paris.

(2) Article 6 du décret n° 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.

Cette proposition n'a pas été mise en œuvre, puisque le fichier EDVIRSP a été remplacé par les traitements « Prévention des atteintes à la sécurité publique » (PASP) et « Enquêtes administratives liées à la sécurité publique » (EASP) autorisés par les décrets n^{os} 2009-1249 et 2009-1250 du 16 octobre 2009.

Vos rapporteurs avaient également souhaité que **ce fichier EDVIRSP ne porte que sur un nombre restreint d'individus.** En effet, la rédaction du décret relatif au fichier EDVIGE avait paru trop large à vos rapporteurs, par rapport à la rédaction issue du décret du 14 octobre 1991 portant création du fichier des renseignements généraux (1). À l'inverse, vos rapporteurs souhaitaient que ce fichier ne concerne que « *les personnes, groupes, organisations et personnes morales qui, en raison de leur activité individuelle ou collective, peuvent porter atteinte à la sécurité des personnes et des biens, par le recours ou le soutien actif apporté à la violence, ainsi que les personnes entretenant ou ayant entretenu un lien direct et non fortuit avec celles-ci* » (**Recommandation n° 12, alinéa 1**).

L'article 17 de leur proposition de loi relative aux fichiers de police est l'exacte transposition de la recommandation n° 12. Si cette proposition n'a pu déboucher, **force est de constater que les termes du décret relatif au fichier PASP ne répondent pas aux souhaits de vos rapporteurs**.

En effet, l'article 1er du décret n° 2009-1249 du 16 octobre 2009 porte sur « *des personnes* », sans que l'on puisse en déduire que les personnes morales ou organisations en fassent nécessairement partie. Au terme de la présentation de PASP qui a été faite à vos rapporteurs (2), il semble que seuls des individus, personnes physiques, puissent être fichés. Les organisations ou personnes morales pourront en revanche apparaître dans la note liée à la fiche individuelle.

Par ailleurs, vos rapporteurs avaient retenu **deux critères cumulatifs permettant l'inscription d'une personne à ce fichier** : la possible atteinte à la sécurité des biens ou des personnes *et* le recours ou le soutien actif apporté à la violence. Cette rédaction limitait grandement le champ de ce fichier. Or, l'article 1er du décret précité fait de la condition de violence un simple exemple ou une simple catégorie de l'atteinte à la sécurité publique. Son second alinéa dispose ainsi que « *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* ».

Enfin, là où vos rapporteurs visaient très précisément une atteinte à la **sécurité des biens ou des personnes**, le décret se contente de la notion d'atteinte

---

(1) Décret n° 91-1051 du 14 octobre 1991 portant création du fichier des renseignements généraux.

(2) Audition de Mme Claude Jacopin et Mme Sylvia Viteritti de la direction des systèmes d'information et de la communication (DSIC), de MM. Vincent Lafon et Antoine Delouvrier du service des technologies et des systèmes de l'information de la sécurité intérieure (ST(SI)2) et de M. Loïc Alixant, de la sous-direction de l'information générale du 31 mars 2011.

à la « *sécurité publique* », nettement moins précise. Cependant, la CNIL, dans sa délibération n° 2009-355 du 11 juin 2009 relative au fichier de prévention des atteintes à la sécurité publique juge cette notion, qu'elle définit comme « *l'absence de périls pour la vie, la liberté ou le droit de propriété des personnes* », « ***plus restrictive que celle qui avait été retenue s'agissant du fichier EDVIGE*** ».

De façon générale, la CNIL estime que le décret n° 2009-1249 du 16 octobre 2009 portant création du fichier PASP permet un usage plus encadré des données personnelles que les précédents projets de décrets qui lui avaient été soumis, concernant EDVIGE puis EDVIRSP. Si vos rapporteurs sont conscients des progrès accomplis par ce nouveau décret, ils déplorent que leurs recommandations n'aient pas été suivies.

2. Les enquêtes administratives réalisées par les services de police et de gendarmerie : de faibles avancées

Les enquêtes administratives qui permettent l'accès à la nationalité ou à un emploi peuvent avoir des conséquences extrêmement lourdes pour les personnes qui en font l'objet. Aussi vos rapporteurs avaient-ils préconisé que les enquêtes administratives, lorsqu'elles sont confiées par le Préfet à un service de police, soient menées par les services départementaux d'information générale (SDIG), qui dépendent de la sous-direction de l'information générale de la direction centrale de la sécurité publique (**Recommandation n° 47**). En effet, il était apparu qu'**un service spécialisé devait être en charge de ces enquêtes qui exigent un degré élevé d'analyse de l'information**.

Cette proposition n'a pas été mise en œuvre. En effet, aux termes du décret n° 2009-1250 du 16 octobre 2009 relatif à la création d'un fichier des enquêtes administratives, les enquêtes administratives qui peuvent être confiées aux SDIG sont uniquement celles relevant du premier alinéa de l'article 17-1 de la loi du 21 janvier 1995 d'orientation et de programmation relative à la sécurité, à savoir celles effectuées en vue de « *décisions administratives de recrutement, d'affectation, d'autorisation, d'agrément ou d'habilitation, prévues par des dispositions législatives ou réglementaires, concernant soit les emplois publics participant à l'exercice des missions de souveraineté de l'État, soit les emplois publics ou privés relevant du domaine de la sécurité ou de la défense, soit les emplois privés ou activités privées réglementées relevant des domaines des jeux, paris et courses, soit l'accès à des zones protégées en raison de l'activité qui s'y exerce, soit l'utilisation de matériels ou produits présentant un caractère dangereux* ».

Or**, il existe d'autres types d'enquêtes administratives, comme les enquêtes en vue d'une naturalisation, qui, bien que confiées à des services de police, ne sont pas nécessairement confiées à des SDIG**. Par exemple, en ce qui concerne en particulier les enquêtes de naturalisation, et comme l'indique une

circulaire du ministre de l'intérieur du 21 juillet 2008 [1], elles sont confiées aux directions départementales de sécurité publique ou à la gendarmerie nationale, en fonction du domicile de l'intéressé ou, dans certains cas, aux services départementaux du renseignement intérieur. Par ailleurs, **lors d'un déplacement dans le Val d'Oise [2], vos rapporteurs ont pu constater que certaines enquêtes de police étaient réalisées par la sûreté urbaine et non par le SDIG.**

Vos rapporteurs avaient également souhaité qu'un **fichier distinct du fichier relatif aux atteintes à la sécurité publique soit créé** pour permettre la conservation des données relatives à des enquêtes administratives défavorables (**Recommandation n° 12, alinéa 2**).

Cette recommandation a fait l'objet d'une mise en œuvre partielle. En effet, si un fichier distinct a bien été créé pour la police nationale par le décret précité, toutes les enquêtes administratives, quel que soit le caractère favorable ou défavorable de l'avis auquel elles conduisent, y sont conservées. Par ailleurs, **en ce qui concerne les enquêtes administratives confiées à la gendarmerie nationale, aucune d'entre elles ne sera conservée**, comme l'a indiqué le Général Jacques Mignaux [3], directeur général de la gendarmerie nationale. Pour chaque enquête administrative, les enquêteurs pourront recourir aux fichiers d'antécédents judiciaires et de sécurité publique, mais « *devront repartir de zéro* ».

Vos rapporteurs avaient également souhaité que les personnes faisant l'objet d'une enquête administrative et figurant dans des fichiers d'antécédents judiciaires en tant que mis en cause soient informées de la **possibilité d'être entendues par le service responsable de l'enquête administrative** pour exposer leur cas et, éventuellement, l'urgence de leur situation en matière d'accès à l'emploi (**Recommandation n° 48**). Il s'agissait de rendre obligatoire une bonne pratique issue de certains services.

Cette recommandation n'a pas été suivie. Toutefois, comme l'ont indiqué les directions générales de la police et de la gendarmerie nationales, les décisions de l'autorité administrative ne sont jamais prises sur le seul fondement de la consultation des fichiers d'antécédents judiciaires ou de l'enquête administrative diligentée. Ces considérations, bien que consacrées par le Conseil constitutionnel [4], semblent être un faible remède aux problèmes de délais et d'interprétation soulevés par le premier rapport de vos rapporteurs.

---

(1) Circulaire NOR INT/K/08/00139/C du 21 juillet 2008 portant sur la réorganisation des services de renseignement du ministère de l'intérieur et la mise en place de l'organisation territoriale.

(2) Déplacement du 21 mars 2011 à l'hôtel de police de Cergy.

(3) Audition du 23 mars 2011 du Général Jacques Mignaux, directeur général de la gendarmerie nationale.

(4) Décision n° 2003-467 DC du 13 mars 2003, considérant n° 34 : « Considérant, en outre, qu'en vertu de l'article 2 de la loi du 6 janvier 1978 susvisée, que ne remettent pas en cause les dispositions contestées : " Aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé " ; que les données recueillies dans les fichiers ne constitueront donc, dans chaque cas, qu'un élément de la décision prise, sous le contrôle du juge, par l'autorité administrative ».

La CNIL s'est également émue des conséquences que peut avoir l'inexactitude des données contenues dans le fichier EASP sur la situation de la personne. Elle a ainsi demandé, dans sa délibération n° 2006-356 relative au fichier EASP, qu'aucune décision défavorable ne soit prise avant vérification des données tirées de fichiers d'antécédents judiciaires. Elle a également souligné, dans sa délibération n° 2010-427 du 25 novembre 2010 relative à la modification des décrets portant création des fichiers PASP et EASP, **l'inexistence de procédures de contrôle de l'exactitude des données**, en relevant que « *les procédures garantissant que les données enregistrées dans ces traitements sont en permanence exactes, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées n'ont pas été portées à la connaissance de la commission* ». Force est de constater que ces deux recommandations, qui rejoignent les préoccupations de vos rapporteurs, n'ont pas été mises en œuvre.

3. La destruction effective du fichier alphabétique de renseignement et ses conséquences

Le fichier alphabétique de renseignement (FAR), devenu parfaitement obsolète, devait être entièrement détruit au 24 octobre 2010 (1). En mars 2009, vos rapporteurs s'étaient inquiétés de l'absence de directives envoyées aux brigades territoriales gestionnaires dans la perspective de la destruction du fichier. Aussi vos rapporteurs avaient-ils recommandé que soient données, dans les meilleurs délais, des instructions précisant les critères ainsi que les modalités de transfert, de destruction et d'archivage des données contenues dans le FAR (**Recommandation n° 56**).

Le général Jacques Mignaux, directeur général de la gendarmerie nationale, a indiqué, lors de son audition par la commission des Lois le 13 octobre 2010 que « *la gendarmerie [...] a supprimé ses fichiers mécanographiques [...] Sont concernés le fichier de la batellerie, le fichier des personnes nées à l'étranger FPNE et surtout le fichier alphabétique de renseignements FAR [...] Les fichiers FAR et le FPNE sont totalement neutralisés : ils ont été retirés de toutes les brigades territoriales et de toutes les unités. Toutes les fiches ont été rassemblées dans des armoires fortes, cadenassées, et le moment venu, elles seront détruites* ».

Force est de constater que des résultats positifs ont été obtenus, avec toutefois un certain retard : **le 3 mars 2011, le FAR était entièrement détruit**. Certes, les directives (2) ont été envoyées à une date tardive au regard de l'objectif initial du 24 octobre 2010, ce qui a retardé la destruction du FAR. Néanmoins, cette entreprise a pu être réalisée de façon satisfaisante. Si la CNIL n'a pas encore eu l'opportunité de constater la disparition effective des fiches papier composant

(1) Article 21 de la loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(2) Cf. Annexe n° 4.

le FAR, vos rapporteurs ont trouvé, à la brigade territoriale d'Auvers-sur-Oise [(1)], des armoires vides, là où se trouvaient auparavant les fiches du FAR. Les procès-verbaux de destruction [(2)], dont certains sont reproduits en annexe, attestent de la bonne conduite de la destruction de ce fichier devenu obsolète.

Vos rapporteurs s'étaient également interrogés sur les **conséquences de la destruction de ce fichier pour les forces de gendarmerie** et avaient ainsi souhaité que soit définie au plus vite la nature exacte du fichier ayant vocation à remplacer le FAR, en déterminant avec précision la finalité assignée à ce nouveau traitement ainsi que la description générale de ses fonctions, les catégories de données à caractère personnel enregistrées, leur origine et les catégories de personnes concernées (**Recommandation n° 55**).

La destruction du FAR faisait craindre aux gendarmes une prise de risque plus importante lors des interventions de terrain. Ce fichier permettait en effet aux gendarmes, avant toute intervention, de vérifier si la personne était connue pour des faits de violence ou pour tout autre fait susceptible de rendre l'intervention plus complexe (détention d'arme, personne suicidaire, chien dangereux…). Comme l'a indiqué le général Jacques Mignaux à la commission des Lois le 13 octobre 2010, « *il est demandé aux gendarmes de connaître les populations, qu'elles soient installées depuis longtemps, de passage ou présentes épisodiquement ; or ils en arrivent à ne plus savoir qui vit dans leur circonscription, ce qui pose des problèmes pour des affaires ayant du reste plus souvent trait à l'intérêt des familles qu'à des enquêtes judiciaires* ». Les gendarmes de la brigade d'Auvers-sur-Oise ont également fait part à vos rapporteurs de la prudence dont ils devaient redoubler, lors de leurs interventions sur le terrain, en l'absence du FAR [(3)].

La recommandation n° 55 a été suivie, puisqu'un nouveau fichier, la base de données de sécurité publique (BDSP), va bientôt voir le jour. Un des modules de ce nouveau fichier aura ainsi pour objet de sécuriser les interventions des gendarmes par la conservation de données relatives à la dangerosité des personnes (cf. *infra*).

(1) Déplacement du 21 mars 2011 auprès de la brigade de gendarmerie d'Auvers-sur-Oise.
(2) Cf. Annexe n° 4.
(3) Déplacement du 21 mars 2011 auprès de la brigade de gendarmerie d'Auvers-sur-Oise.

LA BASE DE DONNÉES DE SÉCURITÉ PUBLIQUE DE LA GENDARMERIE NATIONALE

En matière de sécurité publique, le fichier BDSP de la gendarmerie nationale fait actuellement l'objet de trois décrets en Conseil d'État (n^{os} 2011-340, 2011-341 et 2011-342 du 29 mars 2011) et comporte **quatre modules distincts** :

Le premier porte sur la **gestion des événements d'ampleur** (GEA) et vise à fournir aux autorités les informations nécessaires à la prise de décision lors d'un événement d'ordre public. Celui-ci ne comporte aucune donnée nominative et ne fait donc pas l'objet d'une déclaration.

Le second module, intitulé « **Gestion des sollicitations et interventions** » (GSI) doit permettre d'apporter une réponse adaptée aux sollicitations des usagers (appels 17) et assurer l'engagement des moyens humains et matériels de la gendarmerie de la façon la plus efficace possible. En effet, alors que la gendarmerie reçoit environ 10 millions d'appels par an, seuls 13 % d'entre eux donnent lieu à une intervention. Ce module doit permettre d'améliorer le service rendu à l'usager.

Le module de **gestion de l'information et de prévention des atteintes à la sécurité publique** (GIPASP) permet de recueillir, de conserver et d'analyser les informations concernant des personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique. Ce logiciel permettra également de faciliter le partage d'information avec les services départementaux de l'information générale (SDIG) de la police nationale. Seul ce module pourra être utilisé dans le cadre des enquêtes administratives. Il dispose d'une **capacité maximum de 999 999 fiches**, stockables pendant 40 ans, soit soixante fois moins que le fichier alphabétique de renseignements qu'il a pour vocation de remplacer.

Enfin, un quatrième module porte sur la **sécurisation des interventions et sur les demandes particulières de protection** (SIDPP). Ainsi, en cas d'intervention au domicile d'une personne, les gendarmes pourront savoir si celle-ci est connue de leurs services pour des faits de violence ou autres (arme, chien dangereux, tentatives de suicide, violences conjugales, agressivité constatée lors d'une précédente intervention…). En effet, les interventions étaient responsables, en 2010, de près de 2 200 blessés parmi les gendarmes.

Certains des modules de BDSP sont d'ores et déjà en cours de déploiement, après une **expérimentation dans le Nord-Pas-de-Calais**. Le logiciel a été réalisé par la société Thalès, sur la base du logiciel utilisé par les pompiers, ce qui a permis son développement rapide. La direction générale de la gendarmerie nationale a souhaité que tous les gendarmes reçoivent une **certification spécifique, relative aux libertés publiques**, et signent un document avant le déploiement du logiciel. Par rapport à l'équivalent PASP de la police nationale, la **traçabilité de GIPASP** est renforcée, puisque toutes les opérations, et non pas uniquement les consultations, seront tracées par le logiciel.

C. DES PROGRÈS ACCOMPLIS CONCERNANT L'INSCRIPTION DES MINEURS

Le cadre juridique entourant l'inscription de personnes mineures au sein de fichiers de police a connu, depuis la publication du précédent rapport, des évolutions favorables et conformes, pour la plupart, à l'esprit des recommandations formulées par vos rapporteurs. Notamment, un équilibre a su être trouvé entre la prise en compte, par les outils informatiques utilisés par les forces de l'ordre, d'une réalité criminologique nouvelle et la nécessité d'octroyer aux mineurs un droit à l'oubli en matière de fichiers.

1. L'inscription des mineurs au sein des fichiers de renseignement désormais possible et encadrée

Le fichier d'exploitation documentaire et de valorisation de l'information relative à la sécurité publique (EDVIRSP), qui était en projet lors de la rédaction du précédent rapport de la mission d'information, répond aujourd'hui au nom de PASP pour « **Prévention des atteintes à la sécurité publique** », et a également vocation à remplacer le fichier de gestion des violences urbaines (GEVI) utilisé par la préfecture de police de Paris. Accessible aux fonctionnaires dûment habilités de la direction centrale de la sécurité publique de la police nationale et aux agents des services départementaux d'information générale et de la préfecture de police, **les termes du décret portant création du fichier PASP répondent en partie aux recommandations émises par vos rapporteurs en 2009 en ce qui concerne les mineurs.**

Vos rapporteurs avaient souhaité que les mineurs de plus de treize ans puissent être inscrits dans les fichiers de renseignement relatifs aux bandes. En effet, eu égard au développement de phénomènes de bandes violentes et à la place occupée par les personnes mineures dans leurs activités criminelles [(1)], **l'inscription des mineurs répondait à une préoccupation forte des services.** C'est notamment ce qu'ont souligné les fonctionnaires de la direction du renseignement de la préfecture de police de Paris (DRPP) [(2)] à vos rapporteurs.

L'opinion de vos rapporteurs avait cependant divergé sur les critères permettant l'inscription des mineurs dans ce fichier. Si votre rapporteur était favorable à ce que tout mineur soit inscrit dans GEVI, dès lors qu'il est susceptible de porter atteinte à la sécurité des personnes et des biens en raison de son activité individuelle ou collective (**Recommandation n° 17**), votre rapporteure avait préféré limiter la possibilité d'inscription au fichier GEVI aux mineurs de plus de treize ans qui, d'une part, étaient référencés dans un fichier d'antécédents judiciaires (STIC ou JUDEX) et qui, d'autre part, pouvaient, « *en raison de leur*

(1) Si les chefs de bande sont généralement majeurs, leurs « petites mains » qui font office de dealers ou de guetteurs, sont eux mineurs. Au total, les fonctionnaires de la direction du renseignement intérieur de la préfecture de police de Paris, rencontrés le 3 février 2011, évaluent à 60 % la part des mineurs dans les bandes responsables de violences urbaines.

(2) Déplacement du 3 février 2011 à la Préfecture de police de Paris.

activité individuelle et collective, porter atteinte à la sécurité des personnes et des biens, par le recours ou le soutien actif apporté à la violence, ainsi que les personnes entretenant ou ayant entretenu un lien direct et non fortuit avec ceux-ci » (**Recommandation n° 17 bis**).

La recommandation de vos rapporteurs a été partiellement mise en œuvre. En effet, le décret n°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, qui a vocation à remplacer l'application GEVI utilisée par les fonctionnaires de la préfecture de police (cf. *infra*), rend possible l'inscription au fichier des mineurs de plus de treize ans. Toutefois, le critère tenant à l'inscription des mineurs dans des fichiers d'antécédents judiciaires n'a pas été retenu.

Vos rapporteurs avaient également émis le souhait, en mars 2009, que l'inscription de mineurs au sein des fichiers de renseignement soit soumise à des critères plus stricts que ceux qui prévalaient alors dans le projet de décret relatif au fichier EDVIRSP. Notamment, il semblait primordial que soit substituée à la notion de risque d'« *atteinte à la sécurité publique* » une notion moins subjective. Cette proposition avait fait l'objet de deux recommandations distinctes. Votre rapporteur souhaitait limiter l'inscription au fichier EDVIRSP aux mineurs de plus de treize ans (**Recommandation n° 16**), tandis que votre rapporteure y ajoutait un critère tenant aux antécédents judiciaires et au recours ou au soutien actif à la violence (**Recommandation n° 16 *bis***).

Ces recommandations ont été partiellement suivies. En effet, seuls les mineurs de plus de treize ans « *dont l'activité individuelle ou collective indique qu'[ils] peuvent porter atteinte à la sécurité publique* », notamment lorsqu'ils sont « *susceptibles d'être [impliqués] dans des actions de violence collectives, en particulier en milieu urbain* » peuvent aujourd'hui être inscrits dans PASP. Contrairement aux souhaits de votre rapporteure, ce dernier élément ne constitue pas un critère d'inscription au fichier. En outre, l'exigence formulée par votre rapporteure de n'inscrire que les mineurs figurant aux fichiers des antécédents judiciaires, et contre laquelle s'inscrivait votre rapporteur, n'a pas été satisfaite. Enfin, la notion de « *sécurité des personnes et des biens* », défendue par vos rapporteurs du fait de sa plus grande précision, n'a pas été retenue. En revanche, **l'inscription des personnes entretenant ou ayant entretenu un lien direct et non fortuit avec ces mineurs**, voulue par votre rapporteure tant pour EDVIRSP que GEVI, figure bien à l'article 2 du décret du 16 octobre 2009 précité.

Des dispositions identiques ont été retenues pour le module GIPASP de la base de données de sécurité publique (BDSP) de la gendarmerie nationale, créé par le décret n° 2011-340 du 29 mars 2011 portant création d'un traitement de données à caractère personnel relatif à la gestion de l'information et la prévention des atteintes à la sécurité publique.

2. La mise en place d'un véritable droit à l'oubli pour les mineurs

Conformément aux **recommandations n° 20 et 21** de vos rapporteurs et à l'article 17 de leur proposition de loi relative aux fichiers de police, les fichiers PASP et GIPASP créent un **droit à l'oubli pour les mineurs**. En effet, chacun des décrets précités dispose que les données relatives à des mineurs « *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* ». Ainsi, les éléments enregistrés seront effacés le jour du troisième anniversaire de l'enregistrement, à défaut de nouvel événement.

Par ailleurs, **le souhait de vos rapporteurs de voir un magistrat référent veiller sur la bonne application de ce droit à l'oubli s'est concrétisé (Recommandation n° 21)**. En effet, le décret n° 2010-1540 du 13 décembre 2010 (1) prévoit la nomination d'un référent national, membre du Conseil d'État, dont la tâche principale est de s'assurer de l'effacement des données concernant les mineurs. Toutefois, il semble que ce magistrat n'ait pas encore été désigné.

Vos rapporteurs avaient également souhaité **permettre au magistrat référent d'autoriser le maintien, dans le fichier, des informations relatives au mineur**. Dès lors que ce maintien est autorisé par le magistrat, une réunion annuelle avec les services gestionnaires était prévue, à l'issue de laquelle le magistrat pouvait requérir l'effacement des données (**Recommandation n° 21**). Mais, contrairement à cette recommandation et à l'article 17 de leur proposition de loi relative aux fichiers de police, **les décrets précités ne permettent pas aux services de demander au magistrat le maintien des informations au-delà du délai prévu**.

Cependant, **afin de limiter les possibilités d'inscription au fichier après la majorité de l'individu**, et conformément à l'esprit des recommandations de vos rapporteurs, le magistrat référent évalue tous les ans, à compter de la majorité de la personne, l'opportunité de la conservation des données relatives à un fait commis étant mineur. **Un véritable droit à l'oubli est donc organisé par ces décrets.**

En outre, la direction générale de la gendarmerie nationale a mis en œuvre de façon plus poussée le droit à l'oubli. Concernant la base de données de sécurité publique, **une purge automatique des données interviendra aux 18 ans de la personne inscrite au fichier alors qu'elle était mineure**, tandis que les gendarmes du système des opérations et du renseignement en charge de l'administration de BDSP purgeront manuellement le fichier trois ans après l'enregistrement d'un fait, lorsqu'aucun nouvel événement n'est intervenu (2).

---

(1) Décret n° 2010-1540 du 13 décembre 2010 modifiant le décret n° 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.

(2) Déplacement du 25 mai 2011 auprès du centre de renseignement opérationnel de la gendarmerie nationale (CROGEND).

D. LES DONNÉES SENSIBLES TOUJOURS AU CŒUR DU DÉBAT

Vos rapporteurs avaient souhaité, en 2009, que la collecte des données sensibles soit autorisée, non par un simple décret, mais par le législateur lui-même, afin de mieux encadrer les fichiers traitant ces informations. Même si la réforme législative espérée n'est pas intervenue, la collecte des données sensibles s'est quelque peu améliorée, notamment au sein des fichiers de renseignements.

1. La collecte des données sensibles semble aujourd'hui plus encadrée

Que ce soit dans le cadre des fichiers relatifs aux atteintes à la sécurité publique, ou bien dans celui des enquêtes administratives, la collecte des données sensibles est aujourd'hui plus encadrée que par le passé. Toutefois, les recommandations de la CNIL n'ont été qu'imparfaitement suivies pour certains fichiers.

a) La collecte des données sensibles dans le cadre des atteintes à la sécurité publique et des enquêtes administratives

Alors que le fichier EDVIGE autorisait largement la collecte et la conservation des données sensibles que sont l'origine raciale ou ethnique, la santé, la vie sexuelle, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, **le nouveau fichier de prévention des atteintes à la sécurité publique vise des données de nature plus restreinte**. Ainsi, l'article 3 du décret n° 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 ne vise que les données relatives au signalement, à l'origine géographique et aux activités politiques, philosophiques, religieuses ou syndicales.

Si l'on omet l'origine géographique, qui avait fait l'objet de divergences entre vos rapporteurs (cf. *infra*), **les termes du décret sont proches de ceux de l'article 17 de la proposition de loi cosignée par vos rapporteurs**, qui permettait la collecte, à titre dérogatoire, des signes particuliers et objectifs comme éléments de signalement, mais aussi des activités – non des opinions – politiques, philosophiques, religieuses et syndicales, dès lors que celles-ci avaient un lien avec la finalité du fichier.

En outre, **un garde-fou important a été posé par le décret : ces éléments ne peuvent en aucun cas faire l'objet d'une recherche aveugle** visant à sélectionner toutes les personnes répondant à un critère particulier, comme l'ont indiqué à la mission d'information MM. Vincent Lafon et Antoine Delouvrier du service des technologies et des systèmes de l'information de la sécurité intérieure [(1)]. L'article 3 du décret précité dispose d'ailleurs qu'« *il est interdit de*

(1) Audition du 31 mars 2011 de Mmes Claude Jacopin et Sylvia Viteritti de la direction des systèmes d'information et de la communication (DSIC), de MM. Vincent Lafon et Antoine Delouvrier du service des

sélectionner dans le traitement une catégorie particulière de personnes à partir de ces seules données », comme le précisait déjà le décret de 1991 relatif au FRG. Le fichier GIPASP [(1)] de la gendarmerie nationale reprend ces dispositions protectrices.

En matière d'enquêtes administratives, vos rapporteurs avaient souhaité qu'aucune donnée sensible, y compris celles enregistrées dans la catégorie « signalement », ne puisse être enregistrée dans le fichier relatif aux enquêtes administratives, afin de différencier clairement les finalités du fichier PASP de celles du fichier relatif aux enquêtes administratives (**Recommandation n° 13**).

L'article 18 de la proposition de loi cosignée par vos rapporteurs devait transcrire cette recommandation dans le droit positif. Par dérogation à l'interdiction de collecter des données sensibles prévue par l'article 8 de la loi du 6 janvier 1978 précitée, il était toutefois possible de conserver des données relatives aux activités des individus en rapport avec des **groupes de combats ou des milices armées**. Cette proposition de loi n'a cependant pas abouti.

Par ailleurs, **il semble que cette recommandation ait été partiellement mise en œuvre par le décret du 16 octobre 2009 précité.** En effet, le fichier des enquêtes administratives liées à la sécurité publique, créé par le décret n° 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, permet la conservation des seules données portant sur l'état civil, la profession et les coordonnées des personnes inscrites au fichier, mais aussi de photographies.

Le premier alinéa de l'article 3 du décret dispose que « *l'interdiction prévue au I de l'article 8 de la loi du 6 janvier 1978 susvisée s'applique au présent traitement* », ce qui interdit normalement la collecte et la conservation des données sensibles. Toutefois, **le décret autorise à titre dérogatoire la collecte des données relatives aux activités religieuses, politiques, syndicales ou philosophiques lorsqu'elles révèlent un comportement incompatible avec l'exercice des fonctions ou des missions envisagées**. Cependant, ces données ne pourront apparaître que dans le rapport d'enquête administrative joint à la fiche individuelle et ne pourront faire l'objet d'aucune recherche automatisée.

b) Le fichage des « personnalités » aujourd'hui limité

Plus largement, vos rapporteurs avaient souhaité abandonner définitivement l'inscription dans tout fichier, quelles que soient sa nature et sa portée, des personnes physiques ayant sollicité, exercé ou exerçant un mandat

---

technologies et des systèmes de l'information de la sécurité intérieure (ST(SI)2) et de M. Loïc Alixant, de la sous-direction de l'information générale.

(1) Décret n° 2011-340 du 29 mars 2011 portant création d'un traitement de données à caractère personnel relatif à la gestion de l'information et la prévention des atteintes à la sécurité publique.

politique, syndical ou économique ou qui jouent un rôle institutionnel, économique, social ou religieux significatif (**Recommandation n°15**), couramment appelées « personnalités ».

LE FICHAGE DES « PERSONNALITÉS », DU FRG AUX NOUVEAUX FICHIERS DE POLICE

Le décret du 14 octobre 1991 [(1)] relatif au fichier des renseignements généraux (FRG) permettait de ficher les « *personnes physiques ou morales qui ont sollicité, exercé ou exercent un mandat politique, syndical ou économique ou qui jouent un rôle politique, économique, social ou religieux significatif, sous condition que ces informations soient nécessaires pour donner au Gouvernement ou à ses représentants les moyens d'apprécier la situation politique, économique ou sociale et de prévoir son évolution* ». Par ailleurs, par dérogation à l'interdiction de collecter des données qui font « *apparaître, directement ou indirectement, les origines raciales ou les opinions politiques, philosophiques ou religieuses ainsi que les appartenances syndicales des personnes* » posée par la loi du 6 janvier 1978, il était possible de ficher les activités politiques, philosophiques, religieuses ou syndicales de toutes les personnes inscrites au FRG. Les missions assignées au service des renseignements généraux étant le suivi de l'opinion publique, des conflits sociaux et la surveillance des groupes à risque, il apparaissait alors utile au travail de renseignement de pouvoir enregistrer des données relatives aux personnalités.

La réforme des renseignements généraux, en 2008, devait indirectement changer la donne. En effet, en recentrant l'action de renseignement sur les intérêts fondamentaux de la nation, l'enregistrement de données relatives aux personnalités ne semblait plus nécessaire. Toutefois, il a fallu attendre le déclenchement de la polémique entourant le décret relatif au fichier EDVIGE [(2)], qui devait remplacer pour partie le FRG, pour que cette évolution ait lieu. Le décret relatif au fichier EDVIGE organisait ainsi une collecte beaucoup plus large des données sensibles. Si l'inscription des personnes « *ayant sollicité, exercé ou exerçant un mandat politique, syndical ou économique* » ou qui jouent un rôle significatif était encore possible, leurs « *opinions* » politiques, philosophiques, religieuses ou syndicales pouvaient également être collectées à titre exceptionnel. Le passage de l'« *activité* », donnée objective, à l'« *opinion* », subjective, entrait en contradiction avec l'esprit de la loi du 6 janvier 1978. Face à la vive émotion suscitée par ce décret, le choix a été fait de l'abandonner. Il a été remplacé, en 2009, par deux fichiers distincts, PASP et EASP, conformément aux recommandations de vos rapporteurs (cf. *infra*).

De fait, la recommandation n° 15 de vos rapporteurs n'est qu'imparfaitement mise en œuvre. Même si les responsables politiques, syndicaux et religieux ne sont plus fichés du seul fait de ces activités, ces données

(1) Décret n° 91-1051 du 14 octobre 1991 portant application aux fichiers informatisés, manuels ou mécanographiques gérés par les services des renseignements généraux des dispositions de l'article 31, alinéa 3, de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

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

peuvent encore figurer dans plusieurs fichiers, dès lors qu'elles sont en lien direct avec la finalité du fichier.

Ainsi, le décret relatif au **fichier PASP** [(1)], s'il restreint les personnes susceptibles d'y être inscrites à celles qui menacent la sécurité publique, son article 3 permet la collecte, à titre dérogatoire, de données relatives « *à des activités politiques, philosophiques, religieuses ou syndicales* ». Deux garde-fous ont néanmoins été prévus (cf. *supra*) : d'une part, la finalité du fichier doit être respectée ; d'autre part, ces données ne peuvent faire l'objet d'une recherche automatisée.

De la même façon, dans le décret portant création du **fichier EASP** [(2)], si l'interdiction posée par l'article 8 de la loi du 6 janvier 1978 s'applique, il n'est pas question de priver les services d'une information sur le comportement de la personne dans les cas où celui-ci a une motivation politique, religieuse, philosophique ou syndicale. Des données relatives aux activités politiques, religieuses ou syndicales peuvent donc figurer dans les notes jointes à la fiche proprement dite. Il convient toutefois de noter que celle-ci ne peut pas faire l'objet d'une recherche informatique. Votre rapporteure regrette pour sa part que de telles données puissent être enregistrées dans le fichier EASP.

L'évolution est donc largement positive, par rapport au fichage des personnalités anciennement organisé par le FRG (cf. encadré ci-dessus). Cependant, vos rapporteurs ont pu constater lors d'un déplacement que l'ancien **fichier des renseignements généraux**, s'il devait être **expurgé des fiches des « personnalités »**, reversées aux archives départementales ou détruites par les services eux-mêmes, continuait d'être **utilisé de façon inappropriée** par certains services qui, au lieu de reverser ces fiches aux archives, les conservent par devers eux, sans les détruire.

Par ailleurs, **certains fichiers permettent encore l'enregistrement de données relatives aux mandats politiques**. C'est notamment le cas du fichier des courses et jeux, qui est d'ailleurs destinataire d'une partie des fiches du FRG. Ce fichier [(3)], qui a pour objet la conservation de données relatives aux personnes physiques ou morales ayant fait l'objet d'un agrément, ainsi que des personnes physiques interdites de jeux, permet l'enregistrement d'informations relatives aux mandats électifs des personnes. La CNIL, dans sa délibération [(4)] sur le projet d'arrêté, a interrogé le ministère de l'Intérieur sur la nécessité de collecter ces données. Il semble qu'elles soient nécessaires à la vérification d'une incompatibilité posée par l'arrêté du 14 mai 2007 relatif à la réglementation des

(1) Décret n° 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.

(2) Décret n° 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.

(3) Arrêté du 8 novembre 2010 portant création au profit de la direction centrale de la police judiciaire d'un fichier des courses et jeux.

(4) Délibération n°2010-068 du 11 mars 2010 portant avis sur un projet d'arrêté portant création au profit de la direction centrale de la police judiciaire d'un fichier des courses et jeux.

jeux dans les casinos, dont l'article 12 dispose que « *le directeur responsable et les membres du comité de direction sont agréés par le ministre de l'Intérieur sous réserve de ne point remplir des fonctions électives dans la commune siège de l'établissement* ».

Si la CNIL s'est satisfaite de la précision apportée par le ministère, concernant l'absence d'informations relatives aux opinions politiques (1), votre rapporteure estime qu'un **risque de dérive** existe. Si cette donnée est effectivement nécessaire, il aurait fallu qu'elle soit, d'une part, **considérée comme une donnée sensible** et que, d'autre part, elle ne puisse être collectée que pour les personnes occupant les fonctions de directeur ou de membres du comité de direction, si son objet est bien de vérifier la compatibilité des fonctions.

c) L'état de santé et le handicap : des données dont le caractère sensible a été oublié

Transposant la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, la loi du 6 août 2004 a modifié de manière significative la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Notamment, elle a renforcé le traitement applicable aux données dites « sensibles », en y incluant expressément les données « *relatives à la santé ou à la vie sexuelle* » des personnes.

Or, le décret du 13 avril 2011 (2) relatif au fichier d'exécution des services commandés pour la réalisation des transfèrements et extractions (ESCORTE), qui permet la gestion des opérations de transfèrements et d'extractions des détenus, permet la collecte de données relatives à la santé de la personne détenue : « *maladies, mesures médicales ou prophylactiques préconisées, handicap…* ». Si une telle collecte n'est pas contraire à la loi du 6 janvier 1978, la CNIL a souligné, dans sa délibération (3), que « *le projet de décret ne précise pas que le traitement contient des données sensibles qui relèvent de l'article 8 de la loi du 6 janvier 1978 modifiée en août 2004. Elle estime que ce point devrait être précisé aux termes du projet de décret quand bien même seules les données relatives à la santé du détenu sont susceptibles d'être enregistrées* ». Par ailleurs, « *elle prend acte que le ministère s'engage à compléter le projet de décret afin de préciser à l'article 2 : " les données relatives à l'état de santé du détenu peuvent, en application du IV de l'article 8 de la loi du 6 janvier 1978, être enregistrées dans le présent traitement, dans la limite des finalités définies à l'article 1er "* ».

---

(1) Peuvent ainsi être collectées les données relatives « mandats électifs exercés dans la commune siège de l'établissement (à l'exclusion de toute mention relative aux opinions politiques) ».

(2) Décret n° 2011-397 du 13 avril 2011 autorisant la création d'un traitement de données à caractère personnel dénommé « Exécution des services commandés pour la réalisation des transfèrements et extractions » (ESCORTE).

(3) Délibération n° 2010-426 du 25 novembre 2010 portant avis sur un projet de décret en Conseil d'État autorisant la création d'un traitement de données à caractère personnel, dénommé « exécution des services commandés pour la réalisation des transfèrements et extractions » (demande d'avis n° 10013480).

Vos rapporteurs constatent toutefois que cette recommandation de la CNIL n'a pas été suivie, puisque cette précision ne figure pas dans le texte du décret précité. Si vos rapporteurs sont conscients de la nécessité, pour les gendarmes effectuant ces escortes, de disposer de telles informations, une mise en conformité avec la loi du 6 janvier 1978 modifiée par la loi du 6 août 2004 demeure souhaitable.

2. Origine géographique et origine raciale : la confusion des genres

Parmi les données sensibles, la mention de l'origine ethnique ou raciale est probablement celle qui suscite les controverses les plus vives. La polémique qui a émergé à l'automne dernier, relative à la classification hypothétique des populations roms, en témoigne.

a) L'origine géographique : une notion à manipuler avec précaution

La notion d'origine géographique est, aujourd'hui comme hier, sujette à caution. Si certains, comme l'association SOS Racisme [(1)], y voient un **moyen détourné d'identifier l'origine ethnique ou raciale des personnes**, l'origine géographique est, pour d'autres, un **élément contextuel de signalement des personnes**. C'est pourquoi l'association avait demandé que le décret PASP soumis au groupe de contrôle des fichiers de police, dont elle fait partie, ne fasse plus mention de l'origine géographique comme donnée susceptible d'être enregistrée. Cette demande a été réitérée dans un communiqué du groupe du 18 octobre 2010. Il convient de noter que l'origine géographique ne figure pas, en tant que telle, parmi les données sensibles dont la collecte est en principe interdite, sauf à considérer qu'elle soit, indirectement, un indicateur de l'origine ethnique ou raciale des personnes.

Force est de constater que les décrets [(2)] relatifs à la prévention des atteintes à la sécurité publique semblent valider cette seconde hypothèse, en inscrivant l'origine géographique parmi les données sensibles collectées à titre dérogatoire. C'est donc qu'**il s'agit bien, derrière ce vocable, d'identifier l'origine ethnique ou raciale des personnes.**

Cependant, dans une note du 18 octobre 2009 adressée aux préfets [(3)], **il est fait référence aux « quartiers » de certaines villes pour éclairer la notion d'origine géographique** : « *Les données relatives à l'origine géographiques des personnes se limitent à l'indication de leur provenance ; en effet, dans les phénomènes de bandes, l'appartenance à un même quartier ou le partage d'un même lieu de naissance peuvent, par exemple, jouer un rôle déterminant* ».

---

(1) Audition du 13 mai 2011 de Mme Émilie Perrier, responsable du pôle anti-discriminations et de M. Guillaume Ayne, directeur général de l'association SOS Racisme.

(2) Décret n° 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 et décret n° 2011-340 du 29 mars 2011 portant création d'un traitement de données à caractère personnel relatif à la gestion de l'information et la prévention des atteintes à la sécurité publique.

(3) Cf. Annexe n° 8.

D'ailleurs, le fichier PASP limite les indications d'origine géographique au lieu de naissance des personnes, par un thésaurus fermé. Aux dires mêmes de ses concepteurs, cette précaution permet d'éviter les formulations malencontreuses ou la création de codes internes visant à suivre telle ou telle catégorie de la population inscrite au fichier en fonction de leur origine ethnique ou raciale.

Vos rapporteurs s'étaient d'ailleurs divisés, en mars 2009, sur la question de **la collecte des données relatives à l'origine géographique des personnes, entendue comme simple élément de signalement**. Votre rapporteur souhaitait que puissent être conservées, au titre des données sensibles susceptibles d'être collectées et conservées dans EDVIRSP, la notion d'« *origine géographique* » comme élément de signalement des personnes (**Recommandation n° 14**). À l'inverse, votre rapporteure entendait limiter les données sensibles collectées et conservées dans EDVIRSP au titre du signalement aux seuls « *signes physiques particuliers, objectifs et inaltérables* » (**Recommandation n° 14 bis**).

La recommandation de votre rapporteur a été formellement mise en œuvre. Les données sensibles susceptibles d'être collectées portent sur l'origine géographique, tant pour le fichier PASP que pour le fichier GIPASP. Toutefois, ces données se distinguent, dans l'esprit des rédacteurs de ces décrets, des données relatives au signalement des personnes, qui font l'objet d'un alinéa différent. Votre rapporteur se félicite que la notion d' « *origine géographique* » ait été retenue, tant elle semble indispensable à l'élucidation de nombreuses affaires. Pour votre rapporteure, le risque est élevé de voir cette notion utilisée de façon détournée pour évoquer l'origine raciale ou ethnique des personnes.

b) Le maintien d'une typologie ethno-raciale pour les fichiers d'antécédents judiciaires et de signalement

Vos rapporteurs avaient sollicité **la suppression de la typologie ethno-raciale** qui existait en 2009 pour le STIC-Canonge [(1)], très subjective et susceptible d'induire des comportements racistes. Il était alors possible de remplacer cette typologie par des éléments objectifs de portrait-robot, comme la couleur des yeux, des cheveux, de la peau (**Recommandation n° 22**).

Toutefois, c'est la typologie établie par le groupe de contrôle sur les fichiers de police présidé par M. Alain Bauer qui a été retenue pour le STIC-Canonge puis pour le nouveau traitement des antécédents judiciaires (TAJ), qui assure la fusion des fichiers d'antécédents judiciaires de la police et de la gendarmerie. Or, par rapport à la typologie utilisée auparavant, seule la mention de « *gitan* » est supprimée, ce qui constitue un bien faible changement au regard des enjeux. **La recommandation n° 22 n'a donc pas été mise en œuvre.**

(1) Ce fichier a vocation à permettre l'identification de l'auteur d'une infraction à partir de son signalement.

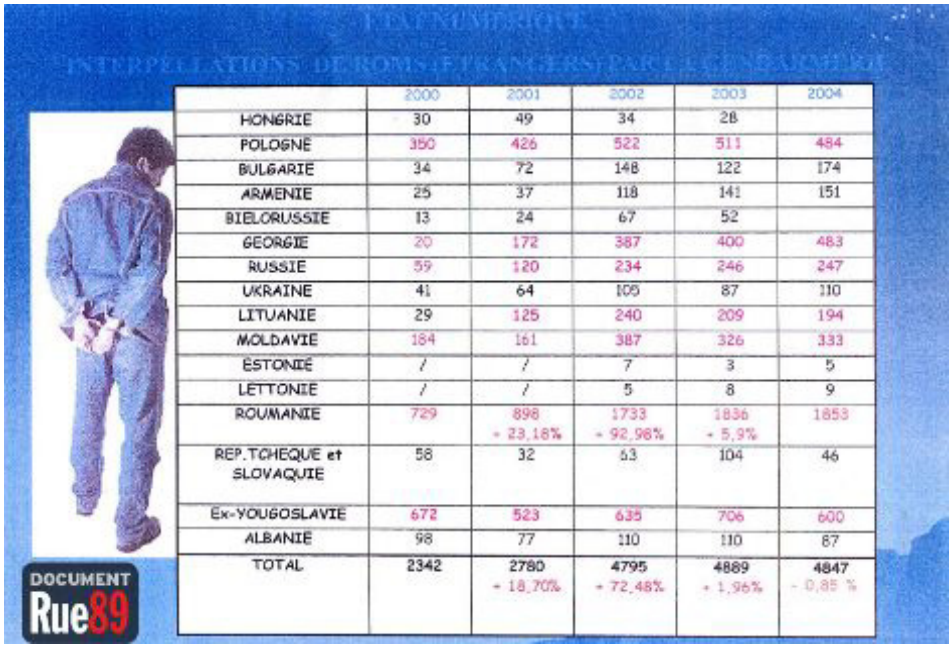
c) Le respect de la loi du 6 janvier 1978 au cœur des préoccupations de vos rapporteurs

La question de la collecte et de la conservation des données sensibles est une préoccupation constante de vos rapporteurs. Il importe en effet que le cadre défini par l'article 8 de la loi du 6 janvier 1978 soit parfaitement respecté, afin d'assurer le plein respect des droits et libertés des individus. C'est tout particulièrement le cas des données relatives aux origines raciales ou ethniques qui ont, à l'occasion de la polémique déclenchée par le fichage supposé des populations roms par la gendarmerie nationale, de nouveau attiré l'attention de vos rapporteurs.

En octobre 2010, **une vive polémique relative au fichage des populations roms sur des bases ethno-raciales** a en effet éclaté, à la suite de la publication par un blog dépendant du journal Le Monde [(1)] et par Rue89 [(2)] de documents internes à un office de la gendarmerie, l'Office central de lutte contre la délinquance itinérante (OCLDI). Plusieurs documents, dont un tableau reproduit ci-après, laissaient à penser qu'un fichier dédié aux « minorités ethniques non sédentarisées » ou MENS était alimenté par la gendarmerie nationale. Une note adressée au parquet faisait état de la consultation du « *fichier MENS (OCLDI) sur les liens de famille (généalogie)* ». Au-delà de la possible utilisation de données sensibles en dehors du cadre légal défini par la loi « Informatique et Libertés », c'est le fichage de certaines populations sur des bases raciales qui a alors suscité une vive inquiétude.

(1) http://libertes.blog.lemonde.fr/2010/10/07/le-fichier-des-roms-du-ministere-de-linterieur/.
(2) http://www.rue89.com/2010/10/07/les-preuves-de-lexistence-dun-fichier-ethnique-sur-les-roms-170000.

« ÉTAT NUMÉRIQUE DES INTERPELLATIONS DE ROMS (ÉTRANGERS) PAR LA GENDARMERIE » : EXTRAIT D'UNE PRÉSENTATION DE L'OCLDI PUBLIE PAR RUE89



	2000	2001	2002	2003	2004
HONGRIE	30	49	34	28	
POLOGNE	350	426	522	511	484
BULGARIE	34	72	148	122	174
ARMENIE	25	37	118	141	151
BIELORUSSIE	13	24	67	52	
GEORGIE	20	172	387	400	483
RUSSIE	59	120	234	246	247
UKRAINE	41	64	105	87	110
LITUANIE	29	125	240	209	194
MOLDAVIE	184	161	387	326	333
ESTONIE	/	/	7	3	5
LETTONIE	/	/	5	8	9
ROUMANIE	729	898 + 23,18%	1733 + 92,98%	1836 + 5,9%	1853
REP.TCHEQUE et SLOVAQUIE	58	32	63	104	46
Ex-YOUGOSLAVIE	672	523	635	706	600
ALBANIE	98	77	110	110	87
TOTAL	2342	2780 + 18,70%	4795 + 72,48%	4889 + 1,96%	4847 - 0,85 %

Source : article du 7 octobre 2010 publié sur le site Rue89.com.

TABLEAU FOURNI PAR LA GENDARMERIE À LA MISSION D'INFORMATION

ETAT NUMERIQUE

DES INTERPELLATIONS D'ETRANGERS PAR LA GENDARMERIE

	2000	2001	2002	2003	2004
HONGRIE	30	49	34	28	44
POLOGNE	350	426	522	511	484
BULGARIE	34	72	148	122	174
ARMENIE	25	37	118	141	151
BIELORUSSIE	13	24	67	52	27
GEORGIE	20	172	387	400	483
RUSSIE	59	120	234	246	247
UKRAINE	41	64	105	87	110
LITUANIE	29	125	240	209	194
MOLDAVIE	184	161	387	326	333
ESTONIE	/	/	7	3	5
LETTONIE	/	/	5	8	9
ROUMANIE	729	898 + 23,18%	1733 + 92,98%	1836 + 5,9%	1853
REP.TCHEQUE et SLOVAQUIE	58	32	63	104	46
Ex-YOUGOSLAVIE	672	523	635	706	600
ALBANIE	98	77	110	110	87
TOTAL	2342	2780 + 18,70%	4795 + 72,48%	4889 + 1,96%	4847 - 0,85 %

Afin de vérifier la véracité de ces informations, la CNIL, saisie d'une plainte émanant de plusieurs associations, a effectué **plusieurs contrôles à l'office central de lutte contre la délinquance itinérante (OCLDI) et au service technique de recherches judiciaires et de documentation (STRJD)** de la gendarmerie nationale. Ces contrôles ont donné lieu à un premier rapport préliminaire, rendu public le 14 octobre 2010, puis à un rapport définitif le 25 novembre 2010.

Les conclusions de la CNIL indiquent qu'**aucun fichier pérenne et structuré relatif aux gens du voyage ou aux populations roms** n'a été trouvé. Cette affirmation a d'ailleurs été réitérée au cours d'une audition organisée par vos rapporteurs le 2 février 2011. De même, **aucune base relative à la généalogie** de certaines catégories de la population n'est utilisée aujourd'hui par l'OCLDI, d'après les conclusions de la CNIL. Le groupe de contrôle des fichiers de police, présidé par M. Alain Bauer, dans son communiqué du 18 octobre 2010, tire les mêmes conclusions.

Cependant, la CNIL a relevé de **nombreuses irrégularités** au cours de ses contrôles. Notamment, l'OCLDI utilise une base de données, alimentée par des données issues des fichiers d'antécédents judiciaires STIC et JUDEX, de messages de service opérationnels émanant des deux forces et des procédures traitées par l'office. Cette base de données n'a fait l'objet d'aucune déclaration auprès de la CNIL. Toutefois, la CNIL indique que ladite base de données, qui contient 52 769 fiches de personnes, ne comporte aucune donnée relative à l'origine ethnique ou raciale des personnes. Par ailleurs, un projet de texte réglementaire est en cours d'élaboration par le ministère de l'Intérieur [(1)].

Par ailleurs, les contrôles de la CNIL ont révélé l'existence d'un **fichier, non appréhendé comme tel par les services de gendarmerie, constitué par les messages électroniques envoyés par les brigades territoriales** au STRJD. Ces messages, qui indiquent l'identité, la commune de rattachement, le lieu de contrôle, les dates de séjour et l'immatriculation des véhicules de personnes itinérantes, contiennent ponctuellement les mentions « MENS », « gitan », « roms » ou « tzigane ». Pour la CNIL, « *la centralisation de données doit s'analyser comme un seul et même traitement ayant pour finalité le recueil de renseignements susceptibles de fonder un travail de rapprochement criminel sur les " gens du voyage "* ».

En outre, un **fichier d'analyse criminelle non déclaré à la CNIL, ANACRIM**, est utilisé, dans le cadre d'enquêtes précises, par les forces de gendarmerie de l'OCLDI et du STRJD. Le logiciel *Analyst's NoteBook* ®, couramment appelé ANACRIM, est un outil de travail à vocation temporaire. Il permet, sur une enquête particulière, de faire du rapprochement, par exemple de données téléphoniques, et assure ainsi une représentation graphique des éléments de cette enquête (relations entre les personnes, numéros de téléphone et bornes

(1) Courrier en date du 9 août 2011 du ministre de l'Intérieur (cf. annexe n° 5).

utilisées, véhicules…). Seules les pièces de procédure, sur réquisition d'un magistrat ou d'un officier de police judiciaire en cas de flagrance, alimentent le logiciel. **Le caractère temporaire du fichier utilisé ne saurait faire obstacle à ce qu'il soit considéré comme un traitement de données à caractère personnel par la CNIL**.

Enfin, les personnels de l'OCLDI et du STRJD utilisent le **fichier de suivi des titres de circulation délivrés aux personnes sans domicile ni résidence fixe** (SDRF), alors même que ce fichier est strictement administratif et ne peut en aucun cas être utilisé à des fins judiciaires.

Le général Jacques Mignaux, directeur général de la gendarmerie nationale, entendue par la commission des Lois le 13 octobre 2010, s'est félicité du résultat des contrôles de la CNIL relatif à l'existence d'un fichier MENS. Il a cependant reconnu l'existence d'un **fichier de rapprochement**, appelé **« base OCLDI », qui n'a fait l'objet d'aucune déclaration auprès de la CNIL**. De même, il a admis **l'existence passée d'un fichier généalogique, Généatic**, acquis en 2000 par la cellule interministérielle de lutte contre la délinquance itinérante, qui a précédé l'OCLDI. Ce fichier, tombé en désuétude, a vraisemblablement été **détruit en décembre 2007**. Il n'avait toutefois **pas été porté à la connaissance du groupe de contrôle sur les fichiers de police, ni à celle de vos rapporteurs lors de leur précédente mission**. Enfin, le général Jacques Mignaux a justifié l'absence de déclaration du fichier ANACRIM par le caractère temporaire des données intégrées. Toutefois, d'autres fichiers utilisés illégalement par la gendarmerie nationale intègrent des données sur une échelle de temps longue et ne peuvent dès lors pas être justifiés par le caractère ponctuel de leur exploitation.

Afin de se forger, sur cette affaire, une opinion éclairée, vos rapporteurs se sont déplacés auprès des deux services en cause et ont sollicité le ministère de l'Intérieur et la CNIL à plusieurs reprises, pour obtenir la communication de certains documents et informations.

L'OFFICE CENTRAL DE LUTTE CONTRE LA DÉLINQUANCE ITINÉRANTE

Héritier de la cellule interministérielle de lutte contre la délinquance itinérante (CILDI), l'office central de lutte contre la délinquance itinérante (OCLDI), créé par le décret n° 2004-611 du 24 juin 2004, est rattaché à la sous-direction de la police judiciaire de la direction générale de la gendarmerie nationale. Composé de 47 personnels, parmi lesquels des gendarmes, des policiers, des inspecteurs des impôts et des douanes, l'OCLDI peut être saisi par un magistrat, par les brigades territoriales ou d'office, notamment lorsque plusieurs départements sont impliqués.

L'OCLDI a pour domaine de compétence la lutte « *contre la criminalité et la délinquance commises par des malfaiteurs d'habitude qui agissent en équipes structurées et itinérantes en plusieurs points du territoire* ». La délinquance itinérante se manifeste par des atteintes aux biens à caractère sériel, commises par des délinquants organisés agissant sur plusieurs zones d'action.

L'OCLDI a pour mission de favoriser la circulation des informations entre les différentes administrations, d'analyser les comportements des auteurs d'infractions et leurs modes opératoires, de coordonner les investigations relatives à ces infractions, d'assister les unités de gendarmerie et les services de police, d'intervenir pour effectuer ou poursuivre des recherches à l'étranger si nécessaire et d'être le point de contact des organismes internationaux et services spécialisés des autres États. L'office participe également à des actions de formation, d'information et de prévention.

Pour mener à bien ses missions, l'OCLDI utilise une base de données, intitulée « base OCLDI », qui permet à ses analystes d'opérer des rapprochements entre diverses sources d'information relatives à des faits délictueux : les demandes adressées par les unités, les procédures judiciaires, les fichiers d'antécédents judiciaires, les messages opérationnels transmis par les unités ou les administrations… Cette base de données, qui contient 52 769 fiches de personnes, fournit également des informations statistiques sur la délinquance itinérante. Non déclarée à la CNIL, cette base de données fait l'objet d'un projet de texte réglementaire actuellement en cours d'élaboration.

Lors de leur déplacement auprès de l'OCLDI, vos rapporteurs ont pu constater *de visu* l'existence de la base de données incriminée. Il a également été porté à leur connaissance qu'un logiciel de développement appelé WinDev était utilisé par plusieurs services pour mettre au point leurs propres fichiers. Vos rapporteurs ont également pu comparer le tableau à l'origine de la polémique (1) avec celui fourni par la gendarmerie nationale (2). Ils ont constaté que ces tableaux différaient sur certains points, comme leur titre, certaines de leurs données, et leur

(1) Cf. supra.
(2) Cf. Annexe n° 9.

aspect général. **Vos rapporteurs se sont interrogés sur l'interprétation à donner à ces différences, sur la nature exacte des données présentées dans ces tableaux et sur les conclusions à en tirer s'agissant de l'existence ou non d'un fichier relatif aux populations roms.**

Par ailleurs, concernant une demande d'informations adressée au ministre de l'Intérieur relative à la transmission du nombre de personnes interpellées, depuis 2000, année après année, par la gendarmerie nationale, selon leur nationalité, **vos rapporteurs ne peuvent que déplorer que ces informations ne leur aient pas été communiquées**. De telles informations auraient pu permettre de vérifier que les données présentées dans le tableau incriminé ne portaient effectivement pas sur les seules personnes d'origine rom.

S**'il est certain qu'aucun fichier ethnique n'existe aujourd'hui à l'OCLDI ou au STRJD**, les différents éléments dont il a été fait état plus haut n'ont pas permis à votre rapporteure de confirmer ou d'infirmer l'existence passée d'un tel fichier. Votre rapporteure est persuadée qu'un fichier MENS a existé au travers du fichier généalogique détruit en 2007 et demeure troublée par certains éléments. Elle rappelle qu'une procédure judiciaire est en cours à la suite de la plainte de plusieurs associations. Elle déplore en outre la persistance de mentions ethniques dans certains fichiers de la gendarmerie nationale. Votre rapporteur, quant à lui, a été pleinement convaincu par les explications fournies et les documents présentés.

*

De façon générale, vos rapporteurs ne doutent pas de la volonté des services de police et de gendarmerie de respecter pleinement le droit des fichiers de police. En tout état de cause, cette affaire met en lumière la difficile utilisation de la notion d'origine géographique à des fins statistiques, qui sème toujours le doute sur l'intention de ses utilisateurs.

Vos rapporteurs se félicitent par ailleurs que des projets de textes réglementaires soient en cours de préparation pour quatre bases de données utilisées par la gendarmerie nationale : les bases criminalistiques départementales, la base de donnée relative aux victimes non identifiées, la base de données relatives aux escroqueries et le fichier des objets d'art volés [(1)].

Au total, sur les 31 recommandations formulées par vos rapporteurs, 8 ont fait l'objet d'une mise en œuvre complète et 9 d'une application partielle. 14 recommandations ont été, pour l'instant, laissées de côté.

(1) Courrier en date du 9 août 2011 du ministre de l'Intérieur (cf. annexe n° 5).

TROISIÈME PARTIE : LE DÉVELOPPEMENT D'UNE CULTURE « INFORMATIQUE ET LIBERTÉS » DANS L'UTILISATION DES FICHIERS DE POLICE

Depuis la publication du précédent rapport de la mission d'information, vos rapporteurs ont pu constater l'émergence d'une culture « Informatique et libertés » dans la gestion des fichiers de police. Or, en 2009, un tel changement n'était pas acquis.

L'utilité de ces fichiers repose à titre principal sur la qualité des données intégrées. Aussi est-il fondamental que les informations enregistrées soient tout à la fois exactes, actualisées et pertinentes. De nombreux efforts ont été consentis, ces deux dernières années, en ce sens. L'intégration des données fait aujourd'hui l'objet de contrôles poussés, les délais d'intégration des données ont été réduits, les suites judiciaires sont plus facilement transmises. Dans un avenir proche, le déploiement d'un système intégré entre la police et la justice devrait encore contribuer à l'amélioration de l'exactitude des données.

Par ailleurs, l'utilisation de ces fichiers est de plus en plus encadrée et contrôlée. Des cartes électroniques seront bientôt déployées pour permettre l'accès personnel des policiers et gendarmes aux fichiers de police. Des procédures de contrôle se mettent progressivement en place, pour détecter les comportements abusifs. Enfin, des efforts particuliers de pédagogie et de formation sont déployés pour créer les conditions de l'émergence d'une culture « Informatique et libertés » en France.

A. UNE PLUS GRANDE FIABILITÉ DANS L'ALIMENTATION DES FICHIERS

Dès l'étape de l'enregistrement des données, si les recommandations de vos rapporteurs n'ont pas toutes été suivies d'effet, des progrès sensibles ont été accomplis. Toutefois, vos rapporteurs regrettent qu'aucun effort n'ait été consenti en matière de formation et de valorisation des personnels affectés à l'enregistrement des données.

1. La formation et l'information des utilisateurs améliorées

Les fichiers de police sont aujourd'hui un outil indispensable utilisé quotidiennement par les forces de l'ordre, qu'il s'agisse de fichiers généralistes, comme le fichier d'antécédents judiciaires de la police, le STIC, ou de fichiers spécialisés, comme le fichier SALVAC dédié à la criminalité sérielle (cf. *infra*). Les fichiers font désormais l'objet d'une formation et d'une communication spécifiques, seules à mêmes de faire émerger une véritable « culture Informatique et libertés » en France.

En ce qui concerne la police nationale, **il semble que la formation initiale et continue des policiers ait été renforcée** (1). La CNIL dispense ainsi une brève formation dans le cadre du cursus des futurs commissaires de police. Le pôle juridique du cabinet du directeur général de la police nationale a également rédigé un support de formation approfondi qui a été remis, avec une **mallette pédagogique**, à la sous-direction de la formation de la direction des ressources et des compétences de la police nationale en décembre 2010. Un mémento a par ailleurs été confié aux référents Informatiques et Libertés de la gendarmerie nationale (2).

Toutefois, ces initiatives ne correspondent pas tout à fait à l'esprit de la **recommandation n° 54** de la mission d'information, qui souhaitait qu'un **guide méthodologique plus opérationnel**, détaillant avec précision les critères et les modalités de production, de traitement, de transfert, de destruction et d'archivage des données contenues dans les fichiers de police, soit rédigé à l'attention des services.

La gendarmerie nationale a cependant mis en place un **séminaire d'approfondissement** pour les commandants des groupements de gendarmerie départementale, de sections de recherches et d'offices centraux au début de l'année 2011. Une autre session est prévue courant 2012. **La mise en place de nouveaux fichiers est également l'occasion de mettre en œuvre une politique de formation ambitieuse**. Par exemple, pour le traitement des antécédents judiciaires (TAJ), des **stages d'une durée allant d'un à cinq jours**, selon les unités et le type d'utilisateur, ont été réalisés. Plus largement, la formation initiale des gendarmes-adjoints volontaires, des sous-officiers et des officiers met en œuvre une **triple approche des fichiers de police : juridique, technique et éthique** (3).

Enfin, les deux forces ont **recours à l'intranet pour diffuser les bonnes pratiques en matière de fichiers de police**. Des didacticiels sont disponibles en permanence sur l'intranet de la gendarmerie nationale (4) et ce depuis deux ans. La police nationale a, quant à elle, mis en place en février 2011 un espace consacré aux fichiers de police sur l'intranet de la DGPN, accessible à tous les fonctionnaires (5).

2. Des contrôles qualité entourant l'enregistrement des données

L'intégration des données au sein des fichiers de police, étape essentielle à leur efficacité, fait l'objet d'une attention particulière. Différentes procédures et garde-fous concourent aujourd'hui à assurer la fiabilité des données.

---

(1) Audition de M. Frédéric Péchenard, directeur général de la police nationale, le 16 mars 2011.
(2) Audition du Général Jacques Mignaux, directeur général de la gendarmerie nationale, le 23 mars 2011.
(3) Idem.
(4) Idem.
(5) Audition de M. Frédéric Péchenard, directeur général de la police nationale, le 16 mars 2011.

En ce qui concerne des fichiers déjà existants, comme le fichier des empreintes génétiques (FNAEG) [1], des progrès ont été accomplis. Ainsi, la **transmission électronique des résultats d'analyse génétique par les laboratoires limite considérablement le nombre d'erreurs** que provoqueraient des saisies manuelles successives. Ce fichier, qui comporte aujourd'hui 1,8 million de profils, est devenu un outil de travail indispensable pour les forces de l'ordre. Il est donc particulièrement important que les données enregistrées fassent l'objet de procédures limitant autant que possible les erreurs liées à une saisie manuelle.

Mais le contrôle de la qualité des données est également pris en compte dès le développement de nouveaux logiciels. Ainsi, dans le futur système appelé « NS2I », le logiciel de rédaction des procédures de la police nationale (LRPPN) devrait alimenter directement le logiciel de traitement des antécédents judiciaires TAJ [2], ce qui limitera grandement le risque d'erreurs de saisies. Par ailleurs, la mise en place de **thésaurus fermés**, qui ne permettent pas aux personnels renseignant les fichiers de remplir librement les champs, assure un certain degré d'exactitude des données, en limitant les erreurs liées à une saisie manuelle des informations. C'est notamment le cas du logiciel de rédaction des procédures actuellement développé par la police nationale, dont les thésaurus sont, pour la plupart, normés [3].

Dans le cadre plus particulier du déploiement de TAJ, anciennement dénommé ARIANE, vos rapporteurs avaient souhaité qu'un **processus de contrôle qualité et d'enrichissement des données** soit **défini de façon précise** (**Recommandation n° 30**). Aucun élément d'information allant dans ce sens n'a été transmis à la mission d'information.

Toutefois, plusieurs éléments concourent à assurer l'exactitude des données contenues dans le fichier TAJ. En premier lieu, la gestion administrative du fichier ne dépendra que d'un seul service, si bien que les doublons qui existaient auparavant entre la police et la gendarmerie seront naturellement évités. Ensuite, l'enregistrement des données sera soumis à de nombreux thésaurus fermés, ce qui limitera les erreurs (cf. *supra*), tandis que la transmission des données entre le fichier TAJ, LRPPN et la nouvelle chaîne applicative supportant le système d'information opérationnel pour le pénal et les enfants (CASSIOPEE) sera automatisée. Enfin, un garde-fou important a été institué en ce qui concerne LRPPN : les données nominatives issues des procédures ne seront remontées au fichier TAJ, en ce qui concerne les personnes mises en cause, qu'à la clôture de l'enquête réalisé par l'officier de police

(1) Déplacement du 16 mai 2011 auprès du service central de documentation criminelle de la sous-direction de la police technique et scientifique.

(2) Idem.

(3) Déplacement du 3 mars 2011 à la 3e division de police judiciaire.

judiciaire, et non pas « *au fil de l'eau* », ce qui garantit un niveau d'exactitude des données plus élevé qu'auparavant [(1)].

3. Le statut des agents administratifs affectés à l'alimentation des fichiers : une problématique délaissée

Vos rapporteurs avaient constaté, en 2009, que **le statut des agents administratifs affectés à l'alimentation des fichiers de police** était un **facteur majeur de qualité dans l'intégration des données**. Peu formés, sans connaissances juridiques, ces personnels peu valorisés sont pourtant la clé de voûte du système de fichiers. Si l'intégration des données est sujette à erreur, c'est en effet tout l'édifice qui s'effondre. C'est pourquoi vos rapporteurs avaient proposé que ces personnels bénéficient d'une part, d'une **formation adaptée (Recommandation n° 25)** et, d'autre part, d'une **politique de revalorisation, d'intéressement et de validation des acquis de l'expérience (Recommandation n° 29)** assurant leur stabilité dans les fonctions qu'ils occupent.

Aucune de ces deux recommandations n'a été intégralement mise en œuvre. Si les policiers et gendarmes qui consultent les fichiers bénéficient aujourd'hui de formations minimales en matière de fichiers de police, ce n'est pas le cas des agents administratifs, qui continuent à se former, pour la plupart, par eux-mêmes. Seul leur professionnalisme les pousse à acquérir des connaissances pointues en matière de procédure pénale. Toutefois, **à l'occasion de la modernisation de nombreux fichiers de police, il est possible que la direction générale de la police nationale mette en œuvre des formations spécifiques à destination de ces personnels.**

Par ailleurs, il convient de noter que **le problème ne se pose pas avec la même acuité au sein de la gendarmerie nationale, où ce sont principalement des gendarmes qui sont chargés de l'alimentation des fichiers**. Certains militaires bénéficient même d'une formation très pointue, que ce soit les analystes criminels, titulaires d'un master, ou les gendarmes affectés au sein de brigades départementales de renseignements et d'investigations judiciaires (BDRIJ), qui passent cinq semaines au centre national de formation à la police judiciaire de Fontainebleau [(2)].

B. UNE MEILLEURE TENUE ET MISE À JOUR DES FICHIERS DE POLICE

L'exactitude des informations contenues dans les fichiers de police est l'un des piliers de leur efficacité. Plusieurs conditions sont requises afin que ces fichiers comportent des données utiles : la rapidité de l'enregistrement des informations, le traitement en temps réel des modifications et l'existence d'un

(1) Déplacement du 16 mai 2011 auprès du service central de documentation criminelle de la sous-direction de la police technique et scientifique.

(2) Audition du Général Jacques Mignaux, directeur général de la gendarmerie nationale, le 23 mars 2011.

contrôle qualité poussé. Dans ces domaines, des progrès inégaux ont été accomplis depuis mars 2009.

1. Une réduction du stock de données en souffrance

L'insuffisance patente des effectifs, au sein des services gestionnaires, était responsable, en 2009, d'un retard non négligeable dans l'intégration des données, particulièrement dommageable en matière de fichiers de police. Aussi vos rapporteurs avaient-ils recommandé le recrutement de contractuels en nombre suffisant pour permettre aux services régionaux de documentation criminelle de résorber le stock de procédures en attente de traitement s'agissant du STIC (**Recommandation n° 28**).

Cette recommandation a été mise en œuvre, ce qui a contribué à la réduction des stocks pour certains fichiers. Cette démarche a été notamment engagée par le service gestionnaire du fichier des personnes recherchées, à Écully, qui a eu recours à l'embauche d'une dizaine de vacataires pour réduire le stock de près de 4500 fiches en souffrance [(1)]. Par ailleurs, le service régional de documentation criminelle (SRDC) de Versailles, a embauché des vacataires afin de résorber le stock de procédures en attente de traitement dans le STIC [(2)].

De la même façon, la division de la statistique et de la documentation criminelle de la préfecture de police a pu réduire le retard accumulé par l'augmentation permanente des effectifs et l'emploi de travailleurs handicapés [(3)]. Alors qu'auparavant, le délai d'intégration était de 4 mois à Paris et de 9 mois dans les départements de la petite couronne, il a été respectivement réduit à 2 mois et 4 mois. **En moyenne, il faut donc attendre 3 mois pour que les fiches papier soient intégrées au STIC, ce qui correspond au standard établi par l'inspection générale de la police nationale**. Enfin, les difficultés de numérisation constatées en 2009 ont été en partie résolues par l'**acquisition de nouveaux scanners.** Ce sont ainsi près de 8 millions de feuillets qui ont été numérisés en 2010.

Des solutions techniques ont également permis d'accélérer le processus d'intégration des données en ce qui concerne le fichier des empreintes génétiques (FNAEG). Concernant les empreintes génétiques des personnes mises en cause, le retard constaté par la mission d'information semble aujourd'hui résorbé. **Depuis le début de l'année 2009, l'équipe d'Écully travaille presque à flux tendus**, l'intégration de données étant lissée sur une à deux semaines. Ce progrès a pu être accompli grâce à la **transmission électronique des résultats d'analyses génétiques par les laboratoires**. En outre,

---

(1) Déplacement auprès du service central de documentation criminelle de la sous-direction de la police technique et scientifique le 16 mai 2011.

(2) Réponse de la direction générale de la police nationale et de la gendarmerie nationale aux recommandations de la mission, 7 mars 2011.

(3) Déplacement à la préfecture de police de Paris du 3 février 2011.

les urgences sont traitées dans la journée, y compris la nuit, depuis la mise en place, il y a un an, d'un service d'**astreinte**.

La modernisation des équipements et l'automatisation des processus ont induit d'importants changements en matière de gestion des ressources humaines. Le SCDC n'a aujourd'hui plus besoin de vacataires. Les agents administratifs autrefois dédiés à la saisie des résultats des laboratoires sont aujourd'hui préférentiellement remplacés par des analystes, l'activité étant plus tournée vers la validation des résultats que vers la saisie des données. **L'effectif total est ainsi passé, grâce à l'automatisation, de 90 à 40 personnes** environ, pour **20 000 profils individus intégrés par mois**, soit deux fois plus qu'en 2008.

2. Une mise à jour plus rapide des données par une coopération accrue entre les parquets et les gestionnaires de fichiers

La rectification comme l'effacement des données, dont la rapide exécution assure l'exactitude des données contenues dans les fichiers de police, sont en passe d'être améliorés, grâce au déploiement d'un nouvel environnement informatisé.

a) La transmission bientôt automatisée des suites judiciaires

Vos rapporteurs avaient constaté, dans leur précédent rapport, qu'un certain nombre de personnes demeuraient fichées au fichier d'antécédents judiciaires de la police nationale, le STIC, alors même qu'elles avaient bénéficié d'un classement sans suite. Deux causes étaient à l'origine de cette **imperfection du STIC** : d'une part, l'**absence de transmission des suites judiciaires** par les parquets et, d'autre part, la **réticence des services de police à intégrer les suites judiciaires données par voie téléphonique**, en temps réel, par les parquets.

Aussi vos rapporteurs avaient-ils préconisé **que les services de police se voient contraints, par le biais d'une circulaire** rappelant les conditions d'inscription d'une personne mise en cause dans les fichiers d'antécédents, **de prendre en compte les suites judiciaires données en temps réel par les parquets (Recommandation n° 26)**. Il avait également été recommandé que l'échange de données entre la chaîne applicative supportant le système d'information opérationnel pour le pénal et les enfants (CASSIOPEE) et le nouveau fichier commun des antécédents judiciaires, TAJ, ex-ARIANE, soit réalisé au plus vite (**Recommandation n° 34**).

Pour ce qui est du traitement en temps réel des suites judiciaires, si **aucune consigne n'a été donnée en ce sens aux forces de police par le ministère de l'Intérieur** (1), **des progrès sensibles ont été accomplis** dans la mise à jour du STIC. Notamment, la division de la statistique et de la

(1) « Eléments de réponse au questionnaire adressé à M. Alex Türk, Président de la CNIL », 1er décembre 2010.

documentation criminelle de la préfecture de police de Paris [1] a indiqué à vos rapporteurs que **les délais d'obtention des suites judiciaires auprès des parquets de Paris et de la petite couronne étaient passés de 6 mois en 2009 à 2 mois** seulement aujourd'hui. La réactivité des parquets est donc largement accrue dans ce domaine. C'est notamment vrai pour le parquet de Créteil [2], très prompt à transmettre les suites judiciaires. Ainsi, depuis la parution du rapport de la CNIL sur la gestion du STIC [3] en 2009, de nombreux efforts ont été faits par les parquets.

Le déploiement de l'application CASSIOPÉE [4] devrait en outre résoudre le problème de la transmission des suites judiciaires par les tribunaux et, donc, les problèmes afférents d'effacement et de rectification. Cependant, cette application ne sera mise en application à Paris qu'en 2012. Le tribunal de grande instance de Paris sera ainsi le dernier à être raccordé, au grand regret des services rencontrés par vos rapporteurs : « *à chaque fois que l'on s'approche de l'horizon, CASSIOPÉE recule* ». Pour le reste de la France, la transmission des données entre CASSIOPÉE et le fichier TAJ devrait être opérationnelle à la fin de l'année 2011. Si les recommandations de vos rapporteurs n'ont pas été suivies, des résultats équivalents à ceux visés par la mission devraient donc être atteints à terme.

b) L'effacement des données facilité

Afin de tirer toutes les conséquences d'une décision d'effacement prise par le procureur, vos rapporteurs avaient recommandé que ces décisions fassent l'objet d'une **transmission immédiate aux services gestionnaires des fichiers STIC-Canonge et FNAEG (Recommandation n° 35)**. Cette proposition avait vocation à remédier à l'absence d'interconnexion entre ces fichiers et les fichiers d'antécédents judiciaires.

Vos rapporteurs entendaient traduire cette recommandation en des termes juridiques, par l'article 15 de leur proposition de loi n° 1659 relative aux fichiers de police. En effet, cet article visait à introduire un nouvel alinéa à l'article 21 de la loi n° 2003-239 pour la sécurité intérieure : « *Les décisions d'effacement ou de rectification des informations nominatives prises par le procureur de la République sont transmises aux responsables de tous les traitements automatisés pour lesquels ces décisions ont des conséquences sur la durée de conservation des données personnelles* ».

Si cette proposition n'a pas abouti, une disposition proche a été introduite par la loi du 14 mars 2011 précitée. Le **nouvel article 230-8 du code de procédure pénale** dispose ainsi que *« les décisions d'effacement ou de*

(1) Déplacement du 3 février 2011 à la Préfecture de police de Paris.
(2) Idem.
(3) « Conclusions du contrôle du système de traitement des infractions constatées », Rapport remis au premier ministre, *20 janvier 2009.*
(4) Cf. Rapport d'information de M. Etienne Blanc sur les carences de l'exécution des peines et l'évaluation de l'application Cassiopée (n° 3177, session 2010-2011).

rectification des informations nominatives prises par le procureur de la République sont portées à la connaissance des responsables de tous les traitements automatisés pour lesquels, sous réserve des règles d'effacement ou de rectification qui leur sont propres, ces mesures ont des conséquences sur la durée de conservation des données personnelles ».

De plus, le caractère immédiat de la transmission pourrait être assuré, dans un avenir proche, par la modernisation des fichiers d'antécédents judiciaires. En particulier, **le STIC-Canonge, bientôt intégré au nouveau fichier d'antécédents judiciaires TAJ, sera continuellement mis à jour, grâce à l'automatisation de la transmission des suites judiciaires**. Pour le reste, une interconnexion ou un rapprochement entre le FNAEG et le fichier TAJ serait peut-être nécessaire. Certains services sont d'ailleurs convaincus de la nécessité d'une telle évolution (1). Au-delà du fait qu'elle garantirait la mise à jour des données contenues au FNAEG, elle présenterait l'avantage de fiabiliser les données nominatives du fichier d'antécédents judiciaires, en évitant, par exemple, les homonymies et les doublons, qui sont aujourd'hui fréquents.

Enfin, la modernisation des fichiers de police permet de créer des garde-fous informatiques susceptibles de remédier aux failles d'une organisation humaine. Ainsi, en ce qui concerne le fichier commun d'antécédents judiciaires TAJ, **les données nominatives seront automatiquement effacées à l'issue de la durée de conservation, qui varie suivant la gravité des faits** (2). Il en va de même pour la base de données de sécurité publique créée par la gendarmerie nationale, notamment ce qui concerne les mineurs susceptibles d'être inscrits à ce fichier (3).

3. Le stock de données erronées demeure une préoccupation majeure

Vos rapporteurs s'étaient inquiétés, en 2009, de ce que **le nouveau traitement ARIANE, aujourd'hui renommé TAJ, hérite des erreurs contenues dans le fichier d'antécédents judiciaires de la police nationale**. En effet, le STIC contenait un certain nombre d'inexactitudes, aussi bien en matière de qualification des faits que d'actualisation des données. Le 20 janvier 2009, la CNIL a remis un rapport (4) faisant suite au contrôle du fichier d'antécédents judiciaires de la police nationale, le STIC. Parmi les investigations que la CNIL a menées dans le cadre du droit d'accès indirect, il s'est avéré qu'en 2008 **seules 17 % des fiches de personnes comportaient des informations tout à fait exactes**. Ce taux d'erreur pose problème aux fonctionnaires de police, dont l'un

(1) Déplacement auprès du service central de documentation criminelle de la sous-direction de la police technique et scientifique le 16 mai 2011.

(2) Déplacement de la mission d'information au service technique de recherches judiciaires et de documentation (STRJD) le 17 janvier 2011.

(3) Déplacement au centre de renseignement opérationnel de la gendarmerie nationale (CROGEND) du 25 mai 2011.

(4) « Conclusions du contrôle du système de traitement des infractions constatées (STIC) *», Rapport remis au Premier ministre le 20 janvier 2009.*

d'entre eux a indiqué à vos rapporteurs que « *le STIC est tellement peu fiable qu'on ne peut rien en faire* ».

Face à cet important taux d'erreur, vos rapporteurs avaient souhaité **que la reprise des données du STIC et de JUDEX vers le fichier TAJ fasse l'objet d'une procédure de contrôle spécifique**, tendant à garantir l'exactitude initiale des données. À cet effet, une commission, présidée par un procureur général et associant l'IGPN, l'IGGN et la CNIL devait être chargée de définir les modalités de reprise de l'ensemble des données figurant dans le STIC et dans JUDEX. De façon générale, vos rapporteurs souhaitaient que soient consacrés à ce chantier considérable le temps et les moyens nécessaires (**Recommandation n° 32**).

Si aucune commission n'a vu le jour, **certaines procédures ont été mises en place par les deux forces dans la perspective de la reprise de données par TAJ. Toutefois, ces initiatives ne sont pas tout à fait satisfaisantes.**

En effet, si quelques **contrôles qualité ponctuels** ont été menés par la police nationale, **aucun nettoyage complet de la base de données du STIC**, pourtant sujette à erreurs, n'a été entrepris. Certes, un effort particulier a été fait en matière d'enregistrement des suites judiciaires, de vérification des personnes mises en cause mineures de moins de 10 ans et de saisies d'objets. Si le nettoyage complet de cette base particulièrement volumineuse était en effet une opération complexe, il eût été bon d'aller plus avant dans le processus de rectification des données. L'argument selon lequel le STIC, plus « normé » que JUDEX, n'aurait dès lors pas besoin d'un contrôle poussé, ne tient pas face aux nombreuses inexactitudes que ce fichier comportait en 2009.

La gendarmerie nationale a entrepris un processus de correction de la base de données JUDEX. En effet, la gendarmerie nationale avait constaté que l'existence de champs libres avait pu conduire, dans de nombreux cas, à la présence d'informations non pertinentes relatives aux auteurs et victimes. Si vos rapporteurs sont tout à fait persuadés que la gendarmerie n'avait aucunement l'intention de ficher certaines catégories de la population, il est clair que les informations relatives à l'orientation sexuelle, aux origines ethniques ou à l'état de santé des personnes inscrites dans ces fichiers y figuraient illégalement. La gendarmerie nationale a donc remplacé la typologie Canonge et son équivalent JUDEX par un référentiel limitant les mentions possibles à une typologie ethno-raciale déterminée et réalisée suivant les recommandations du groupe Bauer. Elle a également procédé à l'effacement de données relatives aux origines ethniques et raciales, à l'orientation sexuelle, aux opinions politiques, philosophiques, aux pratiques religieuses, aux appartenances syndicales, aux modes de vie et états de santé, lorsqu'elles ne sont pas des éléments constitutifs de l'infraction. Enfin, elle a supprimé les données nominatives contenues dans les

fiches dites de procédure [(1)]. Au total, 120 000 fiches ont été corrigées ou supprimées.

Ce nettoyage de la base de données a permis de mettre JUDEX en conformité avec la loi. Ce travail a mobilisé près de **dix équivalents temps plein pendant douze mois environ.** Il convient toutefois de noter que le travail effectué par la gendarmerie, si important soit-il, ne concerne qu'une faible part des données reprises par TAJ. Aussi, de façon générale, **il est fort probable que les critiques adressées au STIC soient valables pour TAJ.** Il appartiendra au service gestionnaire de ce fichier de procéder à l'élimination des potentielles erreurs.

C. LE CONTRÔLE INTERNE DE L'UTILISATION DES FICHIERS DE POLICE RENFORCÉ

Une fois le fichier de police créé, le principal enjeu consiste à assurer la sécurisation de l'accès aux données et de leur utilisation. De nombreux progrès ont été accomplis dans ce domaine, au gré des avancées technologiques et de la modernisation de nombreux traitements de données à caractère personnel. Toutefois, certains services exercent encore un contrôle inadéquat de la bonne utilisation des fichiers de police.

1. Le contrôle renforcé de l'accès aux fichiers

La mission d'information avait pu constater, en 2009, que **si les consultations abusives de fichiers de police étaient rares, la sécurisation des postes de travail par de simples mots de passe, parfois prêtés à d'autres collègues ou négligemment affichés à proximité de l'ordinateur, n'était pas satisfaisante**. À l'époque, la gendarmerie envisageait de déployer des cartes à puce électroniques permettant l'identification personnelle de chaque fonctionnaire consultant un fichier de police. Vos rapporteurs avaient recommandé que ce procédé soit étendu à l'ensemble des forces de l'ordre, en remplacement des multiples codes d'accès que policiers et gendarmes devaient utiliser pour consulter les différents fichiers (**Recommandation n° 45**).

La sécurisation de l'accès aux fichiers de police est sur le point d'être passablement améliorée. En effet, le service des technologies et des systèmes d'information de la sécurité intérieure du ministère de l'Intérieur conduit un projet visant à équiper **chaque fonctionnaire d'une carte à puce personnelle** assurant, entre autres, son accès aux différents fichiers de police pour lesquels il bénéficie d'une habilitation. Pour limiter les risques de prêt ou de perte, la puce sera, en fait, intégrée à la carte professionnelle des policiers.

Cette carte professionnelle électronique a d'ores et déjà commencé à être **délivrée aux gendarmes**, comme a pu le constater la mission d'information lors

(1) À la différence des fiches « Auteurs », les fiches « Procédures » ne sont pas expurgées avec l'écoulement du temps.

d'un déplacement auprès de la brigade de gendarmerie d'Auvers-sur-Oise [(1)]. En ce qui concerne la police nationale, le déploiement devait débuter à l'été 2011. Il a en réalité été initié le 4 novembre 2011 et doit se poursuivre jusqu'en juin 2012. En dehors du procès-verbal électronique, l'accès aux fichiers de police par le biais de cette nouvelle carte ne sera effectif qu'après 2012 pour la police nationale. Toutefois, pour M. Frédéric Péchenard, directeur général de la police nationale [(2)], c'est la biométrie qui s'imposera, à moyen terme, comme norme de sécurisation de l'accès aux fichiers de police.

FACSIMILÉ DE LA CARTE D'ACCÈS AUX FICHIERS DE POLICE DE LA POLICE NATIONALE

Source : direction générale de la police nationale.

Cette carte à puce devait, dans l'esprit de vos rapporteurs, remplacer les nombreux mots de passe attribués aux policiers et aux gendarmes leur permettant d'accéder aux différents fichiers de police. En effet, leur multiplication était susceptible d'engendrer des comportements à risque, consistant par exemple en l'affichage des mots de passe à proximité du poste de travail. Force est de constater aujourd'hui que **les cartes à puce n'ont pas vocation à remplacer entièrement l'accès aux fichiers par le biais d'un mot de passe**. En effet, les cartes à puce, d'ores et déjà déployées en gendarmerie, permettent l'identification de l'utilisateur *via* leur insertion dans un terminal semblable à celui d'une carte bleue, doublé d'un mot de passe. Par ailleurs, les gendarmes ont également accès aux fichiers *via* les terminaux embarqués utilisant le réseau RUBIS, qui fonctionnent aujourd'hui grâce à l'introduction d'un identifiant et d'un mot de passe. L'accès aux fichiers sur ces terminaux, par le biais de la nouvelle carte professionnelle électronique, est progressivement mis en place.

Enfin, **la sécurisation de l'accès aux fichiers de police passe aussi par l'information des utilisateurs**. Dans cette optique, des messages sont automatiquement générés lors de la consultation de fichiers par les gendarmes,

(1) Déplacement du 21 mars 2011 auprès de la brigade de gendarmerie d'Auvers-sur-Oise.
(2) Audition du 16 mars 2011 de M. Frédéric Péchenard, directeur général de la police nationale.

leur indiquant les précautions à prendre s'ils sont amenés à quitter momentanément leur poste de travail. Les différents écrans d'accueil des fichiers indiquent également aux utilisateurs dans quel cadre juridique, judiciaire ou administratif, ils sont autorisés à consulter ces fichiers. C'est notamment le cas du fichier des personnes sans domicile fixe (SDRF), dont l'écran d'accueil rappelle que « *ce traitement est mis en œuvre à des fins administratives* » uniquement. Il est également rappelé que tout contrevenant s'expose aux sanctions prévues par l'article 226-211 du code pénal [(1)]. On peut regretter que ces précautions ne soient pas étendues aux fichiers consultés par les policiers, *via* le logiciel CHEOPS.

2. Un bilan nuancé des procédures de contrôle de l'utilisation des fichiers

Vos rapporteurs avaient émis le souhait, en 2009, que les comportements anormaux révélateurs de consultations abusives soient mieux appréhendés, par le biais d'un **contrôle en temps réel (Recommandation n° 46)**, au lieu de déclencher une enquête *a posteriori*, comme c'était alors le cas. Cette solution, non exclusive d'un contrôle *a posteriori*, devait permettre de **détecter en amont toute utilisation abusive de fichiers de police**.

Une telle évolution semble être en cours. En effet, la **traçabilité complète des consultations** est au cœur de tous les fichiers de police actuellement développés. Ainsi, le nouveau **traitement des antécédents judiciaires TAJ** a été conçu avec une **traçabilité « haute »** : les données de connexion, qui comptent l'identifiant de l'utilisateur, la date, l'heure et la nature de la consultation, sont conservées pendant cinq ans et centralisées auprès de l'inspection générale de la gendarmerie nationale.

Toutefois, **cela ne constitue pas, à proprement parler, une révolution**. En effet, l'accès à la plupart des fichiers de police, et notamment au STIC, passe par le portail CHEOPS, qui conserve les traces de toute intervention pendant cinq ans. Le STIC offre une traçabilité plus grande encore, puisque, contrairement à CHEOPS, il est possible de savoir quelle fiche a été consultée ou modifiée. C'est également le cas du logiciel de gestion des violences urbaines (GEVI), développé par la préfecture de police de Paris, qui permet de connaître la date et l'heure d'une consultation, ainsi que l'identité de la personne ayant consulté ou modifié une fiche [(2)].

Outre le fait que la traçabilité demeure au cœur des préoccupations, les directions générales de la police nationale comme de la gendarmerie nationale ont mis en place des **procédures de contrôle**. Ainsi, des contrôles sont effectués

---

(1) « Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en oeuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende. *»*

(2) Déplacement du 3 février 2011 auprès de la Préfecture de police de Paris.

périodiquement par la direction générale de la police nationale grâce à des **relevés mensuels du volume de connexions**. En outre, il est procédé à des **audits ponctuels et aléatoires sur les connexions**.

Surtout, depuis mai 2009, et pour faire suite aux observations de la CNIL, l'inspection générale de la police nationale (IGPN) effectue des **contrôles inopinés dans les services territoriaux de police** afin de vérifier les conditions d'utilisation des fichiers de police. Six contrôles inopinés ont eu lieu en 2009 et une **vingtaine en 2010**. Ces contrôles, particulièrement utiles, permettent de mettre au jour des pratiques inadaptées, d'orienter en conséquence les consignes données aux services et de les assister dans la mise en œuvre quotidienne des règles d'utilisation des fichiers de police.

La gendarmerie, dans ce domaine, n'est pas en reste. Comme la police nationale, l'IGGN diligente fréquemment des **contrôles sur place** qui donnent lieu à des rapports suivis. Elle a également enjoint à certaines unités de niveau départemental ou régional de réaliser une **autoévaluation** de leur utilisation des fichiers de police, afin de les sensibiliser à la question et de leur permettre de repérer leurs éventuelles faiblesses. Cette procédure, qui porte sur vingt à cinquante unités par an, constitue un préalable à un contrôle *in situ*. Ces autoévaluations orientent les contrôles ultérieurs en faisant apparaître d'éventuelles contradictions.

Enfin, 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. À l'aide d'un logiciel spécifique, il trace les connexions et repère les consultations anormales. Ce logiciel permet, fichier par fichier, d'identifier des unités ou des gendarmes au comportement anormal au regard des normes habituellement constatées et de leurs profils, sur des périodes données. **Seule cette initiative répond véritablement à la recommandation émise par vos rapporteurs**.

3. Le problème des fichiers de police locaux

Le principal enjeu, en matière de fichiers de police, est aujourd'hui celui de la **création, par des unités locales, de traitement de données personnelles non perçus comme tels**. En effet, la définition extensive qu'en donne la loi est à l'origine de l'illégalité d'un très grand nombre de fichiers. Face à cet état de fait, les directions générales des deux forces ont pris un certain nombre de mesures encourageantes, susceptibles de permettre le développement d'une véritable culture « Informatique et libertés » en France.

L'article 2 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés définit les traitements automatisés de données à caractère personnel de façon très large. Notamment, « *tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés* » et regardant la sécurité publique constitue un fichier de police soumis au contrôle de

la CNIL. Ainsi, **un simple fichier informatique, sous forme d'un traitement de texte, d'un tableur ou d'une boîte de réception de messages électroniques, peut constituer un fichier au sens de la loi, dès lors qu'une recherche automatisée peut permettre de retrouver des données personnelles** (1).

Toutefois, comme l'ont indiqué à la mission d'information des représentants de la CNIL, **il arrive que les services locaux de police ou de gendarmerie ne soient pas pleinement conscients de l'étendue et de la portée de cette définition légale**. De même, le caractère temporaire de certains fichiers, utilisés comme des outils de travail dédiés à une enquête précise, a pu faire penser qu'ils ne rentraient pas dans le cadre défini par la loi du 6 janvier 1978 (2). Enfin, comme l'ont affirmé certains interlocuteurs à vos rapporteurs, **l'habitude a été prise de ne pas déclarer les fichiers de police locaux**.

De fait, de nombreux fichiers de police locaux existent qui n'ont pas fait l'objet d'une déclaration auprès de la CNIL. En effet, **chaque unité de police ou de gendarmerie a pu développer, au niveau local, ses propres outils de travail**. **M. Alain Bauer, président du groupe de contrôle sur les fichiers de police** (3) a ainsi porté à l'attention de la mission d'information l'existence de centaines de fichiers de police non déclarés créés au niveau local, notamment en matière de fourrières. Toutefois, il convient de noter que l'illégalité de tels fichiers réside, pour une grande majorité d'entre eux, dans l'absence de déclaration et non dans leur non-respect des règles de fond posées par le législateur (4).

La direction générale de la police nationale devait achever, en mars 2011, un **recensement des fichiers utilisés par les forces de police**. Notamment, les fichiers non déclarés devaient être repérés par ce biais. Les résultats de cette étude ne sont pas parvenus à vos rapporteurs, en dépit de demandes réitérées en ce sens.

Les directions générales de la police et de la gendarmerie nationales semblent toutefois avoir récemment pris conscience du problème.

Ainsi, outre les actes-cadres permettant une régularisation, par un acte réglementaire unique, de tous les fichiers locaux ayant la même finalité (cf. *supra*), **des correspondants Informatique et libertés locaux ont été désignés par les directions générales**. En ce qui concerne la gendarmerie nationale, 32 référents principaux et 19 référents auxiliaires ont été placés, dès le 1er janvier 2011, auprès des commandants de région, afin de veiller à ce que d'éventuels projets de fichiers locaux satisfassent à la loi et aux règlements(5). Ces officiers supérieurs de la gendarmerie exercent ces **fonctions de sentinelle et d'information** en plus de leurs fonctions habituelles, ce qui évite tout problème de défiance à l'égard d'intervenants extérieurs. La mise en place progressive de ces relais déconcentrés

(1) Audition de la CNIL du 2 février 2011.
(2) Idem.
(3) Audition de M. Alain Bauer du 26 janvier 2011.
(4) Idem.
(5) Audition du 23 mars 2011du Général Jacques Mignaux, directeur général de la gendarmerie nationale.

devrait à terme assurer la diffusion d'une culture du fichier au sein des forces de l'ordre, si toutefois un effort conséquent est fourni en matière de communication [(1)].

Au final, **parmi les onze propositions faisant l'objet de cette partie, seules deux ont été effectivement mises en œuvre. Trois d'entre elles ont donné lieu à une application partielle, et six sont restées lettre morte.**

(1) Cf. Infra*, Partie III, A.*

QUATRIÈME PARTIE : GOUVERNANCE, LOGICIELS ET INFRASTRUCTURES: UNE MODERNISATION EN CHANTIER

L'efficacité des fichiers de police ne réside pas uniquement dans la qualité des données qui y sont inscrites. Elle repose également sur la qualité des équipements et des infrastructures permettant leur utilisation. C'est pourquoi vos rapporteurs avaient proposé plusieurs mesures tendant à moderniser certains fichiers de police et à améliorer les infrastructures existantes. Ces recommandations ont été, pour certaines, suivies. Plusieurs fichiers, rénovés et modernisés, devraient ainsi voir le jour sous peu. De même, les équipements se modernisent petit à petit, grâce au déploiement de bornes dédiées. Le développement de nouveaux fichiers a, en outre, été rendu possible par l'apparition de nouvelles structures de gouvernance, dont la montée en puissance est tout à fait prometteuse.

A. DE NOUVELLES STRUCTURES DE GOUVERNANCE DES FICHIERS DE POLICE

En 2009, vos rapporteurs avaient constaté que si les talents informatiques ne manquaient pas au sein de la police comme de la gendarmerie, **le développement de nouveaux fichiers de police ne s'opérait pas dans des conditions tout à fait satisfaisantes**. En effet, outre le risque de doublons entre les deux forces de l'ordre, la séparation des équipes de gestion administrative et financière de celles chargées de la définition technique des programmes n'assurait pas le développement optimal de nouveaux logiciels.

C'est pourquoi vos rapporteurs avaient suggéré qu'une **équipe dédiée associant les deux forces** soit chargée d'assurer la gestion de tout nouveau projet de fichier commun à la police et à la gendarmerie. Cette équipe intégrée devait être dirigée par un seul chef de projet assisté d'un comité représentant toutes les directions intéressées, pour assurer le pilotage juridique, technique et financier du projet (**Recommandation n° 51**). De même, il avait paru bénéfique à vos rapporteurs que la police et la gendarmerie réfléchissent ensemble à leurs besoins futurs, au sein d'une **structure intégrée** (**Recommandation n° 52**).

Ces propositions ont été mises en œuvre par la création d'un service commun aux deux forces, désormais associées au sein du service des technologies et des systèmes d'information de la sécurité intérieure (**ST(SI)^2**) du ministère de l'Intérieur, créé par un arrêté du 27 août 2010 [(1)]. Ce service est chargé de conduire, dans ses aspects techniques et de développement, tous les grands projets de traitements communs relatifs à la sécurité intérieure. Il est en réalité issu de la fusion du service des technologies de la sécurité intérieure (STSI), créé en mai 2005 au sein de la direction de l'administration de la

(1) Arrêté du 27 août 2010 modifiant l'arrêté du 23 décembre 2009 portant organisation de la direction générale de la gendarmerie nationale.

police nationale (DAPN), et de la sous-direction des télécommunications et de l'informatique (SDTI) de la direction générale de la gendarmerie nationale (DGGN).

Le ST(SI)^2 doit disposer, à terme, d'un **effectif de 288 personnes**, parmi lesquels 149 gendarmes et 139 policiers. À l'heure actuelle, seuls 100 policiers sur les 139 prévus ont été affectés au service. Afin d'éviter toute rivalité, **les postes sont répartis de façon paritaire** jusqu'au niveau de chef de section. Parmi les quatre sous-directions – systèmes d'information, réseaux téléphoniques, coordination, soutien à l'utilisateur – deux ont été confiées à des gendarmes, et deux autres à des policiers. Le poste de chef de service qu'occupe actuellement le Général Bernard Pappalardo [(1)] pourrait d'ailleurs être confié à un policier, un préfet ou à tout autre haut fonctionnaire. Toutefois, il semble que le service ait rencontré **quelques difficultés** tenant à la nécessité d'intégrer et de concilier **deux histoires et deux cultures très différentes**.

Le mode de fonctionnement de l'ancienne sous-direction des technologies de l'information de la gendarmerie nationale, qui s'appuyait sur des officiers de gendarmerie ayant reçu une formation d'ingénieur ou d'informaticien, a été transposé à la nouvelle structure. La gendarmerie nationale s'appuie en effet depuis longtemps sur une **communauté de développeurs**. Ces gendarmes, qui développent des logiciels sur leur temps libre, créent des **applications qui, en plus d'être gratuites, sont parfaitement adaptées aux besoins de leurs utilisateurs**. La gendarmerie nationale les a regroupés et a mis en place des séminaires de travail de quinze jours, deux fois par an.

La mise en place de ce service est assurément avantageuse. Au plan financier d'abord, il représente une **considérable économie de moyens**. D'une part, parce qu'il permet d'éviter que des logiciels aux finalités semblables soient développés parallèlement par les deux forces ; d'autre part, parce que le recours au secteur privé est plus limité et les coûts résultant du maintien en condition opérationnelle réduits [(2)]. En outre, le fait que la maîtrise d'œuvre soit en partie assurée par le service constitue **un atout considérable en termes de réactivité**. L'adaptation de certains fichiers de police aux nouvelles règles entourant la garde à vue a ainsi pu intervenir très rapidement et à peu de frais.

Le service s'est ainsi vu confier, pendant sa phase de montée en charge, le développement de nombreux fichiers de police, notamment le fichier des interdits de stades ou encore la modernisation du fichier des empreintes génétiques. Pour le développement du fichier **TAJ**, le ST(SI)^2 a fait appel à des développeurs industriels, le service ne disposant pas des compétences nécessaires pour des projets de cette importance. En revanche, le développement de **LRPPN** est demeuré à la charge de la police nationale et de la DSIC, le ST(SI)^2 ne

(1) Audition du 9 mars 2011 du Général Bernard Pappalardo, chef du service des technologies et des systèmes d'information de la sécurité intérieure.

(2) Une part importante du coût du développement d'un logiciel par une entreprise réside dans la formation de techniciens susceptibles, à l'avenir, d'assurer le maintien en condition opérationnelle dudit logiciel.

disposant pas encore de la force de frappe nécessaire. Cependant, il a entamé, dès décembre 2010, par le biais de sa communauté d'informaticiens, le développement d'un logiciel de rédaction des procédures de la sécurité intérieure (LRPSI), commun aux deux forces.

Au final, la nouvelle gouvernance des fichiers de police constitue un progrès indéniable par rapport à la situation passée. Cependant, il est encore trop tôt pour déterminer si la greffe que constitue la création du ST(SI)^2 prendra véritablement, comme l'ont démontré les débats entourant le développement de LRPPN (cf. *infra*).

B. LA RÉNOVATION RÉUSSIE D'IMPORTANTS FICHIERS DE POLICE

Depuis plusieurs années, d'importants travaux de modernisation des fichiers de police ont été entrepris par la police comme par la gendarmerie. Deux chantiers principaux ont occupé les services responsables du développement de ces nouveaux logiciels : le traitement des antécédents judiciaires (TAJ) d'une part, et le logiciel de rédaction des procédures de la police nationale (LRPPN) d'autre part.

1. La modernisation significative des fichiers d'antécédents judiciaires et de sécurité publique

a) TAJ, le nouveau fichier d'antécédents judiciaires

Le nouveau traitement des antécédents judiciaires (1) (TAJ) est un fichier d'antécédents judiciaires dont la vocation première est d'assurer la fusion entre le STIC et JUDEX, bases de données relevant respectivement de la police et de la gendarmerie. En effet, l'existence d'une **base commune aux deux forces** présente de nombreux avantages. Outre le fait qu'elle permet d'**éviter les doublons** entre le STIC et JUDEX, elle est nécessairement **plus exhaustive** et constitue un **gain de temps** pour les forces de l'ordre, qui n'ont plus qu'un seul fichier à consulter. Elle permet également de **mutualiser les moyens dédiés à sa gestion**, grâce à une administration unique confiée à la police nationale (2).

(1) TAJ est la nouvelle appellation du fichier ARIANE.

(2) Le service central de documentation criminelle de la sous-direction de la police scientifique et technique est en charge de l'administration fonctionnelle de TAJ.

D'ARIANE À TAJ

En mars 2009, le développement d'ARIANE se heurtait à certaines difficultés. Notamment, il fallait convertir en format informatique les 2,5 millions de fiches de personnes et les 30 millions de fiches de procédure que comportait JUDEX, les 5,6 millions de fiches contenues dans le STIC, ainsi que les données issues du STIC-Canonge. Le toilettage des fichiers existants comme la reprise des données s'annonçaient difficiles et un retard d'environ huit mois avait déjà été pris sur le calendrier initial. Force est de constater que ce retard s'est accru. En effet, alors qu'en mars 2009, la reprise des données était sur le point de commencer et devait durer six mois, elle n'a en réalité débuté qu'en août 2010. Toutefois, en janvier 2011, 55 millions de fiches avaient d'ores et déjà été transférés. La vérification en service régulier a commencé en mars 2011, dans trois sites expérimentaux. Au total, alors que le déploiement devrait être opéré au 1er septembre 2010, celui-ci ne sera effectif qu'en 2012. Le décret, sur lequel la CNIL s'est d'ores et déjà prononcée, devrait être publié dans les prochaines semaines.

Vos rapporteurs ont pu constater que la nouvelle ergonomie de ce logiciel en fait un **fichier particulièrement moderne**. Très intuitif, le fichier TAJ permet de **rechercher les antécédents judiciaires d'une personne connue**, grâce à la fonction « Consultation », mais également d'**identifier une personne** à partir de deux éléments distincts, comme la nature de la procédure et le véhicule utilisé lors de l'infraction. Cette fonctionnalité nouvelle sera accessible à tous les enquêteurs, ce qui permettra par exemple aux brigades territoriales de base de réaliser des rapprochements à un niveau équivalent à celui dont disposent aujourd'hui les brigades de recherche spécialisées.

Le fichier TAJ permettra également d'**opérer des rapprochements** à partir d'un nombre plus élevé d'éléments, comme les caractéristiques de l'auteur ou les objets utilisés au cours de l'infraction. Toutefois, cette fonction ne sera pas accessible à tous les utilisateurs et ne sera accordée qu'aux unités d'investigation spécialisées.

Ces nouvelles fonctionnalités accordées à un plus grand nombre d'utilisateurs s'accompagnent de **procédures de contrôle renforcées** et automatisées. L'accès au fichier TAJ fait l'objet de procédures plus complexes, impliquant l'usage d'une carte à puce personnelle et de codes d'accès. Par ailleurs, le fichier TAJ est assorti de **garanties concernant la durée de conservation des données**. Ainsi, les données relatives à une personne mise en cause seront automatiquement effacées à l'issue de la durée de conservation, qui varie suivant la gravité des faits de 5 à 40 ans.

Malgré un certain retard par rapport au calendrier initial, ce projet est aujourd'hui très avancé, puisque le fichier TAJ devrait être déployé, dès la parution du décret l'autorisant, au premier semestre de l'année 2012, à raison

d'une quinzaine de commissariats et groupements de gendarmerie par mois. La date exacte du passage au fichier TAJ dépendra, dans chaque département, de l'avancée de la formation des utilisateurs.

b) De nouveaux fichiers dans le domaine de l'information générale

D'importants projets de modernisation ont également vu le jour dans le domaine du renseignement de sécurité publique. En effet, tant la police que la gendarmerie ont entrepris de développer de nouveaux outils permettant de répondre au mieux aux besoins des forces de l'ordre.

La direction des systèmes d'information et de la communication (DSIC) du ministère de l'Intérieur a travaillé en étroite collaboration avec le service des technologies et des systèmes d'information de la sécurité intérieure ($ST(SI)^2$) au développement de deux logiciels, l'un dédié aux enquêtes administratives, l'autre à la prévention des atteintes à la sécurité publique. Ces deux outils, qui seront utilisés par des services spécialisés de la police nationale [(1)], ont été conçus en 2009, à la suite de la parution de deux décrets autorisant leur utilisation [(2)].

Le **fichier des enquêtes administratives liées à la sécurité publique** (EASP) a vocation à intégrer des données relatives aux personnes ayant fait l'objet d'une enquête administrative, que son issue ait été favorable ou défavorable, dans le but d'éviter la réalisation de nouvelles enquêtes lorsque les personnes figurent déjà dans ce fichier. Une fiche nominative, à laquelle peut être joint le rapport d'enquête, indique l'identité et les coordonnées de la personne, de même que la nature de l'enquête. Une volumétrie importante a été prévue pour ce fichier, puisque 90 000 enquêtes administratives sont réalisées annuellement en France.

Le **fichier de prévention des atteintes à la sécurité publique** (PASP) a pour finalité de recueillir, de conserver et d'analyser les informations concernant les personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique, notamment lorsqu'elles sont susceptibles d'être impliquées dans des actions de violence collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives. Il a vocation à intégrer certaines données issues du fichier de gestion des violences urbaines (GEVI) de la préfecture de police de Paris comme du fichier des Archives Information générale (AIG), lui-même issu de la purge de l'ancien fichier des renseignements généraux. Il se substitue également au système AGIL de remontée de notes utilisé par les services départementaux de l'information générale (SDIG).

Les notes réalisées par les SDIG sont importées dans le logiciel après validation au niveau local puis national, par un archiviste ou un autre agent

(1) Ces outils seront accessibles aux fonctionnaires des sûretés départementales comme à ceux des services départementaux d'information générale.

(2) Décret n° 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 et décret n°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.

administratif. L'intégration se fait par le biais d'un thésaurus précis de thèmes. Une notice, relatant le thème et la date de création, est alors rédigée. Après intégration de la note du SDIG peut être réalisée une fiche individuelle, validée au niveau local puis par l'État-major de la sous-direction de l'information générale ou de la préfecture de police de Paris. Ces fiches individuelles ne sont pas toujours réalisées, notamment si la personne apparaissant dans la note ne présente aucune dangerosité.

Ces deux projets ont été menés de façon satisfaisante, même si le développement d'EASP accuse aujourd'hui un certain retard [(1)]. **Les utilisateurs ont été étroitement associés au développement de ces deux logiciels**, qui semblent dès lors **adaptés à leurs besoins**. En outre, les délais de développement ont été relativement courts en comparaison d'autres projets de même nature. Le fichier PASP, dont le développement a débuté en 2009, devrait être déployé en avril 2012. Aucune date n'est en revanche prévue pour le déploiement du fichier EASP.

La gendarmerie nationale développe également un nouvel outil en matière de sécurité publique. La nouvelle base de données de sécurité publique de la gendarmerie nationale (BDSP) comporte **quatre modules distincts** (cf. *supra*) qui facilitent notamment la gestion des événements d'ampleur, des interventions des gendarmes, des appels émanant de particuliers et des données relatives aux atteintes à la sécurité publique.

2. Le logiciel de rédaction des procédures de la police nationale : un rendez-vous manqué ?

Vos rapporteurs avaient souhaité, en 2009, que **le logiciel ARDOISE de rédaction des procédures, devant alimenter, à terme, le nouveau fichier d'antécédents judiciaires, soit rapidement remplacé par un outil plus performant et plus adapté aux besoins de ses utilisateurs** (**Recommandation n° 31**).

Le service central de la documentation criminelle (SCDC) d'Écully développe actuellement, en lien avec la DSIC du ministère de l'Intérieur, un nouveau logiciel de rédaction des procédures, dénommé LRPPN. **Des finalités ambitieuses ont été assignées à ce nouveau fichier de police**. En effet, LRPPN doit non seulement permettre la rédaction de procédures, mais il a également vocation à alimenter TAJ, le nouveau fichier d'antécédents judiciaires, et à assurer la remontée d'une information de nature statistique. Contrairement à l'ancien LRP DOS, qui ne visait qu'à générer des procédures papier, LRPPN doit répondre à des **objectifs bien plus nombreux et diversifiés**.

---

(1) Audition du 31 mars 2011 de Mmes Claude Jacopin et Sylvia Viteritti de la direction des systèmes d'information et de la communication (DSIC), de MM. Vincent Lafon et Antoine Delouvrier du service des technologies et des systèmes de l'information de la sécurité intérieure (ST(SI)2) et de M. Loïc Alixant, de la sous-direction de l'information générale.

C'est en partie ce qui ralentit le processus de développement de ce logiciel, entamé il y a déjà dix ans. En effet, il semble que **les services aient du mal à conceptualiser le logiciel et à définir ses fonctionnalités**, ce qui divise tant les techniciens que les utilisateurs du logiciel. À terme, ce fichier fera partie d'un **nouvel environnement intégré** assurant l'échange automatisé de données entre la police et la Justice [(1)].

Une version non définitive a été expérimentée par plusieurs services de police, que vos rapporteurs ont pu rencontrer. **Les opinions divergent fortement parmi les utilisateurs** et le nouveau logiciel est parfois mal accepté, notamment par les services de police judiciaire. Sa **faible ergonomie**, ses **nombreuses défaillances techniques**, notamment liées à son accès *via* CHEOPS, son **caractère peu intuitif** et inadapté à la réalité du travail des forces de l'ordre ont été soulignés par certains services.

Toutefois, il est normal, en phase de test, que des correctifs soient nécessaires. D'ailleurs, près de 90 % des remarques émanant des services utilisateurs semblent avoir été prises en compte par le SDCD [(2)], puisque 120 corrections ont été apportées à la première version. D'autres services, notamment de sécurité publique, insistent au contraire sur la **plus-value représentée par LRPPN II, par rapport à l'ancien logiciel de rédaction des procédures**, parfaitement obsolète.

Cependant, comme cela a été indiqué à vos rapporteurs au cours de plusieurs déplacements à Laval [(3)] et à Strasbourg [(4)], quelques améliorations pourraient encore être apportées au nouveau fichier, notamment en matière d'**aide à l'enquête**. En effet, à l'heure actuelle, le logiciel ne génère pas automatiquement certaines pièces de procédure, comme l'avis à la famille d'une personne gardée à vue. Contrairement au logiciel utilisé par la gendarmerie, il n'émet pas de signal d'alerte en fin de garde à vue. Or, ces éléments constituent autant de **garde-fous permettant d'assurer le respect de la procédure pénale**.

Par ailleurs, certains militent pour **l'établissement, dès ce stade, d'une qualification pénale**. Il a en effet été indiqué à vos rapporteurs que les procédures envoyées par la police nationale aux parquets n'étaient, pour la plupart, pas qualifiées pénalement, contrairement à celles transmises par la gendarmerie nationale. Or, le fichier ne propose aujourd'hui qu'une qualification « policière » des infractions, qui relève plus du mode opératoire que du code NATINF utilisé par la Justice [(5)].

En outre, il apparaît que ce nouveau fichier constituera assurément une perte de temps pour les fonctionnaires non encore aguerris à son utilisation.

---

(1) Cf. Annexe n° 10.
(2) Déplacement du 27 juin 2011 au commissariat central de Laval en Mayenne.
(3) Idem.
(4) Déplacement du 11 juillet 2011 au commissariat central de Strasbourg.
(5) Par exemple, il sera question d'un vol avec effraction plutôt que d'un vol aggravé.

Notamment, **la multitude de champs à remplir**, même si certaines étapes peuvent aujourd'hui être repoussées dans le temps, constitue une **charge de travail supplémentaire pour les enquêteurs**. Il a d'ailleurs été signalé à vos rapporteurs lors d'un déplacement au commissariat central de Strasbourg (1) que le **dépôt de plainte prenait deux fois plus de temps** par ce biais, passant de vingt à quarante minutes, ce qui risque d'engendrer un temps d'attente plus long pour les usagers victimes d'une infraction. Mais, dans la mesure où LRPPN alimentera directement le fichier TAJ pour ce qui est des victimes et des infractions, on peut considérer que les données qui y seront intégrées devront faire l'objet d'une formalisation plus poussée et nécessairement plus chronophage.

Enfin, certains observateurs remettent en cause le **schéma de remontée des données statistiques** retenu par le nouvel environnement intégré. À l'heure actuelle, le **fichier de l'état 4001** collecte les données au niveau national. Au plan local, des logiciels de statistiques opérationnelles permettent d'animer l'action policière départementale. Si le futur logiciel de rédaction de procédures LRPPN remonte directement les données au niveau national, les unités locales ne seront plus à même de réaliser leurs propres statistiques au niveau départemental. Pour certains interlocuteurs rencontrés par vos rapporteurs, il serait plus judicieux d'adopter le modèle de la gendarmerie nationale, dont les messages d'information statistique (2) sont traités au niveau local avant d'alimenter mensuellement le fichier de l'état 4001.

Face au **mécontentement soulevé par l'expérimentation** du logiciel et au **retard pris dans son développement**, deux missions d'inspection ont été diligentées et des **solutions alternatives** ont été un temps envisagées. Notamment, l'adaptation du logiciel de rédaction des procédures de la gendarmerie nationale, LRPGN, connu en 2009 sous le nom d'**ICARE**, est considérée par certains comme un moyen approprié de sortir rapidement de la crise générée par LRPPN. Il permettrait en effet de doter rapidement la police nationale d'un outil adapté à la rédaction des procédures, en attendant le développement d'une nouvelle version de LRPPN ou d'un logiciel de procédure commun aux deux forces.

Toutefois, plusieurs arguments ont été avancés contre la mise en œuvre de cette possibilité. Loin d'être aussi intégré que le futur LRPPN, LRPGN ne serait pas en mesure d'assurer la remontée de l'information statistique, qui est une des finalités de LRPPN II. En outre, **les méthodes de travail de la police et de la gendarmerie seraient si différentes qu'aucune adaptation du logiciel ne permettrait d'y remédier**. Enfin et surtout, un **facteur culturel** s'oppose à ce que la police nationale travaille avec les outils de la gendarmerie nationale, même sous une forme adaptée. Votre rapporteure déplore qu'aucune investigation plus poussée ne soit intervenue pour éprouver la solidité de ces arguments et envisager l'adaptation à la police nationale du logiciel utilisé par la gendarmerie.

---

(1) Déplacement du 11 juillet 2011 auprès du commissariat central de Strasbourg.

(2) Les messages d'information statistiques (MIS) sont des messages comportant des indications sur le fait délictueux : lieu, catégorie d'événement, heure, auteur, etc. Ces MIS sont réalisés par les gendarmes dans les quatre jours de la constatation des crimes et délits pénaux.

Le ST(SI)^2 a également amorcé le **développement d'un logiciel de rédaction des procédures de la sécurité intérieure (LRPSI)**, commun aux deux forces. Mais **ce projet ne pourra aboutir avant plusieurs années**, si bien que la mission de l'inspection générale de l'administration (1), qui a rendu ses conclusions en mars 2011, a recommandé **la poursuite du projet LRPPN** et l'octroi de nouveaux crédits permettant de procéder aux dernières corrections nécessaires à la connexion avec le fichier TAJ. Votre rapporteur, s'il est favorable au déploiement de LRPPN tel qu'il a été engagé, souhaiterait toutefois que le projet LRPSI puisse déboucher dans un avenir proche, à horizon de deux ans. Votre rapporteure ne peut que soutenir une telle proposition, dès lors que le logiciel commun aux deux forces répond aux besoins des policiers comme des gendarmes et allie efficacité et ergonomie.

Vos rapporteurs regrettent toutefois que le premier rapport relatif au déploiement de ce nouveau logiciel, réalisé par les deux inspections générales de la police et de la gendarmerie nationales et dont les conclusions différaient apparemment du rapport de l'inspection générale de l'administration, ne leur ait pas été communiqué conformément à leur demande.

3. L'urgence de moderniser le fichier des personnes recherchées comme le fichier des brigades spécialisées

Si de nombreux travaux de modernisation des fichiers ont aujourd'hui été entrepris, il importe que cette initiative soit étendue à d'autres fichiers de police, comme le fichier des personnes recherchées, utilisé quotidiennement par l'ensemble des forces de l'ordre, ou le fichier des brigades spécialisées, outil indispensable à la coordination des services en matière de lutte contre la criminalité organisée. En effet, ces deux fichiers reposent sur des technologies obsolètes préjudiciables à leur efficacité.

Vos rapporteurs avaient souligné, en mars 2009, à quel point il était nécessaire de moderniser de toute urgence le **fichier des brigades spécialisées, outil de surveillance du milieu criminel et d'échange d'informations entre les services concernés par la lutte contre la criminalité organisée (Recommandation n° 49)**, dont le fonctionnement même était compromis du fait de son obsolescence.

Le premier rapport du groupe de travail sur les fichiers de police présidé par M. Alain Bauer mentionnait déjà, en 2006, qu'une réflexion avait été amorcée en ce sens. Force est de constater aujourd'hui que cette réflexion ne semble pas avoir atteint un niveau supérieur. En effet, d'après les réponses fournies par la direction générale de la police nationale (2), la modernisation de ce fichier est toujours « *à l'étude* ». **Vos rapporteurs ne se sont pas vus fournir d'éléments**

(1) Rapport sur le logiciel de rédaction des procédures dans la police et la gendarmerie nationales, établi par M. Richard Castéra, inspecteur générale de l'administration, 30 mars 2011.

(2) Réponse du 7 mars 2011 des directions générales de la police et de la gendarmerie nationales au questionnaire de suivi des recommandations.

plus tangibles, ce qui semble attester de l'état peu avancé de cette entreprise de modernisation.

Le fichier des personnes recherchées (FPR) semble frappé de la même obsolescence technique que le fichier des brigades spécialisées. Or, ce fichier est consulté en permanence par les forces de l'ordre, portant le nombre de consultations annuelles à environ 10 millions. Créé en 1969, le FPR est un fichier très ancien, qui repose sur une technologie dépassée que la direction des systèmes d'information et de la communication (DSIC) du ministère de l'Intérieur ne parvient plus à gérer. Si l'interface de consultation a été modernisée, l'alimentation proprement dite se fait toujours par le biais de l'ergonomie d'origine. Enfin, ce fichier n'étant accessible que par le biais de la passerelle CHEOPS, sa consultation est parfois rendue impossible pendant plusieurs heures (1) (cf. *infra*).

LE FICHIER DES PERSONNES RECHERCHÉES, LE FICHIER LE PLUS CONSULTÉ

Le fichier des personnes recherchées (FPR) est un fichier très ancien, dont la police nationale dispose **depuis 1969**. Il assure le recensement des personnes faisant l'objet d'une mesure de recherche ou de vérification de leur situation juridique et permet ainsi de faciliter les recherches effectuées par les services de police et de gendarmerie. Le FPR comporte **21 types de fiches**, selon les causes ayant motivé l'inscription au FPR : aliénés, mineurs en fugue, évadés, contrainte par corps, contrôle judiciaire, débiteurs envers le Trésor, étrangers, déserteurs… Il comportait, au 1er mars 2011, **416 000 fiches**, ce qui correspond à la volumétrie moyenne du fichier.

Ce fichier est utilisé en permanence par les forces de l'ordre. En effet, le FPR est consulté pour toutes les personnes arrêtées, interpellées ou gardées à vue, pour celles pour lesquelles il existe des raisons plausibles de soupçonner qu'elles ont commis un crime ou un délit, qu'elles sont sur le point de le faire, qu'elles peuvent fournir des renseignements utiles à l'enquête ou qu'elles ont fait l'objet de recherches de la part de l'autorité judiciaire. Le FPR est également consulté pour prévenir une atteinte à l'ordre public ainsi qu'en cas de contrôle d'identité, de même que pour toute personne dans l'incapacité de prouver son identité. Il peut être consulté lorsque l'enquêteur dispose d'éléments complets d'identité (code « IN »), ou juste du nom de la personne (code « RE »). Environ **dix millions de requête**s sont ainsi effectués tous les ans par les forces de police et de gendarmerie.

Source : audition du 7 avril 2011 de M. Éric Brendel, chef du service central de documentation criminelle de la police nationale (SCDC), et du Colonel Francis Hubert, chef du service technique de recherches judiciaires et de documentation de la gendarmerie nationale (STRJD).

(1) Déplacement du 21 mars 2011 à l'hôtel de police de Cergy-Pontoise.

Sur le fond, **le FPR n'est pas tout à fait adapté au travail des forces de l'ordre**. Outre sa fonction de consultation, **il devrait être doté d'une fonction de diffusion**. Ainsi, en cas d'évasion d'un établissement pénitentiaire, une information spécifique devrait parvenir aux patrouilles officiant dans le périmètre géographique concerné, *via* le FPR. À l'heure actuelle, quand une personne est recherchée, la direction centrale de la police judiciaire (DCPJ) fait parvenir à tous les services des circulaires de recherche sous format papier, qui sont alors noyées parmi d'autres documents. Face à cela, il n'est pas impossible que les services se soient d'ores et déjà munis de tels fichiers, non déclarés, afin de centraliser l'identité des personnes recherchées de leur secteur géographique.

La traçabilité des consultations est également problématique. En effet, à l'heure actuelle, il est possible de connaître l'identité de la personne qui s'est connectée, ainsi que la date et l'heure de la connexion, mais pas les données relatives à la recherche qu'elle a effectuée. Par ailleurs, bien souvent, la consultation proprement dite est réalisée par le chef de poste [(1)], qui reçoit les demandes de consultation par talkie-walkie et les effectue en temps réel. Les demandes sont alors retranscrites dans un registre papier, support qui n'offre pas toutes les garanties nécessaires à la bonne traçabilité des consultations.

Lorsque le contrôle est positif, les enquêteurs doivent respecter la « **conduite à tenir** » indiquée sur la fiche FPR. Il peut s'agir d'inviter la personne à suivre les enquêteurs au poste de police, de conduire la personne au poste contre son gré ou, au contraire, de recueillir des éléments d'information sur place, sans indiquer à la personne qu'elle est recherchée. Cependant, il apparaît que ces conduites à tenir **manquent souvent de précision et de clarté**, ce qui oblige le service inscripteur à entrer en contact avec les services demandeurs. Par exemple, si la conduite à tenir consiste à inviter la personne à venir au poste de police, il faut également indiquer le comportement à adopter lorsque celle-ci décline la proposition.

Cependant, il semble que **le ST(SI)^2 se soit saisi du problème et ait entamé une réflexion sur le développement d'un nouveau FPR**, plus performant et plus adapté aux besoins des forces de l'ordre, qui devrait aboutir en 2014 [(2)].

Proposition n° 4

Moderniser rapidement le fichier des personnes recherchées (FPR), afin d'en faire un outil performant et réactif.

(1) Idem.

(2) Audition du 7 avril 2011 de M. Éric Brendel, chef du service central de documentation criminelle de la police nationale (SCDC), et du Colonel Francis Hubert, chef du service technique de recherches judiciaires et de documentation de la gendarmerie nationale (STRJD).

4. Reconnaissance faciale et interconnexion : l'avenir des fichiers d'identification ?

Le recours au fichier des empreintes digitales (FAED), qui comportait 3,7 millions d'empreintes en 2010, et au fichier des empreintes génétiques (FNAEG), qui compte 1,8 million de profils, est aujourd'hui incontournable. Mais l'usage des fichiers d'identification pourrait connaître un développement très important dans les années à venir, soit qu'ils compléteraient les finalités d'autres fichiers par le biais d'une interconnexion, soit que de nouveaux moyens d'identification biométrique apparaissent.

a) L'interconnexion des fichiers d'identification aux fichiers d'antécédents judiciaires, une demande récurrente

La notion d'interconnexion est particulièrement complexe, la loi n'en donnant **pas de définition précise**. Toutefois, le Conseil d'État, dans un arrêt récent, est venu préciser les contours de la notion d'interconnexion. Ainsi, « *une interconnexion doit être regardée comme l'objet même d'un traitement qui permet d'accéder à, d'exploiter et de traiter automatiquement les données collectées pour un autre traitement et enregistrées dans le fichier qui en est issu* » (1). De cette définition, la CNIL (2) a retenu **trois critères** lui permettant d'identifier un traitement d'interconnexion : son objet porte sur la **mise en relation de fichiers** ou traitements de données à caractère personnel ; il concerne **au moins deux fichiers** ou traitements distincts ; il agit dans le cadre d'un **processus automatisé**. Ainsi, lorsque la mise en relation des données n'est que ponctuelle ou non automatisée, la CNIL considère qu'il s'agit d'un simple rapprochement de fichiers.

L'interconnexion de fichiers distincts comporte, pour la CNIL, quatre risques majeurs. Tout d'abord, l'interconnexion peut conduire à ce que le nouveau traitement ainsi formé ait d'autres finalités que celles initialement prévues. L'interconnexion peut se révéler une **extension occulte du champ du fichier** mis en œuvre. Par ailleurs, l'interconnexion fait peser un risque sur le respect des **secrets professionnels** ; elle ne doit pas permettre de réaliser de façon pratique ce que le législateur a entendu proscrire. Ainsi, lorsque des fichiers comportant des données couvertes par le secret sont interconnectés à d'autres fichiers, le législateur doit intervenir afin de lever les obligations liées au secret. En outre, l'interconnexion peut avoir un effet néfaste sur la **durée de conservation** des données, si le fichier de destination dispose d'une durée de conservation plus grande. Enfin, la **sécurité des données** peut être malmenée par une interconnexion ne faisant pas l'objet de mesures de sécurité renforcées.

(1) CE, 19 juillet 2010, Base élèves.

(2) Audition du 29 juin 2011 de M. Yann Padova, secrétaire général de la Commission nationale de l'informatique et des libertés (CNIL).

Toutefois, **lorsque l'interconnexion assure une protection plus efficace des droits et libertés, la CNIL y est favorable** (1). Par exemple, lorsque l'interconnexion permet une mise à jour instantanée des données, comme c'est le cas de l'interconnexion entre TAJ et CASSIOPEE, les suites judiciaires étant alors directement intégrées au nouveau fichier des antécédents judiciaires, la CNIL ne peut que l'encourager.

Or, l'**interconnexion des fichiers d'identification que sont le FAED et le FNAEG** avec les fichiers d'antécédents judiciaires constitue une demande récurrente de certains services de police. En effet, une telle interconnexion permettrait selon eux de **fiabiliser les données intégrées dans le fichier TAJ** et de repérer plus aisément l'utilisation d'alias et les problèmes d'homonymie. Une telle opération de rapprochement des données est d'ailleurs prévue, comme l'a indiqué la CNIL à la mission. En effet, à chaque inscription d'une personne dans le fichier TAJ, il sera procédé automatiquement à une recherche dans le FNAEG et le FAED. Le cadre légal étant le même, c'est-à-dire l'enquête judiciaire, la CNIL ne voit pas d'opposition à une telle interconnexion.

Tel n'est pas le cas d'une éventuelle **interconnexion du FPR aux fichiers d'identification**. En effet, si, dans le cadre d'une enquête judiciaire, les données prélevées sur une scène de crime peuvent être utilement comparées à celles du FPR, à l'inverse, la vérification de l'inscription d'une personne aux fichiers d'identification dans le cadre d'un contrôle d'identité dépasse largement les finalités du FPR. Une telle interconnexion devrait dès lors être extrêmement encadrée afin de recevoir l'aval de la CNIL.

b) Vers un fichier autonome de reconnaissance faciale ?

Le mercredi 22 juin 2011, M. Frédéric Péchenard, directeur général de la police nationale, déclarait à la commission des Finances de l'Assemblée nationale (2) : « *on se dirige vers la* ***création d'un troisième fichier de reconnaissance faciale****, qui pourrait servir à l'exploitation des données de vidéo surveillance* ». Ce fichier, à l'instar des fichiers des empreintes génétiques et digitales, permettrait d'effectuer des rapprochements entre d'une part, des photographies prises, par exemple, dans le cadre de la vidéosurveillance et, d'autre part, les photographies tirées de la base de données. Comme pour le FAED et le FNAEG, le logiciel procédera par points de comparaison et proposera à l'enquêteur plusieurs solutions possibles classées par ordre de pertinence.

Un tel dispositif est d'ores et déjà prévu par le fichier TAJ, sans pour autant constituer, pour l'heure, un fichier autonome. En effet, les fiches relatives aux personnes associent une photographie signalétique à une identité. Des

(1) Audition du 29 juin 2011 de M. Yann Padova, secrétaire général de la Commission nationale de l'informatique et des libertés (CNIL).

(2) Audition, ouverte à la presse, de M. Frédéric Péchenard, directeur général de la Police nationale, et du général Jacques Mignaux, directeur général de la Gendarmerie nationale, sur le projet de loi de règlement pour 2010 (n° 3507).

rapprochements pourront être effectués grâce à un logiciel de reconnaissance automatisée de l'image intégré au fichier TAJ, qui a d'ailleurs repris environ 1,7 million de clichés issus du STIC-Canonge (1). Néanmoins, contrairement aux fichiers d'identification actuels, la médiation d'un ou plusieurs analystes qualifiés ne semble pas prévue par le dispositif. Dans ce contexte, les garanties offertes semblent largement insuffisantes au regard des exigences de la CNIL.

En effet, la CNIL, qui s'est prononcée sur le fichier TAJ et son module de reconnaissance faciale, considère que **les données biométriques sont des données particulièrement sensibles, dont l'utilisation doit être particulièrement encadrée** : « *À la différence de toute autre donnée à caractère personnel, la donnée biométrique n'est donc pas attribuée par un tiers ou choisie par la personne : elle est produite par le corps lui-même et le désigne ou le représente, lui et nul autre, de façon immuable.* ***Elle appartient donc à la personne qui l'a générée et tout détournement ou mauvais usage de cette donnée fait alors peser un risque majeur sur l'identité de celle-ci*** » (2). Il en va de même pour les données relatives au visage ou à la physionomie des personnes. En effet, pour la CNIL, même s'il ne s'agit pas de traces physiques, « *l'association entre vidéoprotection et dispositifs de reconnaissance faciale aboutit à un résultat similaire en créant des traces informatiques en lieu et place des traces physiques laissées par les empreintes digitales* » (3).

La reconnaissance automatisée par l'image, si elle est relativement développée au plan technique, connaît un **taux d'erreur bien plus élevé** que les fichiers d'identification actuels, qui ne laissent que très rarement place au doute. Aussi importe-t-il que les **garanties entourant ce fichier soient au moins aussi importantes que pour le FAED et le FNAEG**. En premier lieu, la base de données ne pourra être composée que de l'image de personnes judiciairement mises en cause. En second lieu, il convient de laisser ouverte la possibilité, pour les personnes à l'encontre desquelles il existe une ou plusieurs raisons plausibles de soupçonner qu'elles ont commis des infractions définies, de comparer leurs photographies sans les conserver. De même, l'effacement des données doit être possible pour les personnes contre lesquelles il existe des indices graves ou concordants indiquant qu'elles ont commis les infractions définies.

MM. Michel Gaudin et Alain Bauer, auteurs du *Livre blanc sur la sécurité publique*, ont proposé le développement d'une « *base nationale des photographies* », distincte de TAJ, ainsi que d'un « *système d'information global permettant le rapprochement des différentes traces criminalistiques* » (4) et de **bornes multimodales** permettant la prise d'empreintes et la consultation simultanée des fichiers d'identification digitale, génétique et faciale. Enfin, ils proposent d'approfondir la recherche en matière de reconnaissance de tatouages,

---

(1) Livre blanc sur la sécurité publique, p.91, 26 octobre 2011.

(2) Note d'observations de la Commission nationale de l'informatique et des libertés concernant la proposition de loi relative à la protection de l'identité, séance plénière du 25 octobre 2011, p. 2.

(3) Ibid.

(4) Livre blanc sur la sécurité publique, p.172, 26 octobre 2011.

de personnes en mouvement, de signatures vocales ou encore de traces olfactives. Cela permettrait, selon les auteurs, d'abandonner les descriptions des personnes utilisées au cours des enquêtes, notamment en matière d'origines ethniques, de plus en plus « *en décalage avec la réalité sociale* ». Par ailleurs, la combinaison des différentes méthodes de reconnaissance biométrique permettra selon eux d'atteindre un taux plus élevé d'élucidation, par exemple lorsque les données digitales ou génétiques prises séparément ne sont que partielles. Votre rapporteur est tout à fait favorable à ces propositions, qui seront à même de donner aux forces de l'ordre les moyens de lutter plus efficacement contre la délinquance. Votre rapporteure, sans écarter la mise en place à long terme de tels dispositifs, considère que la priorité, dans un contexte budgétaire contraint, doit être donnée à la modernisation de fichiers de police déjà existants et particulièrement utiles, comme le FPR.

C. L'INFRASTRUCTURE DES RÉSEAUX ET LES MOYENS TECHNIQUES RELATIFS AUX FICHIERS DE POLICE : DES INQUIÉTUDES

Un des axes majeurs d'amélioration, souligné par le rapport de la mission d'information, avait été l'installation de terminaux dédiés à l'alimentation et à la consultation de certains fichiers. Il semble aujourd'hui qu'une attention particulière doit être portée au réseau informatique des forces de l'ordre, dont la qualité variable porte une atteinte considérable au bon fonctionnement des fichiers de police.

1. Le déploiement de terminaux dédiés à l'enregistrement des données et à la consultation des fichiers

En 2009, vos rapporteurs avaient constaté que la contribution de la gendarmerie nationale à l'alimentation du fichier des empreintes digitales (FAED) était insuffisante, du fait d'un manque de moyens techniques. En effet, les brigades territoriales n'étant pas dotées de bornes d'enregistrement des données décadactylaires, l'information mettait du temps à parvenir au service technique des recherches judiciaires et de documentation (STRJD) chargé de l'intégration des données au FAED. Aussi vos rapporteurs avaient-ils recommandé que **des bornes de signalisation T1 et T4 [(1)] soient déployées au sein des unités de la gendarmerie nationale,** aussi bien dans les 100 brigades départementales de renseignements et d'investigations judiciaires que dans les unités territoriales les plus chargées (**Recommandation n° 23**).

Cette proposition est en cours de mise en œuvre. Ce sont ainsi 22 terminaux de signalisation T4 qui ont été installés en 2010 dans les principales brigades départementales de renseignements et d'investigations judiciaires de la

(1) Les bornes de type T1, de forte capacité en volume de données et d'un coût unitaire de 75.000 euros, permettent la capture, sans encrage, sur un bloc optique et la numérisation immédiate des relevés dactyloscopiques, tandis que les bornes T4, d'un coût unitaire de 15.000 euros, offrent seulement une faculté de numérisation des fiches papiers.

direction générale de la gendarmerie nationale. Le plan de déploiement devait se poursuivre dès le 1er semestre de l'année 2011 avec la mise en place de 52 bornes supplémentaires.

Outre la nécessité d'alimenter rapidement les fichiers de police, il convient également d'**assurer, par des moyens techniques appropriés, la mise à jour immédiate des données contenues dans les fichiers de police**. Tel était l'objet de la **recommandation n° 40** formulée en mars 2009 par vos rapporteurs, qui souhaitaient voir installés au plus vite dans les parquets des TGI des terminaux permettant l'accès direct aux données figurant dans les traitements STIC et JUDEX, afin de donner un caractère effectif au contrôle exercé par le procureur de la République en matière de fichiers d'antécédents judiciaires.

Cette proposition devrait être mise en œuvre dans le cadre du passage au traitement des antécédents judiciaires (TAJ) (1). Si l'accès direct aux fichiers d'antécédents judiciaires, dans les tribunaux, n'avait pas été mis en œuvre du fait notamment de la nécessité de prévoir deux terminaux distincts pour le STIC et JUDEX (2), la mise en place d'un fichier unique, TAJ, résout théoriquement ce problème puisque ce nouveau fichier pourra vraisemblablement être consulté directement par les parquets.

2. Un réseau défectueux qui nuit à l'utilité des fichiers de police

Il a été fait mention de façon récurrente, au cours des déplacements de la mission d'information, des **défaillances du réseau informatique de la police nationale**. Certains services distants ne bénéficieraient ainsi que de **52 kilo-octets de bande passante**, ce qui rend les fichiers de police difficilement consultables (3). En effet, la plupart d'entre eux fonctionnent selon un **mode « client-serveur »** : l'utilisateur doit être connecté en permanence à une base nationale unique, *via* Internet, pour accéder aux données. Ainsi, **si le réseau proprement dit connaît une défaillance momentanée, les fichiers de police fonctionnant en mode client-serveur ne sont pas consultables**.

Il semble que le réseau de la police nationale soit sujet à de **fréquentes coupures**. Notamment, le réseau de la 3e division de police judiciaire de Paris (4) souffre d'**instabilité chronique**. Les coupures sont fréquentes et parfois extrêmement longues, jusqu'à plusieurs jours, gênant sérieusement le travail des policiers. **L'augmentation des flux échangés via Internet et l'obsolescence du réseau sont vraisemblablement à l'origine de ces défaillances.** Or, le réseau sera soumis, dans un avenir proche, à des flux plus importants de données, avec la progression de la dématérialisation des procédures. Notamment, certaines pièces

(1) Réponse du 7 mars 2011 des directions générales de la police et de la gendarmerie nationales au questionnaire de suivi des recommandations.

(2) Pour ce qui est de la gendarmerie, des expérimentations ont été menées en 2010 auprès des cours d'appel de Douai et d'Amiens, mais les consultations de JUDEX étaient demeurées assez faibles.

(3) Déplacement du 27 juin 2011 au commissariat de Laval.

(4) Déplacement du 3 mars 2011 auprès de la 3e division de police judiciaire de Paris.

de procédure devront être échangées sous un format correspondant à celui d'une photographie, le rendant ainsi extrêmement lourd. L'inadaptation du réseau à ces nouvelles méthodes se traduira assurément par des coupures de plus en plus fréquentes.

Les services de police pâtissent des défaillances du réseau, mais également de celles des logiciels eux-mêmes. Notamment, **l'instabilité chronique du logiciel CHEOPS, portail qui permet d'accéder à l'ensemble des fichiers de police, est très problématique**. D'ailleurs, les services ayant expérimenté le nouveau logiciel de rédaction des procédures de la police nationale (LRPPN), accessible uniquement via CHEOPS, ont été contraints de recourir, de temps à autre, à l'ancien logiciel de rédaction des procédures, qui utilise encore le système d'exploitation *disk operating system* (DOS) [(1)], lorsque CHEOPS n'était pas disponible.

Il conviendrait donc d'**assurer l'accès à ces fichiers sur un mode plus léger que l'actuel mode « client-serveur »,** comme c'est le cas pour la gendarmerie nationale, qui utilise une architecture web nécessitant moins de bande passante. Cependant, une nouvelle version de CHEOPS est en cours de développement qui mettra peut-être un terme à ces défaillances techniques. Par ailleurs, afin de garantir l'accès aux fichiers de police, il conviendrait de mettre en place des **serveurs relais régionaux** permettant de pallier les défaillances du serveur national.

Proposition n° 5

Engager un chantier de modernisation des infrastructures de réseaux de la police nationale.

Il semble donc nécessaire de **réaliser des investissements dans le domaine des infrastructures de réseau**. Cette responsabilité relève de la direction des systèmes d'information et de communication du ministère de l'Intérieur (DSIC), qui doit aujourd'hui prendre la mesure du problème. Certes, les logiciels utilisés par les forces de l'ordre, pour certains très anciens et consommateurs de bande passante, sont également en cause. **Un effort conjoint doit donc être réalisé par la DSIC comme par les services en charge du développement des logiciels afin de garantir la continuité de l'accès aux fichiers de police.**

Sur six recommandations, quatre ont fait l'objet d'une mise en œuvre complète ou partielle, tandis que deux n'ont pas été suivies d'effet.

(1) Déplacement du 11 juillet 2011 au commissariat central de Strasbourg.

CINQUIÈME PARTIE : L'UTILITÉ DES FICHIERS EN MATIÈRE DE LUTTE CONTRE LA DÉLINQUANCE SÉRIELLE DE NATURE SEXUELLE

Les fichiers de police occupent aujourd'hui une place non négligeable dans la lutte contre la délinquance sérielle de nature sexuelle. En amont, le développement de l'analyse criminelle, depuis les années 1990, permet d'effectuer des rapprochements à partir de données objectives issues des procédures judiciaires. L'analyse criminelle, couplée à l'analyse comportementale, fondée sur les sciences du comportement, facilite l'élucidation d'enquêtes portant sur des crimes et délits sériels. En France, le système d'analyse des liens de la violence associée aux crimes (SALVAC) met en œuvre ces méthodes d'origine anglo-saxonne et connaît d'excellents résultats en matière de crimes et délits sexuels.

En aval, une fois les auteurs de violences sexuelles condamnés par la justice, les fichiers peuvent faciliter le contrôle social auquel sont soumises ces personnes. C'est notamment la vocation première du fichier judiciaire automatisé des auteurs d'agressions sexuelles et violentes (FIJAISV), qui permet de suivre les auteurs de violences sexuelles après leur libération, lorsqu'ils sont soumis par la justice à une obligation de justification d'adresse. Toutefois, il convient de ne pas surestimer les capacités de ces fichiers, qui ne peuvent que soutenir l'action policière et judiciaire proprement dite.

A. LE DÉVELOPPEMENT DES FICHIERS D'ANALYSE CRIMINELLE EN MATIÈRE DE DÉLINQUANCE SEXUELLE : UNE UTILITÉ AVÉRÉE

L'analyse criminelle se diffuse progressivement, depuis une dizaine d'années déjà, au sein de la police comme de la gendarmerie. Si les forces de gendarmerie développent actuellement un logiciel d'analyse criminelle, ANACRIM Nouvelle génération, la police dispose depuis 2002 d'un fichier d'origine canadienne, le système d'analyse des liens de la violence associée aux crimes (SALVAC).

1. Le fichier SALVAC, une précieuse aide à l'enquête en matière de crimes et délits sexuels à caractère sériel

Le fichier SALVAC, exploité par une cellule dédiée à l'analyse criminelle, peut constituer, sous certaines conditions, une précieuse aide à l'enquête dans le cadre des crimes et délits sexuels à caractère sériel.

a) La mise en place d'une cellule dédiée à l'élucidation des infractions sexuelles à caractère sériel

Au début des années 2000, la recrudescence des agressions sexuelles a conduit à la création d'une cellule dédiée à l'élucidation des crimes et délits sexuels au sein de l'Office central pour la répression des violences aux personnes (OCRVP), organe spécialisé dans la grande criminalité. La cellule SALVAC [(1)], qui porte le nom du logiciel utilisé, a été mise en place en octobre 2002. Elle compte aujourd'hui une dizaine de personnes, dont un chef de centre, M. Frédéric Malon, ainsi que neuf officiers de police judiciaire formés à l'analyse comportementale et à l'utilisation du logiciel d'analyse criminelle SALVAC, parmi lesquels quatre gendarmes.

La cellule SALVAC est compétente pour les **infractions sexuelles à caractère sériel,** les homicides à caractère sériel ou sexuel, qui répondent à un mode opératoire particulier ou qui sont dénués de mobile apparent, les enlèvements non parentaux et non crapuleux, le plus souvent pédophiles, les découvertes de cadavres et les disparitions inquiétantes. Experte en analyse criminelle des comportements, la cellule SALVAC fournit une aide non négligeable aux enquêteurs qui sollicitent son avis. **Ce travail, particulièrement efficace en matière de viols et d'agressions sexuelles**, fonde la légitimité de la cellule SALVAC.

L'analyse comportementale proprement dite s'opère à partir de trois éléments : le **comportement verbal**, c'est-à-dire les paroles prononcées par l'agresseur, souvent identiques d'une agression à l'autre ; son **comportement physique**, notamment sa violence ; enfin, le **comportement sexuel** de l'auteur, c'est-à-dire ses orientations sexuelles, ses pratiques, ses cibles de prédilection. Des éléments objectifs, comme les véhicules, les armes, les lieux, l'approche de la victime par ruse, surprise ou « attaque éclair », ou encore les précautions prises par l'auteur, sont également analysés pour procéder à des rapprochements et fournir des pistes aux enquêteurs.

b) Le fichier SALVAC, un outil précieux d'analyse comportementale

La cellule SALVAC dispose, pour effectuer les rapprochements fondés sur l'analyse criminelle, d'un logiciel éponyme d'origine canadienne. Le fichier SALVAC est la version française du logiciel canadien *Violence crime linkage analysis system* (VICLAS). Au milieu des années 1980, à la suite de plusieurs enquêtes complexes sur des meurtres en série commis sur différents territoires canadiens, les forces de police canadiennes ont constaté qu'il était impératif de mettre en place un système permettant de repérer les crimes sériels violents et leurs auteurs. Après un examen du *Violent Criminal Apprehension Program* (VICAP) américain, le logiciel utilisé par le *Federal bureau of investigations* (FBI), les policiers canadiens ont mis au point un système équivalent en 1991.

(1) Déplacement du 14 mars 2011 à l'Office central pour la répression des violences aux personnes.

Ce système a été transposé en France, ainsi que dans de nombreux autres pays européens, sous le nom de SALVAC. Le Canada a d'abord mis gratuitement à disposition de la police française une première version de SALVAC, en 2003. Des policiers et gendarmes français ont été formés au Canada, avant de former eux-mêmes des enquêteurs en France. Les **licences d'utilisation**, d'un montant de **25 000 à 30 000 euros**, sont aujourd'hui renouvelées chaque année.

La cellule reçoit les informations émises par les services de police et de gendarmerie, mais lit également la presse. Elle opère alors une sélection des événements entrant dans son champ de compétence et entre en contact avec le service enquêteur, afin que celui-ci remplisse un **questionnaire SALVAC composé de 156 items**, correspondant aux données requises par le logiciel et décrivant précisément les circonstances de l'infraction (lieux, victimologie, mode opératoire…). Ce questionnaire est envoyé aux enquêteurs dès le début de l'enquête et peut être assorti de diverses pièces de procédures, notamment les procès-verbaux.

Lorsque la cellule SALVAC est saisie par un service enquêteur, un analyste affecté à l'enquête intègre les données issues du questionnaire et des pièces de procédure dans le logiciel. Un second analyste vérifie la **bonne intégration des données**. Cette étape est d'une **importance cruciale pour garantir la fiabilité du rapprochement opéré par le logiciel**. Ensuite, l'analyste interroge le logiciel afin qu'il effectue un premier rapprochement, sur la base des critères dictés par l'utilisateur. En cas de lien positif, une seconde analyse complète est effectuée, sans concertation, par un autre analyste.

L'analyste en charge du dossier rédige enfin un **rapport, transmis aux services enquêteurs concernés et aux magistrats, faisant état des rapprochements possibles avec d'autres affaires**. L'analyse ne fait que proposer un rapprochement, que les services enquêteurs doivent infirmer ou confirmer par une enquête. Une formation continue est organisée mensuellement en interne, afin d'harmoniser les pratiques des analystes, notamment en matière de protocole de saisie des données.

2. Une initiative utile et efficace qui mérite d'être mieux reconnue par les services de police

Depuis sa création, la cellule SALVAC a rendu **environ 280 rapports de rapprochements**, parmi lesquels **24 séries se sont révélées exactes, qui concernaient environ 130 dossiers**. Une cinquantaine de rapprochements seulement se sont révélés non pertinents. Les autres rapports de rapprochement n'ont pas fait l'objet d'une vérification par les enquêteurs. La cellule SALVAC, qui a pour ambition de devenir l'**interlocuteur privilégié des enquêteurs dans le domaine des crimes et délits sériels**, fait preuve de **réactivité** lorsqu'une demande émane spontanément d'un service enquêteur. Les analystes reçoivent ainsi **deux à trois demandes spontanées par semaine** et y répondent immédiatement. Dans le cadre d'une garde à vue, une **procédure d'urgence** peut

même être enclenchée. Par ailleurs, la cellule SALVAC tente de travailler à partir d'**informations actualisées**, en enregistrant le plus rapidement possible les dossiers qui lui remontent. Les fonctionnaires affectés à la cellule SALVAC sont parvenus à réduire le stock d'affaires en souffrance et aujourd'hui, un dossier est enregistré dans les six mois.

Ces taux de réussite peuvent paraître faibles au premier abord, mais ils s'expliquent en partie par la **nécessaire montée en charge du fichier**. En effet, si celui-ci comporte aujourd'hui environ **9 900 entrées**, il a fallu attendre que le chiffre de 5 000 soit atteint pour disposer de résultats tangibles. Par ailleurs, une partie des rapports de rapprochement rendus par la cellule SALVAC n'a pas été évaluée par les enquêteurs destinataires du rapport, ceux-ci ne souhaitant parfois pas rouvrir d'anciens dossiers.

Divers problèmes nuisant à l'efficacité du travail de la cellule ont été rapportés à la mission d'information. Tout d'abord, la cellule SALVAC connaît un véritable **problème d'effectifs**, les policiers mutés dans d'autres services n'étant actuellement pas remplacés. La cellule ne compte aujourd'hui que 9 personnes, au lieu des quinze équivalents temps plein prévus. Cela nuit assurément à la rapidité avec laquelle les données sont intégrées et les rapprochements effectués.

Par ailleurs, le *turn over* actuel dont souffrent les effectifs induit une **perte de compétences particulièrement dommageable**. En effet, ce sont souvent de jeunes officiers de police judiciaire qui postulent à l'OCRVP, pensant devenir *profilers*. Mais ils ressentent assez rapidement le besoin de retourner sur le terrain. Or, la formation complète d'un analyste prend trois à quatre ans environ. Il n'y a donc pas de retour sur investissement possible dans un tel schéma. À l'inverse, il conviendrait de recruter des enquêteurs relativement avancés dans leurs carrières, plus aguerris, afin de gagner en crédibilité vis-à-vis des services locaux.

Ensuite, l'efficacité du travail fourni par les analystes repose sur la qualité du questionnaire rempli par les enquêteurs. Or, c'est là une **tâche complexe pour les services de police et de gendarmerie**. La **remontée des données est relativement mauvaise**, surtout en ce qui concerne la police nationale, qui ne retourne que 50 % des questionnaires envoyés, contre 80 % pour la gendarmerie. Cet écart s'explique également par le fait que la police est destinataire d'un plus grand nombre de questionnaires que la gendarmerie, du fait de son champ de compétence.

De fait, **le questionnaire ne semble pas être la priorité des services**. Les enquêteurs, surtout au début de l'enquête, ne souhaitent pas passer deux à trois heures à remplir un questionnaire dont ils ignorent généralement l'utilité. De même, les **questionnaires complémentaires sont rarement renseignés** lorsque de nouvelles informations parviennent aux enquêteurs, si bien que la mise à jour du fichier SALVAC se fait souvent par la presse. Toutefois, il est apparu que **certains enquêteurs utilisaient le canevas du questionnaire SALVAC pour mener leurs auditions, preuve de son utilité**.

De façon générale, il apparaît que la cellule SALVAC pourrait bénéficier d'un effort de sensibilisation et de formation. **La formation des enquêteurs constitue un moment propice à la découverte de la cellule SALVAC**. L'inclusion d'un module SALVAC dans la formation des officiers de police judiciaire est actuellement à l'étude. Cela permettrait de cibler l'information sur ceux qui y auront ensuite recours. En outre, l'amélioration de la qualité des données pourrait passer par la désignation d'un **référent local SALVAC**. Celui-ci aiderait les enquêteurs à remplir le questionnaire SALVAC, assurant ainsi la fiabilité des données remontées à la cellule SALVAC, à l'image de ce qui se pratique au sein de la 2e division de police judiciaire de Paris (1).

Proposition n° 6

Désigner, au sein de chaque service de police judiciaire, un référent SALVAC formé au questionnaire et qui jouerait le rôle d'intermédiaire auprès de la cellule.

B. LE FIJAISV, UN FICHIER INDISPENSABLE MAIS FAILLIBLE

Les fichiers de police tiennent une place de plus en plus importante dans la prévention de la récidive des auteurs de violence sexuelle. Notamment, le fichier judiciaire automatisé des auteurs d'agressions sexuelles et violentes (FIJAISV) a vocation à assurer un véritable contrôle social sur les délinquants sexuels. Toutefois, plusieurs freins aussi bien législatifs que culturels limitent aujourd'hui sa portée et son efficacité.

1. Un contrôle social reposant sur une obligation de justification d'adresse

Le FIJAISV assure un suivi automatisé et individualisé des auteurs de violences sexuelles condamnés par la justice, qui sont soumis, par la loi, à des obligations variables de justification d'adresse. Mais il est également utilisé quotidiennement par les services de police et de gendarmerie, dans le cadre d'enquêtes portant sur des crimes et délits à caractère sexuel, afin de faciliter l'identification de leurs auteurs.

a) Un fichier dont la vocation est d'assurer un contrôle social sur les délinquants sexuels

Le fichier judiciaire automatisé des auteurs d'agressions sexuelles et violentes (FIJAISV) n'est pas, à proprement parler, un fichier de police, puisqu'il est placé sous la responsabilité du ministère de la Justice. Néanmoins, ce fichier exigeant, pour son fonctionnement, le concours des forces de l'ordre, il a paru nécessaire à vos rapporteurs de s'y intéresser. **Créé par la loi n° 2004-204**

(1) Idem.

du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, ce fichier ne concernait initialement que des auteurs d'infractions à caractère sexuel. Depuis l'entrée en vigueur de la loi n° 2005-1549 du 12 décembre 2005 relative au traitement de la récidive des infractions pénales, **certains auteurs de crimes et délits violents peuvent également être inscrits au FIJAISV**.

LE FIJAISV, UN FICHIER GÉRÉ PAR LA POLICE MAIS ADMINISTRÉ PAR LA JUSTICE

Le FIJAISV vise à prévenir la récidive **des auteurs d'infractions sexuelles ou violentes** déjà condamnés et à faciliter l'identification des auteurs de ces infractions. Y sont inscrites les personnes condamnées, même non définitivement, à des infractions sexuelles ou violentes ou encore les personnes ayant exécuté une composition pénale, mises en examen par une juridiction d'instruction, ayant fait l'objet d'un non-lieu, d'une relaxe, ou d'un acquittement fondé sur des motifs tenant à l'abolition des facultés de discernement, mais aussi les ressortissants français ayant été condamnés à l'étranger pour de telles infractions. Il compte aujourd'hui environ **54 900 personnes**.

Le FIJAISV est alimenté par le procureur de la République s'agissant des condamnations prononcées même de façon non définitive, des compositions pénales et des décisions fondées sur l'irresponsabilité pénale du mis en cause. L'inscription est faite **par le juge d'instruction** en cas de mise en examen assortie d'un placement sous contrôle judiciaire ou d'assignation à résidence avec surveillance électronique. Enfin, pour les condamnations prononcées par des juridictions étrangères, c'est le procureur de la République ou le service gestionnaire du fichier destinataire des avis adressés aux autorités françaises qui sont en charge de l'inscription.

Le service gestionnaire du FIJAISV est le service du Casier judiciaire national, qui dépend de la direction des affaires criminelles et des grâces du ministère de la Justice. Il est situé à Nantes. Il est composé de quatre personnes, et d'un magistrat référent.

Le FIJAISV fait mention des éléments d'identité (nom, prénom, sexe, date et lieu de naissance, nationalité, alias éventuel, et dans certains cas, la filiation), **de l'adresse de la personne inscrite et de la décision de justice fondant l'inscription au fichier** (nature de l'infraction, nature et date de la décision, peines ou mesures prononcées, juridiction les ayant prononcées, date et lieu des faits commis). Les personnes inscrites au fichier doivent notifier tout changement d'adresse aux autorités. La **mise à jour du fichier est alors faite par les services de police ou de gendarmerie**, par l'intermédiaire de moyens de télécommunication sécurisés et après vérification de l'identité de la personne inscrite au fichier.

Ce fichier comporte l'identité, le passé judiciaire et les adresses successives de personnes ayant commis les infractions mentionnées à l'article

706-47 du code de procédure pénale [1]. Les auteurs d'infractions à caractère sexuel sont obligatoirement inscrits au FIJAISV lorsque la peine encourue est supérieure à cinq ans d'emprisonnement. Dans le cas contraire, l'inscription est laissée à l'appréciation des juridictions. Les mêmes règles sont applicables aux décisions émanant des juridictions étrangères [2].

Le but de ce fichier est clairement exprimé à l'article 706-53-1 du code de procédure pénale : « *prévenir le renouvellement des infractions mentionnées à l'article 706-47* » et « *faciliter l'identification de leurs auteurs* ». De fait, les obligations liées à l'inscription au FIJAISV permettent d'exercer un véritable contrôle social sur les individus et les conduit, comme nous l'a indiqué Mme Élise Thévenin-Scott, magistrat référent du FIJAISV [3], à « *se réinterroger périodiquement sur leur comportement passé* ».

b) Un dispositif complexe reposant sur des obligations de justification d'adresse à géométrie variable

Les personnes inscrites au FIJAISV sont soumises à des **régimes de justification d'adresse qui varient en fonction de la gravité de l'infraction** commise. Lorsque la peine encourue est inférieure ou égale à dix ans, la personne inscrite ne justifie son adresse qu'une fois par an. Lorsque la peine encourue est supérieure à dix ans, un régime de justification semestriel s'applique. Toutefois, si la personne en question présente une dangerosité particulière, il est possible de lui appliquer un régime mensuel. Enfin, lorsque la peine encourue est supérieure à dix ans et que la personne est en état de récidive légale, alors le régime mensuel s'applique obligatoirement [4]. Par ailleurs, **tout changement d'adresse doit être notifié dans les quinze jours**.

(1) « Les dispositions du présent titre sont applicables aux procédures concernant les infractions de meurtre ou d'assassinat d'un mineur précédé ou accompagné d'un viol, de tortures ou d'actes de barbarie ou pour les infractions d'agression ou d'atteintes sexuelles ou de proxénétisme à l'égard d'un mineur, ou de recours à la prostitution d'un mineur prévues par les articles 222-23 à 222-31, 225-7 (1°), 225-7-1, 225-12-1, 225-12-2 et 227-22 à 227-27 du code pénal. Ces dispositions sont également applicables aux procédures concernant les crimes de meurtre ou assassinat commis avec tortures ou actes de barbarie, les crimes de tortures ou d'actes de barbarie et les meurtres ou assassinats commis en état de récidive légale. *»*

(2) Article 706-53-2 du code de procédure pénale.

(3) Déplacement du 23 mai 2011 au service du casier judiciaire national (CJN) à Nantes.

(4) Article 706-53-5 du code de procédure pénale.

RÉGIMES DE JUSTIFICATION DES PERSONNES INSCRITES AU FIJAISV

	Peine encourue inférieure à dix ans d'emprisonnement	**Peine encourue supérieure ou égale à dix ans d'emprisonnement**
Par défaut	Régime annuel	Régime semestriel
Circonstance particulière de dangerosité	X	Régime mensuel facultatif
État de récidive légale	X	Régime mensuel obligatoire

Source : déplacement du 23 mai 2011 au service du casier judiciaire national (CJN) à Nantes.

Alors que les personnes inscrites au FIJAISV pouvaient, jusqu'à l'entrée en vigueur de la loi n° 2010-242 du 10 mars 2010 tendant à amoindrir le risque de récidive criminelle et portant diverses dispositions de procédure pénale, **justifier de leur adresse par le biais d'une lettre recommandée avec accusé de réception auprès du service du casier judiciaire national**, seules les personnes résidant à l'étranger disposent aujourd'hui de cette faculté. **Les autres personnes inscrites doivent obligatoirement justifier de leur adresse, physiquement ou par lettre recommandée, auprès d'un service de police ou de gendarmerie**. Cela a largement contribué à améliorer le contrôle social exercé sur ces individus par le biais du fichier et a permis aux commissariats de police et aux brigades de gendarmerie d'acquérir une **connaissance plus fine des auteurs de violences sexuelles de leur secteur géographique**.

DISPOSITIONS NOUVELLES RELATIVES AU FIJAISV INTRODUITES PAR LA LOI DU 10 MARS 2010 VISANT À AMOINDRIR LE RISQUE DE RÉCIDIVE

L'article 12 de la loi du 10 mars 2010 visant à amoindrir les risques de récidive introduit plusieurs modifications dans le fonctionnement du FIJAISV :

- Seules les personnes résidant à l'étranger peuvent justifier leur adresse auprès du Casier judiciaire national ;

- Le texte permet de sanctionner le fait, pour une personne, de ne pas justifier de son adresse immédiatement après la notification de son inscription au fichier, et non plus au bout d'un an ;

- Les personnes condamnées pour des crimes ou des délits passibles de dix ans d'emprisonnement doivent toutes, mêmes celles dont les condamnations ne sont pas définitives, justifier de leur adresse tous les six mois. Par cohérence, ces obligations cessent toutefois de s'appliquer lorsque la personne est incarcérée ;

- L'information de la personne inscrite au fichier peut désormais se faire par recours à la force publique, après autorisation du procureur de la République, si la notification à la personne ou l'envoi d'une lettre recommandée n'ont pas pu être réalisés ;

- Le fichier est désormais accessible aux greffes des établissements pénitentiaires, qui peuvent accéder au FIJAISV pour y faire figurer les dates d'incarcération et de libération d'un condamné enregistré dans ce fichier.

- Afin d'améliorer les capacités d'investigation des services de police et de gendarmerie, la loi donne la possibilité aux officiers de police judiciaire de consulter le FIJAISV dans le cadre de leurs investigations, sans qu'une garde à vue soit nécessaire ;

- Le service gestionnaire du FIJAISV informe le service gestionnaire du fichier des personnes recherchées des effacements liés au décès de la personne, à l'enregistrement de la date de notification ou à l'effacement judiciaire de l'inscription, qui rendent nécessaire l'effacement du fichier des personnes recherchées ;

- Le texte permet d'accélérer l'inscription au fichier des personnes recherchées (FPR) des personnes inscrites au FIJAISV qui ne résident plus à l'adresse indiquée, en prévoyant que le procureur de la République inscrit désormais « *sans délai* » cette personne au FPR.

c) Un fichier utilisé quotidiennement par les services enquêteurs

Ce fichier permet également, comme l'a indiqué à vos rapporteurs la brigade des mineurs de la direction territoriale de la sécurité de proximité du Val-de-Marne [(1)], de **faciliter la localisation et l'identification d'auteurs d'agressions sexuelles**. Lorsque l'agresseur est inconnu, le FIJAISV permet de repérer les auteurs d'infractions à caractère sexuel résidant dans un périmètre géographique donné. Il est alors possible, en comparant le signalement dont les policiers disposent aux fiches issues du STIC-Canonge, de trouver l'auteur des faits, si tant est qu'il ait déjà été condamné pour des faits semblables.

Mais le FIJAISV représente également un intérêt certain pour les personnes connues. Il a ainsi été indiqué à vos rapporteurs que, dans le cas d'un individu ayant transmis son numéro de téléphone à de jeunes filles à travers la grille d'un collège, se rendant ainsi coupable de corruption de mineurs [(2)], l'interrogation du FIJAISV avait permis de savoir s'il était connu de la justice pour des faits de même nature et s'il faisait l'objet d'une alerte pour non justification d'adresse. Ce fichier constitue donc une aide à l'enquête non négligeable pour les services de police.

2. Des failles juridiques et des dysfonctionnements qui suscitent le malaise des forces de l'ordre

Le FIJAISV fait aujourd'hui l'objet de plusieurs critiques, qui tiennent tant à l'existence de certaines failles juridiques, qu'à une pratique policière et judiciaire parfois peu adaptée. Si d'importantes modifications ont été récemment apportées, il n'en reste pas moins que ce fichier fait porter sur les forces de l'ordre et les magistrats des responsabilités qui dépassent largement les capacités de ce traitement de données à caractère personnel.

a) La faible application du suivi mensuel pour les délinquants sexuels les plus dangereux

Si l'utilité du FIJAISV est avérée, le cadre juridique entourant ce fichier est perfectible. En effet, plusieurs éléments ont été portés à la connaissance de vos rapporteurs qui indiquent que le fonctionnement du FIJAISV n'est pas tout à fait satisfaisant aujourd'hui.

En premier lieu, une **faille juridique importante** a été soulevée par Mme Élise Thévenin-Scott, magistrate en charge du FIJAISV [(3)], en matière de **suivi mensuel des récidivistes**. Le régime mensuel est obligatoire pour les personnes ayant commis des infractions punies de dix ans d'emprisonnement et en état de récidive légale. Toutefois, cette obligation juridique est soumise à une décision expresse des juridictions de jugement ou d'application des peines,

(1) Déplacement du 24 mars 2011 à la direction territoriale de la sécurité de proximité du Val-de-Marne.
(2) Idem.
(3) Déplacement du 23 mai 2011 au service du casier judiciaire national (CJN) à Nantes.

comme le dispose l'article 706-53-5 : « *Si la dangerosité de la personne le justifie, la juridiction de jugement ou, selon les modalités prévues par l'article 712-6, le juge de l'application des peines peut ordonner que cette présentation interviendra tous les mois. Cette décision est obligatoire si la personne est en état de récidive légale*. »

Une circulaire du Garde des sceaux [(1)]précise d'ailleurs que « *la juridiction de jugement condamnant une personne en état de récidive légale pour un crime ou un délit puni de 10 ans d'emprisonnement mentionné à l'article 706-47 du code de procédure pénale doit obligatoirement ordonner que la personne sera inscrite au FIJAIS sous le régime de la présentation mensuelle. Le dispositif de la décision de condamnation doit donc expressément et obligatoirement mentionner une telle mesure* ».

Or, il semble que les magistrats omettent parfois de préciser que le régime mensuel s'applique, si bien que le nombre de personnes inscrites au FIJAISV et qui répondent à ce régime est inférieur à ce qu'il devrait être si le droit était correctement appliqué. En effet, **seules 14 personnes inscrites au FIJAISV font l'objet d'un suivi mensuel obligatoire**. Il conviendrait donc de supprimer cette condition ou, à tout le moins, de permettre à la cellule FIJAISV de réparer les oublis des juridictions. Par ailleurs, **les juridictions prononcent assez rarement le suivi mensuel possible en cas de dangerosité de la personne** et devraient être encouragées dans cette voie. Enfin, il serait souhaitable que le procureur, qui représente les intérêts de la société, puisse également demander un suivi mensuel dans le cadre de l'application des peines.

Proposition n° 7

Modifier la loi afin que l'obligation de justification mensuelle d'adresse soit appliquée de façon effective.

b) Un taux important de défaut de notification qui fragilise le dispositif

Il est également apparu qu'**un problème majeur existait en matière de notification**. La notification à la personne est en effet indispensable au déclenchement du dispositif prévu par le FIJAISV, puisqu'elle constitue le point de départ des obligations qui incombent à la personne inscrite au fichier. Lorsque la personne est détenue, la notification de son inscription au FIJAISV intervient au moment de sa libération. Ce système fonctionne relativement bien, l'administration pénitentiaire étant en charge de la notification et envoyant ensuite le procès-verbal de notification à la cellule FIJAISV [(2)]. Elle sera d'ailleurs bientôt

(1) Circulaire de la DACG n° CRIM 08 - 16/Q du 29 octobre 2008 concernant l'application de l'article 42 de la loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance et du décret d'application n° 2008-1023 du 6 octobre 2008.

(2) Cf. Annexe n° 11.

en mesure d'enregistrer elle-même les informations dans le fichier, grâce à la loi du 10 mars 2010 visant à amoindrir les risques de récidive, qui a rendu le fichier accessible aux greffes des établissements pénitentiaires (1).

En revanche, lorsque la personne n'est pas incarcérée, la notification peut intervenir, en principe, directement après le jugement. Elle est alors effectuée par le bureau d'exécution des peines, ou à la fin de l'audience, par la juridiction. Cela n'est toutefois possible que lorsqu'il existe un bureau d'exécution des peines ou que le condamné est présent à l'audience. Ainsi, **seules 15 % des notifications sont réalisées à l'audience** (2), alors même que c'est là le moment le plus propice pour expliquer à la personne ses obligations judiciaires. Si la notification n'a pas pu intervenir à ce moment-là, elle se fait par lettre recommandée voire par un officier de police judiciaire. Mais, là encore, cela suppose que la personne réside à une adresse connue. Ainsi, **près de 9 000 personnes sont inscrites au FIJAISV sans pour autant être suivies, faute de notification** (3).

c) Un mécanisme d'alerte récemment amélioré mais encore perfectible

En outre, les récentes affaires judiciaires ont révélé une **faille importante du dispositif d'alerte du FIJAISV**. En cas de non justification d'adresse, une alerte est automatiquement émise par le logiciel FIJAISV. Tous les matins, ces alertes sont envoyées au ministère de l'Intérieur, qui les transmet automatiquement aux communes concernées, afin que les forces de police ou de gendarmerie diligentent une enquête. Si la personne n'est pas retrouvée, un magistrat est saisi pour permettre son inscription au fichier des personnes recherchées. De fait, l'inscription au FPR d'une personne défaillante pouvait, il y a peu de temps encore, prendre plusieurs mois (4). Deux circulaires (5) ont cependant permis qu'à l'avenir, les enquêteurs chargés de l'alerte prennent contact sans délai avec le parquet, afin que celui-ci inscrive la personne au FPR avant même la fin de l'enquête proprement dite. Depuis février 2011, l'inscription d'une personne en défaut de justification d'adresse est presque immédiate (6) (7).

---

(1) Article 12 de la loi n° 2010-242 du 10 mars 2010 tendant à amoindrir le risque de récidive criminelle et portant diverses dispositions de procédure pénale.

(2) Déplacement du 23 mai 2011 au service du casier judiciaire national (CJN) à Nantes.

(3) Idem.

(4) Par exemple, Tony Meilhon a fait l'objet d'une alerte FIJAISV le 1er septembre 2010, mais n'a été inscrit au FPR que le 4 janvier 2011.

(5) Circulaire de la direction des affaires criminelles et des grâces n° CRIM 210-10/E8 du 19 mai 2010 relative à la présentation des dispositions de la loi n° 2010-242 du 10 mars 2010 tendant à amoindrir le risque de récidive criminelle et portant diverses dispositions de procédure pénale et n° CRIM-AP 09.910.D2 du 28 janvier 2011 relative au suivi des personnes inscrites au FIJAISV.

(6) Audition du 7 avril 2011 de M. Éric Brendel, chef du service central de documentation criminelle de la police nationale (SCDC), et du Colonel Francis Hubert, chef du service technique de recherches judiciaires et de documentation de la gendarmerie nationale (STRJD).

(7) Cf. Annexe n° 12.

LES ALERTES ÉMISES PAR LE FIJAISV

Le ministère de l'Intérieur est informé quotidiennement par le service gestionnaire du FIJAISV des nouvelles inscriptions, des changements d'adresse et des défauts de justification d'adresse. **L'application génère automatiquement des alertes en direction du ministère de l'Intérieur, c'est-à-dire des messages d'information sécurisés transmis quotidiennement par le fichier**. Ces alertes sont envoyées 8 jours après la date anniversaire de la justification d'adresse, afin de prendre en compte la possibilité de justifier de son adresse par lettre recommandée. **Le ministère de l'Intérieur ne stocke pas ces informations**. Cela lui permet d'informer les commissariats et les brigades de gendarmerie territorialement compétents. Ces messages contiennent le code de la commune (« *code commune* ») concernée par l'alerte, ce qui assure la transmission immédiate du message aux commissariats locaux. **L'ensemble est entièrement dématérialisé et automatisé**. Il existe deux types d'alertes, les premières qui informent un service de l'inscription au FIJAISV d'une personne demeurant dans sa circonscription ou de son changement d'adresse, les secondes informant le service que la personne inscrite est en défaut de justification d'adresse. En cas de défaut de justification, le service de police ou l'unité de gendarmerie destinataire l'alerte devra en accuser réception et renseigner l'écran de justification du FIJAISV, après vérification concrète de la situation de la personne concernée et sans délai.

En outre, les **alertes émises en cas de défaut d'adresse, trop nombreuses** du fait de l'élargissement progressif du champ du fichier, motivent insuffisamment les services locaux de police et de gendarmerie qui doivent établir la nouvelle adresse du délinquant. **Au total, ce sont près de 2 500 alertes qui sont émises chaque mois** (1). Il a également été indiqué à vos rapporteurs que ces notifications sous format papier étaient fréquemment égarées et qu'il était dès lors nécessaire aux fonctionnaires de police de consulter d'eux-mêmes le fichier pour comptabiliser les alertes et mener à bien les diligences exigées par la loi (2).

Concernant **l'inscription au fichier des personnes recherchées** (FPR), celle-ci intervient désormais théoriquement plus rapidement. Néanmoins, elle repose en grande partie sur la réactivité du service inscripteur. Or, en ce qui concerne la police nationale, la cellule du service central de documentation criminelle de la police nationale chargée du FPR est en sous-effectif et accuse un retard de près de 4 500 fiches (3). Si la priorité est donnée aux demandes urgentes, arrivant par téléphone, mail ou fax, qui sont alors traitées dans les 24 heures, **il est possible que l'inscription soit retardée si la demande est faite par simple**

(1) Déplacement du 23 mai 2011 au service du casier judiciaire national (CJN) à Nantes.
(2) Déplacement du 11 juillet 2011 au commissariat central de Strasbourg.
(3) Déplacement du 16 mai 2011 auprès du service central de documentation criminelle.

courrier [1]. Enfin, l'inscription au FPR, même si elle est réalisée immédiatement, peut prendre jusqu'à une heure et demie, délai jugé trop long par certains.

d) Le découragement des forces de l'ordre

Le FIJAISV est aujourd'hui un fichier dont les finalités sont mal comprises du grand public. Comme il a été indiqué à vos rapporteurs, ce fichier est à l'origine d'un **malaise certain au sein des forces de l'ordre**. En effet, à chaque fois qu'un délinquant sexuel inscrit au FIJAISV récidive, la police est mise en cause, alors même qu'aucune faute des services de police n'est établie par l'inspection générale de la police nationale (IGPN). Les citoyens ne comprennent pas qu'un délinquant connu des services de police ne soit pas surveillé en permanence. **Le contrôle social exercé par le fichier est de fait un contrôle discontinu**, même si certains délinquants sexuels sont soumis à des obligations plus fortes que d'autres.

Mais **le découragement policier provient également du fait que les personnes défaillantes, lorsqu'elles sont finalement retrouvées, ne subissent pas la peine de deux ans d'emprisonnement et 30 000 euros d'amende** pourtant prévue par l'article 706-53-5 du code de procédure pénale pour défaut de justification d'adresse [2]. Il est ainsi fréquent que les personnes retrouvées déclarent seulement leur nouvelle adresse, sans être déférées devant un magistrat.

Certaines critiques sont également émises en ce qui concerne le fonctionnement même du fichier. En effet, en dépit des obligations qui pèsent sur les personnes qui y sont inscrites, ce fichier répond à un **régime déclaratoire et repose donc en partie sur la bonne foi des personnes qui déclarent leurs adresses**. Ainsi, il est fréquent que les adresses déclarées soient fausses ou incomplètes [3], ce qui rend la tâche des policiers plus complexe.

Par ailleurs, le fichier n'est pas parfaitement à jour, puisque les juridictions connaissent d'importants retards dans l'inscription des personnes au FIJAISV. À ce jour, **il s'écoule en moyenne 110 jours entre la décision judiciaire et l'inscription** proprement dite [4]. Il arrive ainsi fréquemment que des personnes viennent justifier de leur adresse alors qu'elles ne sont pas matériellement inscrites au fichier. Toutefois, 50 % des décisions sont enregistrées dans les deux semaines qui suivent la décision judiciaire.

Enfin, le système d'alerte ne permet pas de distinguer les alertes réellement inquiétantes de celles qui résultent d'un simple oubli de la part des personnes inscrites. Cette **absence de discrimination**, liée à l'informatisation, ne permet donc pas aux services de police de prioriser facilement leurs recherches [5]. La consultation du fichier et du passé judiciaire des individus est alors nécessaire

(1) Déplacement du 16 mai 2011 auprès du service central de documentation criminelle.
(2) Audition du 16 mars 2011 de M. Frédéric Péchenard, directeur général de la police nationale.
(3) Déplacement du 24 mars 2011 à la direction territoriale de la sécurité de proximité du Val-de-Marne.
(4) Déplacement du 23 mai 2011 au service du casier judiciaire national (CJN) à Nantes.
(5) Idem.

pour identifier les alertes les plus pressantes [(1)]. Plus largement, il semble que **l'extension du fichier aux auteurs de crimes violents** nuise à son efficacité et **freine l'émergence d'une véritable culture du FIJAISV**, initialement dédié aux auteurs de crimes et délits à caractère sexuel. Ainsi, comme l'ont indiqué à vos rapporteurs des fonctionnaires de police, « *le système du FIJAISV est aujourd'hui victime de son succès* », ses failles étant en partie imputables à l'extension récente de son champ.

*
* *

(1) Déplacement du 23 mai 2011 au service du casier judiciaire national (CJN) à Nantes.

EXAMEN EN COMMISSION

Au cours de la réunion du mercredi 21 décembre 2011, la Commission examine le rapport d'information de Mme Delphine Batho et M. Jacques Alain Bénisti sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police.

M. le président Jean-Luc Warsmann. Je laisse à présent la parole à Mme Delphine Batho et à M. Jacques Alain Bénisti, rapporteurs de la mission conduite en application de l'article 145-8 du Règlement, pour la présentation du rapport sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police.

M. Jacques Alain Bénisti, rapporteur. Monsieur le président, mes chers collègues, après des travaux qui ont duré plus d'un an, Delphine Batho et moi sommes en mesure de vous présenter aujourd'hui les conclusions de notre second rapport sur les fichiers de police. En effet, en mars 2009, nous vous avions soumis un premier rapport qui formulait cinquante-sept propositions tendant à refondre totalement le cadre législatif des fichiers de police, à améliorer leur efficacité et à mieux assurer la protection des droits et libertés. Ce second rapport rend compte, pour sa part, des suites qui ont été données à ces recommandations, dont beaucoup ont souligné le caractère trop ambitieux.

Comme le premier rapport, celui-ci a vu le jour dans un contexte bien particulier. En octobre 2010, la commission des Lois a auditionné le général Jacques Mignaux, directeur général de la gendarmerie nationale, au sujet de l'existence réelle ou supposée d'un fichier destiné aux gens du voyage. C'est à cette occasion que nous avons demandé, ma collègue Delphine Batho et moi-même, au président Warsmann de nous permettre de réaliser une seconde mission, cette fois en application de l'article 145-8 du Règlement de l'Assemblée nationale.

À partir de novembre 2010, nous avons entendu un nombre important de personnes : le directeur général de la police nationale, M. Frédéric Péchenard, ainsi que, à nouveau, son homologue de la gendarmerie nationale, le général Mignaux ; la Commission nationale de l'informatique et des libertés (CNIL), à trois reprises, avec son président de l'époque, M. Alex Türk, et son secrétaire général ; M. Alain Bauer, président du groupe de contrôle sur les fichiers de police ; les personnes responsables du développement et de la gestion des plus importants fichiers de police que sont le Traitement des antécédents judiciaires (TAJ), qui organise la fusion du Système de traitement des infractions constatées (STIC) et du système judiciaire de documentation et d'exploitation (JUDEX), mais aussi le fichier des personnes recherchées (FPR), le fichier des empreintes génétiques (FNAEG) ou encore le logiciel de rédaction des procédures de la police nationale.

Plus encore que des auditions, nous avons effectué de nombreux déplacements, dans les commissariats et les brigades de gendarmerie, là où sont utilisés, au quotidien, les fichiers de police. La mission s'est ainsi rendue à Laval,

Strasbourg, Écully, siège de la police scientifique et technique, mais aussi, en région parisienne, dans le Val-de-Marne, le Val-d'Oise, à la Préfecture de police de Paris, à Rosny-sous-Bois, au service technique de recherches judiciaires et de documentation de la gendarmerie nationale. Nous nous sommes également rendus auprès de plusieurs offices centraux, comme l'office central pour la répression des violences aux personnes et l'office central de lutte contre délinquance itinérante (OCLDI).

Ces auditions et déplacements nous ont permis de nous forger une opinion éclairée sur le suivi des recommandations du premier rapport. Mais, avant d'aborder plus précisément les conclusions du présent rapport, je souhaiterais vous faire part d'un point de vue plus général sur cette seconde mission. J'ai en effet le sentiment très net que les choses ont changé. Une importante évolution des mentalités a, je crois, été déclenchée par notre premier rapport. Tous les acteurs que nous avons pu rencontrer en ont témoigné : une prise de conscience réelle a eu lieu depuis mars 2009. Une nouvelle culture « Informatique et libertés » semble émerger et se développer sur notre territoire.

Il faut d'ailleurs saluer ici l'œuvre des directions générales de la police et de la gendarmerie nationales, qui ont déployé d'importants efforts pour parvenir à ce résultat : nomination de policiers et de gendarmes aux fonctions de référents et de conseillers « Informatiques et libertés », diffusion de bonnes pratiques et d'outils pédagogiques, développement de formations plus poussées en matière de fichiers de police et d'éthique au sein des écoles de police et de gendarmerie.

Au-delà de ce seul sentiment, je crois que les choses ont évolué de façon plus palpable, par l'important mouvement de régularisation des fichiers de police. La CNIL s'est d'ailleurs prononcée, en 2011, sur une vingtaine de fichiers de police. Un nombre important de décrets a été pris qui assure la conformité au droit d'un plus grand nombre de fichiers. Des textes réglementaires sont également en préparation, qui devraient bientôt aboutir.

Mais, plus encore, je tiens à porter à votre connaissance un élément qui me semble tout à fait pertinent et emblématique du changement de logique qui est intervenu. Pour plusieurs fichiers, leur développement informatique et leur déploiement ont été conditionnés à la parution d'un texte réglementaire les rendant parfaitement conformes à la loi « Informatique et Libertés » de 1978. Tel est le cas pour les fichiers d'information générale que sont le fichier de prévention des atteintes à la sécurité publique et le fichier relatif aux enquêtes administratives liées à la sécurité publique ; nous avons constaté que leur développement informatique n'a débuté qu'après la parution des deux décrets les autorisant. Pour le Traitement des antécédents judiciaires (TAJ), son déploiement sur le territoire national est soumis à la parution prochaine de son décret. Vous me direz que c'est là la moindre des choses ! Mais ce n'est pas ce que nous avions constaté en 2009. Je crois qu'au contraire, cela dénote un véritable changement des pratiques en matière de fichiers de police.

Certes, un certain nombre de fichiers sont, encore aujourd'hui, utilisés de façon illégale, n'ayant pas été soumis à l'avis de la CNIL et à la publication d'un texte réglementaire. Mais si l'on observe plus attentivement les chiffres, ce sont près de 86 % de ces fichiers qui feront, dans un avenir que nous espérons proche, l'objet d'une régularisation. C'est en tout cas ce qui résulte des informations reçues par le ministère de l'Intérieur. Preuve de sa bonne foi, celui-ci s'est doté d'un outil juridique intéressant permettant d'assurer la régularisation massive de fichiers de police développés par des services locaux.

En effet, chaque commissariat, chaque brigade, a développé, pour répondre à ses propres besoins, ce que la CNIL analyse comme des fichiers de police au sens de la loi. Ainsi, il existe un nombre très important de fichiers non déclarés, qui concernent la gestion des fourrières, des assignations à résidence ou des demandes de protection, qui répondent à une même finalité. Dans ce cas, le ministère de l'Intérieur prévoit des actes-cadres qui permettront de régulariser, en une seule fois, ces fichiers aux finalités communes.

Pour ce qui est plus précisément du suivi de nos cinquante-sept recommandations, le bilan est globalement positif. Deux ans et demi après, plus de 40 % d'entre elles ont été, totalement ou partiellement, mises en œuvre. J'ajoute immédiatement, afin que les services de police et de gendarmerie ne soient pas jugés responsables de ce score que certains pourraient juger insuffisant, que, parmi les recommandations aujourd'hui non suivies d'effet, figurent une part importante de recommandations de nature législative, que seul le Parlement pouvait mettre en œuvre.

Mme Delphine Batho, rapporteure. Monsieur le président, mes chers collègues, en 2009, le Parlement s'est saisi, pour la première fois, de la question des fichiers de police et a réalisé, à cette occasion, un important travail d'information. Le rapport que nous vous soumettons aujourd'hui, qui fait le point sur le suivi des recommandations de notre premier rapport d'information, montre qu'il est nécessaire que l'Assemblée nationale reste particulièrement attentive à ce sujet. En effet, la massification du nombre de fichiers et des personnes inscrites dans ces fichiers, déjà soulignée en 2009, s'est poursuivie.

Je souhaiterais à ce propos vous faire part des derniers éléments quantitatifs dont nous disposons. Le fichier des antécédents judiciaires de la police nationale, le STIC, est passé, depuis notre dernière mission, de 3,96 millions à 6,5 millions de personnes mises en cause, et de 28 millions à 38 millions de victimes inscrites. En ce qui concerne le FNAEG, nous sommes passés de 800 000 à 1,79 million de Français inscrits dans ce fichier.

De la même façon, alors que nous avions recensé, en 2009, 58 fichiers de police, nous en avons dénombré, au cours de cette mission-ci, près de 80. Certes, un nombre important des nouveaux fichiers recensés existaient au moment de la première mission, mais n'avaient pas été portés à la connaissance du Parlement. C'est une anomalie à laquelle nous tentons de répondre. J'ajoute que le

recensement auquel nous avons procédé cette fois-ci n'est vraisemblablement pas exhaustif. Sur ces 80 fichiers, 62 sont utilisés de façon opérationnelle. La moitié d'entre eux ne disposent pas d'une base juridique solide et n'ont pas fait l'objet d'une déclaration auprès de la CNIL. Toutefois, comme l'a indiqué notre collègue Jacques Alain Bénisti, pour 86 % de ces fichiers non déclarés, des textes réglementaires sont en préparation, dont nous espérons qu'ils permettront une régularisation prochaine de ces fichiers.

Comme l'indiquait Jacques Alain Bénisti, 40 % des recommandations de notre rapport ont été mises en œuvre, ce qui montre qu'une prise de conscience a eu lieu. Pour ma part, j'aurais tendance à souligner que 60 % de nos recommandations n'ont pas été suivies. En particulier, la révolution juridique que nous appelions de nos vœux en matière de fichiers de police, qui devait donner au Parlement un rôle prééminent dans la création de ces fichiers et ainsi, assurer un contrôle démocratique sur ces derniers, n'a pas eu lieu. C'était là l'objet de la proposition de loi, co-signée par Jacques Alain Bénisti et moi-même, qui n'a cependant pas pu aboutir compte tenu de l'opposition du Gouvernement.

Certes, par la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure dite « LOPPSI II », un nouveau cadre a été donné à certaines catégories de fichiers, comme les fichiers de rapprochement. Mais, outre que ce cadre ne correspond pas aux finalités d'importants fichiers comme CORAIL et LUPIN, du fait de la décision du Conseil constitutionnel qui a suivi le vote de cette loi, l'existence d'un cadre juridique au sein du code de procédure pénale n'empêche nullement le pouvoir réglementaire de déclarer certains fichiers sur le fondement de l'article 26 de la loi « Informatique et Libertés ». La situation, de ce point de vue, est donc toujours insatisfaisante. Une seule recommandation, parmi les modifications législatives que nous proposions, a été suivie d'effet : la représentation pluraliste des parlementaires membres de la CNIL, qui devrait être appliquée d'ici peu, lors du renouvellement de ses membres.

La protection des droits et libertés était également une de nos préoccupations majeures. Nous avions en effet défendu l'idée selon laquelle une meilleure protection des droits et libertés des citoyens dans l'utilisation de leurs données personnelles et une meilleure performance des fichiers de police utilisés par les policiers et gendarmes, loin d'être des objectifs contradictoires, allaient de pair. Des données ciblées et précises doivent assurer tout à la fois la fiabilité et l'efficacité des fichiers, mais également la protection des droits et libertés. Nous avions ainsi formulé une trentaine de recommandations visant à améliorer cette protection.

Certaines de ces recommandations ont été suivies d'effet : un point de droit a été clarifié en matière de prélèvement biologique pour une inscription au FNAEG, qui permet de mieux les encadrer ; le délai de réponse du procureur aux demandes de rectification a été réduit à un mois par la loi d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011,

conformément à nos recommandations ; s'il n'existe, pour l'heure, aucun traitement en temps réel pour les demandes de rectification, un magistrat référent est prévu par la loi, qui sera l'interlocuteur privilégié des personnes inscrites au sein de fichiers de police.

Cependant, comme le montre un graphique figurant dans notre rapport que nous vous soumettons aujourd'hui, le nombre de dossiers en souffrance à la CNIL, pour l'exercice du droit concret d'accès indirect des citoyens, a encore augmenté, ce qui explique les importants délais de traitement dont pâtissent ces demandes, de l'ordre d'un an à un an et demi.

En matière d'information générale, certaines de nos recommandations ont également été suivies, en ce qui concerne par exemple le fichier de prévention des atteintes à la sécurité publique, qui a vocation à remplacer le fichier EDVIGE. Un fichier distinct a, par ailleurs, été créé, comme nous le demandions, en matière d'enquêtes administratives. Le fichier alphabétique de renseignement de la gendarmerie nationale, composé de fiches en papier, a bel et bien été détruit. Les modalités de conservation des données relatives aux mineurs ont également évolué dans le sens d'un véritable droit à l'oubli.

Le bât blesse, en revanche, en matière de données sensibles. Certes, des garde-fous ont été posés en ce qui concerne les activités politiques, syndicales ou associatives au sein des fichiers d'information générale. En revanche, demeure la possibilité dans les fichiers de renseignements de la police comme de la gendarmerie, d'indiquer l'origine géographique des personnes. Si mon collègue Jacques Alain Bénisti y est favorable, je considère qu'il s'agit là d'une façon détournée d'évoquer l'origine ethnique réelle ou supposée des personnes. En revanche, nous avions proposé, Jacques Alain Bénisti et moi-même, l'abandon de la typologie ethno-raciale utilisée par le STIC-Canonge et son remplacement par des éléments objectifs de portrait robot. Nous regrettons que cette recommandation n'ait pas été suivie.

En ce qui concerne la question du fichier MENS, qui est à l'origine de cette nouvelle mission qui nous a été confiée, le rapport fait état des contrôles opérés par la CNIL et des résultats de notre déplacement auprès de l'office central de lutte contre la délinquance itinérante. La CNIL, lors de ces contrôles à l'office central de lutte contre la délinquance itinérante, a relevé de nombreuses irrégularités, notamment l'utilisation d'un fichier non déclaré, dans lequel figurent environ 52 000 personnes. Si nous n'avons pas connaissance de l'utilisation, aujourd'hui, d'un fichier fondé sur des bases ethniques, certaines données sensibles de cette nature continuent d'être collectés dans ces fichiers. Pour ma part, je crois que le fichier MENS dont il a été question en octobre 2010 a pu être, en réalité, le fichier Généatic, détruit en 2007.

La troisième partie de notre rapport porte sur les progrès en matière d'utilisation des fichiers. Notre collègue Jacques Alain Bénisti a d'ores et déjà évoqué les évolutions positives intervenues dans ce domaine, sur lesquelles je ne

reviens donc pas. Je tiens cependant à préciser que le fichier qui a vocation à remplacer le STIC et JUDEX, qui s'est, un temps, appelé ARIANE, puis Traitement des procédures judiciaires, et qui se nomme aujourd'hui TAJ, devrait commencer à être déployé au cours du premier semestre 2012. Si la gendarmerie nationale a réalisé un important effort de nettoyage de leur base de données, nous regrettons que la police nationale n'ait pas fait de même. En effet, cela signifie qu'une part importante des données erronées contenues dans le STIC va être transmise à ce nouveau fichier. Par ailleurs, nous souhaiterions insister sur la nécessité de moderniser le fichier des personnes recherchées, qui est aujourd'hui le fichier le plus utilisé par les forces de l'ordre, avec près de 10 millions de consultations par an. Cet outil est aujourd'hui parfaitement obsolète, ce qui soulève d'importants problèmes opérationnels. Un effort particulier doit donc être accompli pour développer une nouvelle version de ce fichier.

Par ailleurs, a été portée à notre connaissance l'existence des problèmes techniques récurrents d'indisponibilité des fichiers de police, liés à la vétusté du réseau informatique de la police nationale et à l'accroissement de leur utilisation. Pour finir, nous avons souhaité porter une attention particulière aux fichiers de lutte contre la délinquance sérielle de nature sexuelle. Notre rapport décrit de façon précise les difficultés du fichier SALVAC comme du fichier judiciaire automatisé des auteurs d'infractions sexuelles ou violentes et propose plusieurs améliorations.

M. Philippe Gosselin. Je me réjouis des avancées présentées par le rapport de nos collègues. Certes, il existe sans doute des points à améliorer. Néanmoins, étant par nature quelqu'un de positif, je constate que l'état d'esprit, comme les pratiques, ont réellement changé. Ces progrès sont à mettre au bilan du Gouvernement mais aussi de l'ensemble des acteurs, qui ont tenté de faire progresser la question des fichiers.

Il ressort de cet excellent rapport que la régularisation des fichiers, par rapport à la situation de 2009, a nettement progressé, puisque 86 % des fichiers non déclarés vont faire l'objet d'une régularisation et d'une mise en conformité rapide avec les textes. Certes, les esprits chagrins souligneront que 14 % ne font actuellement l'objet d'aucun texte réglementaire en cours d'élaboration. Mais je note qu'en 2011, de nombreux fichiers ont été régularisés et que de nombreux textes réglementaires ont été pris. La CNIL a adopté de nombreux avis, ce dont je peux témoigner en tant que membre de cette commission.

Il convient de souligner qu'une véritable culture de l'informatique et des libertés se développe et qu'une réelle prise de conscience a eu lieu, ce à quoi le précédent rapport d'information a incontestablement contribué.

Une précision mérite d'être apportée s'agissant du pluralisme de la CNIL évoqué par Mme Delphine Batho. Ce pluralisme existe déjà puisque le Sénat vient de désigner M. Gaëtan Gorce comme commissaire.

M. le président Jean-Luc Warsmann. Je tiens à remercier Delphine Batho et Jacques Alain Bénisti pour ce travail considérable. En effet, leurs travaux ont indéniablement fait avancer ce sujet au cours de la législature. Et ce dernier rapport met utilement en lumière les efforts qu'il reste à faire.

La Commission autorise à l'unanimité le dépôt du rapport d'information en vue de sa publication.

SYNTHÈSE DES PROPOSITIONS

Proposition n° 1 : modifier rapidement le cadre juridique des fichiers de police conformément aux recommandations n° 1 à 10 du précédent rapport.

Proposition n° 2 : donner très rapidement une base juridique solide aux fichiers de police d'ores et déjà utilisés par les forces de l'ordre et qui correspondent à un besoin réel des services.

Proposition n° 3 : donner un cadre législatif adapté aux fichiers de rapprochements en matière de petite et moyenne délinquance sérielle et conforme à la décision du Conseil constitutionnel.

Proposition n° 4 : moderniser rapidement le fichier des personnes recherchées, afin d'en faire un outil performant et réactif.

Proposition n° 5 : engager un chantier de modernisation des infrastructures de réseaux de la police nationale.

Proposition n° 6 : désigner, au sein de chaque service de police judiciaire, un référent SALVAC formé au questionnaire et qui jouerait le rôle d'intermédiaire auprès de la cellule.

Proposition n° 7 : modifier la loi afin que l'obligation de justification mensuelle d'adresse soit appliquée de façon effective.

GLOSSAIRE

ANACRIM	Analyse Criminelle
ARDOISE	Application de recueil de la documentation opérationnelle et d'informations statistiques sur les enquêtes
ARIANE	Application de rapprochements, d'identification et d'analyse pour les enquêteurs
BDRIJ	Brigade départementale de renseignements et d'investigations judiciaires
BDSP	Base de Données de Sécurité Publique
CASSIOPEE	Chaîne Applicative Supportant le Système d'Information Opérationnel pour le Pénal et les Enfants
CHEOPS	Circulation hiérarchique des enregistrements opérationnels de police sécurisés
CNIL	Commission nationale de l'Informatique et des Libertés
CORAIL	Cellule Opérationnelle de Rapprochements et d'Analyse des Infractions Liées
DLPAJ	Direction des libertés publiques et des affaires juridiques
DCRI	Direction centrale du renseignement intérieur
DCSP	Direction Centrale de la Sécurité Publique
DGGN	Direction Générale de la Gendarmerie Nationale
DGPN	Direction Générale de la Police Nationale
DSIC	Direction des Systèmes d'Information et de Communication
EASP	Enquêtes Administratives Liées à la Sécurité Publique
EDVIGE	Exploitation Documentaire et Valorisation de l'Information
EDVIRSP	Exploitation documentaire et la valorisation de l'information relative à la sécurité publique

FAED	Fichier Automatisé des Empreintes Digitales
FBS	Fichier des Brigades Spécialisées
FNAEG	Fichier National des Empreintes Génétiques
FVV	Fichier des Véhicules Volés
FIJAISV	Fichier judiciaire national automatisé des auteurs d'infractions sexuelles et violentes
FOVeS	Fichier des Objets Volés et des véhicules Signalés
FPR	Fichier des personnes recherchées
FRG	Fichier des Renseignements Généraux
FAR	Fichier Alphabétique du Renseignement
GEVI	Gestion des violences urbaines
JUDEX	Système Judiciaire de Documentation et d'Exploitation
IGA	Inspection générale de l'administration
IGPN	Inspection générale de la police nationale
LRPGN	Logiciel de Rédaction des Procédures de la Gendarmerie Nationale
LUPIN	Logiciel d'Uniformisation des Procédures d'Identification
LRPPN	Logiciel de Rédaction des Procédures de la Police Nationale
LRPSI	Logiciel de Rédaction des Procédures de la Sécurité Intérieure
MENS	Minorités Ethniques Non Sédentarisées
OCLDI	Office Central de Lutte contre la Délinquance Itinérante
PASP	Prévention des Atteintes à la Sécurité Publique
SALVAC	Système d'Analyse et de Liens de la Violence Associé au Crime
SCDC	Service Central de la Documentation Criminelle
SDIG	Sous-Direction de l'Information Générale

SDIG	Service Départemental de l'Information Générale
STIC	Système de Traitement des Infractions Constatées
ST(SI)²	Service des Technologies et des Systèmes d'Information de la Sécurité Intérieure
STRJD	Service technique de recherches judiciaires et de documentation
SRDC	Service régional de documentation criminelle
TAJ	Traitement des antécédents judiciaires

LISTE DES PERSONNES AUDITIONNÉES

Mercredi 1er décembre 2010

Commission nationale de l'information et des libertés

- M. Alex TÜRK, président,
- Mme Florence FOURETS, directrice des relations avec les usagers et du contrôle,
- Mme Sophie VULLIET-TAVERNIER, directrice des affaires juridiques, internationales et de l'expertise.

Mercredi 26 janvier 2011

- M. Alain BAUER, président du groupe de contrôle sur les fichiers de police.

Mercredi 2 février 2011

Commission nationale de l'information et des libertés

- Mme Florence FOURETS, directrice des relations avec les usagers et du contrôle,
- M. Thierry CARDONA, ingénieur au service des contrôles.

Mercredi 9 mars 2011

- Général Bernard PAPPALARDO, chef du service des technologies et des systèmes d'information de la sécurité intérieure.

Mercredi 16 mars 2011

Direction générale de la police nationale

- M. Frédéric PÉCHENARD, directeur général de la police nationale,
- M. Jean MAFART, conseiller juridique.

Mercredi 23 mars 2011

Direction générale de la gendarmerie nationale

- Général Jacques MIGNAUX, directeur général de la gendarmerie nationale,
- M. Emmanuel DUPIC, magistrat, conseiller juridique et judiciaire,

— Lieutenant-colonel Yvan CARBONNELLE, chargé de projet.

Mercredi 30 mars 2011

Direction centrale de la sécurité publique

— M. Christian HIRSOIL, sous-directeur de l'information générale.

Mercredi 31 mars 2011

— M. Loïc ALIXANT, sous direction de l'information générale,

— MM. Vincent LAFON et Antoine DELOUVRIER, service des technologies et des systèmes d'information de la sécurité intérieure,

— Mme Claude JACOPIN et Mme Sylvia VITERITTI, direction des systèmes d'information et de la communication.

Mercredi 7 avril 2011

— M. Éric BRENDEL, chef du service central de documentation criminelle de la police nationale,

— Colonel Francis HUBERT, chef du service technique de recherches judiciaires et de documentation de la gendarmerie nationale.

Mercredi 11 mai 2011

Association SOS Racisme

— Mme Émilie PERRIER, responsable du pôle anti-discriminations,

— M. Guillaume AYNE, directeur général de l'association SOS Racisme.

Mercredi 18 mai 2011

— M. François FELTZ, procureur général près la cour d'appel d'Orléans et référent FNAEG.

Mercredi 29 juin 2011

Commission nationale de l'information et des libertés

— M. Yann PADOVA, secrétaire général,

— M. Émile GABRIE, service des affaires juridiques,

— M. Geoffroy SIGRIST, attaché parlementaire.

LISTE DES DÉPLACEMENTS EFFECTUÉS

Mardi 17 janvier 2011

Service Technique de Recherches Judiciaires et de Documentation

- Général Jacques HÉBRARD, commandant du pôle judiciaire de la gendarmerie nationale,
- Colonel Francis HUBERT, chef du service technique de recherches judiciaires et de documentation de la gendarmerie nationale (STRJD),
- Lieutenant-Colonel Yvan CARBONNELLE, chargé de projet,
- Lieutenant-Colonel Jacques FOMBONNE, sous-direction de la police judiciaire (SDPJ),
- Lieutenant-Colonel Bernard POPINEAU, commandant la division des opérations judiciaires du STRJD,
- Lieutenant-Colonel Éric FREYSSINET, commandant la division de lutte contre la cybercriminalité du STRJD,
- Lieutenant-Colonel Hubert CHARVET, commandant la division des applications judiciaires du STRJD.

Jeudi 3 février 2011

Préfecture de police de Paris

- Direction du renseignement de la préfecture de police,
- Direction de la sécurité de proximité de l'agglomération parisienne,
- Service régional de l'identité judiciaire de la direction régionale de la police judiciaire de Paris,
- Division de la statistique et de la documentation opérationnelle.

Jeudi 3 mars 2011

3e direction de police judiciaire de Paris

- M. Jean-Jacques HERLEM, directeur adjoint de la DRPJ,
- M. Yves CRESPIN, chef du 3ème district,
- M. Éric FRANCELET, chef du service informatique de la police judiciaire,
- M. Philippe DALBAVIE, conseiller juridique du préfet de police,

– Mme Catherine DUCARRÉ, commandant du service central de documentation criminelle.

Lundi 14 mars 2011

Office central de lutte contre les violences faites aux personnes

– M. Frédéric MALON, chef de l'OCRVP.

Lundi 21 mars 2011

Circonscription de sécurité publique de Cergy

– M. Frédéric AURÉAL, directeur départemental de la sécurité publique,

– M. Jean-Luc FAIVRE, commissaire divisionnaire, chef d'état major de la DDSP du Val d'Oise,

– M. Bertrand CHAMOULAUD, commissaire en charge du service départemental d'information générale.

Brigade de gendarmerie d'Auvers-sur-Oise

– Colonel Philippe CAUSSE, commandant du groupement de gendarmerie départementale du Val d'Oise,

– Lieutenant Frédéric CHASTAN, commandant de la brigade territoriale autonome d'Auvers-sur-Oise.

Jeudi 24 mars 2011

Direction territoriale de la sécurité de proximité du Val de Marne

– M. Jean-Yves OSES, directeur territorial de la sécurité de proximité du Val-de-Marne

– M. Jean-Paul PECQUET, commissaire divisionnaire, directeur territorial adjoint.

Lundi 16 mai 2011

Service central de documentation criminelle, Écully

– M. Bruno PEREIRA COUTINHO, sous directeur de la police scientifique,

– M. Éric BRENDEL, chef du service central de documentation criminelle de la police nationale.

Lundi 23 mai 2011

Institut génétique Nantes-Atlantique

— Pr. Jean-Paul MOISAN, président du conseil d'administration de l'IGNA.

Casier judiciaire national, Nantes

— M. Philippe DELARBRE, magistrat et chef du Casier judiciaire national,

— Mme Élise THÉVENIN-SCOTT, magistrate et référente nationale du FIJAISV.

Mercredi 25 mai 2011

Centre de renseignements et d'opérations de la gendarmerie nationale

— Général de division David GALTIER, directeur des opérations et de l'emploi,

— Colonel Denys MOREE, chef du bureau de la veille opérationnelle et directeur du programme BDSP,

— Lieutenant-Colonel Stéphane DUDOUIT, adjoint,

— Lieutenant-Colonel Stéphane DEPASSIO de la section du système des opérations et du renseignement.

Lundi 27 juin 2011

Commissariat central de Laval, Mayenne

— M. SAUNIER, commissaire divisionnaire,

— M. Freddy BOURGEOIS, officier de police, chef de la brigade d'investigation,

— M. Thierry LE SOUDEER, commandant de police,

— M. David FLAGEUL, capitaine, chef du groupe de voie publique,

— Mme Rachel PECOT, brigadier-chef, brigade des familles.

Lundi 11 juillet 2011

Direction départementale de la sécurité publique du Bas-Rhin

— M. Luc-Didier MAZOYER, contrôleur général, directeur départemental,

— M. Stéphane LACOUR, commissaire divisionnaire, chef du service de sécurité de proximité,

— M. Patrick ROUSSEL, commissaire divisionnaire, chef du service d'investigation et de recherches,

- M. Jacques BLANCK, commandant de police, chef du service de quart,
- M. Christian WETTLING, commandant de police, chef de la brigade criminelle,
- M. Francis BACH, commandant de police, chef d'état-major,
- M. Laurent GUILLO, brigadier chef, responsable du bureau départemental des systèmes d'information et des télécommunications.

ANNEXES

SYNTHÈSE DU SUIVI DES RECOMMANDATIONS		
OBJET DE LA RECOMMANDATION	**SUIVI DES RECOMMANDATIONS**	**PAGE**
Recommandation n° 1 Modifier l'article 13 de la loi du 6 janvier 1978 relatif à la composition de la CNIL, afin que les deux députés et les deux sénateurs, membres de l'autorité de contrôle, soient désignés respectivement par l'Assemblée nationale et par le Sénat, « *de manière à assurer une représentation pluraliste* ».	Mise en œuvre	Partie I, page 17
Recommandation n° 2 Seule la loi doit pouvoir autoriser la création d'un fichier de police. En conséquence, modifier l'article 26 de la loi du 6 janvier 1978, afin que les fichiers ou toute catégorie de fichiers intéressant la sécurité publique et ceux qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ne soient autorisés que par la loi.	Non mise en œuvre	Partie I, page 18

Recommandation n° 3 Toute loi autorisant la création d'un fichier de police devra au minimum préciser l'identité du responsable du traitement, la finalité et la dénomination du traitement ainsi que la description générale de ses fonctions, le service chargé de la mise en œuvre, le service auprès duquel s'exerce le droit d'accès (direct ou indirect), les catégories de données à caractère personnel enregistrées, leur origine et les catégories de personnes concernées par le traitement, les catégories de personnes qui ont accès aux informations enregistrées, les destinataires des informations, les rapprochements et interconnexions, la durée de conservation des données.	Non mise en œuvre	Partie I, page 19
Recommandation n° 4 L'avis de la CNIL sur tout projet de loi autorisant la création de fichiers de police est rendu public et transmis au Parlement simultanément au dépôt, sur le bureau de l'Assemblée nationale ou du Sénat, du projet de loi autorisant la création d'un fichier de police	Non mise en œuvre	Partie I, page 23
Recommandation n° 5 Les projets ou Recommandations de loi autorisant la création de fichiers de police doivent être accompagnés d'une étude d'impact appréciant le volume du fichier considéré ainsi que sa finalité, au regard de l'ensemble des fichiers d'ores et déjà existants. La CNIL sera associée à la réalisation de ces études d'impact préalables.	Non mise en œuvre	Partie I, page 23

Recommandation n° 6 Les projets de loi autorisant la création de fichiers de police doivent prévoir une clause de rendez-vous dans le temps, afin que le Parlement opère à moyen et long terme une évaluation du fichier considéré. Au terme de cette évaluation, qui doit faire l'objet d'un débat en séance publique, le Parlement peut décider de mettre fin, par la loi, au fichier concerné, si la finalité qui avait initialement présidé à sa création n'est plus démontrée.	Non mise en œuvre	Partie I, page 22
Recommandation n° 7 Améliorer les relations de travail entre la CNIL et le ministère de l'Intérieur grâce à la transmission systématique de l'avant-projet de rapport annuel de la CNIL au Ministère de l'Intérieur, afin qu'il puisse formuler toutes les réponses nécessaires aux différentes observations de la CNIL le concernant. L'objectif est de créer, sur le modèle de la Cour des comptes, une procédure contradictoire entre l'autorité de contrôle et les services de police et de gendarmerie, où la première, avant la publication de son rapport définitif, recueille les réponses des seconds aux observations qui leur sont adressées.	Non mise en œuvre	Partie I, page 24
Recommandation n° 8 Étendre la procédure écrite et contradictoire, entre la CNIL et le ministère de l'intérieur, à l'ensemble des traitements de données à caractère personnel mis en œuvre pour le compte de l'État.	Non mise en œuvre	Partie I, page 24

Recommandation n° 9 Créer une procédure de mise en application par étapes des fichiers de police sous le contrôle de la CNIL. En conséquence, introduire dans la loi du 6 janvier 1978 une disposition nouvelle prévoyant que les fichiers relevant de l'article 26 (ceux intéressant la sécurité publique et ceux ayant pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté), une fois autorisés par le législateur et en amont de la publication du décret d'application de la loi, font l'objet, sur le plan technique, d'une procédure de mise en application par étapes, afin qu'ils puissent, à chaque étape clé de leur élaboration et lors de rendez-vous obligatoires, faire l'objet d'une validation conjointe entre la CNIL et le ministère de l'Intérieur.	Non mise en œuvre	Partie I, page 26
Recommandation n° 10 Seule la loi peut autoriser un fichier de police à déroger à l'interdiction de principe, posée par l'article 8 de la loi du 6 janvier 1978, de contenir des données sensibles (origines raciales ou ethniques, opinions politiques, philosophiques ou religieuses, appartenance syndicale et données relatives à la santé et à la vie sexuelle) et ce dans la stricte mesure où les finalités du fichier l'exigent. Modifier en conséquence le IV de l'article 8 de la loi du 6 janvier 1978.	Non mise en œuvre	Partie I, page 21

Recommandation n° 11 Le futur fichier EDVIRSP devra être créé par la loi.	Non mise en œuvre	Partie II, page 47
Recommandation n° 12 D'une part, le fichier EDVIRSP ne concernera que « *les personnes, groupes, organisations et personnes morales qui, en raison de leur activité individuelle ou collective, peuvent porter atteinte à la sécurité des personnes et des biens, par le recours ou le soutien actif apporté à la violence, ainsi que les personnes entretenant ou ayant entretenu un lien direct et non fortuit avec celles-ci* ». D'autre part, un fichier distinct, relatif aux personnes « *faisant l'objet d'enquêtes administratives* » sera créé. Ce traitement de données ne recensera que les personnes ayant fait l'objet d'une décision administrative défavorable.	Mise en œuvre partielle	Partie II, pages 48 et 50
Recommandation n° 13 Prévoir que la collecte et la conservation de données sensibles, dont celles enregistrées dans la catégorie « *signalement* », soient strictement interdites dans le fichier relatif aux enquêtes administratives défavorables.	Mise en œuvre partielle	Partie II, page 58
Recommandation n° 14 de votre Rapporteur Conserver, au titre des données sensibles susceptibles d'être collectées et conservées dans EDVIRSP, la notion d'« *origine géographique* » comme élément de signalement des personnes.	Mise en œuvre	Partie II, page 63

Recommandation n° 14 *bis* de votre Rapporteure Limiter les données sensibles collectées et conservées dans EDVIRSP au titre du signalement aux seuls « *signes physiques particuliers, objectifs et inaltérables* ».	Non mise en œuvre	Partie II, page 63
Recommandation n° 15 Abandonner définitivement l'inscription dans tout fichier, quelles que soient sa nature et sa portée, des personnes physiques ayant sollicité, exercé ou exerçant un mandat politique, syndical ou économique ou qui jouent un rôle institutionnel, économique, social ou religieux significatif.	Mise en œuvre partielle	Partie II, page 59
Recommandation n° 16 de votre Rapporteur Pourront être collectées et conservées dans le futur fichier EDVIRSP les données relatives aux mineurs de plus de treize ans lorsqu'« *en raison de leur activité individuelle ou collective, ils peuvent porter atteinte à la sécurité des personnes et des biens* ».	Mise en œuvre partielle	Partie II, page 55

Recommandation n° 16 *bis* de votre Rapporteure Ne pourront être collectées et conservées dans le futur fichier EDVIRSP et à la seule fin de les inscrire dans l'application « Gestion des violences urbaines » (GEVI), que les données relatives aux mineurs de plus de treize ans qui, d'une part, sont référencés dans un fichier d'antécédents judiciaires (STIC ou JUDEX) et, d'autre part, peuvent, « *en raison de leur activité individuelle et collective, porter atteinte à la sécurité des personnes et des biens, par le recours ou le soutien actif apporté à la violence, ainsi que les personnes entretenant ou ayant entretenu un lien direct et non fortuit avec ceux-ci* ».	Mise en œuvre partielle	Partie II, page 55
Recommandation n° 17 de votre Rapporteur Élargir l'application GEVI, actuellement développée et gérée par la préfecture de police, aux mineurs qui, « *en raison de leur activité individuelle ou collective, peuvent porter atteinte à la sécurité des personnes et des biens* ».	Mise en œuvre partielle	Partie II, page 54

Recommandation n° 17 *bis* de votre Rapporteure Élargir l'application GEVI, actuellement développée et gérée par la préfecture de police, aux mineurs de plus de treize ans, qui, d'une part, sont référencés dans un fichier d'antécédents judiciaires (STIC ou JUDEX) et qui, d'autre part, peuvent, « *en raison de leur activité individuelle et collective, porter atteinte à la sécurité des personnes et des biens, par le recours ou le soutien actif apporté à la violence, ainsi que les personnes entretenant ou ayant entretenu un lien direct et non fortuit avec ceux-ci* ».	Mise en œuvre partielle	Partie II, page 55
Recommandation n° 18 Doter les services départementaux d'information générale (SDIG), situés dans des départements particulièrement confrontés à la gestion des violences urbaines, d'un fichier GEVI à vocation départementale.	Mise en œuvre	Partie II, page 46
Recommandation n° 19 Dans le cas plus spécifique de l'Île-de-France, mettre en place un fichier GEVI à vocation régionale, en permettant l'alimentation et la consultation du fichier GEVI par les fonctionnaires spécialement habilités des services départementaux d'information générale de la région d'Île-de-France.	Mise en œuvre	Partie II, page 46

Recommandation n° 20 Introduire, dans les fichiers de renseignement, un droit à l'oubli pour les mineurs de plus de treize ans avec effacement de l'élément enregistré le jour du troisième anniversaire de son enregistrement, à défaut de nouvel événement.	Mise en œuvre	Partie II, page 56
Recommandation n° 21 Nommer un magistrat référent au plan national, chargé de veiller au respect du droit à l'oubli pour les mineurs à la date du troisième anniversaire de l'inscription dans le fichier. En l'absence de nouvel événement justifiant la conservation des données concernant le mineur, le magistrat s'assure que celles-ci sont effectivement effacées. Si, au regard de tout nouvel événement, les services gestionnaires souhaitent le maintien des informations concernant le mineur, ils doivent alors présenter au magistrat l'ensemble des raisons le justifiant. Dans le cas où un tel maintien des données au-delà du troisième anniversaire est autorisé par le magistrat, les services gestionnaires et le magistrat référent doivent se réunir tous les ans, afin d'étudier de nouveau les raisons justifiant le maintien dans le fichier. S'il estime que la demande de maintien est insuffisamment motivée, le magistrat peut ordonner l'effacement des données.	Mise en œuvre partielle	Partie II, page 56

Recommandation n° 22 Remplacer la typologie ethno raciale du STIC-Canonge et de son équivalent JUDEX par les éléments du portrait-robot, dont la couleur de peau est une composante au même titre que la couleur des yeux et des cheveux, par exemple.	Non mise en œuvre	Partie II, page 63
Recommandation n° 23 Afin de garantir une meilleure alimentation du fichier automatisé des empreintes digitales, déployer de bornes de signalisation T1 et T4 dans les unités de la gendarmerie nationale, aussi bien dans les 100 brigades départementales de renseignements et d'investigations judiciaires que dans les unités territoriales les plus chargées.	Mise en œuvre partielle	Partie IV, page 99
Recommandation n° 24 Lorsqu'il est possible de réaliser un prélèvement biologique à des fins de comparaison sur une personne à l'encontre de laquelle il existe une « *raison plausible* » de soupçonner qu'elle a commis un crime ou un délit, la loi n'énumère pas actuellement les infractions concernées. Il faut renvoyer explicitement à la liste des infractions pour lesquelles l'enregistrement d'un profil génétique est possible. En conséquence, modifier l'alinéa 3 de l'article 706-54 du code de procédure pénale.	Mise en œuvre	Partie II, page 36

Recommandation n° 25 Mettre en place une politique de formation adaptée au profit des agents administratifs affectés à l'alimentation des fichiers.	Non mise en œuvre	Partie III, page 73
Recommandation n° 26 Enjoindre aux services de police de tenir compte sans délai des décisions de classement sans suite formulées par les parquets dans le cadre du traitement en temps réel par le biais d'une circulaire du ministre de l'Intérieur rappelant les conditions d'inscription d'une personne mise en cause dans les fichiers d'antécédents.	Non mise en œuvre	Partie III, page 75
Recommandation n° 27 Remettre à toute personne placée en garde à vue un document d'information précisant que d'éventuelles poursuites judiciaires peuvent entraîner l'inscription dans un fichier d'antécédent judiciaire et récapitulant de manière pratique les différentes possibilités qui sont offertes aux citoyens en matière de droit d'accès, de demande de mise à jour et de rectification des données.	Non mise en œuvre	Partie II, page 43
Recommandation n° 28 Recruter des contractuels en nombre suffisant pour permettre aux services régionaux de documentation criminelle de résorber le stock de procédures en attente de traitement s'agissant du STIC.	Mise en œuvre	Partie III, page 74

Recommandation n° 29 Mettre en place une politique de revalorisation, d'intéressement et de validation des acquis de l'expérience en direction des personnels administratifs chargés de l'alimentation et du contrôle de la qualité des fichiers d'antécédents.	Non mise en œuvre	Partie III, page 73
Recommandation n° 30 Définir un processus de contrôle qualité et d'enrichissement des données dans le cadre du déploiement d'ARIANE.	Non mise en œuvre	Partie III, page 72
Recommandation n° 31 Prévoir un remplacement rapide du logiciel ARDOISE, en tenant compte en amont des réalités du travail des utilisateurs.	Mise en œuvre partielle	Partie IV, page 90
Recommandation n° 32 Confier à une commission, présidée par un procureur général et associant l'IGPN, l'IGGN et la CNIL, le soin de définir les modalités de reprise de l'ensemble des données figurant dans le STIC et dans JUDEX, de telle sorte qu'ARIANE n'hérite pas du stock d'erreurs accumulées dans les traitements actuellement en service. Consacrer les moyens et le temps nécessaires à la réalisation effective de ce chantier considérable.	Non mise en œuvre	Partie III, page 78

Recommandation n° 33 L'utilisation des fichiers d'antécédents judiciaires dans le cadre d'un procès pénal doit respecter la règle du contradictoire. Dans le cas où le ministère public mentionne les affaires pour lesquelles un prévenu ou un mis en examen a été mis en cause, la fiche correspondante doit être versée au dossier.	Non mise en œuvre	Partie II, page 43
Recommandation n° 34 Mettre en place au plus vite le dispositif d'échanges d'informations entre CASSIOPÉE et ARIANE, afin de tenir compte plus rapidement et plus efficacement des changements de qualification et des suites judiciaires.	Non mise en œuvre	Partie III, page 75
Recommandation n° 35 Garantir la transmission systématique des décisions judiciaires d'effacement des fichiers d'antécédents afin de procéder aux effacements correspondants dans le fichier Canonge et dans le FNAEG.	Mise en œuvre partielle	Partie III, page 76
Recommandation n° 36 Réduire à un mois le délai de traitement du dossier en cas de demande de mise à jour émanant d'une personne figurant dans un fichier d'antécédents judiciaires.	Mise en œuvre	Partie II, page 39

Recommandation n° 37 Mettre en place une procédure de traitement en temps réel auprès d'un magistrat référent des fichiers d'antécédents afin de répondre aux demandes de mise à jour présentant un degré d'urgence particulièrement élevé.	Non mise en œuvre	Partie II, page 39
Recommandation n° 38 de votre Rapporteur Maintenir la faculté accordée au procureur de la République de prescrire le maintien dans un fichier d'antécédent judiciaire des données personnelles concernant les personnes mises en cause en cas de décision de relaxe ou d'acquittement devenue définitive.	Mise en œuvre	Partie II, page 40
Recommandation n° 38 *bis* de votre Rapporteure Supprimer la faculté accordée au procureur de la République de prescrire le maintien dans un fichier d'antécédent judiciaire des données personnelles concernant les personnes mises en cause en cas de décision de relaxe ou d'acquittement devenue définitive (modification du III de l'article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure).	Non mise en œuvre	Partie II, page 40
Recommandation n° 39 Élargir le nombre de cas dans lesquels le procureur de la République peut ordonner l'effacement des données personnelles en modifiant le III de l'article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure.	Non mise en œuvre	Partie II, page 41

Recommandation n° 40 Installer au plus vite dans les parquets des TGI des terminaux permettant l'accès direct aux données figurant dans les traitements STIC et JUDEX, afin d'assurer un véritable contrôle par le procureur de la République et d'accélérer le traitement des mises à jour en fonction des suites judiciaires.	Non mise en œuvre	Partie IV, page 100
Recommandation n° 41 Prévoir l'engagement de personnels contractuels ponctuellement nécessaires à la CNIL pour traiter le stock des recours accumulé et garantir ainsi des délais convenables d'exercice du droit d'accès indirect.	Non mise en œuvre	Partie II, page 37
Recommandation n° 42 Instituer un droit d'accès direct des victimes aux fichiers d'antécédents judiciaires.	Non mise en œuvre	Partie II, page 38
Recommandation n° 43 Engager une réflexion sur la création au profit de la CNIL d'une redevance modeste, acquittée par les utilisateurs de l'informatique, en vue d'adapter les moyens de l'autorité de contrôle à la croissance continue des recours.	Non mise en œuvre	Partie II, page 37

Recommandation n° 44 Assurer une transmission systématique à la délégation parlementaire au renseignement de l'ensemble des textes relatifs à la mise en place de traitements automatisés de données à caractère personnel par les services de renseignement, lorsque les textes portant création des fichiers intéressant la sûreté de l'État et la défense ne sont pas publiés au *Journal Officiel*.	Non mise en œuvre	Partie I, page 23
Recommandation n° 45 Remplacer par un contrôle d'accès sécurisé au moyen de cartes à puce la multitude de codes attribués aux policiers et gendarmes pour utiliser les différentes applications dont ils disposent.	Mise en œuvre	Partie III, page 79
Recommandation n° 46 S'orienter vers la mise en place de systèmes d'alerte en temps réel fondés sur l'analyse du comportement de l'utilisateur et permettant de mieux réprimer les détournements de données personnelles figurant dans les fichiers de police.	Mise en œuvre partielle	Partie III, page 81
Recommandation n° 47 Dans les cas où une enquête administrative doit être réalisée par la police nationale, celle-ci doit être confiée seulement au service départemental d'information générale.	Non mise en œuvre	Partie II, page 49

Recommandation n° 48 Avertir systématiquement toute personne figurant comme mis en cause dans un fichier d'antécédents judiciaires et faisant l'objet d'une enquête administrative de la possibilité d'être entendue par les services chargés de cette enquête, pour exposer son cas et, éventuellement, l'urgence de sa situation en termes d'accès à l'emploi.	Non mise en œuvre	Partie II, page 50
Recommandation n° 49 Moderniser de toute urgence le fichier des brigades spécialisées, cet outil des plus utiles en étant malheureusement arrivé au point où son fonctionnement même est désormais compromis.	Non mise en œuvre	Partie IV, page 93
Recommandation n° 50 Définir un cadre législatif approprié pour la mise en œuvre de traitements automatisés de données permettant des rapprochements destinés à la lutte contre la petite et moyenne délinquance sérielle.	Non mise en œuvre	Partie I, page 30
Recommandation n° 51 Pour le développement de chaque nouveau fichier commun à la police et à la gendarmerie, créer une équipe intégrée associant les deux forces, avec un seul chef de projet assisté d'un comité où sont représentées toutes les directions intéressées, pour assurer le pilotage juridique, technique et financier du projet.	Mise en œuvre	Partie IV, page 85

Recommandation n° 52 Associer la police et la gendarmerie dans le cadre d'une véritable démarche intégrée de prospective technique et financière s'agissant des besoins futurs en matière de fichiers.	Mise en œuvre	Partie IV, page 85
Recommandation n° 53 Permettre, à titre provisoire et sur la base du décret du 14 octobre 1991, l'alimentation et la consultation du fichier des renseignements généraux, « gelé » depuis le 1er juillet 2008, dans l'attente de l'adoption d'une loi autorisant la création du futur fichier EDVIRSP.	Non mise en œuvre	Partie II, page 44
Recommandation n° 54 Rédiger un guide méthodologique à l'attention des services, détaillant avec précision les critères et les modalités de production, de traitement, de transfert, de destruction et d'archivage des données contenues dans les fichiers de police.	Mise en œuvre partielle	Partie III, page 71
Recommandation n° 55 Définir au plus vite la nature du fichier qui aura vocation à remplacer le fichier alphabétique de renseignements (FAR) en octobre 2010, en déterminant avec précision la finalité assignée à ce nouveau traitement ainsi que la description générale de ses fonctions, les catégories de données à caractère personnel enregistrées, leur origine et les catégories de personnes concernées.	Mise en œuvre	Partie II, page 52

Recommandation n° 56 Établir dans les meilleurs délais des directives, à l'attention de l'ensemble des brigades territoriales de la gendarmerie nationale, précisant les critères ainsi que les modalités de transfert, de destruction et d'archivage des données contenues dans le FAR, afin que sa disparition soit pleinement effective au 24 octobre 2010.	Mise en œuvre partielle	Partie II, page 51
Recommandation n° 57 Prononcer la destruction des fichiers par la loi. En conséquence, compléter l'article 26 de la loi du 6 janvier 1978, afin que seule la loi puisse mettre fin à l'existence des fichiers intéressant la sécurité publique et ceux qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.	Non mise en œuvre	Partie I, page 22

TABLEAU RECENSANT LES FICHIERS DE POLICE OU À USAGE DE POLICE

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Observations
Accord de Schengen du 9 juin 1990 (décret n° 95-577 du 6 mai 1995)	Système d'information Schengen **(SIS)**	Direction générale de la police nationale (DCPJ)	Recensement : - des personnes recherchées, sous surveillance ou indésirables ; - des véhicules ou objets recherchés.	Alimenté par le fichier des véhicules volés, le fichier des personnes recherchées et le STIC.
Loi n° 90-1131 du 19 décembre 1990 (articles L. 330-1 à L. 330-8 du code de la route)	Fichier national des immatriculations **(FNI)**	Ministère de l'Intérieur (DLPAJ)	Connaître à tout moment la situation administrative et juridique d'un véhicule et d'identifier son propriétaire, notamment dans le cadre de recherches de police	
Loi n° 98-468 du 17 juin 1998 (modifiée par les lois n° 2001-1062 et n° 2003-239)	Fichier national automatisé des empreintes génétiques **(FNAEG)**	Direction générale de la police nationale (DCPJ) - fichier commun à la police et à la gendarmerie	Enregistrement et comparaison des empreintes génétiques.	Le FNAEG comporte aujourd'hui 1,8 million de profils et 138 000 traces. Le décret n°2009-785 du 23 juin 2009 a permis aux agents d'organismes de coopération internationale en matière de police judiciaire ou de services de police ou de justice d'États étrangers de consulter ce fichier.
Loi n° 2004-204 du 9 mars 2004 (modifiée par les lois n° 2005-1549, n° 2006-399, n° 2008-174, n° 2009-1436, n° 2010-242, n° 2011-939)	Fichier judiciaire national automatisé des auteurs d'infractions sexuelles et violentes **(FIJAISV)**	Ministère de la Justice	Prévenir la récidive d'infractions sexuelles ou violentes et faciliter l'identification de leurs auteurs.	Au 30 avril 2011, le FIJAISV comportait 54 883 personnes.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Observations
Loi n° 2005-1549 du 12 décembre 2005, puis loi n° 2011-267 créant les articles 230-20 et suivants du code de procédure pénale. En cours de déclarations auprès de la CNIL.	Logiciel d'analyse criminelle **(ANACRIM)**	Gendarmerie nationale	Rapprochement de données dans le cadre d'une procédure judiciaire particulière complexe, reconstitution du déroulement d'une infraction, rapprochements d'enquêtes différentes afin de mettre en évidence des éléments communs.	Un projet de décret a été déposé à la CNIL.
Loi n° 2005-1549 du 12 décembre 2005, puis loi n° 2011-267 créant les articles 230-20 et suivants du code de procédure pénale	Système d'analyse et de liens de la violence associée au crime **(SALVAC)**	Fichier commun à la police et à la gendarmerie	Opérer des rapprochements en matière de criminalité sexuelle ou violente, pour établir des liens entre procédures judiciaires et mettre en évidence leur caractère sériel.	Le décret n° 2009-786 du 23 juin 2009 a permis la régularisation de ce fichier.
Loi n° 2006-64 du 23 janvier 2006 (article 7), transposant la directive 2004/82/CE du 29 avril 2004, décret n° 2006-1630 du 19 décembre 2006 et arrêté daté du même jour.	Fichier des passagers aériens **(FPA)**	Direction générale de la police nationale (direction centrale de la police aux frontières)	Fichier des données collectées par les entreprises de transport international au moment de l'enregistrement (données dites APIS), envoyées dès la clôture du vol et croisées avec le fichier des personnes recherchées.	L'expérimentation débutée en 2006, renouvelée pour deux ans en janvier 2009, est prolongée jusqu'au 31 décembre 2011 par l'arrêté du 15 mars 2011 portant modification de l'arrêté du 28 janvier 2009 pris pour l'application de l'article 7 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers de données à caractère personnel relatives aux passagers enregistrées dans les systèmes de contrôle des départs des transporteurs aériens.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Observations
Loi n° 2006-64 du 23 janvier 2006 (article 8) arrêté du 2 mars 2007	**Traitement automatisé de contrôle des données signalétiques des véhicules**	Police, gendarmerie et douanes	Rapprochement des données issues des dispositifs de lecture automatisée de plaques d'immatriculation (LAPI) embarqués dans des véhicules avec le fichier des véhicules volés et signalés (FVV).	L'arrêté du 18 mai 2009 portant création d'un traitement automatisé de contrôle des données signalétiques des véhicules a assuré la régularisation de ce fichier.
Article L. 611-3 à L. 611-5 du code de l'entrée et du séjour des étrangers et du droit d'asile (article R. 611-18 à R. 611-24 du même code)	Traitement automatisé de données à caractère personnel de ressortissants étrangers qui, ayant été contrôlés à l'occasion du franchissement de frontières, ne remplissent pas les conditions d'entrée requises ou « fichier des non-admis » **(FNAD)**	Secrétariat général à l'immigration et à l'intégration	Lutter contre l'entrée et le séjour irrégulier des étrangers.	Fichier créé à titre expérimental pour une durée de deux ans à compter du 25 juillet 2007. La durée de l'expérimentation a été portée à quatre ans par le décret n° 2009-1483 du 1er décembre 2009. Si le FNAD n'a pas été pérennisé à la suite de l'expérimentation, l'un de ses modules, intitulé « Gestion informatisée des procédures d'immigration » fera l'objet d'une déclaration à la CNIL.
Article L.611-3 du code de l'entrée et du séjour des étrangers et du droit d'asile (articles R. 611-25 à R. 611-34 du même code – décret n° 2007-1890 du 26 décembre 2007)	Traitement automatisé de données à caractère personnel relatives aux étrangers faisant l'objet d'une mesure d'éloignement **(ELOI)**	Secrétariat général à l'immigration et à l'intégration	Enregistrement des données à caractère personnel relatives aux étrangers faisant l'objet d'une mesure d'éloignement.	Abrogé par le décret n°2011-638 du 8 juin 2011, et remplacé par le fichier AGDREF2 (cf. *infra*).

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Observations
Article L. 611-6 du code de l'entrée et du séjour des étrangers (articles R. 611-8 à R. 611-15 du même code, modifié par le décret n° 2010-645).	Traitement automatisé de données à caractère personnel relatives aux étrangers sollicitant la délivrance d'un visa **(VISABIO)**	Ministère des affaires étrangères et secrétariat général à l'immigration et à l'intégration	Lutter contre la fraude documentaire et l'usurpation d'identité et faciliter l'instruction des demandes de visa.	
Décret n° 55-1397 du 22 octobre 1955	Fichier relatif à la carte nationale d'identité	Ministère de l'intérieur (DLPAJ)	- Mettre en œuvre les procédures de délivrance et de renouvellement ; - Limiter les risques de contrefaçon et de falsification ; - Faciliter l'action des policiers et gendarmes lors du franchissement des frontières.	
Décrets n° 87-249 du 8 avril 1987 et n° 2005-585 du 27 mai 2005	Fichier automatisé des empreintes digitales **(FAED)**	Direction générale de la police nationale (DCPJ) - fichier commun à la police et à la gendarmerie	Enregistrement et comparaison des empreintes digitales.	
Décret n° 91-1051 du 14 octobre 1991	Fichiers des renseignements généraux **(FRG)**	Direction générale de la police nationale (renseignements généraux)	Centralisation des informations sur les personnes : - pouvant porter atteinte à la sûreté de l'État ou à la sécurité publique par la violence ; - ayant sollicité ou sollicitant l'accès à des informations protégées ; - exerçant ou ayant exercé un mandat électif ou jouant un rôle politique, économique, social ou religieux significatif.	Fichier gelé à compter du 1er juillet 2008, seul le transfert des données vers d'autres fichiers jusqu'au 31 décembre 2009 était rendu possible par le décret n° 2008-631 du 27 juin 2008. Or, des opérations de transfert avaient encore lieu en 2011.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Observations
Décret n° 91-1051 du 14 octobre 1991 (créé en 1996, GEVI a pour base juridique le décret de 1991, sa conformité avec ce texte ayant été reconnue par la CNIL dans sa décision du 19 novembre 1996).	Gestion des violences **(GEVI)**	Préfecture de police de Paris	Recueil d'informations sur des individus majeurs ou des 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.	Le fichier GEVI sera vraisemblablement remplacé par le fichier PASP (cf. *infra*), qui reprend ces fonctionnalités.
Décret du 29 mars 1993 (article D. 611-1 à D. 611–7 du code de l'entrée et du séjour des étrangers et du droit d'asile)	Système informatisé de gestion des dossiers des ressortissants en France **(AGDREF)**	Ministère chargé de l'immigration (fichier national) et préfectures (fichiers départementaux)	Notamment permettre aux services de la police et de la gendarmerie de vérifier la régularité du séjour en France (article D. 611-3).	Abrogé par le décret n°2011-638 du 8 juin 2011, et remplacé par le fichier AGDREF2 (cf. *infra*).
Décret n° 2001-583 du 5 juillet 2001, modifié par le décret n° 2006-1258 du 14 octobre 2006.	Système de traitement des infractions constatées **(STIC)**	Direction générale de la police nationale	Faciliter la constatation des infractions pénales, le rassemblement des preuves et la recherche de leurs auteurs, ainsi que l'exploitation de ces données à des fins statistiques.	Ce fichier sera bientôt remplacé par le Traitement des procédures judiciaires (cf. *infra*).
Décret n° 2005-1726 du 30 décembre 2005	Fichier relatif aux passeports **(Delphine et TES)**	Ministère de l'intérieur (DLPAJ)	- Mettre en œuvre les procédures d'établissement, de délivrance et de renouvellement des passeports ; - Prévenir et détecter leur falsification ou contrefaçon.	
Décret n° 2006-1411 du 20 novembre 2006.	Système judiciaire de documentation et d'exploitation **(JUDEX)**	Gendarmerie nationale	Faciliter la constatation des infractions pénales, le rassemblement des preuves et la recherche de leurs auteurs.	Ce fichier sera bientôt remplacé par le Traitement des procédures judiciaires (cf. *infra*).

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Observations
Décret du 27 juin 2008, non publié au *Journal officiel*	Centralisation du renseignement intérieur pour la sécurité du territoire et les intérêts nationaux **(CRISTINA)**	Direction générale de la police nationale (DCRI)	Lutte contre toutes les activités susceptibles de constituer une atteinte aux intérêts fondamentaux de la nation.	
Décret n° 2008-1109 du 29 octobre 2008 (expérimentation) En cours de déclaration auprès de la CNIL	Traitement de données « pré plainte en ligne » **(PPL)**	Direction générale de la police nationale	Permettre à la victime ou à son représentant de faire une déclaration en ligne, pour certaines infractions, et d'obtenir un rendez-vous pour la signature de la plainte.	Expérimenté depuis la fin 2008 dans deux puis quatre départements, ce fichier est en cours de déclaration auprès de la CNIL, qui a rendu un avis le 25 octobre 2011 sur un projet d'arrêté.
Arrêté du 20 décembre 1972 (la base juridique actuelle est constituée par l'article L. 225-1 à L. 225-9 du code de la route)	Fichier national des permis de conduire **(FNPC)**	Ministère de l'intérieur (DLPAJ)	Enregistrer et gérer toutes les informations relatives aux permis de conduire, en particulier les droits de conduire de tout conducteur.	
Arrêté du 29 août 1991, modifié par l'arrêté du 3 novembre 2006 (traitement régi par l'article 7 de la loi n° 2006-64 du 23 janvier 2006)	Fichier national transfrontière **(FNT)**	Direction générale de la police nationale (direction centrale de la police aux frontières)	Collecte des informations concernant les embarquements et débarquements de passagers aériens à destination ou en provenance de pays « sensibles ».	

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Observations
Arrêté du 28 octobre 1992 (modifié par l'arrêté du 13 mai 1998)	Traitement automatisé d'informations nominatives de gestion et de suivi des procédures et du courrier dans les unités élémentaires de la gendarmerie – Bureautique brigade 2000 **(BB 2000)**	Gendarmerie (au sein de chaque brigade territoriale)	Application locale destinée à gérer le service et les registres et de permettre un partage de l'information sur la connaissance de la circonscription de l'unité.	Ce fichier devrait être remplacé par PULS@R (cf. *infra*).
Arrêté du 22 mars 1994 (modifié par l'arrêté du 28 février 2005)	Fichier de suivi des titres de circulation délivrés aux personnes sans domicile ni résidence fixe **(SDRF)**	Gendarmerie (STRJD)	Suivi des titres de circulation délivrés aux personnes sans domicile ni résidence fixe, soumises aux dispositions de la loi n° 69-3 du 3 janvier 1969.	Afin d'asseoir la finalité exclusivement administrative de ce fichier, sa gestion a été confiée début 2011 au centre technique de la gendarmerie nationale, unité administrative et non judiciaire.
Arrêté du 19 décembre 1994 (modifié par l'arrêté du 30 juillet 2002)	Fichier de suivi des personnes faisant l'objet d'une rétention administrative **(SUICRA)**	Gendarmerie	Assurer le suivi des personnes faisant l'objet d'une décision de rétention.	Supprimé par l'arrêté du 4 avril 2011 portant abrogation de l'arrêté du 19 décembre 1994 relatif à la mise en œuvre du traitement automatisé d'informations nominatives concernant la population faisant l'objet d'une décision de rétention administrative
Arrêté du 24 février 1995	Main courante informatisée **(MCI)**	Direction générale de la police nationale	Gérer l'emploi des effectifs, les événements et les déclarations des usagers.	Ce fichier sera bientôt remplacé par la Nouvelle main courante informatisée (cf. *infra*).
Arrêté du 15 mai 1996 (modifié par l'arrêté du 2 septembre 2005)	Fichier des véhicules volés **(FVV)**	Police et gendarmerie	Faciliter les recherches : - pour la découverte et la restitution de véhicules volés ; - la surveillance de véhicules signalés dans le cadre d'activités répressives ou préventives ; - des personnes susceptibles d'utiliser un véhicule volé ou signalé.	Ce fichier sera bientôt remplacé par le fichier des objets et des véhicules signalés (cf. *infra*).

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Observations
Décret n° 2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées (auparavant : arrêté du 15 mai 1996)	Fichier des personnes recherchées **(FPR)**	Police et gendarmerie	Faciliter la recherche de personnes recherchées (au titre de décisions judiciaires, faisant l'objet d'une enquête, étrangers faisant l'objet d'une décision d'expulsion, mineurs en fugue, personnes disparues, etc.).	Une réflexion sur la modernisation du FPR est en cours.
Arrêté du 28 octobre 1996 (modifié par l'arrêté du 20 février 2003)	Fichier national automatisé des personnes incarcérées	Administration pénitentiaire	Gestion des affectations des détenus et production de statistiques sur la population pénale.	
Arrêté du 13 septembre 2002	Service central de préservation des prélèvements biologiques **(SCPPB)**	Gendarmerie	Assurer la gestion des prélèvements biologiques effectués dans le cadre d'affaires judiciaires concernant l'une des infractions mentionnées à l'article 706-55 du code de procédure pénale et entraînant l'enregistrement au FNAEG.	
Arrêté du 28 août 2007	Fichier national des interdits de stade **(FNIS)**	Direction générale de la police nationale (DCSP)	Prévenir et lutter contre les violences lors des manifestations sportives, notamment en garantissant la pleine exécution des mesures administratives et judiciaires d'interdiction de stade.	Ce fichier est alimenté par les fiches judiciaires ou administratives des interdits de stade inscrites dans le FPR.
Arrêté du 15 novembre 2007, modifié par un arrêté du 24 mars 2009	Application de gestion du répertoire informatisé des propriétaires et possesseurs d'armes **(AGRIPPA)**	Ministère de l'intérieur (DLPAJ)	Traitement automatisé de données à caractère personnel concernant les détentions d'armes et de munitions.	

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Observations
Aucun texte (créé en 1942)	Fichier de la batellerie	Gendarmerie nationale	Suivi des mariniers ainsi que des bateaux affectés au transport fluvial de marchandises.	Ce fichier est neutralisé depuis plusieurs années mais sera intégralement conservé à des fins historiques. Il a été transféré cet été au service historique de la défense – département gendarmerie (SHDGN).
Instruction initiale de 1971	Fichier alphabétique de renseignements **(FAR)**	Gendarmerie nationale	Permettre aux brigades de gendarmerie d'acquérir une connaissance approfondie de la population, notamment en vue de la réalisation d'enquêtes administratives.	Le FAR était intégralement détruit au 3 mars 2011, à l'exception des fonds des brigades de Colmar, Lunel, Gujan-Mestras et Ploërmel, conservés à des fins historiques.
Aucun texte (créé en 1975)	Fichier des personnes nées à l'étranger **(FPNE)**	Gendarmerie (STRJD)	Enregistrement de toute personne née à l'étranger entrant en contact avec la gendarmerie.	Ce fichier a été détruit durant l'été 2011, à l'exception des fiches de la lettre B, conservées à des fins historiques.
Aucun texte (créé en 1982)	Fichier des avis de condamnations pénales **(FAC)**	Gendarmerie	Compléter le FAR avec les renseignements collectés auprès des greffes des tribunaux (condamnations exécutoires inscrites au bulletin n° 2 du casier judiciaire).	Ce fichier, qui faisait partie du FAR, était détruit au 3 mars 2011.
Créé en 1987 et déclaré à la CNIL en 1991.	Fichier de travail de la police judiciaire **(FTPJ)**	Direction générale de la police nationale (SRPJ)	Collecte d'informations sur des délinquants spécialisés.	N'a fait l'objet d'aucun texte réglementaire à ce jour.
Aucun texte	Fichier des brigades spécialisées **(FBS)**	Direction générale de la police nationale (seuls les personnels disposant d'une habilitation spéciale, en nombre réduit, ont accès à ce fichier)	Fichier de travail des services de police spécialisés luttant contre la grande délinquance et le crime organisé. Il a pour objectif d'utiliser au mieux les diverses informations collectées à l'occasion de la surveillance du milieu criminel, de permettre des échanges confidentiels entre services spécialisés et d'autoriser tous les croisements de recherche possibles entre les informations figurant dans la base.	Si ce fichier ne dispose d'aucune base réglementaire, il apparaît cependant dans l'arrêté du 15 janvier 2010 fixant le contenu et les modalités des examens professionnels pour l'accès au grade de brigadier de police.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Observations
Aucun texte (déclaré à la CNIL simultanément à la déclaration du STIC)	Logiciel de rédaction des procédures **(LRP)**	Direction générale de la police nationale	Rédiger les procès verbaux et les rapports administratifs ou judiciaires.	Ce fichier sera bientôt remplacé par LRPPN (cf. *infra*).
Règlement (CE) n° 1338/2001 du 28 juin 2001 définissant des mesures nécessaires à la protection de l'euro contre le faux monnayage	Fichier national du faux monnayage **(FNFM)**	Police et gendarmerie	Recenser les affaires relatives au faux monnayage commises sur le territoire national (données relatives à l'affaire, à l'infraction, aux coupures saisies, à l'identité des mis en cause et à leur signalement).	Mis en service lors de la mise en circulation de l'euro, le 1er janvier 2002. Il permet de satisfaire aux obligations de centralisation au niveau national des informations relatives au faux monnayage ainsi qu'à celles d'information d'Europol (article 8 du règlement).
Aucun texte	Fichier des objets signalés **(FOS)**	Gendarmerie nationale	Vérifier si un objet bien identifié a été signalé par les unités de gendarmerie à l'occasion d'une enquête judiciaire ou par le SIS comme étant volé.	Ce fichier sera bientôt remplacé par le fichier des objets et véhicules signalés (cf. *infra*).
Aucun texte	Gestion du terrorisme et des extrémismes violents **(GESTEREXT)**	Préfecture de police de Paris	- Prévenir les actes de terrorisme ; - Surveiller les individus, groupes, organisations et phénomènes de société susceptibles de porter atteinte à la sûreté nationale.	Un projet de décret est en cours de rédaction.
Aucun texte (créé en 2008)	Outil de centralisation et de traitement opérationnel des procédures et des utilisateurs de signatures **(OCTOPUS)**	Préfecture de police de Paris	Recherche des auteurs de « tags » (identification des auteurs de dégradations, établissement de synthèses de faits et de recoupements).	Un projet d'arrêté est en cours de rédaction.
Aucun texte (en phase d'expérimentation depuis décembre 2008)	Logiciel d'uniformisation des prélèvements et identification **(LUPIN)**	Préfecture de police de Paris	Lutter contre les cambriolages en procédant à des rapprochements à partir des données de police technique et scientifique et relatives aux modes opératoires recueillies sur les scènes d'infraction.	Un projet de décret est en cours d'élaboration, sur la base des articles 230-20 et suivants du code de procédure pénale (logiciels de rapprochement judiciaire), introduit par la loi 2011-267 du 14 mars 2011.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Observations
Aucun texte (en phase d'expérimentation depuis 2006)	Cellule opérationnelle de rapprochement et d'analyse des infractions liées **(CORAIL)**	Préfecture de police de Paris (DPJ)	Diffuser aux services d'enquêtes les fiches relatives à des faits sériels, sous la forme d'états opérationnels tirés des infractions, afin de faciliter les rapprochements.	Un projet de texte réglementaire est en cours d'élaboration, sur le fondement de l'article 26 de la loi du 6 janvier 1978.
Aucun texte	Système de traitement des images des véhicules volés **(STIVV)**	Gendarmerie nationale	Exploiter à des fins judiciaires les photographies de certains véhicules prises par les radars automatisés (véhicules volés, mis sous surveillance, etc.).	Un projet de texte réglementaire est en cours d'élaboration.
Aucun texte	**ARAMIS**	Gendarmerie nationale	Système de traitement des informations présentant un caractère opérationnel (gestion des interventions ; messagerie interne de suivi des situations ; renseignement pour le suivi de l'ordre public).	Ce fichier a été remplacé par la base de données de sécurité publique (BDSP, anciennement Athéna) (cf. *infra*).

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Observations
Arrêté du 30 mars 2009 relatif à la répression de certaines formes de criminalité informatique et à la lutte contre la pédopornographie	Base de données de lutte contre la pédopornographie **(CALIOPE)**	Gendarmerie nationale	Logiciel de rapprochement des images pédopornographiques conservées par le centre national d'analyse des images pédopornographiques, mis en place en 2003.	Ce fichier est en cours de déclaration auprès de la CNIL, sur le fondement des articles 230-12 à 230-18 du code de procédure pénale, introduits par la loi du 14 mars 2011.
Aucun texte	Base de l'office central de lutte contre la délinquance itinérante **(Base OCLDI)**	Gendarmerie nationale	Base documentaire relative à la délinquance itinérante permettant un travail de rapprochement judiciaire.	Cette base, alimentée par des fichiers comme le STIC, JUDEX, le FPR, par des messages de services opérationnels et des procédures traitées directement par l'office, comporte environ 53 000 fiches de personnes. Elle devrait bientôt faire l'objet d'un décret.
Aucun texte	Base de données des **victimes non identifiées**	Gendarmerie nationale	Rapprochement entre la description des victimes non identifiées et les disparitions inquiétantes.	Cette base de données rassemble environ 1 000 personnes disparues et autant de victimes non identifiées. Les données relatives aux personnes disparues sont effacées au bout de six mois, sauf si la brigade territoriale demande son maintien. Un projet de texte réglementaire est en cours d'élaboration.
Aucun texte	Base de données relative aux **escroqueries**	Gendarmerie nationale	Base documentaire relative aux escroqueries.	Un projet de texte réglementaire est en cours d'élaboration.
Aucun texte	Base de données relative aux **atteintes aux biens** et à la criminalité organisée	Gendarmerie nationale (STRJD)	Base documentaire de classement des atteintes aux biens (vols à main armée, braquage…)	Un projet de texte réglementaire est en cours d'élaboration.
Aucun texte	Base de données relative aux **objets volés**	Gendarmerie nationale	Base documentaire relative aux objets volés.	Un projet de texte réglementaire est en cours d'élaboration.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Observations
Aucun texte	**Bases criminalistiques départementales**	Gendarmerie nationale	Stockage des éléments matériels probants découverts sur des scènes de crime ou de délit.	Un projet de texte réglementaire est en cours d'élaboration.
Arrêté du 2 mai 2011 relatif aux traitements automatisés de données à caractère personnel dénommés « fichiers des résidents des zones de sécurité » créés à l'occasion d'un événement majeur.	Fichiers des **résidents des zones sécurisées** – Événements majeurs	Police nationale	Gestion des titres permettant l'accès des personnes ou des véhicules aux zones à l'intérieur desquelles sont apportées des restrictions à la libre circulation et à l'exercice de certaines activités, afin de prévenir les troubles à l'ordre public et de garantir la sécurité d'un événement majeur.	Cet arrêté permet la régularisation des fichiers aux finalités identiques développés par des unités locales de police.
Aucun texte	Registres des **fourrières** et des immobilisations	Police nationale	Gestion et recensement des véhicules mis en fourrière à la suite d'une infraction, abandonnés ou détériorés.	Un projet d'acte-cadre est en cours d'élaboration.
Aucun texte	Fichiers de suivi du **contrôle judiciaire**	Préfecture de police	Suivi du respect, par les personnes soumises à un contrôle judiciaire, de leurs obligations de présentation périodique à un service de police ou de gendarmerie.	Un projet d'acte-cadre est en cours d'élaboration.
Aucun texte	Fichiers de suivi des **assignations à résidence**	Préfecture de police	Suivi du respect, par les personnes soumises à une assignation à résidence, de leurs obligations de présentation périodique à un service de police ou de gendarmerie.	Un projet d'acte-cadre est en cours d'élaboration.
Aucun texte	Fichiers de suivi des **permissions de sortir**	Préfecture de police	Gestion des informations relatives aux détenus bénéficiant d'une permission de sortir ou de mesures de semi-liberté.	Un projet d'acte-cadre est en cours d'élaboration.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Observations
Aucun texte	Fichiers des **appels à témoins**	Préfecture de police	Enregistrement des communications téléphoniques de la ligne dédiée aux appels à témoins.	Un projet d'acte-cadre est en cours d'élaboration.
En cours de déclaration auprès de la CNIL	Répertoires locaux pour les opérations de protection des personnes âgées de plus de 65 ans **(RLOPPA)**	Police nationale	Recensement des personnes de 65 ans et plus souhaitant bénéficier d'une vigilance particulière des services de police.	Ce fichier, qui s'inscrit dans le cadre de l'opération « Tranquillité Seniors », est en cours de déclaration auprès de la CNIL, qui a rendu un avis sur un projet d'arrêté le 5 mai 2011.
Aucun texte	Partage de l'information opérationnelle **(PIO)**	Police et gendarmerie nationales	Partage de l'information opérationnelle.	Un projet de texte réglementaire est en cours de déclaration.
Aucun texte	Application de stockage des procédures contrôlées **(ASPC)**	Gendarmerie nationale	Dématérialisation du stockage des procédures judiciaires et administratives de la gendarmerie.	Un projet de texte réglementaire est en cours de déclaration.
Arrêté du 8 novembre 2010 portant création au profit de la direction centrale de la police judiciaire d'un fichier des courses et jeux	**Fichier des courses et jeux**	Police nationale	Surveiller la régularité et de la sincérité des jeux, des courses et des paris par la conservation des données recueillies 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.	Il convient de noter que les mandats électifs exercés dans la commune siège de l'établissement peuvent être enregistrés, « *à l'exclusion de toute mention relative aux opinions politiques* ». Cet élément d'information n'est donc pas considéré comme une donnée sensible au sens de la loi du 6 janvier 1978.
Décret n° 2011-397 du 13 avril 2011	Exécution des services commandés pour la réalisation des transfèrements et extractions **(ESCORTE)**	Police nationale	Ce fichier a pour objet la planification, l'organisation, la gestion et le compte rendu des missions d'extractions et de transfèrements des personnes détenues.	Des données relatives à l'état de santé du détenu peuvent être enregistrées, sans que le décret précise qu'il s'agit de données sensibles au sens de la loi du 6 janvier 1978.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Observations
Article 2336-6 du code de la Défense	Fichier national des interdits d'acquisition et de détention d'armes **(FINIADA)**	Direction des libertés publiques et des affaires juridiques du ministère de l'intérieur	Recensement des personnes interdites d'acquisition et de détention d'armes.	Ce fichier a été régularisé par un décret n° 2011-374 du 5 avril 2011.
Aucun texte	Nouvelle main courante informatisée	Gendarmerie nationale	Modernisation du registre de main courante informatisée.	Un projet de décret est en cours d'élaboration.
Décrets n^{os} 2011-340, 2011-341 et 2011-342.	Base de données de sécurité publique **(BDSP)**, anciennement ATHENA.	Gendarmerie nationale	Quatre modules permettant de gérer les événements d'ampleur, les sollicitations des usagers (appels 17), la sécurisation des interventions et les demandes particulières de protection, de recueillir et de conserver des informations assurant la prévention des atteintes à la sécurité publique.	BDSP, anciennement ATHENA, remplace le FAR et le module ARAMIS.
Aucun texte	Application judiciaire dédiée à la révélation des crimes et délits en série **(AJDRCDS)**	Gendarmerie nationale	Faciliter la détection : - des crimes et délits de même nature et imputables à un même auteur ou groupe d'auteurs ; - des infractions ou comportements délinquants réitérés par un même auteur ou groupe d'auteurs.	Le développement de ce fichier est aujourd'hui compromis par la décision du Conseil constitutionnel relative à la loi d'orientation et de programmation pour la performance de la sécurité intérieure du 14 mars 2011.
Aucun texte	ANACRIM Nouvelle génération **(ANACRIM-NG)**	Gendarmerie nationale	Logiciel d'analyse criminelle permettant d'opérer des rapprochements dans le cadre de procédures complexes.	Ce logiciel temporaire a vocation à remplacer l'outil Analyst's Notebook soumis à des frais de licences annuels. Il devrait être déployé à l'été 2012 et faire bientôt l'objet d'une déclaration à la CNIL.
Décret n° 2009-1249 du 16 octobre 2009	Fichier de prévention des atteintes à la sécurité publique **(PASP)**, anciennement EDVIRSP	Police nationale	Collecte, conservation et traitement des données relatives aux personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique.	Ce fichier reprend une partie des fiches du FRG et se substitue au système AGIL de remontée des notes. Son déploiement est prévu pour 2012.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Observations
Décret n° 2009-1250 du 16 octobre 2009	Fichier des enquêtes administratives liées à la sécurité publique **(EASP)**, anciennement EDVIRSP	Police nationale	Collecte, conservation et traitement des données relatives aux personnes faisant l'objet d'enquêtes administratives.	Aucune date n'est prévue pour le déploiement de ce fichier.
Décret à venir	Traitement des procédures judiciaire **(TPJ)**, anciennement ARIANE	Police et gendarmerie nationales	Faciliter la constatation des infractions, le rassemblement des preuves et la recherche des auteurs.	TPJ, qui assure la fusion du STIC et de JUDEX, doit également être connecté aux logiciels de rédaction des procédures et à CASSIOPEE. Il est actuellement en cours de déclaration à la CNIL. Son déploiement commencera à partir de la publication de l'acte réglementaire l'autorisant, soit au premier semestre 2012.
Aucun texte	Fichier des objets volés et signalés **(FOVES)**	Police et gendarmerie nationales	Vérifier si un objet ou un véhicule ont été signalés ou déclarés volés.	Un projet de texte réglementaire est en cours d'élaboration.
Décret n° 2011-110 du 27 janvier 2011	Logiciel de rédaction des procédures de la police nationale **(LRPPN)**, anciennement ARDOISE	Police nationale	Collecter et archiver les informations recueillies lors des missions de police judiciaire ou administrative (données issues de procès-verbaux, comptes rendus d'enquêtes et rapports administratifs ou judiciaires), réalisation de statistiques.	LRPPN est destiné à terme à remplacer le logiciel de rédaction des procédures et à alimenter le fichier TPJ.
Décret n° 2011-111 du 27 janvier 2011	Logiciel de rédaction des procédures de la gendarmerie nationale **(LRPGN)**, anciennement ICARE	Gendarmerie nationale	Assister les militaires de la gendarmerie dans la rédaction de leurs procès-verbaux.	LRPGN alimentera TPJ et CASSIOPEE.
Arrêtés du 2 décembre 2010	**PULSAR**	Gendarmerie nationale	Gestion des services, des procédures unités, du courrier et des amendes forfaitaires.	PULSAR a remplacé l'application BB2000.

Texte de référence initial	Nom du fichier	Administration gestionnaire	Objet	Observations
Arrêté du 21 septembre 2011 portant création d'un traitement automatisé de données à caractère personnel dénommé « gestion des étrangers en situation irrégulière » (GESI)	Gestion des étrangers en situation irrégulière **(GESI)**	Préfecture de police de Paris	Assurer une gestion en temps réel, de l'interpellation jusqu'à la reconduite, des étrangers en situation irrégulière interpellés par les services de la préfecture de police.	Pour la CNIL, la conformité de cet arrêté avec la directive 2008/115/CE du 16 décembre 2008, dite « directive retour », lorsqu'elle sera transposée n'est pas assurée.
En cours de déclaration auprès de la CNIL	Automatisation du registre des entrées et sorties des recours en matière de contravention **(ARES)**	Préfecture de police	Automatisation du registre des entrées et sorties des recours en matière de contravention	En cours de déclaration auprès de la CNIL, qui a rendu un avis sur un projet d'arrêté le 3 mars 2011.

N° 1659

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

TREIZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 7 mai 2009.

PROPOSITION DE LOI

relative aux **fichiers** *de* **police**,

(Renvoyée à la commission des lois constitutionnelles, de la législation et de l'administration générale de la République, à défaut de constitution d'une commission spéciale dans les délais prévus par les articles 30 et 31 du Règlement.)

présentée par

Mme Delphine BATHO et M. Jacques Alain BÉNISTI,

députés.

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

Le rapport d'information sur les fichiers de police [(1)], adopté par la commission des Lois à l'unanimité le 24 mars 2009, comportait 57 propositions appelant à une refonte du cadre juridique régissant la création et le fonctionnement de ces fichiers, ainsi qu'à un effort soutenu de modernisation technique. Une bonne partie d'entre elles relèvent de mesures réglementaires ou budgétaires, voire de la définition de bonnes pratiques. Toutefois, vingt-six de ces propositions nécessitent des mesures législatives. La présente proposition de loi vise donc à les mettre en œuvre, afin de mener à son terme la démarche engagée par la commission des Lois à la suite des débats suscités par la création du fichier EDVIGE.

I. – Le **titre premier** propose de modifier la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, afin que l'autorisation de créer des fichiers ou des catégories de fichiers de police intéressant la sécurité publique ou ayant pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales, relève désormais de la loi (article 5). Les catégories de fichiers de police correspondent à un ensemble de traitements automatisés distincts mais obéissant à un encadrement législatif commun qui définit leurs objectifs, encadre leurs modalités de fonctionnement et prévoit celles de leur contrôle. La loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure comprend déjà des catégories de fichiers, son article 21 créant un cadre juridique commun pour les fichiers d'antécédents judiciaires (tels que le STIC et JUDEX), tandis que l'article 21-1 encadre les fichiers de rapprochements en matière de crimes et délits sériels (SALVAC et ANACRIM).

Le II de l'article 5 détaille précisément la nature des points sur lesquels le législateur devra statuer pour encadrer les traitements ou catégories de traitement. Les principales caractéristiques des fichiers ou catégories de fichiers devront être déterminées par la loi, qu'il s'agisse des finalités, des catégories de personnes concernées, de la durée de conservation des

(1) Fichiers de police : les défis de la République, *Mme Delphine Batho et M. Jacques Alain Bénisti, rapporteurs,* n 1548.

données ou de la nature du droit d'accès des personnes figurant dans les traitements ainsi autorisés. Est maintenu le principe d'interdiction de la collecte et du traitement des données dites « sensibles » de l'article 8 de la loi précitée, c'est-à-dire les données faisant apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale, ainsi que celles relatives à la santé ou à la vie sexuelle. Alors que les dérogations à cette interdiction relèvent actuellement d'un décret en Conseil d'État, la proposition de loi prévoit de réserver à la loi cette faculté de dérogation. En outre, il est précisé qu'une telle dérogation ne peut intervenir que lorsque la finalité du traitement l'exige. L'avis rendu par la Commission nationale de l'informatique et des libertés (CNIL) sur tout projet de loi autorisant la création d'un fichier devra être transmis au Parlement simultanément au dépôt dudit projet.

Chaque traitement autorisé par la loi devra, en outre, faire l'objet d'un acte réglementaire d'application, la CNIL étant associée en amont aux principales étapes techniques de mise en place du fichier. Il s'agit ainsi de mettre fin à la situation actuelle où sont présentés à cette commission seulement des fichiers qui sont, de fait, entièrement opérationnels, jusque dans leurs moindres détails, ce qui rend coûteuse et difficile la prise en compte des éventuelles demandes de modifications des systèmes informatiques formulées par la CNIL. Dans un souci de simplification des procédures et de réactivité, l'article 4 prévoit que les avis rendus par la CNIL à l'occasion des différentes étapes peuvent être émis par son bureau.

Conformément aux propositions du rapport d'information précité, l'autorisation des fichiers concernant la sûreté de l'État ou la défense continuera à relever d'actes réglementaires, compte tenu de la présence d'informations relevant du secret de la défense nationale dans ces traitements. Les garanties actuelles en matière de dérogation à la publication des actes réglementaires autorisant ce type de traitements de données sont maintenues, tandis que le contrôle démocratique sur ces outils est renforcé par la transmission systématique de ces mêmes actes à la délégation parlementaire au renseignement.

L'article 2 a pour objectif de créer une procédure contradictoire entre la CNIL et les ministères concernés, où la première, avant la publication de son rapport annuel, interroge et recueille les réponses des seconds sur certaines observations qu'elle prévoit de leur adresser.

L'article 3 propose d'introduire, dans la loi précitée du 6 janvier 1978, la notion de représentation du pluralisme politique pour les nominations des deux députés et deux sénateurs membres de la CNIL.

II. – Le **titre II** vise à renforcer le contrôle des fichiers d'antécédents judiciaires, et donc en pratique du système de traitement des infractions constatées (STIC), mis en œuvre par la police nationale, et du système judiciaire de documentation et d'exploitation (JUDEX), géré par la gendarmerie nationale.

L'article 14 propose à cet effet de compléter le contrôle de ces traitements, relevant actuellement du procureur de la République territorialement compétent, en confiant à un procureur général le soin d'assurer la mise à jour en fonction des suites judiciaires et la rectification éventuelle des données dans les cas où les données figurant dans ces fichiers sont susceptibles de faire subir un préjudice immédiat et sérieux à la personne concernée. Il s'agit ainsi de mettre en place une procédure d'urgence, permettant de répondre en temps réel aux demandes de personnes risquant, par exemple, de ne pouvoir accéder à un emploi en raison de mentions erronées figurant dans un fichier d'antécédents judiciaires.

L'article 15 prévoit, en outre, de renforcer le contrôle exercé par le procureur de la République sur les fichiers d'antécédents judiciaires et d'en accroître l'efficacité.

Ainsi, il propose d'étendre à l'ensemble des motifs de classement sans suite la faculté accordée au procureur de la République d'ordonner l'effacement de données à caractère personnel. Actuellement, seuls les classements sans suite motivés par une insuffisance de charges peuvent faire l'objet d'une telle décision, ce qui revient en pratique à confier à l'autorité administrative le pouvoir de juger de l'importance des faits, à l'occasion d'enquêtes administratives pour lesquelles la consultation des fichiers d'antécédents judiciaires est autorisée. Désormais, l'autorité judiciaire sera en mesure d'ordonner l'effacement dans des cas où la relativement faible gravité de l'infraction a conduit le ministère public à renoncer à poursuivre, par exemple en cas de désistement de la victime ou de réparation du dommage par l'auteur.

Cet article prévoit ensuite de ramener de trois mois à un mois le délai de traitement du dossier en cas de demande de mise à jour émanant d'une personne figurant dans un fichier d'antécédents judiciaires. Il est par

ailleurs prévu que les décisions d'effacement ou de rectification des informations nominatives figurant dans les fichiers d'antécédents judiciaires doivent être transmises aux responsables des autres traitements de données concernés, afin d'en tirer toutes les conséquences sur la durée de conservation des informations personnelles. En effet, une décision de mise à jour ramenant la qualification de l'infraction constatée de crime à délit, par exemple, doit s'appliquer également à des traitements comme le fichier national automatisé des empreintes génétiques (FNAEG) ou à l'application Canonge du STIC, tout particulièrement en raison des conséquences sur la durée de conservation des données.

Enfin, l'article 15 prévoit que le droit d'accès des victimes figurant dans les fichiers d'antécédents judiciaires s'exerce directement auprès du responsable du traitement. Il n'apparaît en effet pas opportun de maintenir dans ces cas la lente et complexe procédure du droit d'accès indirect par l'intermédiaire de la CNIL.

L'article 16 prévoit que lorsque le procureur de la République souhaite faire mention d'informations provenant d'un fichier d'antécédents judiciaires et concernant un prévenu comparaissant en comparution immédiate, ces informations doivent figurer au dossier que l'avocat peut consulter.

III. – Le **titre III** prévoit la création par la loi de deux nouveaux fichiers, destinés à remplacer le fichier des renseignements généraux. Il tient ainsi compte des propositions du rapport d'information précité visant à distinguer très strictement le fichier des enquêtes administratives de celui destiné à lutter contre les violences urbaines. Conformément aux recommandations de la commission des Lois adoptées le 17 septembre 2008 (2) et à la proposition n° 15 du rapport d'information précité, il ne sera donc désormais plus possible d'inscrire dans un fichier les personnes physiques ayant sollicité, exercé ou exerçant un mandat politique, syndical ou économique ou celles qui jouent un rôle institutionnel, économique, social ou religieux significatif.

L'article 17 prévoit ainsi d'autoriser un fichier exploité par les services chargés de la mission d'information générale du Gouvernement, c'est-à-dire, à la suite de la réforme du renseignement, la sous-direction de l'information générale (SDIG) de la direction centrale de la sécurité

(2) *EDVIGE en débat : les recommandations de la commission des Lois*, rapport d'information n° 1126, M. Jean-Luc Warsmann, président.

publique de la police nationale et la direction du renseignement de la préfecture de police de Paris.

Ce fichier pourra contenir des informations sur les personnes, groupes, organisations et personnes morales qui, en raison de leur activité individuelle ou collective, peuvent porter atteinte à la sécurité des personnes ou des biens, par le recours ou le soutien actif apporté à la violence, ainsi que les personnes entretenant ou ayant entretenu des relations directes et non fortuites avec ceux-ci. Les catégories de données personnelles dites sensibles pouvant être enregistrées sont détaillées également par la loi.

Dans l'esprit des principes rappelés par le Conseil constitutionnel, un régime particulier est prévu pour les mineurs de plus de treize ans. Il repose sur la notion de « droit à l'oubli », les données les concernant ne pouvant être conservées plus de trois ans à défaut d'intervention d'un nouvel évènement justifiant l'inscription dans le fichier. Le contrôle du respect de ces règles, sans préjudice de celui exercé par la CNIL, est confié à un magistrat du parquet. Une possibilité de dérogation à la règle de conservation des données pendant trois ans est autorisée, le service gestionnaire pouvant demander au magistrat précité la prolongation pour un an de la conservation des données. Le magistrat peut l'autoriser au vu des justifications présentées par le service responsable du traitement. En tout état de cause, il ne peut être ordonné une telle mesure à plus de deux reprises. Ainsi, un mineur inscrit dès l'âge de treize ans dans ce fichier, sous réserve de l'absence d'évènement nouveau, dispose de la garantie d'un effacement des données le concernant lorsqu'il aura atteint la majorité.

L'article 18 propose d'autoriser les services de la police et de la gendarmerie nationales à mettre en œuvre des traitements de données concernant les personnes faisant l'objet d'une enquête administrative, par exemple pour l'accès à des professions réglementées, à des zones sensibles, comme les zones aéroportuaires, ou à des informations classifiées. Les données dites sensibles pouvant être collectées s'agissant de ces personnes sont limitées aux activités en liaison avec des associations ou groupements de fait relevant de la loi du 10 janvier 1936 sur les groupes de combat ou les milices privées. Cette dernière loi vise notamment les associations ou groupements de fait provoquant à des manifestations armées, ayant pour but de porter atteinte par la force à la forme républicaine du Gouvernement ou provoquant à la discrimination, à la violence ou à la haine contre une personne ou un groupe de personnes à raison de leur origine, race ou religion.

La durée de conservation des informations est fixée à cinq ans et seules les données concernant des enquêtes administratives ayant conduit à une décision administrative défavorable peuvent être conservées.

Pour ces deux fichiers, il est prévu une « clause de rendez-vous », la durée de validité de la loi les autorisant étant fixée à trois ans et le Gouvernement devant présenter au Parlement trois mois avant cette échéance un rapport d'évaluation.

IV. – Le **titre IV** prévoit un cadre législatif adapté pour la mise en œuvre de traitements automatisés de données destinés à lutter contre certaines formes de délinquance à caractère sériel. Plusieurs initiatives locales d'expérimentations d'outils nouveaux et potentiellement très efficaces sont en effet en cours, et il est nécessaire de bien préciser le champ de ce qui est admis en la matière.

Ces traitements pourront collecter et exploiter des données à caractère personnel recueillies au cours des enquêtes et concernant les délits portant atteinte aux personnes punis de plus d'un an d'emprisonnement ou portant atteinte aux biens et puni de plus de deux ans d'emprisonnement. S'agissant des atteintes aux personnes, le seuil de peine proposé permet de lutter contre l'exhibition sexuelle imposée à la vue d'autrui dans un lieu accessible aux regards du public (article 222-32 du code pénal) ou les atteintes au respect dû aux morts, dont la violation ou la profanation de tombeaux et de sépultures (article 225-17 du code pénal). Pour les atteintes aux biens, le seuil de deux ans d'emprisonnement permet de recueillir dans ces traitements des éléments sur les infractions de destruction, dégradation ou détérioration d'un bien appartenant à autrui (article 322-1 du code pénal) et en cas de délit de « fausse alerte », prévu à l'article 322-14 du code pénal.

Compte tenu de la nature des infractions considérées, la durée de conservation des données est limitée à trois ans. Les victimes disposent, quant à elles, d'un droit d'accès direct aux informations les concernant et peuvent en demander l'effacement en cas de condamnation définitive de l'auteur. En outre, il est prévu que ces traitements ne puissent faire l'objet d'aucune interconnexion avec un autre traitement ou fichier.

Là encore, il est prévu que l'autorisation de ce type de traitements est valable pour une durée de trois ans.

V. – Enfin, l'article 20 propose de mieux encadrer les conditions dans lesquelles il est possible de réaliser un prélèvement biologique à des fins de comparaison sur une personne à l'encontre de laquelle il existe une « *raison plausible* » de soupçonner qu'elle a commis un crime ou un délit. Le texte proposé renvoie donc à la liste des infractions pour lesquelles un prélèvement biologique est possible en vue d'enregistrer un profil dans le fichier national automatisé des empreintes génétiques, telle qu'elle figure à l'article 706-55 du code de procédure pénale.

PROPOSITION DE LOI

TITRE I^ER

MODIFICATIONS DE LA LOI N° 78-17 DU 6 JANVIER 1978 RELATIVE À L'INFORMATIQUE, AUX FICHIERS ET AUX LIBERTÉS

Article 1^er

Au IV de l'article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les mots : « au II de l'article 26 », sont remplacés par les mots : « au I ou au III de l'article 26 ».

Article 2

① Le dernier alinéa de l'article 11 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est complété par la phrase suivante :

② « Préalablement à la présentation de son rapport public annuel, la commission fait connaître aux ministres concernés et aux organismes qui mettent en œuvre des traitements de données à caractère personnel pour le compte de l'État les observations provisoires sur lesquelles elle estime nécessaire de susciter leurs remarques. »

Article 3

Au 1° du I de l'article 13 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, après les mots : « par le Sénat », insérer les mots : « de manière à assurer une représentation pluraliste ».

Article 4

① Après le troisième alinéa de l'article 16 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, l'alinéa suivant est inséré :

② « – au V de l'article 26 ; ».

Article 5

① I. – L'article 26 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est ainsi rédigé :

② « *Art. 26.* – I. – Sont autorisés par la loi les traitements ou catégories de traitements de données à caractère personnel mis en œuvre pour le compte de l'État et :

③ « 1° Qui intéressent la sécurité publique ;

④ « 2° Ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté.

⑤ « Les catégories de traitements de données à caractère personnel sont constituées par les traitements qui répondent à une même finalité, portent sur de mêmes catégories de données et ont les mêmes catégories de destinataires.

⑥ « L'avis de la Commission nationale de l'informatique et des libertés mentionné au *a* du 4° de l'article 11 sur tout projet de loi autorisant la création d'un tel traitement ou d'une telle catégorie de traitements de données est transmis au Parlement simultanément au dépôt du projet de loi.

⑦ « II. – La loi autorisant un traitement ou une catégorie de traitements de données mentionnés au I prévoit :

⑧ « – leurs finalités ;

⑨ « – les services responsables ;

⑩ « – la nature des données à caractère personnel prévues au I de l'article 8 dont la collecte, la conservation et le traitement sont autorisés, dès lors que la finalité du traitement l'exige ;

⑪ « – l'origine de ces données et les catégories de personnes concernées ;

⑫ « – la durée de conservation des informations traitées ;

⑬ « – les destinataires ou catégories de destinataires des informations enregistrées ;

⑭ « – la nature du droit d'accès des personnes figurant dans les traitements de données aux informations qui les concernent ;

⑮ « – les interconnexions autorisées avec d'autres traitements de données.

⑯ « III. – Sont autorisés par décret en Conseil d'État du ou des ministres compétents, après avis motivé et publié de la commission, les traitements de données à caractère personnel mis en œuvre pour le compte de l'État et qui intéressent la sûreté de l'État ou la défense.

⑰ « Ces traitements peuvent être dispensés, par décret en Conseil d'État, de la publication de l'acte réglementaire qui les autorise. Pour ces traitements :

⑱ « – est publié en même temps que le décret autorisant la dispense de la publication de l'acte, le sens de l'avis émis par la commission ;

⑲ « – l'acte réglementaire est transmis à la délégation parlementaire au renseignement.

⑳ « IV. – Les modalités d'application des dispositions mentionnées au I sont fixées par arrêté du ou des ministres compétents. Si les traitements portent sur des données mentionnées au I de l'article 8, ces modalités sont fixées par décret en Conseil d'État.

㉑ « La commission publie un avis motivé sur tout projet d'acte réglementaire pris par le ou les ministres concernés en application d'une loi autorisant un traitement ou une catégorie de traitements de données conformément au I.

㉒ « V. – Un protocole d'accord entre la commission et le ou les ministres concernés détermine les modalités selon lesquelles les demandes d'avis sur les éléments d'information énumérés à l'article 30 sont adressées à la commission lors des principales étapes de la création d'un traitement de données préalablement à la publication de l'acte réglementaire prévu au III ou au IV. »

㉓ II. – Le protocole d'accord mentionné dans le dernier alinéa du I est conclu dans un délai d'un an à compter de la publication de la présente loi.

Article 6

① Le III de l'article 27 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est ainsi rédigé :

② « III. – Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par un acte réglementaire unique. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation. »

Article 7

Au I de l'article 28 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les mots : « des articles 26 ou 27 », sont remplacés par les mots : « des III ou IV de l'article 26 ou de l'article 27 ».

Article 8

① L'article 29 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est ainsi modifié :

② 1° Le premier alinéa de cet article est ainsi rédigé :

③ « I. – Les actes autorisant la création d'un traitement en application de l'article 25, du III de l'article 26 et de l'article 27 précisent : ».

④ 2° Cet article est complété par un II ainsi rédigé :

⑤ « II. – Les actes réglementaires pris en application d'une loi autorisant un traitement ou une catégorie de traitements de données conformément au I de l'article 26 précisent :

⑥ 1° La dénomination du traitement ;

⑦ 2° Le service auprès duquel s'exerce le droit d'accès défini au chapitre VII ;

⑧ 3° Les catégories de données à caractère personnel enregistrées ;

⑨ 4° Le cas échéant, les dérogations à l'obligation d'information prévue au V de l'article 32. »

Article 9

Au premier alinéa du I de l'article 31 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les mots : « au III de l'article 26 », sont remplacés par les mots : « au deuxième alinéa du III de l'article 26 ».

Article 10

Aux 1°, 2° et 3° du II de l'article 45 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les mots : « au II de l'article 26 », sont remplacés par les mots : « au III de l'article 26 ».

Article 11

Au premier alinéa de l'article 49 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les mots : « au II de l'article 26 », sont remplacés par les mots : « au III de l'article 26 ».

Article 12

Au huitième alinéa de l'article 69 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les mots : « au II de l'article 26 », sont remplacés par les mots : « au III de l'article 26 ».

Article 13

① Le deuxième alinéa du III de l'article 6 *nonies* de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires est complété par la phrase suivante :

② « Sont transmis à la délégation les actes réglementaires autorisant des traitements de données à caractère personnel pris en application du premier alinéa du III de l'article 26 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et dispensés de la publication conformément au deuxième alinéa du III du même article. »

TITRE II

CONTRÔLE DES FICHIERS D'ANTÉCÉDENTS JUDICIAIRES

Article 14

① I. – Les traitements automatisés d'informations nominatives mentionnés au I de l'article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure sont placés sous le contrôle d'un procureur général.

② II. – Les personnes mentionnées au II de l'article 21 de la loi n° 2003-239 précitée peuvent saisir ce magistrat lorsque les données qui les concernent présentent un risque d'inexactitude et sont susceptibles de leur faire subir un préjudice immédiat et sérieux.

③ Le magistrat ordonne sans délai au responsable du traitement de procéder aux rectifications nécessaires en cas de requalification judiciaire. En cas de décision de non-lieu ou de classement sans suite, il peut ordonner l'effacement des données personnelles.

Article 15

① I. – Le III de l'article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure est ainsi modifié :

② 1° Après la deuxième phrase, il est inséré une phrase ainsi rédigée :

③ « Le procureur de la République se prononce sur les suites qu'il convient de donner aux demandes d'effacement ou de rectification dans un délai d'un mois. » ;

④ 2° À la dernière phrase, les mots : «, lorsqu'elles sont motivées par une insuffisance de charges, » sont supprimés ;

⑤ 3° Après la dernière phrase, il est inséré une phrase ainsi rédigée :

⑥ « Les décisions d'effacement ou de rectification des informations nominatives prises par le procureur de la République sont transmises aux responsables de tous les traitements automatisés pour lesquels ces décisions ont des conséquences sur la durée de conservation des données personnelles. »

⑦ II. – La seconde phrase du V de l'article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure est ainsi rédigée :

⑧ « Il précise notamment la liste des contraventions mentionnées au I, la durée de conservation des informations enregistrées, les modalités d'habilitation des personnes mentionnées au IV ainsi que les conditions dans lesquelles :

⑨ « – les personnes mentionnées au premier alinéa du II peuvent exercer leur droit d'accès de manière indirecte, conformément aux dispositions de l'article 41 de la loi n° 78-17 précitée ;

⑩ « – les personnes mentionnées au deuxième alinéa du II peuvent exercer leur droit d'accès directement auprès du responsable du traitement, conformément aux dispositions de l'article 39 de la loi n° 78-17 précitée. »

Article 16

① L'article 397-5 du code de procédure pénale est complété par l'alinéa suivant :

② « Si le procureur de la République envisage de faire mention d'éléments concernant le prévenu et figurant dans un traitement automatisé d'informations nominatives prévu par l'article 21 de la loi n° 2003-239 du 18 mars 2003 relative à la sécurité intérieure, ces informations doivent figurer dans le dossier mentionné à l'article 393. »

TITRE III

FICHIERS D'INFORMATION GÉNÉRALE ET D'ENQUÊTES ADMINISTRATIVES

Article 17

① I. – Les services de la direction centrale de la sécurité publique de la police nationale en charge de la mission d'information générale du Gouvernement, ainsi que les services de la préfecture de police de Paris assurant la même mission, sont autorisés à mettre en œuvre des traitements de données à caractère personnel concernant les personnes, groupes, organisations et personnes morales qui, en raison de leur activité individuelle ou collective, peuvent porter atteinte à la sécurité des

personnes ou des biens, par le recours ou le soutien actif apporté à la violence, ainsi que les personnes entretenant ou ayant entretenu des relations directes et non fortuites avec ceux-ci.

② II. – Par dérogation à l'article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, sont autorisés, pour les seules fins mentionnées au I, la collecte, la conservation et le traitement par les services précités des données susceptibles de faire apparaître :

③ – les signes physiques particuliers et objectifs comme éléments de signalement ;

④ – les activités politiques, philosophiques, religieuses ou syndicales.

⑤ III. – Conformément à l'article 6 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et dans la stricte mesure où elles sont nécessaires à la poursuite des finalités mentionnée au I, peuvent être enregistrées dans les traitements précités les catégories de données à caractère personnel suivantes :

⑥ – motif de l'enregistrement des données ;

⑦ – informations ayant trait à l'état civil et à la profession ;

⑧ – adresses physiques, numéros de téléphone et adresses électroniques ;

⑨ – photographies ;

⑩ – titres d'identité ;

⑪ – immatriculation des véhicules ;

⑫ – déplacements ;

⑬ – informations patrimoniales ;

⑭ – antécédents judiciaires.

⑮ IV. – Les fonctionnaires des services mentionnés au I dûment habilités et dans la limite du besoin d'en connaître sont autorisés à accéder aux informations mentionnées au II et au III. La communication de ces informations aux services de la police et de la gendarmerie est subordonnée à une demande écrite qui précise l'identité du consultant, l'objet et les motifs de la consultation. Cette demande ne peut être agréée que par le

sous-directeur de l'information générale ou par le responsable du service départemental d'information générale.

⑯ V. – Conformément à l'article 6 de la loi n° 78-17 précitée, les données mentionnées aux II et III sont conservées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées.

⑰ VI. – Les traitements de données à caractère personnel mentionnés au I peuvent concerner des mineurs de plus de treize ans qui, en raison de leur activité individuelle ou collective, peuvent porter atteinte à la sécurité des personnes ou des biens, par le recours ou le soutien actif apporté à la violence. Les données mentionnées au II et au III concernant ces mineurs ne peuvent être conservées plus de trois ans après l'intervention du dernier évènement ayant justifié leur enregistrement.

⑱ VII. – Les traitements mentionnés au I sont placés sous le contrôle d'un magistrat du parquet. Ce magistrat est chargé de vérifier le respect des règles de conservation des données mentionnées au VI.

⑲ Si, malgré l'absence de nouvel évènement au terme du délai précité de trois ans, le service responsable d'un traitement mentionné au I souhaite y maintenir les informations concernant une personne mentionnée au VI, il présente au magistrat l'ensemble des éléments justifiant cette demande. Le magistrat peut autoriser ce maintien pour une durée d'un an. Un nouvel examen de la situation de la personne concernée intervient à l'issue de ce délai. La prolongation de la durée de conservation des données ne peut être ordonnée plus de deux fois.

⑳ Ce magistrat peut ordonner toutes mesures nécessaires à l'exercice de son contrôle, telles que saisies ou copies d'informations, ainsi que l'effacement d'enregistrements illicites.

㉑ Les pouvoirs qui lui sont confiés s'exercent sans préjudice du contrôle effectué par la Commission nationale de l'informatique et des libertés en application de la loi n° 78-17 précitée.

㉒ VIII. – Les traitements prévus au I ne font l'objet d'aucune interconnexion avec d'autres traitements ou fichiers.

㉓ IX. – Le droit d'accès des personnes mentionnées au I à ces traitements s'exerce de manière indirecte, conformément aux dispositions de l'article 41 de la loi n° 78-17 précitée.

㉔ X. – Les dispositions de cet article sont applicables pendant trois années à compter de la publication de la présente loi. Le Gouvernement remet au Parlement un rapport sur l'application de cet article trois mois avant l'expiration du délai précité.

Article 18

① I. – Les services de la police et de la gendarmerie nationales chargés des enquêtes administratives mentionnées à l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité sont autorisés à mettre en œuvre des traitements de données à caractère personnel concernant les personnes de plus de seize ans faisant l'objet de telles enquêtes.

② II. – Par dérogation à l'article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, sont autorisés, pour les seules fins mentionnées au I, la collecte, la conservation et le traitement par les services précités des données concernant les activités en relation avec des associations ou groupements de fait mentionnés à l'article 1 de la loi du 10 janvier 1936 sur les groupes de combat et milices privées.

③ III. – Conformément à l'article 6 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, et dans la stricte mesure où elles sont nécessaires à la poursuite de la finalité mentionnée au I, peuvent en outre être enregistrées les catégories de données à caractère personnel suivantes :

④ – motif de l'enregistrement des données ;

⑤ – informations ayant trait à l'état civil et à la profession ;

⑥ – adresses physiques, numéros de téléphone et adresses électroniques ;

⑦ – photographies ;

⑧ – titres d'identité ;

⑨ – déplacements ;

⑩ – informations patrimoniales ;

⑪ – antécédents judiciaires.

⑫ IV. – Les données mentionnées aux II et au III ne peuvent être collectées, conservées et traitées que dans la stricte mesure où elles sont nécessaires pour déterminer si le comportement des intéressés n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées compte tenu de leur nature.

⑬ Seules les données concernant les personnes ayant fait l'objet d'une décision administrative défavorable peuvent être conservées, pour une durée de cinq ans à compter de leur enregistrement.

⑭ V. – Dans la limite du besoin d'en connaître, sont autorisés à accéder aux données mentionnées aux II et III les personnels spécialement habilités et individuellement désignés de la police et de la gendarmerie nationales.

⑮ VI. – Les traitements prévus au I ne font l'objet d'aucune interconnexion avec d'autres traitements ou fichiers.

⑯ VII. – Le droit d'accès des personnes mentionnées au I à ces traitements s'exerce de manière indirecte, conformément aux dispositions de l'article 41 de la loi n° 78-17 précitée.

⑰ VIII. – Les dispositions de cet article sont applicables pendant trois années à compter de la publication de la présente loi. Le Gouvernement remet au Parlement un rapport sur l'application de cet article trois mois avant l'expiration du délai précité.

TITRE IV

FICHIERS DE RAPPROCHEMENTS EN MATIÈRE DÉLICTUELLE

Article 19

① Après l'article 21-1 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, il est inséré un article 21-2 ainsi rédigé :

② « *Art. 21-2.* – I. – Les services et les unités de la police et de la gendarmerie nationales chargés d'une mission de police judiciaire peuvent mettre en œuvre des traitements automatisés de données à caractère personnel collectées au cours des enquêtes préliminaires ou de flagrance ou des investigations exécutées sur commission rogatoire afin de faciliter la constatation des délits présentant un caractère sériel, d'en rassembler les

preuves et d'en identifier les auteurs, grâce à l'établissement de liens entre les individus, les événements ou les infractions pouvant mettre en évidence ce caractère sériel :

③ « – par le rapprochement d'informations de police technique et scientifique recueillies sur les lieux des infractions ainsi que des modes opératoires ;

④ « – ou par l'établissement de rapprochements à partir des informations transmises entre officiers de police judiciaire au titre de l'article D. 3 du code de procédure pénale.

⑤ « Ces traitements peuvent concerner tout délit portant atteinte aux personnes puni de plus d'un an d'emprisonnement ou portant atteinte aux biens et puni de plus de deux ans d'emprisonnement.

⑥ « II. – Par dérogation à l'article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, sont autorisés, pour les seules fins mentionnées au I, la collecte, la conservation et le traitement par les services précités des données susceptibles de faire apparaître les signes physiques particuliers et objectifs comme éléments de signalement.

⑦ « III. – Ces traitements peuvent contenir des données :

⑧ « 1° Sur les personnes de plus de treize ans à l'encontre desquelles il existe des indices graves ou concordants qu'elles aient pu participer, comme auteurs ou complices, à la commission d'une infraction mentionnée au I. L'enregistrement des données concernant ces personnes peut intervenir, le cas échéant, après leur condamnation ;

⑨ « 2° Sur les personnes victimes d'une infraction mentionnée au I, sans limitation d'âge.

⑩ « IV. – La durée de conservation des données décomptée à partir de la date de leur enregistrement dans ces traitements est au maximum de trois ans.

⑪ « V. – Les personnes mentionnées au 2° du III peuvent demander l'effacement des données les concernant enregistrées dans le traitement dès lors que l'auteur des faits a été définitivement condamné.

⑫ « VI. – Les dispositions du III de l'article 21 de la loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure sont applicables à ces traitements.

⑬ « VII. – Sont destinataires des données à caractère personnel mentionnées au présent article :

⑭ « – les personnels spécialement habilités et individuellement désignés de la police et de la gendarmerie nationales ;

⑮ « – les magistrats du parquet et les magistrats instructeurs, pour les recherches relatives aux informations dont ils sont saisis.

⑯ « L'habilitation précise la nature des données auxquelles elle autorise l'accès.

⑰ « VIII. – Les traitements prévus au I ne font l'objet d'aucune interconnexion avec d'autres traitements ou fichiers.

⑱ « IX. – En application de l'article 26 de la loi n° 78-17 précitée, un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, fixe les modalités d'application du présent article.

⑲ « Il précise les conditions dans lesquelles :

⑳ « – les personnes mentionnées au 1° du III peuvent exercer leur droit d'accès de manière indirecte, conformément aux dispositions de l'article 41 de la loi n° 78-17 précitée ;

㉑ « – les personnes mentionnées au 2° du III peuvent exercer leur droit d'accès directement auprès du responsable du traitement, conformément aux dispositions de l'article 39 de la loi n° 78-17 précitée.

㉒ « X. – Les dispositions de cet article sont applicables pendant trois années à compter de la publication de la présente loi. Le Gouvernement remet au Parlement un rapport sur l'application de cet article trois mois avant l'expiration du délai précité. »

TITRE V

FICHIER NATIONAL AUTOMATISÉ DES EMPREINTES GÉNÉTIQUES

Article 20

Au troisième alinéa de l'article 706-54 du code de procédure pénale, les mots : « un crime ou un délit », sont remplacés par les mots : « l'une des infractions mentionnées à l'article 706-55 ».

DIRECTIVE ET PROCÈS-VERBAL DE DESTRUCTION DU FAR

GENDARMERIE NATIONALE Groupement de gendarmerie Interdépartemental de Paris				PROCÈS-VERBAL DE RENSEIGNEMENT ADMINISTRATIF		
Code Unité	P.V	Année	Nmr Dossier Justice		N° pièce	N° feuillet
05063	00243	2011			1	1/1

Analyse et références

Objet	Élimination du fichier alphabétique de renseignement (FAR).
Références	- Loi du 06 août 2004 prévoyant la suppression des fichiers mécanographiques et la destruction des fiches papier du FAR - Note-express n° 134 843 GEND/SF/EL du 17 décembre 2010 de la DGGN. - Note-express n° 845 RGIF/BMAT-AMOD du 03 janvier 2011

Le mardi 15 février 2011 à 14 heures et 15 minutes,
Nous soussigné Capitaine BRILLET, Jacques en résidence à PARIS
Vu l'article L.3211-3 du code de la défense
Nous trouvant 43, rue Bruneseau à PARIS (75013), rapportons les opérations suivantes :

Destruction du fichier alphabétique de renseignement et procédés utilisés

Conditionnement des big-bags :
Le fichier alphabétique de renseignement des brigades du groupement de gendarmerie du Val d'Oise est déposé dans des conteneurs « big-bags ». Chaque conteneur « big-bag » est fermé hermétiquement et scellé par l'O.P.J. TC du groupement du Val d'Oise.

Transport des big-bags :
Les big-bags particulièrement lourd sont transportés sur palette du groupement de gendarmerie du Val d'Oise jusqu'au centre d'incinération d'Ivry à Paris avec un poids lourd de la R.G.I.F. conduit sous bonne escorte par un militaire de l'arme.

Incinération :
Les big-bags sont transportés au moyen d'un élévateur jusqu'à la trémie.
Les big-bags sont ensuite ouverts par des personnels de l'arme et leur contenu est déposé dans la trémie, dernier rempart avant le four.

Le 15 février 2011 à 14 heures 15, nous nous présentons à l'usine d'incinération d'Ivry à Paris (75013), 43, rue Bruneseau, afin de procéder à l'incinération du fichier alphabétique de renseignement des brigades du groupement de gendarmerie du Val d'Oise.
Nous sommes reçus par Monsieur VAUCHEL, Daniel, contremaître de la société « Ivry Paris 13 ».
Le fichier alphabétique de renseignement des brigades de ce département composé de 9 big-bags scellés (2 tonnes 610) est transporté sous bonne escorte par des personnels de l'arme de Cergy vers l'incinérateur d'Ivry à Paris. Le contenu des big-bags est ensuite déposé par ces mêmes personnels dans la trémie, dernier rempart avant le four.

Le capitaine BRILLET, Jacques, officier adjoint de commandement affecté au groupement de gendarmerie interdépartemental à Paris, officier de police judiciaire territorialement compétent certifie que les 9 big-bags du FAR du val d'Oise, absorbés par la trappe du four ont bien été incinérés.

(DESTINATAIRES)	*Date de clôture*	*Vu et transmis par :*
[1] - M. le à Monsieur le Préfet du Val d'Oise à Cergy [1] - M. le à Monsieur le Procureur général sous couvert de M. le Procureur de la République à Pontoise [1] - au Général d'armée, Directeur général de la gendarmerie nationale (SRO BVO DGGN) [1] - au Général de corps d'armée, commandant la RGIF (bureau matériel AMOD) [1] - au Colonel, commandant le groupement de gendarmerie du Val d'Oise [1] - au Lieutenant-colonel, commandant le groupement de gendarmerie interdépartemental de Paris [1] - Archives	15 février 2011 *Signature(s)*	Le capitaine BRILLET, Jacques Le 15 février 2011

GENDARMERIE NATIONALE R.G.I.F SECTION D'APPUI JUDICIAIRE G.A.E.E. VINCENNES	RENSEIGNEMENT ADMINISTRATIF DEMANDE DE PRESTATION DE SERVICE		
UPVA 04977/00055/2011		Pièce n°	Feuillet n°

Analyse, référence ou objet :

L'an deux mille onze, le quatorze février à VINCENNES (94),
Nous, soussigné, PERRAUD Jean-Luc, capitaine, officier de police judiciaire à la section d'appui judiciaire, groupe appui évaluation enquête en résidence à VINCENNES.
Vu l'article L.3211-3 du code de la Défense,
Vu la loi du 06 août 2004 prévoyant la suppression des fichiers mécanographiques et la destruction des fiches papiers du FAR,
Rapportons les opérations suivantes que nous avons effectuées,

Prions

Nom et prénom : Monsieur VAUCHEL Daniel contremaître principal de la société « IVRY PARIS 13 »

de procéder aux actes indiqués ci-après qui ne sauraient être différés sans nuire au déroulement de l'enquête :

Mission : Bien vouloir procéder à la destruction par incinération de 09 (NEUF) BIG SACS contenant des fiches cartonnées du FAR-GGD-95, et ce, en présence constante du capitaine BRILLET Jacques, officier logistique du Groupement de Gendarmerie Interdépartemental de PARIS (GGIP).

L'Officier de Police Judiciaire :

Nous, soussigné, BRILLET Jacques, Capitaine,
Officier logistique du GGIP, OPJ
remettons la présente réquisition à la personne requise,
qui nous déclare :

☒ accepter la mission qui lui est confiée

☐ refuser de déférer à la réquisition

A IVRY

La personne présente

L'Officier de Police Judiciaire

Le capitaine BRILLET

UIOM IVRY-PARIS XIII
43 Rue BRUNESEAU
75013 PARIS

IP 13

PROCES VERBAL DE DESTRUCTION

Nous certifions ce jour, avoir procédé à la destruction de ...9.....colis, mis en trémies par vos services, dont nous n'avons pas vérifié le contenu.

PARIS Le : Mardi 15/02/2011.

Le responsable IVRY-PARIS XIII

Nom	VAUCHEL.
Fonction	Contremaitre
Heure	14h15.
signature	

Le responsable des apports

Nom	BRILLET
Fonction	Agent Logistique
Heure	14h15
signature	

NOTE-EXPRESS

~~NON PROTÉGÉ~~ (1)	DIFFUSION RESTREINTE (1)	~~CONFIDENTIEL DÉFENSE~~ (1)

ORIGINE	:	DIRECTION GÉNÉRALE DE LA GENDARMERIE NATIONALE
DESTINATAIRES (pour action)	:	– Région de gendarmerie : d'Île-de-France, d'Aquitaine, de Midi-Pyrénées, de Poitou-Charentes, du Limousin, de Bretagne, de Haute-Normandie, de Basse-Normandie, des Pays-de-la-Loire, du Centre, du Rhône-Alpes, d'Auvergne, de Provence-Alpes-Côte-d'Azur, de Languedoc-Roussillon, de Corse, de Lorraine, d'Alsace, de Champagne-Ardennes, de Bourgogne, de Franche-Comté, du Nord-Pas-de-Calais, de Picardie ; – Commandement de la gendarmerie : de la Guadeloupe, de la Guyane-Française, de la Martinique, de La Réunion, de Mayotte, pour la Polynésie-Française, pour la Nouvelle-Calédonie, pour Saint-Pierre-et-Miquelon. – Gendarmeries spécialisées : Armement – Maritime - Air - Transports aériens – Centre technique de la Gendarmerie nationale. – Service Historique de la Défense – Département gendarmerie nationale.
DESTINATAIRE : (pour information)		– Direction des opérations et de l'emploi.

N° 134 843 17 DEC 2010
GEND/SF/EL

OBJET : Élimination du fichier alphabétique de renseignement (FAR).

PRIMO : Afin de se conformer aux dispositions de la loi du 06 août 2004 prévoyant la suppression des fichiers mécanographiques et la destruction des fiches papier du FAR le recours à une prestation externalisée au plan national ne peut être réalisé au vu des délais incompressibles liés aux dispositions du code des marchés publics. Les régions de gendarmerie doivent donc organiser en interne la destruction des fiches suivant des modalités à leur initiative, sous réserve du cadre général fixé ci-après. Cette demande devra être réalisée avant le 31/01/2011.

SECUNDO : La destruction physique des fiches s'effectuera au niveau minimal du groupement après un regroupement préalable. Les opérations de destruction seront systématiquement suivies et contrôlées par un officier de police judiciaire territorialement compétent qui certifiera par procès-verbal de renseignement administratif le caractère effectif et total de la destruction de toutes les fiches.

TERTIO : Le PV/RA sera rédigé en 3 exemplaires : un destiné au Procureur Général sous couvert du procureur de la République territorialement compétent, un envoyé au Préfet du département et le dernier exemplaire transmis à la DGGN/DOE/SDDOP/BVO par la voie hiérarchique.

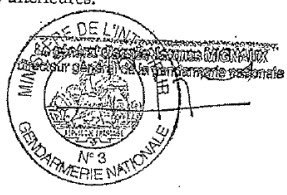
.../...

(1) Rayer la mention inutile - Mettre le TIMBRE correspondant

QUARTO : Les autorités administratives et judiciaires seront préalablement averties des dates et lieux de destruction du FAR. Les commandants de région ont toute latitude pour inviter ces autorités à assister à l'élimination du FAR. Toutefois, aucune communication ne sera faite à l'extérieur de l'institution.

QUINTO : A titre de conservation du patrimoine, les fichiers des brigades de gendarmerie de : COLMAR ; LUNEL ; GUJAN-MAESTRAS et PLOERMEL seront, à la diligence des régions de gendarmerie de rattachement, reversés au Service Historique de la Défense – Département gendarmerie nationale -

SEXTO : La destruction des fichiers de la batellerie et des personnes nées à l'étranger FPNE fera l'objet de directives ultérieures.



NON PROTEGE ~~DIFFUSION RESTREINTE~~ ~~CONFIDENTIEL DEFENSE~~	X	NOTE-EXPRESS	N° 845 RGIF/BMAT-AMOD Du 03 janvier 2011.

ORIGINE	REGION DE GENDARMERIE D'ILE DE FRANCE
DESTINATAIRES	Pour action : Tous groupements de gendarmerie départementale.
	Copies intérieures : Chef d'état-major ; Adjoint au chef d'état-major « Organisation Emploi ».
OBJET	Élimination du fichier alphabétique de renseignement (FAR).
REFERENCE (S)	Note-express n° 134843 GEND/SF/EL du 17 décembre 2010.
PIECE(S) JOINTE(S)	Note-express n° 134843 GEND/SF/EL du 17 décembre 2010. Annexe 1 : Procédures de conditionnement et de collecte du FAR.
TEXTE	PRIMO : En application des directives énoncées dans la note-express de référence, chaque région de gendarmerie doit procéder à la destruction des fiches contenues dans les fichiers alphabétiques de renseignements (FAR) de ses formations pour le 31/01/2011. Le mode d'élimination physique étant à arrêter au plan régional, il est décidé de procéder à l'incinération des FAR par collecte organisée au sein de chaque groupement de gendarmerie départementale. Les modalités relatives à l'établissement des conventions avec les sites d'incinération (sites envisagés : Melun, Créteil, Thiverval et Ivry-sur-Seine) sont à la charge du bureau Matériels-AMOD de la RGIF. Cette disposition ne s'oppose pas à la recherche de conventions locales par les groupements de gendarmerie départementale, dont ils rendront compte sous référence du présent timbre au bureau Matériels-AMOD. SECUNDO : Les destinataires pour action feront procéder, dès que possible, au conditionnement des fiches de renseignement par les unités détentrices de FAR suivant le mode opératoire défini en annexe. Au niveau de chaque groupement, la collecte des FAR à reverser sera à mettre en œuvre pour leur conditionnement. Le bureau Matériels-AMOD fournira des conteneurs de type « big bag ». A compter du 12 janvier 2011, une première dotation de conteneurs « big bag » sera mise en place auprès du magasin RGIF de Beynes. Elle pourra être enlevée par les responsables « gestionnaire matériels » des GGD. En fonction du volume à conditionner, chaque chef du GSRH du GGD formulera son besoin en conteneurs « big bag » auprès de la section Matériels du bureau Matériels-AMOD. Des directives ultérieures seront communiquées pour le conditionnement et le transport des conteneurs.

EXTRAIT DE LA RÉPONSE DU MINISTRE DE L'INTÉRIEUR DU 9 AOÛT 2011

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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

Liste des fichiers de police déclarés depuis 1er juillet 2009 et en cours de constitution

Depuis le 1er juillet 2009, le ministère de l'intérieur a procédé à la déclaration de 12 fichiers de police sur les fondements de l'article 26 ou de l'article 27 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Nom du traitement	Description	Service utilisateur	Références du texte	Fondement juridique (loi informatique et libertés)
SALVAC	Système d'analyse des liens de la violence associée aux crimes	DGPN	décret n° 2009-786 du 23 juin 2009 publié au JO du 25/10/2009	article 26
EASP	Enquêtes administratives liées à la sécurité publique	DGPN	décret n° 2009-1250 du 16 octobre 2009 publié au JO du 18/10/2009	article 26
PASP	Prévention des atteintes à la sécurité publique	DGPN	décret n° 2009-1249 du 16 octobre 2009 publié au JO du 18/10/2009	article 26
COURSES & JEUX	Fichiers des courses et jeux	DLPAJ	arrêté du 8 novembre 2010 publié au JO du 14/11/2010	article 26
ESCORTE	Gestion des extractions et des transfèrements	DGPN	décret n° 2011-397 du 13 avril 2011 publié au JO du 15/04/2011	article 26 II
FINIADA	Fichier national des interdits d'acquisition et de détention d'armes	DLPAJ	décret n°2011-374 du 5 avril 2011 publié au JO du 7/04/2011	article L. 2336-6 du code de la défense
LRPGN	rédaction de procédures	DGGN	décret n° 2011-111 du 27 janvier 2011 paru au JORF le 29 janvier 2011	article 26
PULS@R	Gestion des services, du courrier, des procédures unités et suivi des amendes forfaitaires	DGGN	2 arrêtés signés le 2 décembre 2010 et publiés au JO du 17/12/2010	articles 23 et 26

LRPPN 2	Application de recueil de la documentation opérationnelle et d'informations statistiques sur les enquêtes	DGPN	décret n° 2011-110 du 27 janvier 2011 publié au JO du 29/01/2011	article 26
GIPASP	Traitement de données à caractère personnel relatif à la gestion de l'information et la prévention des atteintes à la sécurité publique	DGGN	décret n° 2011-340 du 29 mars 2011	article 26 II
GSI	Gestion des sollicitations et des interventions	DGGN	décret n° 2011-341 du 29 mars 2011	article 26
SIDPP	Sécurisation des interventions et demandes particulières de protection	Préfecture de police	décret n° 2011-342 du 29 mars 2011	article 26

Par ailleurs, le ministère de l'intérieur a initié plusieurs projets qui nécessiteront la publication de textes réglementaires. Ces projets, dont vous trouverez la liste ci-après, sont en cours d'élaboration :

Nom du traitement	Description	Service utilisateur	Fondement juridique
NMCI	Modernisation du registre de main courante informatisée	DGPN	article 26, arrêté
RLOPPA	Déclaration des répertoires locaux pour les opérations de protection des personnes âgées de plus de 65 ans	DGPN	article 26, arrêté
TPJ	Traitement des antécédents judiciaires mutualisant le STIC et JUDEX	DGGN/DGPN	article 26 II, décret
OCLDI	Fichiers de travail de l'office central de lutte contre la délinquance itinérante (OCLDI) relevant de la direction générale de la Gendarmerie nationale	DGGN	article 26 II, décret
ANACRIM	Logiciels de rapprochement judiciaires de la Gendarmerie nationale	DGGN	article 230-20 et suivants du code de procédure pénale, décret
GESTEREXT	Gestion du terrorisme et des extrémités à potentialité violente	Préfecture de police	article 26, décret
OCTOPUS	Outil de centralisation et de traitement opérationnel des procédures et des utilisateurs de signatures	Préfecture de police	article 26-I-2°, arrêté
LUPIN	Enregistrement des données constatées sur les scènes de	Préfecture de police	article 230-20 et suivants du

	commission de délits passibles de plus de trois ans de prison		code de procédure pénale, décret
ARES	Automatisation du registre des entrées et sorties des recours en matière de contravention	Préfecture de police	article 26, arrêté
CORAIL	Cellule opérationnelle de rapprochement et d'analyse des infractions liées	Préfecture de police	article 26
PIO	Partage de l'information opérationnelle	DGGN/DGPN	article 26
Application de stockage des procédures clôturées	Dématérialisation du stockage des procédures judiciaires et administratives de la gendarmerie	DGGN	article 26
FOVES	Fichiers des objets et des véhicules signalés	DGGN/DGPN/Douanes	article 26
Système de traitement des images des véhicules volés	Base de données des photos de véhicules volés provenant des radars automatiques	DGGN	article 26
Bases criminalistiques départementales	Stockage des éléments matériels probants découverts sur les scènes de crimes ou délits	DGGN	article 26
CALIOPE	Lutte contre la pédopornographie	DGGN	article 26
Base « victimes non identifiées »	Base sur les personnes décédées non identifiées : résolution des disparitions inquiétantes	DGGN	article 26
Base escroqueries	Escroqueries	DGGN	article 26
Base objets d'arts volés	Objets volés	DGGN	article 26

Le ministère a enfin entrepris la déclaration de 6 actes-cadres sur le fondement de l'article 26 de la loi du 6 janvier 1978. L'un d'entre eux a été déclaré le 2 mai 2011.

Nom du traitement	Description	Service utilisateur	Fondement juridique
Fichier des résidents des zones sécurisées évènements majeurs	Arrêté du 2 mai 2011 relatif aux traitements automatisés de données à caractère personnel dénommés « fichiers des résidents des zones de sécurité » créés à l'occasion d'un événement majeur publié au JO du 3/05/2011	DGPN	article 26
Registre des fourrières et des immobilisations	Recenser et gérer les véhicules mis en fourrière ou immobilisés par les services de police à la suite d'une infraction et les véhicules retrouvés à l'état d'épave (abandonnés ou brûlés)	DGPN	article 26
Contrôle judiciaire	Suivi du respect, par les personnes soumises à un contrôle judiciaire par décision d'un juge d'instruction ou de toute juridiction, de l'obligation de se présenter périodiquement à un service de la police ou une unité de la gendarmerie nationales	Préfecture de police	article 26
Assignation à résidence	Suivi des dossiers des personnes qui, dans le cadre d'une mesure d'assignation à résidence prononcée par ordonnance du juge des libertés et de la détention ou par arrêté préfectoral, doivent se présenter périodiquement à un service de la police ou une unité de la gendarmerie nationales	Préfecture de police	article 26
Permission de sortir	Suivi des informations relatives aux permissions de sortir des établissements pénitentiaires et mesures de placement en semi-liberté, accordées par le juge d'application des peines	Préfecture de police	article 26
Appel à témoins	Enregistrement des communications téléphoniques de la ligne appel à témoins	Préfecture de police	article 26

JUGEMENT DU TRIBUNAL DE COMPIÈGNE DU 28 JUIN 2011

Cour d'Appel d'Amiens
Tribunal de Grande Instance de Compiègne
Chambre correctionnelle

Jugement du : **28/06/2011**

N° minute : 562/11

N° parquet : 10188000028

EXTRAIT
des Minutes du Secrétariat Greffe
du Tribunal de Grande Instance
de COMPIÈGNE (60)

Plaidé le 03/05/2011
Délibéré le 28/06/2011

JUGEMENT CORRECTIONNEL

A l'audience publique du Tribunal Correctionnel de Compiègne le TROIS MAI DEUX MILLE ONZE,

Composé de :
Monsieur GOUEZ Patrick, président,

Mademoiselle JACQUELINE Clémence, assesseur,
Madame MARONI Ronit-Lydia, assesseur,

assisté de Madame BERA Madeleine, greffière,

en présence de Madame LONGUAR Léa, substitut du Procureur de la République

a été appelée l'affaire

ENTRE :

Le PROCUREUR DE LA REPUBLIQUE, près ce tribunal, demandeur et poursuivant

ET

Prévenu
Nom : **MATHIEU Xavier**
né le 15 mai 1965 à PARIS 75014
de MATHIEU André et de BRAULT Irène
Nationalité : française
Situation familiale : marié
Situation professionnelle :
Antécédents judiciaires : déjà condamné
demeurant : 64 ruelle Jabelet 60400 PORQUERICOURT FRANCE
Situation pénale : libre

comparant assisté de Maître DUFRESNE-CASTETS Marie-Laure avocat au barreau de CAEN,

Prévenu du chef de :
REFUS, PAR PERSONNE CONDAMNEE POUR DELIT, DE SE SOUMETTRE AU PRELEVEMENT BIOLOGIQUE DESTINE A L'IDENTIFICATION DE SON EMPREINTE GENETIQUE faits commis le 6 juillet 2010 à NOYON

DEBATS

A l'appel de la cause, le président a constaté la présence et l'identité de MATHIEU Xavier et a donné connaissance de l'acte qui a saisi le tribunal.

Le président a instruit l'affaire, interrogé le prévenu présent sur les faits et reçu ses déclarations.

Puis il a été procédé à l'audition, hors la présence l'un de l'autre, des deux témoins cités par la défense, lesquels ont prêté serment de « dire toute la vérité, rien que la vérité ».

Le ministère public a été entendu en ses réquisitions.

Maître DUFRESNE-CASTETS Marie-Laure, conseil de MATHIEU Xavier a été entendu en sa plaidoirie.

Le prévenu a eu la parole en dernier.

Le greffier a tenu note du déroulement des débats.

Puis à l'issue des débats, le président a informé les parties présentes ou régulièrement représentées que le jugement serait prononcé le 28 juin 2011 à 08:30.

A cette date, le jugement a été rendu publiquement par le tribunal,

Composé de :
Monsieur GOUEZ Patrick, président,

Mademoiselle JACQUELINE Clémence, assesseur,
Madame CHASSEUR Perrine, assesseur,

Assisté de Madame BERA Madeleine, greffière, et en présence du ministère public, en vertu des dispositions de la loi du 30 décembre 1985.

Le tribunal a délibéré et statué conformément à la loi en ces termes :

MATHIEU Xavier a comparu à l'audience assisté de son conseil ; il y a lieu de statuer contradictoirement à son égard.

Il est prévenu d'avoir à NOYON, Le 6 juillet 2010, en tout cas sur le territoire national et depuis temps non couvert par la prescription, refusé de se soumettre au prélèvement biologique destiné à l'identification de son empreinte génétique, par personne condamnée pour délit, faits prévus par ART.706-56 §I AL.1, §II AL.1, ART.706-54 AL.1, ART.706-55, ART.R.53-21 C.P.P. et réprimés par ART.706-56 §II AL.1,AL.3 C.P.P.

Par arrêt de la Cour d'appel d'Amiens en date du 5 février 2010, Xavier MATHIEU était condamné pour des faits de dégradation volontaire de biens, délit prévu par les articles 322-2 1°, et 322-1 al.1 du Code pénal, réprimé par les articles 322-2 al.1, 322-15 1°, 2°, 3°, 5° et 6° du Code pénal.

En application des dispositions de l'article 706-55 du code de procédure pénale, le parquet général de la Cour d'appel d'Amiens a demandé qu'il soit procédé à un prélèvement biologique sur sa personne en vue de la saisie de son empreinte génétique dans le fichier national automatisé des empreintes génétiques.

Le 6 juillet 2010, Xavier MATHIEU refusait cette mesure de prélèvement. Il déclarait aux enquêteurs qu'il ne voulait pas que son empreinte ADN figurât sur le même fichier que celui des auteurs d'infractions sexuelles. Il estimait n'avoir pas à être placé sur le même plan que ces délinquants, ajoutant que ce prélèvement porterait atteinte à sa dignité, lui même n'ayant rien d'un délinquant sexuel.

Devant le tribunal, le prévenu reprend les mêmes arguments.

En premier lieu, le prévenu soulève in limine litis des conclusions d'illégalité de l'article R 53-10 § II, issu du décret n° 2004-470 du 25 mai 2004. Il soutient qu'en attribuant au Ministère public le pouvoir de décider de manière discrétionnaire du choix des personnes qui seront convoquées pour un prélèvement d'ADN, cet article donne au même Ministère public un moyen d'influer sur un élément constitutif de l'infraction dont il est rappelé que, s'agissant de règles relevant de la procédure pénale, leur édiction est réservée à la compétence exclusive du législateur.

Sur le fond, il conteste sa responsabilité pénale. Il déclare qu'il est un militant syndical qui a agi à visage découvert pour préserver son emploi, qui constitue son unique moyen de vivre, et à ses yeux un élément primordial de sa reconnaissance sociale ; il reprend qu'il n'est ni un criminel, ni un violeur, ni un pédophile.

Il fait notamment valoir :
-la non-conformité des articles 706-54 à 706-56 - 1 du Code de procédure pénale aux dispositions de la CEDH, demandant dès lors que l'application de ces textes soit écartée
-Que ce prélèvement constitue une atteinte à sa dignité, est disproportionné à la gravité des faits, et est contraire à l'article préliminaire du code de procédure pénale.

SUR CE

La matérialité des faits n'est pas discutée.

Sur l'exception d'illégalité :

Dans son article 706-54, relatif aux principes et à la définition du fichier national automatisé des empreintes génétiques, le Code de procédure pénale prévoit dans son dernier alinéa qu'un décret en Conseil d'État, en l'espèce l'article R 53-10, détermine les modalités d'application du présent texte. Dans son article 706-55, le même code prévoit que ce fichier centralise les traces et empreintes génétiques des auteurs des infractions parmi lesquelles figure celle pour laquelle Xavier MATHIEU a été condamné. Enfin, l'article 706-56 § II prévoit l'infraction de refus de se soumettre au prélèvement, et les peines encourues en pareil cas.

C'est ainsi que les éléments constitutifs, notamment légal et matériel, de l'infraction de refus de se soumettre au prélèvement, et les pénalités encourues sont édictées par le législateur, l'autorité administrative, dans son article R 53-10, ne prévoyant que les modalités d'application du prélèvement et de l'enregistrement des empreintes génétiques au fichier national, d'où il suit que l'exception d'illégalité sera rejetée.

Sur le fond :

Selon les dispositions de l'article 6 de la loi 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, dont il sera rappelé qu'elle a vocation à s'appliquer à tous les fichiers, quelle qu'en soit la nature *(cf. décision du conseil constitutionnel 2003-67 du 13 mars 2003, 26 ème considérant)*, les données recueillies pour les fichiers doivent notamment être adéquates, pertinentes et non excessives au regard, des finalités pour lesquelles elles sont collectées, et de leur traitement ultérieur. En l'occurrence, le FNAEG est destiné à centraliser les empreintes génétiques issues de traces biologiques en vue de faciliter l'identification et la recherche des auteurs d'infractions.

En l'espèce, la condamnation du prévenu est intervenue pour des faits de dégradation volontaire de biens. Ces faits ont été commis en plein jour, dans le cadre d'une manifestation organisée, et s'inscrivent dans une logique parfaitement lisible de combat syndical, et non dans une démarche à vocation purement délinquante et antisociale. Dès lors, il existe bien une disproportion entre le but visé par la loi, qui est de permettre l'élucidation d'infractions commises en récidive en constituant un fichier recueillant l'empreinte ADN des délinquants, et les moyens pour y parvenir, dans le cas d'espèce, le prélèvement d'ADN sur Xavier MATHIEU, dont les faits qui lui valent d'être condamné, ne relèvent aucunement d'un engagement délibéré ou d'un cheminement conscient et volontaire dans la voie délinquante.

C'est ainsi que le recueil de l'ADN du prévenu en vue de son identification et de sa recherche était inadéquat, non pertinent, inutile et excessif. Le prélèvement n'étant pas justifié au regard des dispositions de la loi du 6 janvier 1978 susvisée, il ne saurait être fait grief au prévenu de s'y refuser.

D'où il suit que Xavier MATHIEU sera renvoyé des fins de la poursuite.

PAR CES MOTIFS

Le tribunal, statuant publiquement, en premier ressort et contradictoirement à l'égard de MATHIEU Xavier,

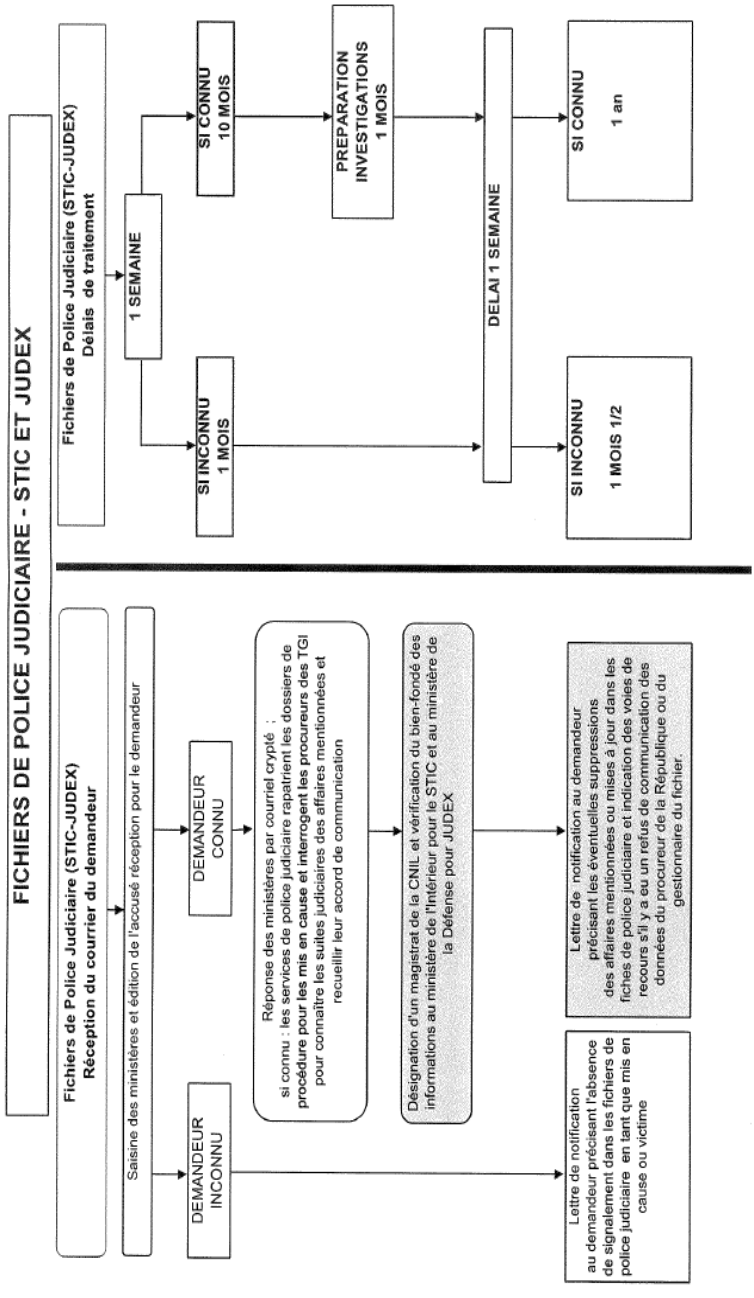
RenvoieMATHIEU Xavier des fins de la poursuite ;

et le présent jugement ayant été signé par le président et la greffière.

LA GREFFIERE LE PRESIDENT

POUR COPIE CERTIFIÉE CONFORME
28/06/2016
LE GREFFIER

SCHÉMA DE LA PROCÉDURE DE DROIT D'ACCÈS AUPRÈS DE LA CNIL



NOTE DU MINISTÈRE DE L'INTÉRIEUR RELATIVE AU FICHIER PASP DU 18 OCTOBRE 2009

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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

Le Préfet,
Directeur du cabinet

Paris, le 18 octobre 2009.

NOTE

à

Mesdames et Messieurs les préfets
Monsieur le Préfet de police
Monsieur le Préfet, Directeur général de la police nationale
Monsieur le Préfet, Secrétaire général du ministère

OBJET : Publication au *Journal officiel* du décret portant création d'un traitement de données à caractère personnel relatif à la prévention des atteintes à la sécurité publique et du décret portant création d'un traitement automatisé de données à caractère personnel relatif aux enquêtes administratives liées à la sécurité publique

P. J. : Décrets n° IOCD0918274D et IOCD0918264D

Je vous prie de bien vouloir trouver ci-joint, pour votre information, le décret portant création d'un traitement de données à caractère personnel relatif à la prévention des atteintes à la sécurité publique et le décret portant création d'un traitement automatisé de données à caractère personnel relatif aux enquêtes administratives liées à la sécurité publique tous deux parus au *Journal officiel* daté du dimanche 18 octobre 2009.

1) Décret portant création d'un traitement de données à caractère personnel relatif à la prévention des atteintes à la sécurité publique

La réforme des services de renseignement du ministère de l'intérieur mise en œuvre par le décret n° 2008-612 du 27 juin 2008 a conduit à supprimer la direction de la surveillance du territoire (DST) et la direction centrale des renseignements généraux (DCRG). Les missions qu'elles assumaient jusqu'alors ont fait l'objet d'une nouvelle répartition, rendant nécessaire un nouveau fondement juridique pour remplacer le fichier des renseignements généraux institué par le décret n° 91-1051 du 14 octobre 1991.

.../...

La mission de renseignement intérieur, au sens strict, est désormais prise en charge par la direction centrale du renseignement intérieur (DCRI), chargée de lutter contre toutes les activités susceptibles de porter atteinte aux intérêts fondamentaux de la nation.

Une mission d'information générale, assurée auparavant par la DCRG, a été confiée à la direction centrale de la sécurité publique (DCSP). Cette mission relève à Paris de la préfecture de police.

La nouvelle mission d'information générale de la DCSP consiste notamment à rechercher, collecter et analyser des renseignements utiles aux préfets ou au Gouvernement pour le maintien de l'ordre public, notamment lorsque ceux-ci se trouvent confrontés à des phénomènes de violence, qui peuvent par exemple être le fait de bandes.

Le traitement de données à caractère personnel dont le présent décret propose la création est un outil indispensable à la sous-direction de l'information générale de la DCSP, aux services d'information générale des directions départementales de la sécurité publique et aux services équivalents de la préfecture de police, pour l'accomplissement de leur mission de prévention des atteintes à la sécurité publique.

Dans la mesure où l'application est susceptible de contenir des données dites « sensibles », au sens du I de l'article 8 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, elle est, conformément aux dispositions du II de l'article 26 de la même loi, autorisée par un décret en Conseil d'Etat après avis motivé et publié de la Commission nationale de l'informatique et des libertés (CNIL). Il s'agit là de la procédure la plus exigeante en matière de création de traitement de données.

Allant au-delà même des strictes exigences légales, le présent décret assortit la création de ce traitement de garanties importantes notamment en termes de durée de conservation des données, de contrôle de leur utilisation et de traçabilité des consultations.

En pratique, le traitement est constitué d'une base centrale unique automatisée qui a pour fonction d'indexer les données de fond détenues par les différents services concernés. Ces dernières se présentent sous trois formes différentes :

- les données contenues dans les fichiers automatisés détenus par les services de renseignement, qui regroupent environ un tiers du total des données ;

- les données figurant dans des fichiers manuels, qui représentent la majorité des données ;

- des documents non indexés qui se trouvent soit dans les services centraux de la sous-direction de l'information générale de la DCSP, où ils sont entièrement numérisés, soit dans les services départementaux, où ils sont pour partie numérisés, pour partie sur support papier.

.../...

L'**article 1er** du décret autorise le ministère de l'intérieur à mettre en œuvre un traitement de données à caractère personnel destiné à prévenir des atteintes à la sécurité publique. La finalité assignée à ce traitement fait obstacle à un fichage aléatoire des personnes. Seules celles dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique sont susceptibles de figurer dans ce fichier. Ce critère d'« activité » est un critère objectif et limite de façon claire le périmètre du traitement.

La référence à la « sécurité publique » est destinée à recouvrir aussi bien les cas de délinquance violente que la criminalité « en col blanc » ou le trafic de stupéfiants. L'efficacité du traitement suppose que puissent également être appréhendés les cas de délinquance grave dans lesquels il n'est pas recouru à la violence physique.

Le second alinéa de l'article premier précise que ce traitement a notamment pour finalité de collecter des données sur les personnes susceptibles de se livrer à des actions violentes collectives, en particulier des violences urbaines et des violences commises dans le contexte de manifestations sportives. L'analyse de telles données permettra de mieux cerner le fonctionnement de certaines bandes urbaines et de prévenir ainsi des troubles futurs à la sécurité publique.

L'**article 2** définit les catégories de données susceptibles de figurer dans le présent traitement. Ces données sont celles strictement nécessaires à la poursuite de la finalité assignée au traitement.

Pour les besoins de la préservation de la sécurité publique, peuvent être enregistrées dans le traitement les données suivantes :

- motif de l'enregistrement des données ;
- informations ayant trait à l'état civil, à la nationalité et à la profession, adresses physiques, numéros de téléphone et adresses électroniques ;
- signes physiques particuliers et objectifs, photographies ;
- titres d'identité ;
- immatriculation des véhicules ;
- informations patrimoniales ;
- activités publiques, comportement et déplacements ;
- agissements susceptibles de recevoir une qualification pénale ;
- personnes entretenant ou ayant entretenu des relations directes et non fortuites avec l'intéressé ;

Cet article précise par ailleurs que le traitement ne comporte aucun dispositif permettant la reconnaissance « faciale » d'une personne à partir de sa photographie.

S'agissant de la référence à des « signes physiques particuliers et objectifs », elle s'entend de signes distinctifs tels, par exemple, qu'un tatouage ou une cicatrice. Elle ne renvoie en aucune manière à des critères de type ethno-racial.

.../...

Les données relatives aux « personnes entretenant ou ayant entretenu des relations directes et non fortuites avec l'intéressé » se limitent à l'identité de ces personnes. Les autres catégories de données ne peuvent être recueillies que si la personne présente elle-même un risque d'atteinte à la sécurité publique justifiant son enregistrement dans le fichier.

L'**article 3** est relatif aux données dites « sensibles ».

Le principe est celui de l'interdiction du recueil et du traitement des données mentionnées à l'article 8 de la loi « informatique et libertés » et dites « sensibles ». Ainsi, le présent traitement ne pourra en aucun cas comporter de données relatives aux origines raciales ou ethniques, à la santé ou à l'orientation ou à la vie sexuelle des personnes.

Conformément aux dérogations prévues par le législateur et dans le strict cadre de la finalité de sécurité publique du traitement, seuls trois types de données sensibles pourront, à titre dérogatoire, y être enregistrés. Il s'agit des signes physiques particuliers et objectifs pris comme éléments de signalement des personnes, de l'origine géographique ou des données relatives aux activités politiques, philosophiques, religieuses ou syndicales.

Pourront par exemple figurer au titre des signes physiques particuliers et objectifs comme éléments contribuant au signalement de la personne, la couleur de ses cheveux, une cicatrice ou un tatouage. Les données relatives à l'origine géographique des personnes se limitent à l'indication de leur provenance ; en effet, dans les phénomènes de bandes, l'appartenance à un même quartier ou le partage d'un même lieu de naissance peuvent, par exemple, jouer un rôle déterminant.

Enfin, c'est uniquement dans le cas où des activités dans les domaines politique, philosophique, religieux ou syndical pourraient porter atteinte à la sécurité publique que ces activités pourraient être mentionnées. Dès lors, la simple adhésion ou participation à un mouvement politique démocratique, ou une candidature dans ce cadre à une élection, ne sauraient, en aucune façon, être mentionnées. En revanche, des activités sectaires qui porteraient atteinte à la sécurité publique pourraient légitimement y figurer.

L'**article 3** précise en outre qu'il continue d'être interdit aux services compétents de procéder à une recherche automatisée en utilisant comme critère de recherche l'une des trois catégories de données sensibles susceptibles de figurer dans le traitement.

L'**article 4** prévoit une durée de conservation pour les données recueillies dans le traitement. Il constitue une garantie supplémentaire, au-delà même des obligations imposées par la loi, en fixant à 10 ans la durée de conservation des données concernant les majeurs enregistrées dans le traitement. Cette durée est calculée à compter de la date du dernier événement de nature à faire apparaître un risque d'atteinte à la sécurité publique ayant donné lieu à un enregistrement dans le fichier.

.../...

L'**article 5** détermine un régime spécifique concernant les mineurs. Eu égard à l'implication croissante de mineurs dans des actes contraires à la sécurité publique, mais également pour tenir compte de l'évolution de leur personnalité avec l'âge, le Gouvernement estime absolument nécessaire d'autoriser le recueil des données concernant les mineurs d'au moins 13 ans, mais en instaurant à leur égard un véritable « droit à l'oubli ».

Comme pour les majeurs, l'enregistrement des données ne se fonde pas sur de simples suspicions mais résulte de la constatation d'activités qui indiquent que le mineur peut porter atteinte à la sécurité publique.

La durée maximale de conservation des données concernant ces mineurs est fixée à trois ans à compter de l'intervention du dernier événement ayant donné lieu à un enregistrement dans le traitement. Elle est donc nettement plus brève que la durée maximale de conservation applicable aux personnes majeures.

Un décret complémentaire à venir instituera un référent national chargé de veiller au respect effectif de ce droit à l'oubli pour les mineurs. Il est prévu qu'il contrôle une fois par an et à l'âge de la majorité si l'inscription de données concernant le mineur est justifiée.

L'**article 6** énumère les personnes susceptibles d'accéder au traitement et celles qui peuvent recevoir des informations qui en sont extraites.

Trois catégories de personnes peuvent accéder au traitement pour les besoins de leur mission générale de prévention des atteintes à la sécurité publique. Cet accès leur donne à la fois la faculté d'alimenter le traitement automatisé en informations nouvelles et de consulter les informations qui y sont contenues.

Ces trois catégories sont :

- les fonctionnaires relevant de la sous-direction de l'information générale de la direction centrale de la sécurité publique, individuellement désignés et spécialement habilités par le directeur central de la sécurité publique ;

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

- les fonctionnaires affectés dans les services de la préfecture de police en charge du renseignement, individuellement désignés et spécialement habilités par le préfet de police.

Outre ces trois catégories, les services chargés de la prévention des violences urbaines et des phénomènes de « bandes » pourront accéder au traitement pour les seuls besoins de leur mission.

.../...

Par ailleurs, pourront être rendus destinataires des informations figurant dans le traitement, dans la limite du besoin d'en connaître, les autorités publiques compétentes pour demander la réalisation d'enquêtes administratives, ainsi que les agents relevant d'un service de la police nationale ou de la gendarmerie nationale. Pour ces derniers agents, l'accès aux informations ne sera toutefois consenti qu'au cas par cas, à la suite d'une demande expresse visée du chef de service du demandeur, précisant l'identité du consultant, l'objet et les motifs de la consultation. Cette qualité de destinataire ne confère pas à leur bénéficiaire la faculté d'alimenter le traitement en informations nouvelles.

L'**article 7** prévoit que l'application mise en œuvre garantit la traçabilité des opérations d'alimentation, consultation et modification des données contenues dans le traitement automatisé de manière à ce que toutes les consultations de ce traitement soient enregistrées et à assurer ainsi une totale transparence. Les données de consultation (identifiant du consultant, date et heure de la consultation) sont systématiquement enregistrées et conservées pendant une durée de cinq ans. Cette durée, qui excède la durée de la prescription du délit de consultations irrégulières du traitement, a été choisie afin de permettre l'exercice de poursuites pénales dans de tels cas.

L'**article 8** prévoit que le traitement et les fichiers ne feront l'objet d'aucune interconnexion, aucun rapprochement, ni aucune forme de mise en relation avec d'autres traitements ou fichiers. Cette disposition constitue une garantie supplémentaire pour les personnes concernées.

L'**article 9** définit les modalités d'exercice du droit d'accès aux données. Conformément aux dispositions prévues par l'article 41 de la loi du 6 janvier 1978, ce droit d'accès s'exercera auprès de la CNIL, dans le cadre du droit d'accès dit « indirect », traditionnel en matière de fichiers de sécurité publique.

Le même article dispose que conformément aux dispositions des articles 32 et 38 de la loi du 6 janvier 1978, les droits d'information et d'opposition ne s'appliquent pas en l'espèce. De tels droits sont en effet incompatibles avec la finalité de sécurité publique du traitement.

L'**article 10** prévoit que le traitement et les fichiers sont soumis au contrôle de la Commission nationale de l'informatique et des libertés. A cet égard, le traitement suit donc le régime de droit commun, tel qu'il est défini à l'article 44 de la loi « informatique et libertés ».

A ce contrôle, le Gouvernement ajoute l'obligation pour le directeur général de la police nationale de présenter chaque année un rapport, transmis à la commission nationale de l'informatique et des libertés, sur ses activités de vérification, de mise à jour et d'effacement des données enregistrées dans le traitement.

L'**article 11** modifie le décret n° 2007-914 du 15 mai 2007 pris pour l'application du dernier alinéa du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, qui fixe la liste des traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique.

.../...

L'**article 12** prévoit l'applicabilité outre-mer des dispositions du présent décret.

2) Décret portant création d'un traitement automatisé de données à caractère personnel relatif aux enquêtes administratives liées à la sécurité publique

La réforme des services de renseignement du ministère de l'intérieur rappelée plus haut a rendu nécessaire un nouveau fondement juridique pour remplacer le fichier des renseignements généraux.

A ce titre, le traitement de données à caractère personnel dont le présent décret propose la création est un outil indispensable à la sous-direction de l'information générale de la DCSP, aux services d'information générale des directions départementales de la sécurité publique et aux services équivalents de la préfecture de police, pour l'accomplissement de leur mission de réalisation d'enquêtes administratives nécessaires à la prévention des atteintes à la sécurité publique.

La création de ce nouveau fichier qui poursuit une finalité de sécurité publique et est susceptible de contenir certaines données dites « sensibles », au sens du I de l'article 8 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés doit, conformément aux dispositions du II de l'article 26 de la même loi, être autorisée par un décret en Conseil d'Etat après avis motivé et publié de la Commission nationale de l'informatique et des libertés (CNIL). Il s'agit là de la procédure la plus exigeante en matière de création de fichiers.

Allant au-delà des exigences légales, le présent décret assortit la création de ce traitement de garanties importantes notamment en termes de durée de conservation des données, de contrôle de leur utilisation et de traçabilité des consultations.

L'**article 1er** du décret expose la finalité du traitement automatisé, qui est destiné à faciliter la réalisation des enquêtes administratives diligentées pour des raisons de sécurité publique. La facilité offerte par ce traitement tient au fait qu'il conservera, pendant une durée encadrée, la mémoire des résultats des enquêtes administratives passées. Ces enquêtes y gagneront en rapidité et en fiabilité.

Les enquêtes administratives dont il s'agit sont définies par renvoi au premier alinéa de l'article 17-1 de la loi n°95-73 du 21 janvier 1995. Cet article ouvre la possibilité de procéder à des enquêtes administratives pour déterminer si le comportement des personnes physiques ou morales est compatible avec l'exercice de certaines fonctions ou de certaines missions représentant des enjeux en termes de sécurité publique.

.../...

Il s'agit, en pratique, des enquêtes administratives menées préalablement aux décisions administratives de recrutement, d'affectation, d'autorisation, d'agrément ou d'habilitation, prévues par des dispositions législatives ou réglementaires. Elles peuvent concerner des emplois publics participant à l'exercice des missions de souveraineté de l'Etat, des emplois publics ou privés relevant du domaine de la sécurité ou de la défense, des emplois privés ou des activités privées réglementées relevant des domaines des jeux, paris et courses, l'accès à des zones protégées en raison de la nature de l'activité qui s'y exerce (centrales nucléaires, aéroports, etc...), l'utilisation de matériels ou produits présentant un caractère dangereux. La liste en est fixée par le décret n°2005-1124 du 6 septembre 2005.

L'**article 2** définit les catégories de données susceptibles de figurer dans le présent traitement. Il rappelle, par une référence à l'article 6 de la loi « informatique et libertés », que seules les données pertinentes au regard de la finalité de sécurité publique poursuivie peuvent être collectées. En d'autres termes, l'objet des enquêtes administratives étant de s'assurer en particulier que l'accès à certaines fonctions ou à certains lieux sensibles ne comporte aucun risque en termes de sécurité publique, le traitement ne contiendra que les données strictement nécessaires à cette appréciation.

Dans ce cadre, peuvent être enregistrées dans le traitement les données suivantes :

- motif de l'enquête ;
- informations ayant trait à l'état civil, à la nationalité et à la profession, adresses physiques, numéros de téléphone et adresses électroniques ;
- photographie ;
- titres d'identité.

Est également conservé, au format « image », le rapport de l'enquête administrative permettant de vérifier si le comportement de la personne concernée est compatible avec l'exercice des fonctions ou des missions envisagées.

La fonction de recherche automatisée incluse dans le traitement ne peut être activée qu'à partir des données relatives au motif de l'enquête (recrutement dans certaines fonctions, accès à certains lieux, etc.) ou des données d'identité. Une recherche à partir de la photographie d'une personne ou à partir des données de fond figurant au format « image » dans le rapport d'enquête est donc impossible. Ce traitement ne constitue donc pas un portail d'entrée permettant un accès indirect aux fichiers consultés pour les besoins de l'enquête. Lesdites données extraites d'autres fichiers sont en effet « gelées » dans le présent traitement au format « image » et ne peuvent être retrouvées dans le cadre d'une recherche automatisée.

L'**article 3** est relatif aux données dites « sensibles ». Le décret interdit le recueil de telles données dans le traitement lui-même.

Ne pourra être enregistrée dans le traitement aucune donnée relative à l'origine raciale ou ethnique d'une personne, à son état de santé ou à sa vie sexuelle ou à ses seules opinions politiques, philosophiques, religieuses ou syndicales.

.../...

C'est uniquement si un comportement, qui peut éventuellement avoir une motivation politique, philosophique, religieuse ou syndicale, est incompatible avec l'exercice des fonctions ou des missions envisagées que ce comportement pourra donner lieu à un enregistrement, en application de l'article 17-1 de la loi n° 95-73 du 21 janvier 1995, qui prévoit que : « Les décisions administratives de recrutement, d'affectation, d'autorisation, d'agrément ou d'habilitation, prévues par des dispositions législatives ou réglementaires, concernant soit les emplois publics participant à l'exercice des missions de souveraineté de l'Etat, soit les emplois publics ou privés relevant du domaine de la sécurité ou de la défense, soit les emplois privés ou activités privées réglementées relevant des domaines des jeux, paris et courses, soit l'accès à des zones protégées en raison de l'activité qui s'y exerce, soit l'utilisation de matériels ou produits présentant un caractère dangereux, peuvent être précédées d'enquêtes administratives destinées à vérifier que le comportement des personnes physiques ou morales intéressées n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées ».

Les remarques faites plus haut quant à l'impossibilité de procéder à une recherche automatisée à partir des données consignées au format « image » dans le rapport d'enquête valent naturellement pour les données sensibles susceptibles d'y figurer.

L'**article 4** limite à 5 ans la durée de conservation des données enregistrées dans le traitement. Cette durée est calculée à compter de la date de leur enregistrement, quel qu'ait été le résultat, favorable ou non, de l'enquête.

L'**article 5** dispose que le traitement peut contenir des données et informations relatives à des mineurs à la double condition qu'ils soient âgés de plus de 16 ans et qu'ils aient fait l'objet d'une enquête administrative les concernant directement. A titre d'exemple, un mineur de plus de 16 ans peut avoir fait l'objet d'une enquête administrative dans le cadre d'une procédure de recrutement.

L'**article 6** énumère les personnes susceptibles d'accéder au traitement et celles qui peuvent recevoir des informations qui en sont extraites.

Trois catégories de personnes peuvent accéder au traitement pour les besoins de leur mission. Cet accès leur donne à la fois la faculté d'alimenter le traitement automatisé en informations nouvelles et d'en consulter les informations existantes.

Ces trois catégories sont :

- les fonctionnaires relevant de la sous-direction de l'information générale de la direction centrale de la sécurité publique, individuellement désignés et spécialement habilités par le directeur central de la sécurité publique ;

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

- les fonctionnaires affectés dans les services de la préfecture de police en charge du renseignement, individuellement désignés et spécialement habilités par le préfet de police.

.../...

Par ailleurs, pourront être rendus destinataires des informations figurant dans le traitement, dans la limite du besoin d'en connaître, les agents relevant d'un service de la police nationale ou de la gendarmerie nationale, ainsi que les autorités publiques compétentes pour demander des enquêtes administratives. Cet accès ne sera toutefois consenti qu'au cas par cas, à la suite d'une demande expresse visée du chef de service du demandeur, précisant l'identité du consultant, l'objet et les motifs de la consultation.

L'**article 7** prévoit que l'application mise en œuvre garantit la traçabilité des opérations d'alimentation, consultation et modification des données contenues dans le traitement automatisé de manière à ce que toutes les consultations de ce traitement soient enregistrées et à assurer ainsi une totale transparence. Les données de consultation (identifiant du consultant, date et heure de la consultation) sont systématiquement enregistrées et conservées pendant une durée de cinq ans. Cette durée, qui excède la durée de la prescription du délit de consultations irrégulières du traitement, a été choisie afin de permettre l'exercice de poursuites pénales dans de tels cas.

L'**article 8** prévoit que le traitement ne fera l'objet d'aucune interconnexion avec d'autres traitements et fichiers. Cette disposition constitue une garantie supplémentaire pour les personnes concernées.

L'**article 9** définit les modalités d'exercice du droit d'accès aux données. Conformément aux dispositions prévues par l'article 41 de la loi du 6 janvier 1978, ce droit d'accès s'exercera auprès de la CNIL, dans le cadre du droit d'accès dit « indirect » traditionnel en matière de fichiers de sécurité publique.

Le même article dispose que le droit d'opposition prévus par l'article 38 de la loi du 6 janvier 1978 ne s'applique pas à ce traitement. L'exclusion du droit d'opposition, prévue à l'article 38 de la même loi, découle de façon logique de la finalité du traitement.

Pour ce qui concerne le droit d'information des personnes mentionnées dans le traitement, le Gouvernement n'a pas entendu faire usage de la faculté d'exclusion ouverte à l'article 32 de la loi du 6 janvier 1978. Un droit à l'information est donc reconnu aux personnes faisant l'objet d'enquêtes administratives à des fins de sécurité publique. En pratique, toute personne faisant l'objet d'une enquête administrative prévue par le premier alinéa de l'article 17-1 de la loi du 21 janvier 1995, sera informée que celle-ci peut donner lieu à une insertion dans le traitement.

L'**article 10** prévoit que le traitement et les fichiers sont soumis au contrôle de la Commission nationale de l'informatique et des libertés. A cet égard, le traitement suit donc le régime de droit commun, tel qu'il est défini à l'article 44 de la loi « informatique et libertés ».

A cette possibilité de contrôle prévue par la loi le Gouvernement a ajouté l'obligation pour le directeur général de la police nationale de présenter chaque année un rapport, transmis à la commission nationale de l'informatique et des libertés, de ses activités de vérification, de mise à jour et d'effacement des données enregistrées dans le traitement.

.../...

- 11 -

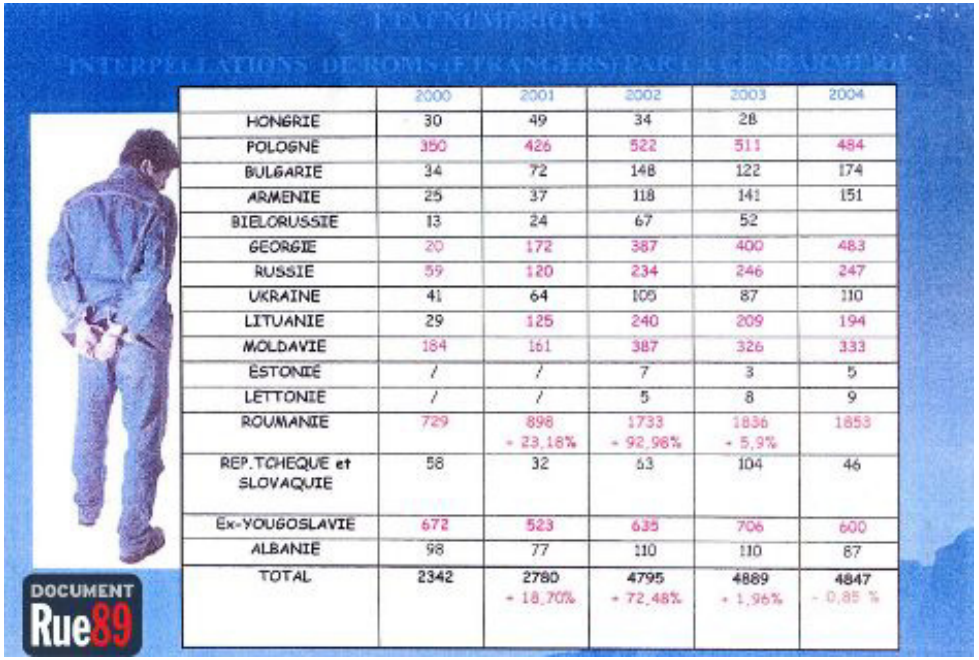
L'**article 11** prévoit l'applicabilité outre-mer des dispositions du présent décret.

Telles sont les informations qu'il m'a semblé important de vous communiquer dès la parution de ces textes.

Michel Barnier

TABLEAUX DE L'ÉTAT NUMÉRIQUE DES INTERPELLATIONS D'ÉTRANGERS PAR LA GENDARMERIE

EXTRAIT D'UNE PRÉSENTATION DE L'OCLDI PUBLIE PAR RUE89



	2000	2001	2002	2003	2004
HONGRIE	30	49	34	28	
POLOGNE	350	426	522	511	484
BULGARIE	34	72	148	122	174
ARMENIE	25	37	118	141	151
BIELORUSSIE	13	24	67	52	
GEORGIE	20	172	387	400	483
RUSSIE	59	120	234	246	247
UKRAINE	41	64	105	87	110
LITUANIE	29	125	240	209	194
MOLDAVIE	184	161	387	326	333
ESTONIE	/	/	7	3	5
LETTONIE	/	/	5	8	9
ROUMANIE	729	898 + 23,18%	1733 + 92,96%	1836 + 5,9%	1853
REP.TCHEQUE et SLOVAQUIE	58	32	53	104	46
Ex-YOUGOSLAVIE	672	523	635	706	600
ALBANIE	98	77	110	110	87
TOTAL	2342	2780 + 18,70%	4795 + 72,48%	4889 + 1,96%	4847 - 0,85 %

Source : article du 7 octobre 2010 publié sur le site Rue89.com.

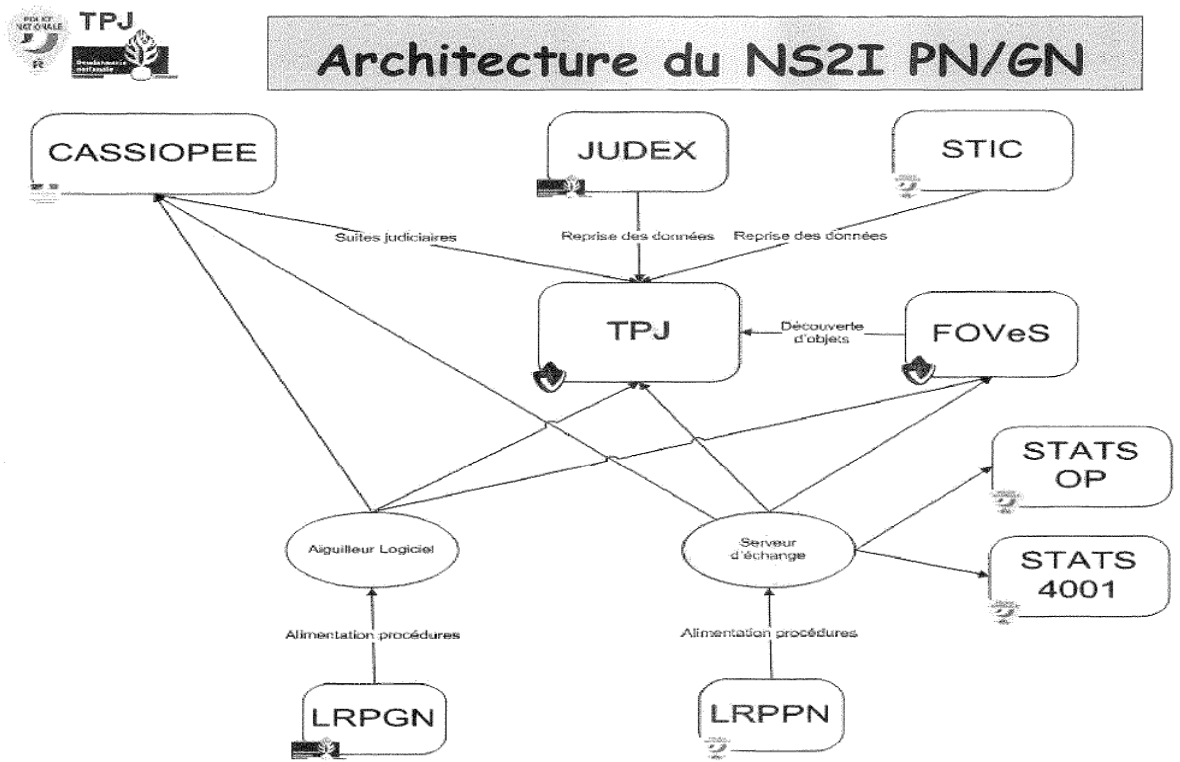
TABLEAU FOURNI PAR LA GENDARMERIE À LA MISSION D'INFORMATION

ETAT NUMERIQUE

DES INTERPELLATIONS D'ETRANGERS PAR LA GENDARMERIE

	2000	2001	2002	2003	2004
HONGRIE	30	49	34	28	44
POLOGNE	350	426	522	511	484
BULGARIE	34	72	148	122	174
ARMENIE	25	37	118	141	151
BIELORUSSIE	13	24	67	52	27
GEORGIE	20	172	387	400	483
RUSSIE	59	120	234	246	247
UKRAINE	41	64	105	87	110
LITUANIE	29	125	240	209	194
MOLDAVIE	184	161	387	326	333
ESTONIE	/	/	7	3	5
LETTONIE	/	/	5	8	9
ROUMANIE	729	898 + 23,18%	1733 + 92,98%	1836 + 5,9%	1853
REP.TCHEQUE et SLOVAQUIE	58	32	63	104	46
Ex-YOUGOSLAVIE	672	523	635	706	600
ALBANIE	98	77	110	110	87
TOTAL	2342	2780 + 18,70%	4795 + 72,48%	4889 + 1,96%	4847 - 0,85 %

SCHÉMA DU NOUVEL ENVIRONNEMENT INTÉGRÉ



FAC-SIMILÉ D'UNE FICHE DE NOTIFICATION AU FIJAISV

Annexe 1

FIJAIS

NOTIFICATION D'UNE INSCRIPTION

(régime de justification annuelle)

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Renseignements relatifs à l'autorité chargée de procéder à la notification des obligations :

Nom de la personne chargée de la notification :

Ministère : Justice Intérieur

Fonction, grade :

Adresse postale du service :

Numéro du dossier FIJAIS (si déjà inscrit):

Renseignements relatifs à l'identité de la personne concernée :

Nom :

Prénom(s) :

Nom d'usage :

Alias éventuels :

Sexe : M F

Date de naissance (en chiffres: jj/mm/aaaa) :

Lieu de naissance (ville et pays) :

Nationalité(s) :

Domicile ou résidence ou commune de rattachement :

Pour les personnes nées hors métropole et DOM :

Nom et prénoms du père :

Nom et prénoms de la mère :

Renseignements relatifs à la décision judiciaire

Date :

Autorité judiciaire à l'origine de la décision :

Par le présent procès verbal établi en trois exemplaires dont un remis à l'intéressé(e), un autre original transmis au gestionnaire du FIJAIS (SGFD, BP 22406, 44324 NANTES CEDEX 3) et le dernier conservé par la juridiction, M., Mme ..... se voit notifier **son inscription** au Fichier judiciaire national des auteurs d'infractions sexuelles ou violentes (FIJAIS) à raison de la décision susvisée et à ce titre, **ses obligations** en application de l'article 706-53-5 du code de procédure pénale :

I. de justifier de son adresse :

en se présentant auprès du commissariat de police ou de la brigade de gendarmerie de son domicile, ou **pour les personnes habitant la ville de Paris**, à la Direction de la Police Judiciaire - SEDJ - Unité Fijais - 1 avenue de la Porte de la Villette - 75019 PARIS..

OU

par lettre recommandée avec demande d'avis de réception auprès des services de police ou de gendarmerie précités, ou **pour les personnes habitant la ville de Paris**, à la Direction de la Police Judiciaire - SEDJ - Unité Fijais - 1 avenue de la Porte de la Villette - 75019 PARIS.

La première fois dans les quinze jours de la présente notification

- **sauf** si elle intervient moins de deux mois avant le premier jour du mois anniversaire de sa naissance;
- **sauf** si en qualité de personne déjà inscrite au FIJAIS, elle est déjà tenue de justifier de son adresse (auquel cas elle sera soumise au plus rigoureux des régimes qui ont pu lui être notifiés).

Puis dans tous les cas, une fois par an
Dans le courant du mois anniversaire de sa naissance (ou du mois de janvier si sa date de naissance est inconnue ou indéterminée).

La personne inscrite est informée :

- qu'elle doit justifier de son adresse au moyen de tout document daté de moins de trois mois à son nom (quittance, facture, relevé de compte...). Si le justificatif produit n'est pas à son nom, il doit être accompagné d'une attestation d'hébergement établie et signée par le titulaire du document.
- que si elle réside ou s'installe à l'étranger, il lui appartient de justifier de son domicile en adressant un courrier avec demande d'avis de réception au service gestionnaire du FIJAIS (SGFD - BP 22406 - 44324 NANTES CEDEX 3 - FRANCE) assorti d'un justificatif de domicile (voir paragraphe ci-dessus), visé par l'autorité étrangère ou le poste diplomatique ou consulaire dont elle dépend ;
- que son obligation de justifier cesse de s'appliquer pendant le temps où elle est incarcérée.

II. de déclarer ses changements d'adresse :

Au plus tard dans un délai de quinze jours après ce changement selon les mêmes modalités que pour la justification d'adresse au moyen de tout document daté de moins de trois mois à son nom (quittance, facture, relevé de compte...). Si le justificatif produit n'est pas à son nom, il doit être accompagné d'une attestation d'hébergement établie et signée par le titulaire du document.

La personne inscrite est informée :

- que tout manquement à ses obligations provoquera l'émission d'une alerte transmise aux services de police ou de gendarmerie de son domicile, pouvant entraîner son inscription dans le fichier des personnes recherchées ainsi que des poursuites pénales ;

- **que le non-respect de ses obligations est puni d'une peine de 2 ans d'emprisonnement et de 30.000 euros d'amende ;**

- qu'en application de la loi informatique et liberté et de l'article 706-53-9 du code de procédure pénale, elle peut obtenir communication de l'intégralité des informations enregistrées dans le fichier la concernant en s'adressant au procureur de la République de son domicile ou à l'agent diplomatique ou au consul de son domicile si elle réside à l'étranger ;

- qu'en application de l'article 706-53-7 du code de procédure pénale les administrations mentionnées à l'article R. 53-8-24 du même code peuvent interroger le fichier pour une personne ayant formé une demande de recrutement, d'affectation, d'autorisation, d'agrément ou d'habilitation concernant une activité ou une profession impliquant un contact avec des mineurs ou dont l'exercice d'une telle activité ou profession doit être contrôlé ;

- qu'elle pourra demander la rectification ou l'effacement dans les conditions des articles 706-53-10, R. 53-8-27 et suivants du code de procédure pénale auprès du procureur de la République de la juridiction de la condamnation à l'origine de son inscription ou, si la décision justifiant son inscription a été prise par une autorité judiciaire étrangère, auprès du procureur de la République près le tribunal de grande instance de Nantes ;

- que les règles de retrait de son identité dans le fichier sont définies par l'article 706-53-4 du code de procédure pénale : « Sans préjudice de l'application des dispositions des articles 706-53-9 et 706-53-10, les informations mentionnées à l'article 706-53-2 concernant une même personne sont retirées du fichier au décès de l'intéressé ou à l'expiration, à compter du jour où l'ensemble des décisions enregistrées ont cessé de produire tout effet, d'un délai de :
« 1° Trente ans s'il s'agit d'un crime ou d'un délit puni de dix ans d'emprisonnement ;
« 2° Vingt ans dans les autres cas.
« L'amnistie ou la réhabilitation ainsi que les règles propres à l'effacement des condamnations figurant au casier judiciaire n'entraînent pas l'effacement de ces informations.
« Ces informations ne peuvent, à elles seules, servir de preuve à la constatation de l'état de récidive.
« Les mentions prévues aux 1°, 2° et 5° de l'article 706-53-2 sont retirées du fichier en cas de décision définitive de non-lieu, de relaxe ou d'acquittement. Celles prévues au 5° sont également retirées en cas de cessation ou de mainlevée du contrôle judiciaire. »

le / / à

EN CAS DE REMISE A PERSONNE
Signature de l'intéressé(e) et s'il y a lieu du représentant légal (mineur, incapable)

Signature de l'autorité
chargée de procéder à la *notification*

EN CAS DE REMISE PAR LRAR
*Joindre **obligatoirement** l'original de l'accusé de réception*

NOTE DU DIRECTEUR GÉNÉRAL DE LA POLICE NATIONALE SUR LES CONDUITES À TENIR À CAS DE DÉFAUT DE JUSTIFICATION AU FIJAISV

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

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

DIRECTION GÉNÉRALE
DE LA POLICE NATIONALE
DGPN/Cab-11- [illegible]
Affaire suivie par : M.BONET
☎ 01 49 27 48 87
E-mail jerome.bonet@interieur.gouv.fr

Paris, le 29 JAN. 2011

Le préfet,
directeur général de la police nationale

à

destinataires in fine

Objet : Rappels sur la conduite à tenir en matière de défaut de justification ou de non changement d'adresse des personnes inscrites au fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes (FIJAIS)

La récente actualité me contraint à vous rappeler la procédure à suivre lors de la réception, par vos services, d'une alerte pour défaut de justification, générée par la défaillance d'un individu dans l'accomplissement des obligations découlant de son inscription au fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes (FIJAIS).

L'absence de justification de domicile ou de déclaration de changement d'adresse est constitutive d'une infraction délictuelle flagrante prévue par l'article 706-53-5 in fine du code de procédure pénale.

Dès réception d'une alerte pour défaut de justification (type DJ), des diligences doivent être immédiatement mises en œuvre afin de faire cesser cette infraction.

Après en avoir accusé réception sur l'application FIJAIS, l'officier de police judiciaire doit, dans les meilleurs délais, déclencher des recherches pour tenter de localiser le délinquant (convocation, vérification de domicile, consultation fichiers, réquisitions auprès des administrations publiques), lesquelles doivent impérativement être consignées dans un procès-verbal.

Si au cours de celles-ci, il apparaît que la personne n'habite plus à l'adresse indiquée au FIJAIS, l'officier de police judiciaire en charge de l'enquête doit en informer, sans délai et sans attendre le résultat de ces investigations, le magistrat de permanence du parquet territorialement compétent qui procédera immédiatement à l'inscription de l'individu au fichier des personnes recherchées (FPR) (fiche J 19).

Cette nouvelle disposition issue de la loi n°2010-242 du 10 mars 2010, dite loi Lamanda (article 706-53-8 alinéa 2), vise à accélérer l'inscription au FPR des personnes parties sans laisser d'adresse. Toutefois, elle ne dispense pas l'enquêteur de mener parallèlement toutes les investigations utiles pour localiser la personne.

Lorsque ces démarches ont été concluantes, l'individu peut, selon les circonstances, faire l'objet d'une mesure de garde à vue ou être simplement entendu. Le procès-verbal d'audition devra impérativement indiquer les raisons pour lesquelles il s'est soustrait à son obligation de justification. Cet acte procédural facilitera l'établissement de la réitération en cas de nouveau défaut de justification.

Vous vous rapprocherez de votre parquet afin que celui-ci définisse une politique pénale claire en la matière, y compris lors du premier défaut de justification : procédure judiciaire systématique pour défaut de justification ou simple régularisation. Sans accord de celui-ci, aucune régularisation n'est envisageable.

Je vous rappelle que l'un des objectifs assignés à ce fichier est de prévenir la le renouvellement des infractions de nature sexuelle ou violente. Il est de la responsabilité de chaque direction d'emploi de mettre en œuvre ces mesures et de permettre aux officiers de police judiciaire d'accomplir cette mission.

Vous veillerez à la stricte application de ces instructions et ne manquerez pas de me tenir informé de toute difficulté rencontrée dans leur mise en œuvre, y compris lorsque ces difficultés auront pour origine le fonctionnement même du fichier ou des politiques pénales locales inadaptées.

Le Préfet
Directeur general de la police nationale

Frédéric PECHENARD