UNIVERSITÉ
PANTHÉON-ASSAS
– PARIS II –

BANQUE DES MEMOIRES

Master de droit pénal et sciences pénales
Dirigé par Mr Yves MAYAUD
2013

Les fichiers de police au service de la procédure pénale

Auteur Marion BIREAU

Sous la direction de Mr Mayaud

Université de Paris II (Panthéon-Assas)

Droit

LES FICHIERS DE POLICE AU SERVICE DE LA PROCEDURE PENALE

Mémoire pour le Master 2 « Droit pénal et sciences pénales »

présenté par Marion Bireau

Année universitaire 2012 - 2013

Sous la direction de Monsieur Yves Mayaud

« Les opinions exprimées dans ce mémoire sont propres à leur auteur et n'engagent pas l'Université de Paris II ».

Remerciements

Je tiens à remercier mon directeur de mémoire, Mr Yves Mayaud, pour son soutien continu dans l'élaboration de cette réflexion et ses précieux conseils.

Je souhaite également remercier Mr Brouillet, ancien officier de gendarmerie, professeur en CPGE et maître de conférence à Sciences Po Paris et chargé de cours à l'Institut d'Etudes Judiciaires d'Assas, pour avoir partagé son expérience et ses avis d'une grande richesse.

Tableau des abréviations

AEDH	Association européenne des droits de l'homme
AJP	Actualité Juridique Pénale
AN	Assemblée nationale
Art.	Article
Bull. crim.	Bulletin de la Chambre criminelle
c/	contre
CA	Cour d'Appel
CE	Conseil d'Etat
CEDH	Cour européenne des droits de l'homme
Circ.	Circulaire
Ch.	Chambre
CP	Code pénal
CPP	Code de procédure pénale
CNIL	Commission nationale informatique et Libertés
Crim.	Criminelle
DC	Décision du Conseil constitutionnel concernant la conformité à la Constitution (art. 54 et 61 de la Constitution)
Décr.	Décret
Ed.	Editions
IEJ	Institut d'Etudes Judiciaires
JORF	Journal officiel de la République Française
N°	Numéro
Op. cit.	Ouvrage cité
p.	Page
Préc.	précédent
QPC	Question prioritaire de Constitutionnalité
R.	Règlement
Rapp.	Rapport
SJA	Semaine juridique administrative
TFUE	Traité sur le fonctionnement de l'Union Européenne
v.	Voir

SOMMAIRE

« Un cœur noble ne peut soupçonner en autrui,

La bassesse et la malice,

Qu'il ne sent point en lui. »

Jean Racine

INTRODUCTION

« Tous les hommes naissent innocents, les coupables sont des hommes, donc pour trouver les coupables, il faut ficher les innocents », c'est ainsi avec sarcasme et réprobation que l'ancien gendarme devenu écrivain et scénariste Georges Moréas explique la tendance actuelle du fichage par un syllogisme à la Socrate[1].Le cumul des données au sein des fichiers de police semble aujourd'hui être devenu une condition de l'efficacité de la procédure pénale et du bon ordre.

Cette tendance est d'autant plus marquée que notre ère est à la fois celle de la mondialisation des flux et celle de *l'homonumericus*. La fluidité des mouvements des biens et des personnes tend à renforcer l'exigence d'en contrôler les déplacements tandis que le développement des nouvelles technologies permet d'accroître la capacité des fichiers de police à travers ses deux finalités que sont la surveillance et l'identification. La conjonction de ces deux évolutions tend à transformer nos repères spatio-temporels, à craindre un avantage donné à la criminalité du fait de la permissivité des mouvements, tout comme à revendiquer une sécurité qui serait assurée par la collecte et le traitement toujours plus rapide des données. L'informatique et la biométrie, qui semblent être l'avenir des traitements automatisés, sont ainsi désignées comme les outils performateurs du fichage policier.

Toutes ces mutations amènent à s'intéresser de plus près aux fichiers de police, que l'on peut définir à l'instar de l'article 2 de la loi de 1978 relative à l'informatique, aux fichiers et aux libertés comme des « traitements de données à caractère personnel » créés et alimentés par les forces de l'ordre, police et gendarmerie. Aujourd'hui informatisés, ces fichiers visent à conserver, consulter, utiliser voire rapprocher des données personnelles en ce sens qu'elles sont relatives à une personne physique identifiée ou pouvant l'être, même indirectement.

Il ne s'agit pas de porter notre réflexion sur les fichiers privés, seulement consultés par la police et non alimentés par ses services, ni sur les fichiers à finalité administrative. En effet, l'intérêt se concentre sur les fichiers de police au sein de la procédure pénale, c'est-à-dire ceux utilisés dans le but de prévenir ou de réprimer les faits délictueux commis.

[1] Georges MOREAS, « Le fichier d'analyse sérielle : nouvelle technique d'enquête », *police et cetera,* 2009.05.29, http://moreas.blog.lemonde.fr/2009/05/29/le-fichier-analyse-serielle-nouvelle-technique-enquete/

Le cadre de la procédure pénale, qui plus est concentré sur les fichiers de police, rappelle le caractère régalien des mesures et l'histoire montre que la logique de surveillance et d'identification des citoyens est inhérente à l'avènement de l'Etat moderne. Pour autant, les pratiques d'identification, visant à certifier l'identité d'une personne par le biais de critères relativement stables, sont apparues très tôt dans l'histoire face aux usurpations d'identité. Dès le premier siècle avant notre ère la lex Licinia Mucia de 95 et la lex Papia de 65 mettent en œuvre des procédures de répression contre ceux qui se comportent comme des citoyens romains sans l'être ; la nécessité est toutefois administrative. De l'antiquité au Moyen-Âge, les techniques d'identification relèvent en grande partie de la parole et du regard, du témoignage et des signes extérieurs tels les armoiries, sceaux ou vêtements, ou encore des relations sociales. L'identité est avant tout collective et a pour finalité le rattachement à une communauté ou une condition sociale. Par la suite, la volonté d'exclure les vagabonds et les mendiants des villes va conduire à une description plus minutieuse des éléments permettant d'identifier les individus jusqu'à aboutir sur la mise en place de sauf-conduit, ancêtre du passeport. L'exigence de « papiers » attestant de son identité devient un instrument privilégié de la police.

La dimension politique de cette logique de contrôle social atteint son apogée avec la formation de l'Etat moderne et la nécessité d'identifier les citoyens, dont les registres de l'état civil confiés au clergé par l'Ordonnance de Villers-Cotterêts en 1539 sont le commencement.

La modernisation va alors s'accompagner d'une bureaucratie efficace alliant identification et surveillance, définie comme l'observation des comportements et des déplacements des individus couplée de la volonté d'en garder la trace pour mieux réutiliser ces informations. Dès lors, le développement des technologies accélère les méthodes de police aux XIXème et XXème siècles et les papiers d'identité sont doublés de la mise en place de véritables « fiches » tenues secrètes pas les services de police afin de mieux contrôler la population.

A l'instar du Panoptique de Bentham, l'objectif est de voir sans être vu et la technique va provoquer un premier scandale avec « l'affaire des fiches » en 1904. Dévoilée par la presse de droite et s'inscrivant dans le combat entre cléricaux et anticléricaux, la révélation de la mise en fiche d'informations telles le suivi des messes ou le choix d'écoles catholiques pour les enfants popularise le mot « fiche » ; le terme « fichier » n'apparaissant que dans les années 1930 de sorte que le contenu et le contenant ont donné le verbe.

Les progrès de la science et du savoir participent d'un large renforcement des fichiers policiers. L'objectif premier, et dernier sans doute, est la reconnaissance du criminel d'habitude, centre des préoccupations de l'anthropologie criminelle naissante à travers les figures de Lombroso pour l'Italie ou Lacassagne pour Lyon. Celui qui va s'imposer comme le maître du fichage est cependant un simple « commis aux écritures » de la préfecture de police de Paris, Alphonse Bertillon, grâce à un système lié à l'identité anthropométrique du squelette. La mesure d'une dizaine de parties du corps humains permet « en vingt secondes d'affirmer l'identité d'un individu et de remplacer tout un état civil »[2]. Le succès de l'identification d'un récidiviste s'étant affublé d'un faux nom trois mois après la mise en place du système en 1882 conduit à une exportation internationale du système Bertillon. Ce dernier a en outre dirigé la professionnalisation des équipes chargées de l'identification et la rationalisation du fichage au point de donner naissance à une véritable « mémoire d'Etat »[3]. Les risques d'erreurs et les difficultés pratiques, notamment pour la prise des mesures à l'égard des femmes et l'évolution du squelette des mineurs, vont vite être dépassés par la découverte de la dactyloscopie et le soutien de la photographie.

Aujourd'hui complétées par le traitement informatique et la biométrie, les fils conducteurs de toute l'évolution des fichiers de police tiennent à deux concepts aux rôles différents, l'un technique et l'autre justificatif.

Le concept ayant accompagné l'évolution technique des fichiers de police tient à la recherche de certitude dans l'identification et la surveillance des personnes[4]. Les lois romaines ou encore l'affaire Martin Guerre, jugé et condamné à mort pour usurpation d'identité en 1557, sont autant d'évènements historiques plaçant la quête de certitude au centre des préoccupations. Objet d'interrogations philosophiques ou économiques, le concept rejoint celui de la connaissance nécessairement limitée des êtres humains ainsi que celui de la prévisibilité, voire de la prédiction. A l'origine critère de la réussite scientifique, comme le montre les exemples de Michel Serres relatifs au météorologue cherchant à prévoir le temps ou à l'astronome prédisant le passage des planètes, l'appréhension de la vérité est aujourd'hui devenue une obsession politique de l'Etat. La globalisation des échanges aussi bien que

[2] Citation de Bertillon extraite de l'ouvrage « Fichés ? photographie et identification 1850-1960 » de J.M. Berlière et P. Fournier, Editions Perrin 2011 p. 53
[3] NOIRIEL Gérard, *L'identification. Genèse d'un travail d'Etat,* Ed. Paris, Belin, 2007
[4] Ayse Ceyhan, « Enjeux d'identification et de surveillance à l'heure de la biométrie », *Cultures & Conflits*, n° 64 (2006) p. 33-47

l'imprévisibilité de l'attaque terroriste sont autant d'atteintes aux repères traditionnels de l'action policière qui ont favorisé l'émergence de techniques prometteuses d'infaillibilité. La biométrie a atteint le paroxysme de cette quête de certitude en isolant une identité biologique unique de la personne. Puisant ces origines dans les termes grecs « bios », la vie, et « metron », la mesure, la biométrie permet de mesurer le vivant à partir de ses caractéristiques invariables. C'est ici toute l'appréhension de l'identité elle-même qui se trouve transformée et réduite. Ainsi la distinction essentielle opérée par Paul Ricoeur entre *l'identité idem,* ce qui est permanent, et *l'identité ipse*, ce qui est changeant et permet de se définir par rapport aux autres, mettait en avant une dualité identitaire source de dignité et de respect car en rapport avec les autres. Or la biométrie ne relève que de l'identité idem au détriment, voire en faisant abstraction, du contexte social. Ainsi pour Didier Bigo ce système met l'individu « dans l'incapacité de dire son identité, de la circonstancier, de la contextualiser et en ce sens, elle est problématique »[5].

Par conséquent, le fichage généralisé conduit à transformer non seulement les rapports sociaux mais aussi notre propre appréhension de l'identité et du corps humain. Cette analyse met en évidence un paradoxe entre les mutations profondes et dangereuses engendrées par ce nouveau regard porté sur l'être humain et l'acceptation générale du système. Cette dissemblance entre l'apparence et la profondeur tient sans doute à une justification officielle très porteuse des fichiers de police car facilement parlante à l'opinion publique ; l'argument de la sécurité semble obstruer toute réflexion approfondie.

C'est ainsi qu'intervient l'autre fil conducteur du développement du fichage policier participant d'une justification des entraves aux libertés : le concept de sécurité.

Il est immédiatement un point crucial à expliciter pour bien s'entendre sur cet argument s'agissant de la distinction entre sûreté et sécurité. Les spécialistes évoquant un « droit à la sécurité » sont à l'origine d'un amalgame dangereux pour la liberté car seul le droit à la sûreté, à la philosophie totalement opposée, est juridiquement reconnu et protégé. Ainsi l'article 9 de la Déclaration Des Droits de l'Homme et du Citoyen[6], s'inscrivant dans le droit fil de l'Habeas Corpus, protège le droit à la sûreté par l'interdiction de toute arrestation, détention ou immixtion arbitraire de l'Etat et par le droit à un juge. La philosophie du concept

[5] Voir l'audition de Didier Bigo par la CNIL, le 11 mars 2005, www.cnil.fr

[6] « Tout homme étant présumé innocent jusqu'à ce qu'il ait été déclaré coupable, s'il est jugé indispensable de l'arrêter, toute rigueur qui ne serait pas nécessaire pour s'assurer de sa personne doit être sévèrement réprimée par la loi. »

tient donc de la protection du citoyen contre l'Etat et ses interventions arbitraires dans les libertés et les droits reconnus aux individus. C'est ici l'existence du contrat social qui place la sûreté au rang d'un droit comme l'explique Thomas Hobbes dans son ouvrage *Le Léviathan*, la prérogative n'est autre que la contrepartie de l'abandon par les hommes des libertés qu'il possédait en l'état de nature. La sûreté est ainsi « la garantie de la sécurité juridique face au pouvoir », elle « constitue la protection avancée de toutes les libertés »[7]. Cette notion tangible, contrôlable car se référant à des faits matériels, est l'antonyme de la sécurité qui relève quant à elle d'un sentiment. La référence à la notion de sécurité est de ce fait pernicieuse car elle joue sur les ressentis, sur l'appréciation subjective et propre à chacun selon la situation sociale dans laquelle il vit. La sécurité participe des affects et non d'une réalité tangible de sorte que tout est permis sur un fondement aussi fragile. Il est permis d'insister sur cette différence que trop de textes internationaux ignorent, au premier rang desquels la Convention européenne des droits de l'homme, car elle fonde les critères d'une conduite de la bonne politique depuis la nuit des temps. Ainsi Aristote, dans son ouvrage *La politique*, explique que les deux affects à éviter pour gouverner rationnellement sont la pitié et la crainte. La peur, le sentiment d'insécurité constamment entretenu par les politiques eux-mêmes est une mauvaise conseillère pour Aristote car elle empêche de délibérer avec toute sa raison. Cette analyse est essentielle pour comprendre le développement des fichiers tout en sachant garder un regard critique sur les arguments tenant à l'insécurité et à la lutte contre le terrorisme.

Enfin, l'analyse de ces deux concepts soutenant le développement des fichiers de police nous conduit à les opposer aux libertés qui seront les références clés de l'analyse. L'objet des atteintes opérées par le fichage des données personnelles est multiple et défini dès le premier article de la loi de 1978 : les fichiers ne doivent « porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles et publiques ». L'objectif est remarquable, sans doute trop au vu des nombreuses exceptions prévues par la suite à l'égard des fichiers de police. La vie privée s'est révélée être la clé de voute de l'étude des fichiers et du respect de la proportionnalité du fait de sa protection envisagée à tous les niveaux de la hiérarchie des normes. Longtemps protégée par le biais de la responsabilité délictuelle sur le fondement général de l'article 1382 du code civil, la vie privée a été affirmé comme un droit autonome en 1970 par une double intervention législative, en droit privée à travers l'article 9 du code civil, en droit pénal par le biais des

[7] Rivero J., *Les Libertés publiques*, t. 2, « Le régime des principales libertés », p. 21, Paris, PUF, coll. «Thémis», 2003

articles 226 et suivants du code pénal. Le Conseil Constitutionnel en a fait un droit protégé au plus haut niveau sur le fondement des articles 2 et 3 de la Déclaration des Droits de l'Homme et du citoyen. Les sages ont notamment rappelé la constitutionnalité du principe à l'occasion de la censure du « fichier des honnêtes gens » qui devait à l'origine accompagner la mise en place de la carte nationale d'identité biométrique au nom de la lutte contre l'usurpation d'identité (de l'incertitude donc)[8]. Enfin, la Convention européenne de 1950 protège la vie privée grâce à l'article 8 et la Cour européenne des droits de l'homme l'applique au cas des fichiers de police français de sorte que l'on peut être assuré de la pertinence de la référence[9].

La protection de la vie privée face aux traitements de données est d'autant plus forte que l'Union européenne a autonomisé la notion. En effet, dans le domaine des fichiers de police automatisés il s'agit dorénavant de parler du principe de « protection des données personnelles ». Proclamé par une Directive de 1995, ce principe n'était toutefois pas applicable aux fichiers participant du troisième pilier de « coopération policière et judiciaire pénale » à l'origine. La Charte Européenne des droits de l'homme proclame de manière générale le principe en son article 8, explicitement distinct de l'article 7 relatif à la vie privée et familiale. La protection des données est un principe plus complet en ce sens qu'il exige une utilisation loyale et à des fins déterminées des fichiers, devant être prévus par la loi, ainsi qu'un droit d'accès et de modification des données, le tout sous le joug du contrôle d'une autorité indépendante[10].

Dès lors, l'enjeu des fichiers de police, s'inscrivant dans le cadre plus large de la procédure pénale, est d'opérer un juste milieu entre les finalités liées au respect de l'ordre public et à la répression des infractions et celle tenant au respect des libertés.

In medio stat virtus, la nuance devra être à l'œuvre tout le long de la réflexion pour évaluer la légitimité démocratique des fichiers (I) ainsi que la loyauté de l'utilisation qui en est faite (II).

[8] Décision n° 2012-652 DC du 22 mars 2012, loi relative à la protection d'identité

[9] Rapport du Président Dean Spielmann de la Cour européenne des droits de l'homme sur « La protection des données dans la jurisprudence de la Cour européenne des droits de l'homme » du lundi 28 janvier 2013

[10] Article 25 Directive du 24 octobre 1995, inspiré de la Convention STE 108 du Conseil de l'Europe de 1981

PARTIE I : LA LEGALISATION DES FICHIERS DE POLICE POUR UN SERVICE LEGITIME DE LA PROCEDURE PENALE

« La loi ne doit établir que des peines strictement et évidemment nécessaires, et nul ne peut être puni qu'en vertu d'une loi établie et promulguée antérieurement au délit, et légalement appliquée. » Ainsi l'article 8 de la Déclaration des Droits de l'Homme et du citoyen proclame le principe de la légalité des délits et des peines, étendu à la procédure pénale. Si celui-ci tend en premier lieu à l'exigence d'une loi, il est aussi immédiatement exigé, comme corollaire indispensable à l'efficacité du principe, la nécessité de la loi.

Les fichiers de police mis au service de la procédure pénale doivent répondre à cette double signification qui donne toute sa portée au principe de légalité. Cependant, la nature de ces traitements de données étant controversée, leur légalisation n'est pas si évidente qu'il n'y paraît et ce premier point mérite des approfondissements au vu des résistances constantes à l'intervention du Parlement (Chapitre I). Le corollaire relatif à la proportionnalité des mesures est un second point crucial dans l'analyse des fichiers de police car permettant de leur donner toute leur légitimité (Chapitre II).

Chapitre 1 : LA NECESSAIRE LEGALISATION DES FICHIERS DE POLICE

A l'heure de la transparence, revendiquée au plus haut niveau de l'Etat, la légalisation des fichiers de police semble être un souhait indispensable pour le bon fonctionnement de la démocratie. Le secret étant le frère de l'arbitraire, la légalisation des fichiers de police apparaît être une évidence. Pourtant, la concurrence de l'efficacité de la procédure pénale tend à amenuiser les exigences en la matière. Cette logique est autrement dénoncée par un ancien membre du conseil d'Etat en ces termes : « Les officiants de l'appareil répressif ont toujours eu le sens de l'ordre avant celui de la légalité, le sens de l'Etat avant le souci du citoyen[11] ».

L'absence de texte étant aujourd'hui une position impossible à défendre par les politiques, même pour les fichiers classés secret-défense, le débat porte sur la compétence de l'auteur des textes. Opter pour celle du Parlement ou de l'exécutif, pour la conception matérielle ou formelle de la légalité, telle est la question qui se pose en théorie (Section 1). Toutefois, les différences pouvant parfois être grandes entre les discours politiques et leur application, la légalisation des fichiers doit impérativement être éclairée par des considérations pratiques pour cerner la réalité (Section 2)

SECTION 1 : LES EXIGENCES THEORIQUES

La légalisation des fichiers de police est un impératif constitutionnel diversement apprécié en droit français (§1). Le renforcement des compétences de l'Union européenne en droit pénal opéré par le Traité de Lisbonne de 2009 oblige à élargir la réflexion aux fichiers européens utilisés au cours de la procédure pénale (§2).

[11] Philippe Boucher, Extrait de *Le Ghetto judiciaire*, Edition Grasset, 1977, ancien journaliste au Monde et membre du Conseil d'Etat

§ 1 La légalisation des fichiers au niveau national

La nécessité d'encadrer l'existence et le fonctionnement des fichiers de police est aujourd'hui unanimement admise d'un point de vue théorique mais le débat persiste quant à la compétence du législateur ou de l'exécutif. La faveur donnée à ce dernier conduit à constater une légalisation laxiste des fichiers de police en général (A), voire proscrite pour ceux classés secret-défense (B).

A _ Les fichiers de droit commun, une légalité laxiste

Nullum crimen, nulla poena sine lege : le principe de légalité exige qu'une personne ne puisse être poursuivie et sanctionnée pour ses actes qu'en vertu d'un texte de loi clairement et préalablement édicté. Défendu par Cesare Beccaria dès le XVIIIème siècle, cette garantie est fondamentale pour lutter contre l'arbitraire et permettre une connaissance effective de la loi par les citoyens. Ainsi, le principe de légalité des délits et des peines est affirmé à tous les niveaux dans la hiérarchie des normes, dans la Constitution grâce à l'article 8 de la Déclaration des Droits de l'Homme et du Citoyen et dans la loi par les articles 111-2 et 111-3 du code pénal. Toutefois, il est une troisième dimension de la légalité, celle de la procédure pénale, qui est intimement liée au droit pénal substantiel de sorte que les mesures prises au cours des poursuites ou suite à un jugement doivent être prévues par un texte. L'analyse de cette légalité procédurale revêt en réalité deux aspects.

L'aspect matériel de la légalité criminelle tient à la simple exigence d'un texte, quel que soit son rang dans la hiérarchie des normes. Cette conception matérielle ne connait pas de résistance au sujet des fichiers de police car tous s'accordent quant à la nécessité de les encadrer pour quitter le secret.

Il s'agit donc plus précisément d'interroger l'aspect formel du principe qui visait à l'origine à promouvoir la compétence exclusive du législateur, représentant élu par le peuple, pour que les lois soient issues de la volonté générale. Cela participe de la « distribution des pouvoirs », chère à Montesquieu[12] et indissociable d'une société démocratique[13].

[12] Montesquieu, *De l'esprit des lois*, 1748
[13] Art. 16 de la Déclaration des Droits de l'Homme et du Citoyen

L'encadrement des fichiers révèle toutefois le déclin de la compétence parlementaire au profit de celle du gouvernement : les impératifs de sécurité et de rapidité, l'efficacité des fichiers et leur technicité, justifieraient cette délégation de pouvoir[14].

Ce déclin est explicitement reconnu dans la loi « Informatique et libertés » du 6 janvier 1978 qui porte création de la CNIL (Commission Nationale de l'Informatique et des Libertés) et a vocation à encadrer tous les traitements de données à caractère personnel à l'exception de ceux destinés à des finalités strictement personnelles. En son article 26, cette loi autorise une mise en œuvre des traitements de données pour le compte de l'Etat par un simple arrêté, après avis motivé et publié de la Commission, s'ils intéressent « la sûreté de l'Etat, la défense ou la sécurité publique » ou s'ils « ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations ou des mesures de sûreté.» De plus, l'article précise que les fichiers contenant des données dites « sensibles », en principe interdites comme nous le verrons par la suite, sont autorisés par décret en Conseil d'Etat.

La loi prévoit donc explicitement une délégation du pouvoir de créer des fichiers de police en faveur de l'exécutif. Cette position est soutenue par les conseillers spécialisés dans les fichiers comme Mrs Alain Bauer et Christophe Soullez dont les propositions pour améliorer la transparence des fichiers sont concentrées sur la communication publique et l'information, sans faire état de la compétence législative[15].

Ainsi par exemple, le Fichier Informatisé du Terrorisme (FIT) dont la finalité est la centralisation d'informations concernant des personnes pouvant, en raison de leur activité individuelle ou collective, porter atteinte à la sûreté de l'Etat, a été légalisé par un décret[16]. D'autres tels le Fichier des Personnes Recherchées (FPR), ou le Fichier des Véhicules Volés (FVV) ont été créés par de simples arrêtés[17].

[14] Entretien avec Mr Soullez lors d'une conférence sur les fichiers de police à l'IEJ d'Assas le 17 novembre 2012
[15] Rapport « fichiers de police et de gendarmerie : comment améliorer leur fonctionnement » de 2007
[16] Décr. n° 91-1052 du 14 octobre 1991
[17] Arrêtés du 15 mai 1996 et 2 septembre 2005

Cependant, il ne faut point prendre pour acquis cette dilution de la légalité. Des voix discordantes continuent à se faire entendre pour réclamer le respect d'un débat démocratique face à ce « basculement inquiétant de l'Etat de droit à l'Etat sécuritaire »[18].

Ces contestations, bien légitimes à notre goût, s'appuient sur le respect de la vie privée, la prévention des atteintes aux libertés individuelles et collectives et la protection des données pour réclamer la transparence et la compétence des élus parlementaires. A cet égard, plusieurs rapports, issus du Sénat comme de l'Assemblée Nationale, exigent que la création des fichiers, leur finalité, leurs modalités et leur disparition relèvent de la compétence de la loi[19]. Le dernier rapport des députés dénonce une « inertie législative » suite aux recommandations[20] faites en 2009 concernant justement la modification de l'article 26 de la loi de 1978. Celles-ci exigeaient l'autorisation de la loi lors de la création des fichiers de police et tendaient à donner une véritable portée au principe de légalité en précisant que les éléments essentiels relevant du cadre juridique de ces fichiers devaient aussi être prévus par la loi. De tels éléments sont notamment ceux relatifs à l'identité du responsable du traitement, la finalité et la dénomination du fichier, les services chargés de sa mise en œuvre ou de l'exercice du droit d'accès, les types de données pouvant être enregistrées ou encore la durée de conservation et les personnes habilitées à consulter le fichier. Une proposition de loi avait juridiquement traduit ces recommandations mais, bien qu'adoptée à l'unanimité par la Commission des lois, elle a été rejetée par l'Assemblée Nationale[21].

Les citoyens avertis[22] sont aussi nombreux à demander l'intervention de la loi à l'instar de la Ligue des droits de l'homme, du syndicat des avocats de France ou du syndicat de la magistrature. Il ne s'agit pas de remettre en cause l'existence des fichiers et leur utilité mais seulement de souligner leur caractère attentatoire aux libertés, du moins leur potentiel liberticide. En effet, les fichiers contiennent des données intrusives telles notre photo, notre empreinte génétique, voire pour certains nos activités politiques ou syndicales : le risque de

[18] JJ Lavenue, « Anormalité, surveillance et fichiers de police » in *Vidéo-surveillance et détection automatique des comportements anormaux.* Editions du Septentrion Juillet 2011 pp. 9-31.
[19] Rapport d'information déposé à l'Assemblée Nationale le 21 décembre 2011 par la commission des lois constitutionnelles, de la législation et de l'administration générale de la république dirigée par Mme Delphine Batho et Mr Jacques Alain Bénisti
Rapport d'information n°441 du Sénat, groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques du 27 mai 2009
[20] Recommandations n°2 et 3 du Rapport de l'Assemblée nationale de 2009
[21] Proposition de loi n° 1659 rejetée le 24 novembre 2009
[22] Pétition « Fichiers : l'urgence d'un débat au Parlement », cosignée par P. Piazza et des magistrats http://bugbrother.blog.lemonde.fr/2009/12/02/fichiers-lurgence-dun-debat-au-parlement/#more-499

dérives « orwéliennes » n'est pas exclu. En outre, les conséquences en termes de soupçons éveillés tout au long de la procédure pénale ont été soulignées pour certains fichiers. Ceci notamment pour les fichiers d'antécédents tels le STIC[23] et le JUDEX[24] renfermant le signalement des personnes mises en cause dans les crimes et délits constatés par les services de l'ordre, et créés par des décrets. Ces fichiers sont certes indispensables au travail des enquêteurs mais ils risquent de l'orienter du fait de la stigmatisation de l'individu qui ne peut se défaire de son passé. Ainsi, Mr Marot dénonce « une mémoire sans oubli ni pardon » qui risque de préfigurer une « peine perpétuelle »[25]. Dans cette perspective de défense de la compétence parlementaire, deux arguments juridiques méritent d'être analysés.

Au niveau législatif, une première disposition liée aux règles de la preuve en droit pénal peut venir au soutien de l'intervention d'une loi. L'article 427 du code de procédure pénale énonce que, « hors les cas où la loi en dispose autrement », les infractions peuvent être établies par tout mode de preuve contradictoirement discutée devant le juge, qui décide selon son intime conviction. Le principe tient donc à la liberté de la preuve, sauf caractère déloyal ou illicite du mode de preuve. Les fichiers de police participent tout à fait de la notion de preuve, définie par Domat comme « ce qui persuade l'esprit d'une vérité »[26] et leur rôle est même multiple. Ainsi les fichiers relatifs à l'identification des personnes tels le Fichier National Automatisé des Empreintes Génétiques (FNAEG) ou le Fichier National des Empreintes Digitales (FNED) servent à prouver la culpabilité d'une personne ; d'autres relatifs au passé judiciaire d'un individu tels le STIC, le JUDEX ou le Fichiers Judiciaire des Auteurs d'Infractions Sexuelles (FIJAIS) orientent le flair des enquêteurs et permettent au juge une meilleure personnalisation de la peine. Cette portée probatoire, confrontée au risque d'arbitraire dans la tenue de fichiers en l'absence de tout cadre, justifie le fait que les fichiers semblent appartenir à la toute première dérogation envisagée par l'article, celle visant « les cas où la loi en dispose autrement ». Ainsi les fichiers échappent bien heureusement au principe de la liberté pour rejoindre le cas où la loi intervient de manière spécifique pour encadrer un mode de preuve. Cet encadrement est tout à fait indispensable afin qu'ils soient établis sur des critères objectifs et dans des conditions prédéfinies.

[23] Système de traitement des infractions constatées de la police, décret du 5 juillet 2001
[24] Système Judiciaire de Documentation et d'Exploitation de la gendarmerie, décret du 17 novembre 2006
[25] AJP 2007 p. 61, « Fonctions et mutations des fichiers de police » Pierre-Yves Marot
[26] J. Domat, « Les lois civiles dans leur ordre naturel », Paris, éd. Cavelier t.1, p. 204, 1771.

Il pourrait être opposé une interprétation large du mot de « loi » comme visant toute norme contraignante à portée générale, et donc les règlements. Or, ce serait oublier le principe kelsénien de la pyramide des normes que l'on peut avancer en retour pour défendre la compétence de la loi au sens strict. Pour les cas où l'on veut déroger à une règle d'origine légale qu'est l'article 427, seule une norme supérieure ou de même niveau dans la pyramide en a la capacité. A tout le moins, la force de la loi au sens strict s'en ressent une nouvelle fois.

Au niveau constitutionnel, la première disposition favorable à la compétence parlementaire tient à l'article 34 qui confie à la loi le soin de « fixer les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ». Sur ce fondement, certains auteurs envisagent la dénonciation de la voie règlementaire empruntée pour de nombreux fichiers et envisagent leur censure grâce au soutien de la Question Prioritaire de Constitutionnalité offert par la loi constitutionnelle du 23 juillet 2008.

Toutefois, le succès d'une telle prétention n'est pas assuré car la loi de 1978 « Informatique et libertés » est justement venue chapeauter l'ensemble et c'est elle qui autorise la compétence règlementaire dans les limites des prescriptions légales. Dès lors, il semble que ce n'est plus la répartition des compétences ni la compétence autonome du règlement des articles 34 et 37 de la Constitution qui sont en jeu. La loi de 1978 ferait donc écran à cet argument juridique par l'établissement d'une compétence liée du règlement.[27]

L'autre article à valeur constitutionnelle pouvant aller en notre sens tiendrait à l'article 8 et à la légalité des délits et des peines. Il est tout à fait logique d'interroger le caractère punitif d'une inscription dans un fichier de police pour se demander s'il ne relèverait pas de la qualité de peine. Sur ce point, les hautes juridictions françaises comme européennes nient cette qualité pour lui préférer celle de mesure de sûreté, à vocation préventive et non répressive. Cette analyse peut toutefois être contestée sur plusieurs points. Tout d'abord de manière générale, être fiché dans les dossiers de la police amène une suspicion à l'égard de la personne qui n'est pas sans effet négatif à l'avenir. Mais surtout, pour des fichiers spécifiques que sont le FNAEG (Fichier National Automatisé des Empreintes Génétiques) et le FIJAIS (Fichier Judiciaire des Auteurs d'Infractions Sexuelles), cette approche semble trop éloignée de la réalité. Pour le FNAEG, l'annexion d'un délit en cas de refus de prélèvement des

[27] F. Bottini « A quand une QPC sur le cadre législatif des fichiers de police ? », SJA du 2 mai 2011

empreintes, qui se veut en outre systématiquement poursuivi[28], indique à merveille la volonté très ferme du gouvernement de collecter les données pour mieux pouvoir punir les délinquants. La proximité à la fois temporelle et philosophique du délit et du prélèvement des empreintes révèle le caractère « sanctionnateur » du FNAEG. Cette analyse est d'autant plus perceptible dans le cas du FIJAIS où toute inscription au fichier génère des obligations, notamment des déclarations de changement d'adresse, qui sont pénalement sanctionnées. Il apparaît donc que cette inscription est répressive puisque le non-respect des exigences qu'elle entraine automatiquement est une infraction. Sans doute est-il nécessaire de se remémorer ici les critères définissant « l'accusation en matière pénale » de l'article 6 de la Convention européenne[29] : la classification interne, la nature de l'infraction et la sévérité de la peine potentielle. La classification interne étant un critère tout à fait relatif, et la Cour se contentant de critères alternatifs, il peut sembler que la gravité du délit accompagnant le FIJAIS, puni de deux ans d'emprisonnement et 30 000 euros d'amende[30], illustre une volonté répressive.

Les juridictions portent cependant un regard tout autre sur les choses puisque la Cour de Cassation aussi bien que le Conseil Constitutionnel, et même la Cour Européenne des Droits de l'Homme, refusent de qualifier les fichiers de police de peine, aussi différents soient-ils. La qualité de « mesure de sûreté » ou « mesure de police » leur est ainsi préférée au vu de leur finalité uniquement préventive. Les conséquences sont importantes puisque, au-delà d'une exigence moindre en terme de légalité, le principe de non rétroactivité n'est pas appliqué pour l'inscription aux fichiers de police nouvellement crées ou étendus[31].

Ces trois arguments juridiques viennent appuyer le débat dans le sens d'une légalisation formelle des fichiers, toutefois il est évident que les exigences de sécurité et la peur de l'immobilisme parlementaire l'emportent pour la majorité des fichiers. Un équilibre semble être trouvé au nom du cadre fixé par la loi de 1978 et des garanties offertes par le contrôle de la CNIL.

Il ne faut point perdre de vue le fait que les fichiers de police sont des instruments privilégiés pour les forces de l'ordre afin de prévenir et de réprimer les infractions et donc de garantir nos libertés publiques. A ce titre, la compétence règlementaire permet une évolution rapide de ces

[28] Circ. du 9 juillet 2008 de la Direction des affaires criminelles et des grâces, réf. CRIM-PJ N°08.28.H 5
[29] Arrêt CEDH Engel et autres c. Pays-Bas du 8 juin 1976
[30] Art. 706-53-5 CPP
[31] Arrêt CEDH Gardel c. France, Requête no 16428/05, 17 décembre 2009 ;
Décision Conseil Constitutionnel N° 2004-492 DC du 2 mars 2004 ;
Ch. crim, 31 octobre 2006, bull. crim. no 267

outils face à la criminalité aujourd'hui toujours plus mouvante et organisée. Cependant il n'en reste pas moins que cela participe d'une conception laxiste du principe de légalité au nom d'impératifs sécuritaires et que le débat reste ouvert. Sujet encore plus sensible, le laxisme prend des airs plus radicaux pour les fichiers relevant du secret-défense.

B _ Les fichiers classés secret-défense, une légalité proscrite

Affaire Merah, procès Karachi, le secret-défense est un vieux fantasme qui a alimenté la littérature et le cinéma à travers les âges et les fichiers qui en relèvent n'échappent pas à la suspicion.

L'article 413-9 du code pénal dispose que « présentent un caractère de secret de la défense nationale […] les procédés, objets, documents, informations, réseaux informatiques ou fichiers intéressant la défense nationale qui ont fait l'objet de mesures de protection destinées à restreindre leur diffusion ou leur accès » : il s'agit de sauvegarder les intérêts fondamentaux de la Nation. Cette définition s'applique aux prévisions de la loi de 1978 autorisant la création de certains fichiers par une procédure de déclaration simplifiée sans publication du décret ni contrôle de la CNIL[32].

Les fichiers concernés sont ceux anciennement gérés par la direction de la Surveillance et du Territoire(DST) et les renseignements généraux (RG) qui ont fusionnées le 1er juillet 2008 pour donner la Direction Centrale du Renseignement Intérieur (la DCRI). Il s'agit des fichiers CRISTINA (Centralisation du Renseignement Intérieur pour la Surveillance du Territoire et les Intérêts Nationaux) et GESTEREX (Gestion du Terrorisme et des Extrémistes à potentialité violente) créés en 2008.

Dès lors, non seulement ils échappent à tout débat démocratique mais de plus, le rééquilibrage lié au cadre de la loi de 1978 n'est plus efficace. Si, comme il sera précisé par la suite, un contrôle *a minima* est assuré du fait d'un droit d'accès aux fiches, il n'en reste pas moins que le mystère qui entoure ces fichiers est d'autant plus inquiétant qu'ils sont susceptibles de renfermer des informations très intrusives. Le seul critère étant le respect de la finalité des fichiers, on peut y trouver des informations telles que les activités ou les opinions religieuses, politiques, sexuelles et tout ce que l'on peut imaginer. A ce titre, certains parlementaires ont tenté de percer le secret pour refaire vivre l'esprit démocratique mais ils se sont confrontés à

[32] Art. 26 III et 44 IV loi 1978

un mur, la lutte contre le terrorisme et l'efficacité des services de renseignements étant une priorité absolue[33].

L'absence de légalité des fichiers participant du secret-défense est donc un point de cristallisation entre les différents enjeux en cause, il semble que la protection des intérêts nationaux doive l'emporter mais l'on ne peut faire abstraction des possibles dérives liées au caractère occulte du travail des services de gendarmerie.

Une nuance doit cependant être notée au vu d'une récente évolution liée à un arrêt du Conseil d'Etat. Au départ, onze organisations associatives et syndicales, membres du collectif « Non à Edvige », ont demandé l'annulation du fichier CRISTINA par le biais d'un recours pour excès de pouvoir. Etant donné que le texte règlementaire à l'origine du fichier est couvert par le secret-défense, elles se sont appuyées sur les deux décrets connexes, modifiés par celui-ci, portant création du fichier et le dispensant de publication au Journal Officiel. Le Conseil d'Etat, face à l'impossibilité d'accéder directement au texte, a voulu ménager le droit à un recours effectif à valeur constitutionnelle[34] et le droit au secret. De ce fait, par un jugement avant-dire droit du 31 juillet 2009[35], la juridiction suprême a demandé communication du texte classé secret-défense et des décrets connexes au Ministre de l'Intérieur afin de pouvoir se prononcer sur le fond de la demande et assurer le respect du droit au recours. En revanche, pour ne pas entraver le droit au secret, le Conseil d'Etat a exclu le caractère contradictoire de la procédure pour le décret en cause. La solution de conciliation trouvée par les juges semble en l'espèce logique et proportionnée, même si le principe du contradictoire est entamé, car le droit au recours est respecté[36].

Cette décision est porteuse d'enseignement en ce qu'elle ouvre un possible contrôle des fichiers classés secrets, de sorte que le respect des exigences légales pourra être évalué par le Conseil d'Etat. Il reste que les obstacles liés au secret rendent difficile l'exercice concret des droits de la défense et que la juridiction fait partie de l'ordre administratif et non judiciaire. On pouvait donc s'interroger sur la réelle portée de ce contrôle et sur le caractère fictif du

[33] Question parlementaire de Mr Marlin Franck le 2 septembre 2008, http://questions.assemblee-nationale.fr/q13/13-29950QE.htm
[34] Conseil constitutionnel 21 janvier 1994 décision n°93-335 DC, droit protégé par le juge administratif au vu de CE 29 juillet 1998 Syndicat des avocats de France
[35] Décision Aides et a. N° 320196, au Lebon
[36] Tatiana Grundler « Le droit au recours confronté au secret » in AJDA, N°42, 14 décembre 2009

compromis en apparence trouvé. Au final, le jugement sur le fond a validé le fichier CRISTINA[37].

§ 2 La légalisation des fichiers au niveau européen

La protection des données à caractère personnel, d'autant plus urgente dans un monde globalisé et épris de nouvelles technologies, est un enjeu rattaché aux libertés fondamentales par de nombreux textes de droit européens. A ce stade de la réflexion, il s'agit d'analyser quelle portée ces textes donnent au principe de légalité, à la fois pour les fichiers de police nationaux (A) mais aussi au niveau des traitements de données de l'union (B).

A. L'exigence européenne de légalité au niveau national

Les textes concernant le principe de légalité des fichiers au niveau national sont au nombre de trois.

Tout d'abord la Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000 proclame, en son article 8, que les données à caractère personnel « doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi», seule cette dernière semble pouvoir instaurer la contrainte.

Dans cette logique, la Convention n°108 pour la protection des personnes à l'égard des traitements automatisés de données à caractère personnel[38] est à l'origine d'une recommandation[39] du Comité des ministres du Conseil de l'Europe qui encadre l'exploitation des fichiers de police. Parmi les engagements, le texte exige que la création, l'organisation et les conditions de fonctionnement des fichiers de police relèvent de la loi : c'est une fois de plus défendre la compétence du législateur. Dès lors, il semble que les principes européens, basés sur les mêmes fondements de liberté, de dignité et de vie privée que le droit interne, soutiennent la conception formelle de la légalité.

Cependant la troisième source, spécifique au terrorisme, montre que la logique sécuritaire infiltre tous les niveaux juridiques dans le contexte actuel de tensions. Les lignes directrices

[37] CE, 16 avril 2010, ASSOCIATION AIDES et autres N° 320196
[38] Convention n° 108 du 28 janvier 1981
[39] R. (87)15 du 17 septembre 1987

du comité des ministres du Conseil de l'Europe sur les droits de l'homme et la lutte contre le terrorisme du 11 juillet 2002 défendent l'interdiction de l'arbitraire et la légalité des mesures anti-terroristes. A ce titre, il est indiqué que toute mesure prise par les Etats pour lutter contre le terrorisme doit avoir une « base juridique ». La dilution de la compétence du législateur se fait ici davantage sentir car le domaine de la lutte contre le terrorisme est particulièrement sensible et dérogatoire, comme le montre les mesures spéciales élaborées en matière de garde à vue, des perquisitions et de l'accès à un avocat[40]. Il s'ensuit que dans la partie précisément relative à la collecte et au traitement de données à caractère personnel, le Comité prévoit une possible atteinte au respect de la vie privée des personnes si le fichier est régi par des dispositions appropriées en droit interne, proportionné à l'objectif prévu, et susceptible d'un contrôle par une autorité externe indépendante. Le caractère diffus de la menace terroriste et le contexte de crise alimenté depuis les attentats du 11 septembre semblent ici justifier des dérogations très intrusives. Ainsi, Mme Agnès Blanco dénonce « une véritable inversion du rapport individu/Etat » car aujourd'hui c'est aux citoyens que l'on demande de la transparence tout en protégeant le secret étatique[41].

B. Le respect du principe de légalité au niveau européen

Dans une perspective tout aussi intéressante, il convient d'envisager le respect de la légalité au sein même de l'Union Européenne qui est dotée d'un Parlement : les fichiers de police utilisés dans la procédure pénale créés par l'Union respectent-ils le débat démocratique ?

Six instruments européens supposent la collecte et le stockage de données à caractère personnel au niveau de l'Union Européenne : SIS, VIS, Eurodac, SID, Europol et Eurojust. Cependant le fichier VIS, Système d'Information sur les Visas, ainsi qu'EURODAC, recensant les empreintes digitales des demandeurs d'asile et des clandestins, n'ont pas pour finalité un procès pénal. Le SID quant à lui, Système d'Informations Douanières, couvre un domaine très particulier relatif aux infractions aux règlementations douanières et agricoles de la communauté. Notre réflexion portera donc sur le SIS, Europol et Eurojust.

[40] Art. 706-88 CPP, 706-89 et 706-90 CPP

[41] Agnès Blanco, « Le système français de lutte contre le terrorisme et la garantie de l'Etat de droit », Revue *Regards sur l'actualité* de mars 2009 p.45

D'une part, le fichier ayant un poids important dans le domaine pénal est avant tout le SIS, Système d'Information Schengen, mis en place par la convention d'application de l'Accord Schengen du 14 juin 1985 dans une logique de compensation de la disparition des frontières intérieures de la communauté européenne. Il a pour objet de centraliser des informations, telles des signalements de personnes ou d'objets, détenues par les services de l'ordre afin de promouvoir la sécurité. On parle aujourd'hui du SIS II car le fichier a été modernisé par un règlement de 2006 qui a notamment pour conséquence l'enregistrement des données biométriques[42]. Ce règlement est le fruit d'une codécision entre le conseil de l'Union Européenne (Conseil des Ministres) et le Parlement européen, donc à son égard le débat démocratique et la compétence législative sont respectés.

D'autre part, les deux institutions prépondérantes pour lutter contre les formes de criminalités les plus dangereuses sont Europol et Eurojust.

Europol est « l'Office européen de police » qui a été modernisé par une décision du Conseil du 6 avril 2009 et il est prévu dans ce cadre que l'institution a pour mission de «collecter, stocker, traiter, analyser et échanger des informations et des renseignements » entre les Etats membres[43].

Eurojust est une idée du Conseil européen de Tampere, mise en œuvre par la décision du Conseil du 28 février 2002, dans le but de renforcer la coordination des autorités nationales chargées des poursuites dans le cadre de la lutte contre la criminalité grave, avec un rôle particulier dans le terrorisme. Dans ce cadre, l'institution traite de données relatives aux personnes suspectées d'avoir commis un délit ou condamnées pour un délit pour lequel Eurojust a compétence, aux victimes et aux témoins. Le contenu peut notamment concerner des informations telles l'identité de la personne, son profil ADN, sa photographie ou ses empreintes.

La procédure mise en œuvre pour créer ces deux derniers fichiers est davantage critiquable car le Conseil des Ministres et lui seul s'est prononcé de sorte que le Parlement n'est pas intervenu. Ceci s'explique par le fonctionnement en pilier de la communauté européenne avant 2009, lequel prévoyait une décision par le Conseil, à l'unanimité en matière pénale, le Parlement étant simplement consulté. Depuis le Traité de Lisbonne, des efforts ont été faits

[42] Règlement n°1987/2006 du Parlement européen et du Conseil du 20 décembre 2006.
[43] Art. 4 et 5 de la décision

puisque le principe décisionnel est maintenant celui de la procédure législative ordinaire faisant intervenir le Conseil et le Parlement sur un pied d'égalité[44]. Pour le fichier Europol, ce déficit démocratique a très certainement été volontaire car le Conseil des ministres a réformé le système malgré l'opposition du Parlement qui, consulté, a exprimé son rejet des propositions et expliqué le fait qu'une telle réforme ne pouvait se faire sans son aval. Or cet aval allait lui être donné dès le 1er décembre 2009 grâce à l'entrée en vigueur du Traité de Lisbonne, de sorte qu'il suffisait de reporter la réforme de quelques mois pour que les députés européens puissent s'exprimer… Ainsi l'association européenne pour la défense des droits de l'homme n'hésite pas à parler de « déni de démocratie dans la mise en place du nouvel Office européen de police Europol »[45].

Par conséquent, les fichiers européens Eurojust et Europol n'ont pas été créés dans le respect du principe de la légalité, synonyme de débat démocratique, mais leur avenir gouverné par le Traité de Lisbonne a introduit cette exigence depuis 2009. Toute modification des pouvoirs des institutions devra désormais respecter la procédure législative ordinaire faisant intervenir le Parlement.

Un dernier point plus précis doit toutefois être développé car en réalité c'est dans l'interconnexion des fichiers de police que le bât blesse. A cet égard, l'intégration du Traité de Prüm dans le cadre juridique européen doit retenir l'attention. Ce traité, signé le 27 mai 2005, pose le principe de la disponibilité des informations contenues dans les fichiers de police nationaux afin de renforcer la coopération « notamment dans les domaines touchant à la lutte contre le terrorisme, la criminalité transfrontalière et la migration illégale ». Le caractère particulièrement vaste des atteintes aux libertés qui s'ensuivent aurait dû justifier le respect d'un débat démocratique. Or, c'est tout l'inverse qui s'est passé car le processus décisionnel a limité le rôle du Parlement européen puis, la ratification du traité dans les sept états initialement signataires s'est faite dans l'urgence et sans organiser un tel débat ou de manière très réduite. Il n'y eu aucun débat en Espagne[46], 30 minutes de discussion en Allemagne[47].

[44] Art. 294 du TFUE
[45] Communiqué de l'AEDH« Une motion de rejet du Parlement européen pour dénoncer le déni de démocratie dans la mise en place du nouvel Office européen de police Europol », Bruxelles, le 2 décembre 2009
[46] Jacques Ziller, « Le Traité de Prüm, une vraie-fausse coopération renforcée dans l'espace de sécurité, de liberté et de justice », European University Institute Working Papers Law, n° 2006/32,p. 13
[47] Elspeth Guild et Florian Geyer, "Getting local : Schegen, Prüm and the dancing procession of Echternach" CEPS Journal, 5 décembre 2006, p.3

De surcroit, le traité a ensuite été imposé en bloc aux vingt autres pays de l'Union qui n'ont eu le choix que de l'accepter tel quel ou de le refuser sans pouvoir en discuter les modalités. L'avis du Contrôleur européen de la protection des données (CEPD) suit notre raisonnement car il en conclut que cette procédure a « conduit à ignorer totalement la nécessité d'un processus législatif démocratique et transparent »[48].

Il ressort donc de ces développements que le principe de légalité est en grande partie bafoué. En France, il l'est pour la majorité des fichiers et, pour les cas où il semble respecté au stade de la création générale du fichier, le fait de laisser au gouvernement le soin de fixer les modalités aussi importantes que la durée de conservation ou les conditions d'utilisation du fichier réduit à néant la précaution. Au sein de l'Union, les fichiers ayant été créés avant 2009, la compétence législative n'est guère davantage assurée et le même schéma apparaît puisque les précisions relatives au traitement des données ont échappé au contrôle du Parlement européen.

La critique pourrait alors s'arrêter sur ce point et se contenter d'une légalité matérielle, mais il semble de surcroît que ce strict minima soit difficile à respecter en pratique.

SECTION 2 : UN PROCESSUS IMPARFAIT EN PRATIQUE

Quittant la problématique relative à la place de la loi dans l'encadrement des fichiers, il convient à présent d'analyser les véritables avancées du processus de légalisation au sens large des fichiers.

En effet, si le principe de la légalité des fichiers par le biais de l'intervention d'une loi ou de règlements est inscrit dans les textes, il n'en reste pas moins que le processus de légalisation n'est aujourd'hui qu'imparfaitement réalisé en pratique. Le constat révèle un travail de régularisation titanesque ces dernières années mais aussi des failles qui subsistent : la légalisation des fichiers est « une préoccupation qui demeure »[49]. Il convient d'étudier les progrès volontairement opérés (§1) et le mécanisme de contrôle externe de légalité (§2).

[48] Avis du CEPD du 4 avril 2007 sur le Traité de Prüm, p. 4

[49] Op. cit. Rapport AN de 2011

§ 1 Des efforts volontaires intrinsèquement limités

Le processus de légalisation est intéressant à analyser car malgré les efforts réalisés (A), les limites inhérentes à la protection des données compliquent la réalisation d'une parfaite légalisation (B).

A. Des efforts remarqués

La difficulté pour trouver des chiffres officiels à jour prouve la sensibilité du sujet. En 2009, on recensait une augmentation de 70% des fichiers de police depuis 2006 seulement[50]. Le dernier recensement, en date de 2011, dénombre 70 fichiers de police utilisés et en cours de développement, notre calcul nous conduit donc à une augmentation depuis 2006 de 105% du nombre de fichiers de police[51].

Il faut bien comprendre ici que la plupart des « nouveaux » fichiers ne sont en fait que la régularisation de fichiers préexistants. Ainsi, la dénonciation de l'explosion du nombre de fichiers dans la presse est certes une vigilance indispensable, mais il convient d'approfondir le sens des chiffres avancés à tout va. En effet, la modernisation du service public et l'informatisation des procédures explique en majorité la mise à jour de pratiques anciennes et cela débouche, de manière comptable, sur la création de fichiers. Paradoxalement donc, les chiffres officiels manifestent un progrès remarquable en termes de transparence et l'on ne peut que s'en réjouir.

Le point qu'il est plus pertinent de mettre en relief concerne la part de fichiers aujourd'hui encore dans l'illégalité : le Parlement retient le nombre de 45% pour les fichiers de police qui, déjà utilisés, ne font pas l'objet d'une autorisation de la CNIL. Cependant, parmi ces derniers 24 (soit 86% des fichiers non déclarés) font l'objet d'un projet de texte règlementaire en préparation, et 3 autres d'un projet ainsi que d'un avis de la CNIL. Par conséquent seul un fichier non déclaré n'était pas en cours de régularisation en 2011, 8 autres étaient en cours de développement. Les parlementaires soulignent en outre un effort du gouvernement pour déclarer les fichiers avant ou pendant leur développement, et non plus a posteriori[52].

[50] http://www.vie-publique.fr/politiques-publiques/securite-nationale/fichier-biometrie-libertes-publiques/, on passe de 34 fichiers à 58 utilisés ou en cours de développement

[51] 34 fichiers en 2006, pour arriver à 70 il y a 36 fichiers en sus, soit une augmentation de 36 multiplié par 100, divisé par 34 = 106% !

[52] Op. cit. Rapport AN 2011

La légalisation des fichiers semble donc être en bonne marche et si un seul reste aujourd'hui dans l'illégalité la plus totale, on ne peut que s'en réjouir. Toutefois, la citation de Frédéric Beigbeder pour qui «la naïveté est l'opium des êtres blasés »[53] invite à ne pas se contenter de cette analyse comptable. En effet, les chiffres ne doivent pas cacher les défauts du processus de légalisation qui est loin d'être un travail achevé.

B. Des limites remarquables

L'explication principale de l'imperfectibilité du processus de légalisation tient à l'existence de fichiers locaux totalement inconnus. Il faut ici revenir à la définition du fichier informatique, précisée à l'article 2 de la loi du 6 janvier 1978, qui englobe « tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés». Par conséquent, un traitement de texte, tout aussi bien qu'un tableur ou même une boîte de réception de messages électroniques, peuvent constituer un fichier si une recherche automatisée permet d'accéder à des données personnelles.

Cette conception large, et protectrice, des fichiers de police et de gendarmerie a pour conséquence la simplicité de leur existence, voire l'inconscience de leur création. Ainsi de nombreuses unités locales de police peuvent, même sans se rendre compte de la portée de leurs actes, créer un fichier au sens de la loi. Cette source de difficulté n'est pas hypothétique et un des rapporteurs parlementaires a pu constater « qu'il n'existe pas un seul office central sans sa base de données propre »[54].

L'affaire du fichier MENS (Minorités Ethniques Non Sédentarisées) a fait couler beaucoup d'encre à ce sujet. Le scandale a fait suite à la révélation de documents internes à un office de gendarmerie par des journalistes[55] faisant apparaître un fichage des populations Roms, évidemment sans aucune existence légale et de surcroît fondé sur des critères racistes. Beaucoup a été dit sur le sujet, mais nous nous en tiendrons aux constatations de la CNIL[56] qui a conclu « qu'aucun fichier structuré et pérenne regroupant des données à caractère personnel de nature ethnique visant, en particulier, les "gens du voyage" » n'a été trouvé. Toutefois, elle a constaté l'existence d'un fichier, qui n'aurait pas été appréhendé comme tel par les agents, constitué de messages électroniques envoyés entre brigades. Cette dernière

[53] Frédéric Beigbeder, *L'égoïste romantique,* 2005
[54] Op. cit. Rapport AN 2011
[55] Blog indépendant du Monde et Rue89, notes 94 et 95 du rapport AN 2011
[56] Rapport définitif du 25 novembre 2010 rendu par la CNIL

précision est très intéressante car elle montre qu'il est très simple de verser dans la constitution d'un fichier de police, et donc que la définition est très protectrice des données personnelles. Il reste que l'insouciance des agents est à relativiser face au contenu de ces messages indiquant l'identité, la commune de rattachement, le lieu de contrôle, les dates de séjour, l'immatriculation des véhicules et ponctuellement des mentions « MENS », « gitan », « roms » ou « tzigane » de sorte qu'il s'agit bien de ficher une catégorie de population particulière. Enfin, l'existence passée et jamais déclarée d'un fichier généalogique nommé Généatic a été reconnu de sorte que la député Mme Delphine Batho reste persuadée de l'existence d'un fichier MENS sur les roms au travers celui-ci[57].

Ces exemples montrent les difficultés à parvenir à une légalisation parfaite des fichiers de police mais le point sans doute acquis aujourd'hui est l'imprégnation d'une nouvelle culture informatique dans les services de police et de gendarmerie. On ne peut que souhaiter une prise de conscience grandissante des agents afin que la légalisation des traitements se fasse volontairement. A défaut, le contrôle externe recouvre une pleine utilité.

§ 2 Le contrôle de la légalité

Les solutions face à ce risque de multiplication des fichiers en dehors des marges de la légalité tiennent à la fois de la prévention et de la répression. Il convient pour chacune d'entre elles de se demander si elles respectent l'enjeu démocratique.

A _ Prévenir le développement illégal des fichiers

Afin de prévenir la création de fichiers illicites, il conviendrait d'avertir les agents de la sécurité publique au cours de leur formation et de leur expliciter les conditions d'exploitation de tout traitement de données personnelles pouvant leur servir dans leur fonction. Cette solution a priori est celle conduite par les « correspondants Informatique et Libertés » locaux désignés par les directions générales mis en place pour la gendarmerie, le 1er mars 2011. Le but de ces sentinelles de l'information, est de développer une véritable culture du fichier au sein des services de police.

[57] Général Jacques Mignaux, directeur général de la gendarmerie nationale entendu par la Commission des Lois le 13 octobre 2010

Une autre proposition pour diminuer l'illégalité des fichiers tient au développement de procédures dites de « déclarations-cadres », encouragées par la CNIL et empruntées par le gouvernement. Ces accords permettent de déclarer en même temps plusieurs fichiers aux finalités identiques, ils se révèlent être de précieux outils pour une accélération de la procédure. Ce type de démarche est envisagé à l'article 26 IV de la loi de 1978 pour les fichiers de police ayant une même finalité ainsi que les mêmes destinataires et portant sur des données identiques. De cette manière, le ministère de l'Intérieur a entrepris la régularisation de six catégories de fichiers de police développés localement, notamment pour ceux relatifs au contrôle judiciaire, aux assignations à résidence ou aux permissions de sortir. Cette procédure a tout l'air de réjouir les parlementaires et le groupe de travail présidé par Mr Bauer en 2009 car elle permet une plus rapide légalisation des fichiers. Il ne faudrait cependant pas faire abstraction des failles qu'elle met en évidence et des risques de régularisation à tout va, sans prendre le temps d'examiner les modalités propres à chaque fichier, grâce à un amalgame volontaire.

B _ Contrôler la légalité des fichiers existants

Dans un second temps, il s'agit de contrôler a posteriori tout fichier créé dans les centres de police et de gendarmerie pour vérifier la légalité de leur existence. Cette mission est celle de la CNIL, Commission Nationale de l'Informatique et des Libertés. Cette instance nationale est une autorité administrative indépendante, la première à avoir vu le jour en 1978. Ce statut appelle des précisions sur les moyens de son indépendance avant d'examiner les moyens de son action proprement dite.

1) Les moyens de l'indépendance

Les liens intrinsèques entre une telle instance et le gouvernement manifestent un paradoxe puisqu'elle doit contrôler l'action de celui dont elle tire son autorité. La vigilance doit alors être de mise car la protection des libertés est en principe confiée à l'autorité judiciaire et ce en vertu de l'article 66 de la Constitution. L'administration semble moins bien placée pour cette mission. L'indépendance de la CNIL est par conséquent un sujet sensible et fortement défendu par les agents de la commission. Les garanties juridiques de cette indépendance sont précisées dans la loi de 1978.

La composition des 17 membres de la Commission se veut être le reflet de la société : y siègent deux députés et deux sénateurs respectivement désignés par les chambres avec

l'obligation d'assurer une représentation pluraliste depuis 2011, deux membres du Conseil économique, social et environnemental, deux membres ou anciens membres du Conseil d'Etat, de la Cour de cassation et de la Cour des comptes, et enfin cinq personnalités qualifiées spécialisées dans l'informatique et les libertés individuelles, dont trois nommées par décret et deux par les Présidents des chambres parlementaires. En outre, le Défenseur des droits ou son représentant a une voix consultative.

Le mandat des membres de la Commission est de cinq ans, renouvelable une fois, et il ne peut y être mis fin qu'en cas de démission ou d'empêchement constaté par la commission dans des conditions qu'elle définit elle-même.

Surtout, l'indépendance est défendue par l'incompatibilité avec la qualité de membre du gouvernement, l'interdiction de participer à des contrôles au sein d'un organisme auprès duquel un membre a eu un intérêt direct ou indirect dans les trente-six mois précédents, et l'obligation d'informer la commission de tout intérêt ou toute fonction à venir[58]. Enfin, les membres mais aussi les agents, nommés par le président sont tenus au secret professionnel encadré par le droit pénal[59] et ils ne reçoivent d'instructions d'aucune autorité.

Ces garde-fous juridiques ne satisfont cependant pas tous les défenseurs de la liberté car le caractère administratif de la CNIL entretient les méfiances quant à sa capacité à défendre les libertés individuelles. L'indépendance ne serait « pas dans son ADN » selon Mr David Forest, avocat spécialiste des enjeux informatiques. Selon lui, la CNIL n'est pas un contre-pouvoir car elle héberge des représentants de la majorité politique en son sein. Il dénonce ainsi sa participation à des projets de loi assassins pour les libertés comme celui qui voulait créer le fichier Edvige en 2008 et autoriser les données ethniques. A ce titre, il réclame la création d'une grande ligue de défense des droits et libertés informatiques sur le modèle américain pour sortir de « l'esprit de chapelle » de la commission[60].

Alex Türk, Président de la CNIL de 2004 à 2011, voit quant à lui les choses sous un autre angle et défend avec rigueur l'indépendance de l'institution qu'il dirige. A cette fin, il met l'accent sur la pluralité de sa composition représentant toutes les sensibilités politiques et l'absence de tout débat politicien dans le fonctionnement de la commission. Afin de défendre

[58] Art. 13 à 15 de la loi de 1978
[59] Art. 413-10 CP
[60] « Politique et technique : des problématiques consubstantielles », interview de Mr Forest dans la revue Expertises des systèmes d'information d'avril 2008.

sa propre indépendance, Mr Türk explique qu'il a été désigné président par ses pairs et que sa qualité de sénateur, non inscrit mais du côté de l'ancienne majorité, l'aide certes à obtenir des budgets mais le rend indépendant de l'exécutif[61]. Il reste que le débat fait rage et qu'il a aussi été nommé aux Big Brothers Awards, concours ironique organisé par l'association Privacy International, de 2003 à 2005 qui l'a désigné « gagnant Orwell » en 2010 pour ses prises de positions attentatoires aux libertés individuelles[62].

Le débat est ici éminemment politique, une analyse objective tend à nuancer ces propos concentrés sur la personne de Mr Türk pour considérer le travail de la CNIL dans son ensemble, qui révèle un difficile combat pour contrôler la légalisation des fichiers. Les garanties relatives à l'indépendance de la CNIL peuvent sembler suffisantes en ce sens que l'exécutif ne peut influer directement sur sa composition et ses décisions. La représentation de la société civile et des associations de défense des libertés pourraient être selon nous renforcée. Ces conditions d'indépendance n'ont cependant aucun intérêt si en pratique la CNIL est impuissante à contrôler les fichiers, le budget de l'Etat pouvant moduler la portée effective de ses pouvoirs. L'enjeu principal tient alors aux moyens de travail de la commission.

2) ***Les moyens de l'action proprement dite***

Le point de départ de la réflexion tenant à la légalité des fichiers de police et de gendarmerie utilisés au cours du procès pénal, il convient d'étudier le contrôle réel de la CNIL sur le respect de cette exigence de transparence. Cette mission relève de la compétence de la commission grâce à l'article 11 de la loi de 1978 qui indique qu'elle veille de manière générale à ce que les traitements de données à caractère personnel soient mis en œuvre conformément à cette loi. A cet égard, elle doit être consultée lors de la création de fichiers de police et de gendarmerie et son avis est rendu public. L'efficacité de son contrôle dépend cependant de deux données : ses capacités financières et ses prérogatives juridiques.

Pour l'exercice de son pouvoir de contrôle, l'instance disposait en 2011 de 159 agents et d'un budget de 15,8 millions d'euros répartis à hauteur de 10,3 millions pour le personnel

[61] « Cnil : autoportrait d'un président énervé », interview de Mr Türk dans la revue *Expertises des systèmes d'information* d'octobre 2008.
[62] Association Privacy France, v. http://bigbrotherawards.eu.org

et 5,5 millions d'euros pour le fonctionnement[63]. Ces effectifs sont en augmentation continue et ils ont doublé depuis 2004. Or, ce chiffre reste faible si on le met en perspective avec nos homologues européens qui, en 2008, comptaient 160 agents pour l'autorité espagnole, 170 pour l'autorité britannique, 300 pour l'autorité canadienne et 400 en ce qui concerne l'autorité allemande[64]. En outre, il s'agit de bien comprendre que cet effectif doit répondre à l'ensemble des missions de la CNIL qui recoupent en partie le fait de contrôler tous les traitements informatiques, notamment privés, d'assurer la communication au public, de répondre aux plaintes et aux demandes de consultation ! En réalité, plus de 85% de l'activité de la CNIL en 2011 était dirigée vers les fichiers d'ordre privé. La conclusion s'impose donc d'elle-même : les moyens humains et financiers alloués à la Commission Informatique et Libertés sont largement insuffisants.

Enfin, il est nécessaire de préciser que l'autorité administrative est hyper-centralisée et que les contrôles sont exercés principalement sur Paris. La commission elle-même dénonce une inégalité dans la protection des citoyens et défend à ce titre une allocation de crédits supplémentaires pour créer neufs antennes en province mais ces vœux n'ont pas été exaucés.

Ce manque de ressources rend les contrôles de légalité des fichiers judiciaires bien complexes et il est doublé d'un amoindrissement des prérogatives juridiques, les pouvoirs de la CNIL ayant paradoxalement évolué à l'aune de la loi du 6 août 2004.

Dans un sens positif, ce texte a ouvert un pouvoir de contrôle des pièces sur place aux agents dans les mêmes conditions que les perquisitions, soit entre 6 et 21 heures, ainsi que la possibilité de demander communication de tout document nécessaire à l'exercice de sa mission. Le Procureur de la république territorialement compétent en est préalablement informé. En outre, la commission dispose d'un pouvoir de sanction à l'égard du responsable d'un traitement ne respectant pas les obligations visées par la loi mais il s'agit d'un simple avertissement suivi, s'il est nécessaire, d'une mise en demeure de régulariser dans un délai fixé.

A ce niveau encore, les dérogations sont de mise pour les fichiers de police car il ne peut être prononcé à leur encontre ni sanction pécuniaire, ni injonction de cesser le traitement. Seul un avertissement ou l'information du Premier ministre sont envisagés pour le cas où un fichier de

[63] Rapp. d'activité de la Cnil en 2011, http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/Cnil-RA2011/index.html
[64] Rapp. d'information du Sénat de 2009, « La vie privée à l'heure des mémoires numériques »

police violerait les droit et libertés fondamentaux. En cas d'atteinte « grave et immédiate », le président de la commission peut demander par la voie du référé à la juridiction compétente (administrative) de prendre les mesures de sécurité nécessaires[65]. Ces pouvoirs sont pénalement protégés puisque les articles 226-16 à -24 du code pénal envisagent les infractions à la loi de 1978. Le fait d'entraver l'action de la CNIL, par le refus de communication ou la communication de fausses informations, est puni d'un an d'emprisonnement et de 15 000 euros d'amende.

Les dérogations sont donc légion en la matière si sensible, car teintée de puissance régalienne, des fichiers de police.

Dans un sens plus négatif, la loi de 2004 a mis fin au droit de veto de la CNIL pour les fichiers de police. Contrairement aux traitements des entreprises, les fichiers de sécurité publique sont aujourd'hui soumis à un simple avis consultatif qui, de plus, est enfermé dans un délai de deux mois sous peine d'être réputé positif. Mises en parallèle avec les moyens humains et techniques dont dispose la commission, ces restrictions conduisent inévitablement à un amoindrissement de ses pouvoirs. Le fichier ELOI d'éloignement des étrangers, créé en 2006, a ainsi été mis en œuvre sans que le CNIL ait le temps de se prononcer à son sujet.

A l'évidence, ces pouvoirs sont encore plus réduits en ce qui concerne les fichiers classés secret-défense puisqu'à leur égard aucun contrôle n'est possible, ni par le biais de l'avis ni par des contrôles sur place[66].

Par conséquent, il semble que si les prérogatives de la commission sur le terrain sont théoriquement importantes, le défaut le plus prégnant tient à son avis simplement consultatif.

Pour conclure sur ces exigences théoriques relatives à la légalisation des fichiers de police venant au soutien de la procédure pénale, il apparaît que l'arbitrage entre l'efficacité des fichiers, la rapidité de leur régularisation, et la protection des libertés individuelles se fait en faveur de l'exécutif. Néanmoins, le cumul de l'absence d'intervention de principe de la loi et de l'absence d'avis conforme de la CNIL peut aussi convaincre d'une trop faible protection des citoyens[67]. Ce n'est pas là faire un procès d'intention aux tenants des fichiers de police, mais seulement souligner l'importance du débat démocratique et exiger *a minima* une réelle

[65] Art. 45 de la loi de 1978
[66] Art. 26 III et 44 IV de la loi de 1978
[67] P. Piazza, « L'extension des fichiers de sécurité publique » *Revue Hermès* n°53 d'avril 2009

prise en compte de l'avis d'une instance spécialisée dans la protection des libertés, qui plus est administrative.

Peut-être faut-il ici rappeler la définition de l'état de droit, « système institutionnel dans lequel la puissance publique est soumise au droit », pour persuader, s'il en est besoin, de la nécessité de respecter les principes, essentiels pour les libertés fondamentales. Une trop forte indifférence à ces préceptes conduit aujourd'hui à des critiques de toute part contre « un basculement inquiétant de l'Etat de droit à l'Etat sécuritaire » caractérisé par l'absence de transparence et les suspicions que cela entraine[68]. Un espoir semblait se dessiner avec la promesse de François Hollande d'instaurer un « Habeas Corpus numérique » redonnant compétence au législateur « s'agissant de la création et de la destruction ainsi que de la définition de la finalité des fichiers de police »[69]. Toutefois, les doutes persistent car en réalité la création et la simple définition de la finalité du fichier laisse toujours persister la libre définition du contenu et des conditions d'enregistrement par le pouvoir exécutif. Or, de telles données sont cruciales car elles définissent la légitimité des fichiers de police sur laquelle il convient à présent de se pencher.

[68] Op. cit. « Anormalité, surveillance et fichiers de police », J.J.Lavenue
[69] Interview de l'avocat William Bourdon, membre de l'équipe de campagne de François Hollande, le 16 avril 2012 dans Libération

Chapitre 2 : LA QUÊTE DE LEGITIMITE DES FICHIERS DE POLICE AU SERVICE DE LA PROCEDURE PENALE

La légitimité est la qualité de ce qui est fondé en droit, en justice, ou en équité[70]. Ce n'est donc pas seulement le respect du droit contrairement à ce que pourrait laisser penser son origine étymologique, *legitimus*, conforme au droit. Il s'agit de dépasser le respect de la loi pour convaincre de son bien-fondé, de son caractère équitable. Ainsi l'écrivain français Chamfort s'exprimait au XVIIIème siècle, « Il est plus facile de légaliser certaines choses que de les légitimer »[71].

Pour analyser dans quelle mesure la légitimité des fichiers de police justifie leur poids au sein de la procédure pénale, il ne s'agit pas d'établir une liste exhaustive, et descriptive, des fichiers. A ce titre, un résumé complet des fichiers à finalité judiciaire est présenté en annexe sous forme de tableau. La légitimité des fichiers tenant aux moyens mis en œuvre selon la finalité poursuivie, il s'agit d'examiner l'équilibre trouvé entre la logique sécuritaire et la protection des libertés, à travers les conditions d'enregistrement (Section 1) et le contenu des fichiers (Section 2), en prenant soin de développer les points les plus controversés.

SECTION 1 : UNE ALIMENTATION BASEE SUR LA SUSPICION

Les conditions concernant l'alimentation des fichiers de police présentent un double intérêt pour mesurer leur légitimité, à la fois du point de vue des circonstances à l'origine d'une inscription (§1) et des personnes pouvant être l'objet des fichiers de police, et donc de la mémoire d'Etat (§2).

[70] Définition du Petit Larousse
[71] « Maximes, pensées, caractères et anecdotes », de Sébastien Roch Nicolas dit Chamfort

§1 Quant aux circonstances d'enregistrement

L'article 6 de la loi Informatique et Libertés exige que les données soient recueillies de manière « adéquate, pertinente et non excessive » par rapport à une finalité déterminée. Tout enregistrement de donnée doit répondre à une fin précise, être justifiée par celle-ci. Ainsi, le fichage ne doit pas être généralisé à l'ensemble de la population mais segmenté selon l'utilité recherchée pour chaque type de fichier. Il convient donc d'apprécier la légitimité de l'alimentation des traitements de données selon leur rôle dans la procédure pénale en distinguant les fichiers de police à vocation judiciaire (A), ceux relatifs aux antécédents judiciaires (B), à l'identification (C) et au renseignement (D).
Chaque catégorie de fichier relève de circonstances d'enregistrement différentes, et plus ou moins permissives, selon leur intérêt judiciaire.

A. Les fichiers à vocation judiciaire

Les fichiers à vocation judiciaire servent aux services d'enquête spécialisés afin de diligenter leur travail et de le rendre plus efficace. Ces fichiers sont neutres en ce sens qu'ils fournissent des renseignements objectifs. Il s'agit principalement du Fichier des Objets et Véhicules Signalés (FOVeS), du fichier des propriétaires et possesseurs d'armes (AGRIPPA) et de celui relatifs aux interdits de stade (FNIS).
Le FOVeS, issu de la fusion des fichiers des véhicules volés (FVV) et des objets signalés (FOS), a pour objectif de fournir aux agents une information sur les objets volés, mis sous surveillance ou recherchés. Sur ce point, les conditions d'enregistrement tiennent aux constatations faites dans d'autres procédures ou aux plaintes déposées et visent à faciliter le travail quotidien des agents au niveau des enquêtes. Quotidiennement utilisé par les services de police et de gendarmerie, ce fichier concernant des objets et non des personnes ne soulève pas de critique quant à la légitimité de son existence.
Les fichiers AGRIPPA et FNIS sont respectivement alimentés suite à une décision administrative ou judiciaire d'autorisation ou de refus de détention d'arme, ou d'interdiction d'entrer dans un stade. L'existence d'une décision préalable et la spécialité de ces fichiers assurent le respect de la proportionnalité des atteintes au sein de la procédure pénale.

B. Les fichiers relatifs aux antécédents judiciaires

Les fichiers relatifs aux antécédents judiciaires ont davantage de poids dans le procès pénal car ils orientent non seulement le travail d'enquête initial, mais aussi l'analyse du magistrat lors de la personnalisation de la peine en fin de procès.
Les fichiers les plus importants sont ici le casier judiciaire, le STIC (Système de Traitement des Infractions Constatées) et le JUDEX (système Judiciaire de Documentation et d'Exploitation).

Le casier judiciaire pose peu de difficultés puisque les circonstances d'enregistrement sont des plus objectives. En effet, l'article 768 du code de procédure pénale indique que le fichier est alimenté par suite des condamnations contradictoires ou par défaut, non frappées d'opposition, pour crime, délit, contraventions de 5ème classe, ainsi que les déclarations de culpabilité assorties d'une dispense de peine ou de son ajournement. De plus, les contraventions des quatre premières classes sont indiquées si une mesure d'interdiction, de déchéance ou d'incapacité les accompagne.
D'autres circonstances tiennent notamment aux mesures relatives à l'enfance délinquante, à la faillite personnelle, aux condamnations étrangères ou aux déclarations d'irresponsabilité pénale.
La diversité des causes d'alimentation du casier judiciaire révèle un avantage absolu quant à la légitimité du traitement : seules des décisions définitives et émanant de magistrats sont à l'origine des inscriptions. Les conditions d'enregistrement sont donc ici parfaitement légitimes et si le casier judiciaire est l'objet de crispations, c'est davantage quant à la durée de conservation, étudiée par la suite.

Le STIC et le JUDEX présentent des difficultés plus complexes, du fait d'une permissivité plus large quant aux conditions d'enregistrement. Le texte fondateur du STIC est le décret du 5 juillet 2001, qui précise la finalité de ce fichier en ces mots : « faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs et l'exploitation des données à des fins de recherche statistique ».
Le JUDEX relève du décret du 17 novembre 2006 et il répond aux mêmes finalités et conditions que le STIC, à la différence près qu'il est tenu par les gendarmes et non par les

policiers. Ces deux fichiers seront d'ailleurs fusionné d'ici fin 2013 au sein du TAJ, « Traitement d'antécédents judiciaires »[72].

Les deux fichiers ont un rôle prépondérant au niveau de l'enquête et de l'instruction car ils permettent de recouper les informations et d'effectuer des rapprochements, notamment indispensables pour la lutte contre la délinquance d'habitude.

Leur alimentation est permissive en ce sens qu'elle relève des informations recueillies par les services de police et de gendarmerie au cours des procédures pénales relatives aux crimes, délits et contraventions de 5ème classe, sans vérification de leur réalité délictuelle par un magistrat.

Ainsi, comme le précise l'article 230-7 du CPP, toute information recueillie lors d'une enquête préliminaire, de flagrance ou d'une commission rogatoire qui concerne une victime d'infraction ou une personne à l'encontre de laquelle il existe « des indices graves ou concordants rendant vraisemblable qu'elle ait pu participer, comme auteur ou comme complice, à la commission d'une infraction » peut y être enregistrée. Le fait d'être cité dans une procédure pénale peut donc vite conduire à l'établissement d'un profil au sein de ces fichiers.

Le STIC renfermant de l'ordre de 6 millions de personnes mises en cause au vu du dernier contrôle de la CNIL datant de 2009[73], le débat se fait alors pressentir entre ceux dénonçant l'atteinte portée à la présomption d'innocence,[74] et ceux, confiants dans le travail des policiers, qui défendent l'enregistrement de faits « considérés comme avérés par les officiers de police judicaire »[75] puisqu'étayés par de forts indices.

La question est délicate puisque le travail d'enquête est largement appuyé par ces informations relatives aux procédés, lieux et dates des infractions d'un côté ; alors que l'utilisation faite de ces informations peut préjudicier aux individus concernés et aboutir à une suspicion générale de l'autre.

En réalité, il peut être conclu que les circonstances d'enregistrement, isolées du contenu des données enregistrées, sont bien encadrées et légitimées par rapport à la finalité du traitement tenant à l'efficacité des enquêtes. En effet, cela exige une source de connaissances en amont

[72] Décr. du 6 mai 2012

[73] « Conclusions du contrôle du STIC », rapport de la Cnil remis au Premier ministre le 20 janvier 2009

[74] Virginie Gautron « Usages & mésusages des fichiers de police : la sécurité contre la sûreté ? », AJP 2011 p. 266

[75] Renaud Vedel « Le rôle des fichiers dans l'action opérationnelle des services de sécurité intérieure », AJP 2007 p. 64

de l'intervention d'un magistrat. De plus, l'enregistrement a aussi pour origine toutes les données transmises par la suite, par l'autorité judiciaire.
Dès lors, la dualité des sources du STIC et du JUDEX concourt à la légitimité des traitements. Les difficultés relèvent davantage du contenu et de la fiabilité des informations, qui peuvent aboutir à un décalage entre les informations de départ et les qualifications finalement retenues par les tribunaux. Cela participe d'enjeux distincts qui seront développés dans la continuité de la réflexion.

C. Les fichiers relatifs à l'identification

Les fichiers relatifs à l'identification des personnes semblent relever d'une sensibilité plus accrue du fait de leur caractère attentatoire, non seulement à la vie privée, mais aussi pour certains à notre intimité plus profonde tenant à nos caractéristiques génétiques. Les fichiers d'identification sont principalement le FIJAIS (Fichier Judiciaire des Auteurs d'Infraction Sexuelle), le FAED (Fichier Automatisé des Empreintes Digitales), le FNAEG (Fichier National Automatisé des Empreintes Génétiques) et le FPR (Fichier des Personnes Recherchées).

Le FPR a été créé par un arrêté du 15 mai 1996, profondément modifié en 2005, et il répertorie toutes les personnes faisant l'objet de recherches par l'autorité judiciaire, les services de police, des douanes, les administrations ou les autorités militaires dans le cadre de leurs compétences légales. Alimenté par les services de police et de gendarmerie, et mis en liaison avec le système d'information Schengen (SIS), il prescrit aussi la conduite à tenir en cas de découverte de la personne. Ce fichier, malgré l'étendue de son champ d'application, reste en stricte adéquation avec sa finalité circonscrite et ne renferme aucune donnée biométrique, de sorte que la réponse apportée semble adaptée.

Le FNAED contient quant à lui les empreintes digitales qui relèvent d'une technique ancienne ayant permis l'identification de Mr Scheffer, auteur d'un homicide, pour la première fois en France en 1902. Elles font l'objet de ce fichier informatisé commun à la police et à la gendarmerie depuis un décret du 8 avril 1987. Le FNAED vise à identifier les auteurs d'infraction ainsi qu'à lutter contre les usurpations d'identité. Les circonstances d'enregistrement tiennent à un ordre de recherche par une autorité judiciaire, à une commission rogatoire ou plus largement à l'existence d'indices graves ou concordants de

nature à motiver l'inculpation d'une personne. Les établissements pénitentiaires peuvent aussi relever les empreintes digitales.
Depuis 2006, des bornes de signalisation sont installées dans les services de police afin d'accroître l'efficacité du système et la rapidité de l'enquête grâce à une numérisation de l'empreinte et une réponse immédiate. Au vu de l'utilité des prélèvements effectués lors des enquêtes, la proportionnalité opérée entre l'objectif poursuivi et les circonstances d'enregistrement du fichier tend à justifier la légitimité du fichier. Seule une hypothèse de comparaison de l'empreinte digitale, prévue à l'article 55-1 envers les personnes détenant des informations sur des faits, est critiquable. L'analyse est développée ci-dessous car elle concerne de la même façon le FNAEG.

L'analyse est généralement moins évidente pour un autre fichier d'identification, encadré par la loi cette fois, qu'est le FNAEG. C'est un des fichiers les plus connus par les citoyens car il renferme l'empreinte génétique de certaines personnes.
Objet de fracassantes révélations dans l'affaire Dickinson, de fantasme médiatique aussi bien que d'espoirs dans de sombres procès comme celui de Ranucci ou d'Omar Raddad, le FNAEG suscite moult réactions.
Ayant permis tout à la fois d'identifier des coupables comme d'innocenter des personnes contre qui le sort s'acharnait, le fichier des empreintes génétiques est un puissant instrument du procès pénal. A ce stade de la réflexion, il convient d'examiner les seules conditions d'enregistrement du fichier par rapport à sa finalité, tenant à l'identification des coupables aussi bien que des innocents.
L'article 706-54 du CPP précise que le FNAEG est dans un premier temps destiné à centraliser les empreintes et traces génétiques des personnes, reconnues coupables ou poursuivies mais ayant fait l'objet d'une décision d'irresponsabilité pénale pour trouble mental, des chefs de l'une des infractions de l'article 706-55. Dans un second temps, l'article autorise l'enregistrement des données génétiques des « personnes à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient commis une des infractions de 706-55 », ceci sur simple décision d'un officier de police judiciaire agissant d'office, ou sur demande du procureur de la République ou du juge d'instruction.
Deux points connexes sont alors à approfondir pour évaluer la légitimité de ces prévisions, quant à la liste des infractions concernées, et quant à la constatation de ces infractions.

La liste des infractions justifiant l'alimentation du FNAEG n'a eu de cesse d'être allongée. En effet, si la loi fondatrice du 17 juin 1998 se limitait à l'identification et à la recherche des auteurs des seules infractions de nature sexuelle, les lois de 2001[76] et de 2003[77] ont conduit à une généralisation de l'outil, de sorte qu'aujourd'hui, le fichier concerne l'ensemble des catégories des crimes et des délits. Sont ainsi concernées les infractions de nature sexuelle mais aussi celles attentatoires à la vie, à l'intégrité physique, aux biens ou encore aux intérêts fondamentaux de la nation[78].Si l'avantage de cette extension tient à la possibilité d'identifier les coupables et les innocents en tout domaine, l'inconvénient rejoint le problème d'un fichage toujours plus étendu. Les libertés individuelles et le respect de la vie privée exigent une limitation des cas de prélèvements d'empreintes aux infractions les plus graves. En ce sens, la réponse négative du Ministère de l'Intérieur au souhait d'un député de voir étendre le FNAEG aux infractions routières et financières s'appuie sur le respect de la stricte nécessité devant justifier l'extension du fichier[79].

Quant à la constatation de ces infractions, l'inconvénient tient à la faculté ouverte par la loi de 2003 de ficher les simples suspects d'office pour les officiers de police judiciaire. Les critères d'enregistrement sont ici intéressants et réfléchis car l'on constate une volonté de mesure. L'article 706-54 distingue bien les conditions selon la finalité poursuivie : pour la conservation des données, le texte exige « des indices graves ou concordants rendant vraisemblable la commission de l'infraction », alors que pour la seule comparaison des empreintes, il est prévu« des raisons plausibles de soupçonner » la commission ou la tentative d'une infraction. Cette différence est à souligner car elle montre la volonté du législateur d'être précis dans les circonstances justifiant une conservation des données sensibles. Alors que les raisons plausibles renvoient aux conditions du placement en garde à vue[80], les indices graves ou concordants correspondent aux conditions de la mise en examen[81]: la graduation dans les atteintes aux droits fondamentaux répond ici à une démarche logique et semble légitimer l'alimentation du FNAEG.

[76] Loi du 15 novembre 2001, relative à la sécurité quotidienne, JORF n°266 p. 18215, art. 56
[77] Loi du 18 mars 2003 sur la sécurité intérieure, JORF n°66 p. 4761, son art. 29 élargit le fichier à de simples délits et inclut les suspects
[78] Liste des infractions à l'art. 706-55
[79] Question publiée au JO le 01/01/2013 n° 14 826 et réponse du 2 avril 2013, Dalloz actualité du 22 avril « Refus d'extension du fichier des empreintes génétiques »
[80] Art. 62-2 CPP
[81] Art. 80-1 CPP

Cependant, les circonstances sont plus complexes à la lecture de l'article 55-1 relatif aux pouvoirs de l'officier de police judiciaire dans le cadre d'une enquête de flagrance, s'appliquant avec la même portée en cas d'enquête simplement préliminaire au vu du renvoi opéré par l'article 76-2. La loi prévoit que l'officier peut, à titre de comparaison avec les traces et indices prélevés, faire procéder à un prélèvement externe sur « toute personne susceptible de fournir des renseignements sur les faits en cause ou » à l'encontre de laquelle il existe des raisons plausibles de soupçonner la commission d'une infraction.
A titre d'enregistrement, l'article renvoie alors aux règles propres à chacun des fichiers (FNAEG et FAED). Dès lors, il semble bien que l'article introduit ici une nouvelle hypothèse de comparaison des empreintes, en dehors des prévisions de l'article 706-55, pour les personnes détenant des informations sur les faits! Cette circonstance de relevé de l'empreinte ADN semble totalement disproportionnée au regard même de la finalité du fichier, puisque l'individu n'est ni victime ni soupçonné d'avoir participé à l'infraction. Ce relevé n'est d'ailleurs pas sanctionné en cas de refus mais cette option n'est pas nécessairement connue des individus concernés, la circonstance reste grandement critiquable. Il s'agit ni plus ni moins que de comparer l'empreinte d'un simple témoin et ce n'est pas légitime.
De manière plus générale, la mise en fiche d'individus soupçonnés reste controversée et tend à rapprocher le FNAEG de son homologue britannique, le National DNA Database, mis en place en 1995. Ce fichier est le plus important au monde en terme de pourcentage de la population fichée[82] et l'un des seuls à prévoir une conservation illimitée dans le temps des données, y compris pour des mineurs, des suspects et même des personnes ayant bénéficié d'un acquittement ou de l'abandon des poursuites ! Il est ce faisant le plus liberticide. La comparaison est ici pertinente et tend à montrer que les conditions françaises relatives aux circonstances justifiant l'alimentation du FNAEG restent proportionnées au but recherché et par voie de conséquences légitimes.
Cette position peut être soutenue par la décision du conseil Constitutionnel du 16 septembre 2010[83] qui, statuant sur une question prioritaire de constitutionnalité à l'encontre du FNAEG, a confirmé la proportionnalité des circonstances permettant la conservation des données. A cette occasion, il a souligné l'utilité du fichier dans la manifestation de la vérité, à la fois pour punir et pour innocenter, et considéré que les garanties prévues par le code suffisaient à

[82]Claudine Guerrier « Les fichiers génétiques britannique et français à l'aune des droits de l'homme », revue *Lamy Droit de l'Immatériel,n°56, 2010 p.77-86* : le fichier anglais dénombrait 4,3 millions d'empreintes en 2008 contre 700 000 en France
[83] DC QPC du 16 septembre 2010

exclure les griefs fondés sur la présomption d'innocence, le principe de nécessité ou l'inviolabilité du corps humain. Le Conseil a bien émis deux réserves quant au délai de la conservation des données, et quant aux circonstances pour ce qui relève de la comparaison des empreintes, mais celles-ci ne remettent pas en cause la liste des infractions de l'article 706-55, au contraire, elle la légitime.

En effet, pour le seul rapprochement fondé sur des raisons plausibles de soupçonner une infraction, le conseil ne vient pas fermement opposer à la fascination pour la vérité scientifique, les dangers du soupçon généralisé. La réserve de constitutionnalité s'avère intrinsèquement paradoxale car le conseil précise seulement que la notion de «tout crime ou délit » doit être interprétée comme renvoyant à ceux prévus par l'article 706-55. Par conséquent, il semble à première vue mettre un frein à un rapprochement sans limite en venant contredire la volonté des parlementaires[84], mais au final, il se contente d'une liste tout de même très large.

Enfin, le conseil considère la liste susvisée en adéquation avec l'objectif poursuivi car « apte à contribuer à l'identification et à la recherche des auteurs ». Cette analyse est par conséquent paradoxale en ce sens qu'il semble que le conseil souhaite poser des limites au fichage ADN mais qu'en réalité il prône son utilité technique. Certains auteurs ont ainsi déduit de cette décision un blanc-seing donné au législateur pour allonger sans fin les infractions donnant lieu à l'enregistrement des données puisque toutes serviront à la manifestation de la vérité[85].

L'esprit critique doit s'exercer face à cette expansion des infractions justifiant le relevé de l'empreinte ADN qui semble sans limite et a conduit à une augmentation spectaculaire du nombre de fiches, passées de 2000 à 2 millions de profils entre 2002 et 2012. «Sur ces profils, 1 million sont de simples suspects», rappelle Mathieu Bonduelle, président du Syndicat de la magistrature[86].

Enfin, le FIJAIS est l'ultime fichier d'identification qui cristallise les débats. Créé par la loi du 9 mars 2004, ce fichier a pour objectif la lutte contre la récidive et l'identification des auteurs d'infractions sexuelles ou violentes. L'article 706-47 précise la liste des infractions définissant le champ d'application du fichier. Au départ cantonné aux

[84] Travaux parlementaires de la loi du 14 mars 2003, Rapport n°508 de l'assemblée nationale, première lecture
[85] Jean Danet « Le FNAEG au conseil constitutionnel : deux réserves, une confortation générale », AJP 2010 p. 545
[86] http://www.lefigaro.fr/actualite-france/2012/07/11/01016-20120711ARTFIG00269-le-fichier-des-empreintes-adn-sur-la-sellette.php

infractions de nature sexuelle et au meurtre ou assassinat accompagné d'un viol, de tortures ou actes de barbarie, le champ a été étendu au cas de proxénétisme à l'égard d'un mineur et aux meurtres ou assassinats commis en état de récidive légale et aux actes de torture ou de barbarie. Les conditions circonstancielles de l'enregistrement tiennent à une condamnation, y compris par défaut, et même non définitive, pour l'une de ces infractions, à l'exécution d'une composition pénale, à la mise en examen et même au cas de non-lieu, de relaxe ou d'acquittement qui seraient fondés sur l'abolition des facultés mentales[87]. Enfin, les condamnations de ressortissants français prononcées à l'étranger pour l'une de ces infractions donnent lieu à une fiche. L'inscription est de droit pour les crimes et délits punis de plus de 5 ans d'emprisonnement, elle doit être expressément prononcée par l'autorité judiciaire dans les autres cas.

La légitimité des circonstances adopte un sens tout particulier pour le FIJAIS car les conséquences précisées à l'article 706-53-5 sont bien plus attentatoires que la seule atteinte à la vie privée. En effet, à titre de mesure de sûreté, l'inscription au FIJAIS entraine l'obligation de justifier son adresse une fois par an et de déclarer tout changement dans les quinze jours. En outre, si la personne est définitivement condamnée pour crime ou délit puni de plus de 10 ans d'emprisonnement, cette justification doit être réalisée par une présentation en personne tous les six mois, voire tous les mois si la dangerosité de la personne le justifie ou si elle est en état de récidive légale. A défaut de respecter ces obligations, le système informatique du FIJAIS génère immédiatement une alerte aux services de police ou de gendarmerie qui ouvrent une enquête pénale et peut conduire à l'inscription de la personne dans le FPR. Enfin, la sanction prévue est une peine d'emprisonnement de deux ans et 30 000 euros d'amende.

Par conséquent, les circonstances justifiant l'alimentation du fichier doivent être précisément limitées au vu de la portée des suites que cela entraine. Du point de vue des infractions tout d'abord, malgré son élargissement, le champ pénal reste resserré aux incriminations les plus graves et semble satisfaire le caractère limitatif attendu. Du point de vue du constat de ces infractions ensuite, la légitimité du fichier peut être discutée car le législateur se contente de condamnations non définitives, voire d'acquittements, et surtout de la simple mise en examen par le juge d'instruction. Toutefois l'article 706-53-4 envisage le retrait de telles informations en cas de non-lieu, relaxe ou acquittement non fondé sur l'abolition des facultés psychologiques, de cessation ou mainlevée d'une mesure de contrôle judiciaire, de mort de

[87] Art. 706-51-2 CPP

l'intéressé ou de décision du procureur de la République. La conservation des données respecte donc la finalité du fichier et l'on peut conclure sur ce point au bien-fondé du FIJAIS.

D. Les fichiers de renseignements

La dernière catégorie de fichiers à examiner concerne les fichiers de renseignements. Parmi eux, les fichiers couverts par le secret-défense sont évidemment plus difficile à analyser du fait de la non-publication des décrets en Conseil d'Etat qui en sont à l'origine.
Le fichier CRISTINA (Centralisation du Renseignement Intérieur pour la Sécurité du Territoire et les Intérêts Nationaux) est le fichier de la DCRI, nouvelle Direction Centrale du Renseignement Intérieur depuis la réforme de 2008, qui a institué un service de renseignement unique. Ce fichier de souveraineté ne prévoit aucune durée de conservation et les circonstances de son alimentation sont inconnues. Cependant, les principes posés par la loi de 1978 quant au respect de la finalité et de la proportionnalité des mesures doivent être obligatoirement respectés. Dès lors, les circonstances sont présumées commandées par l'intérêt qu'elles présentent au regard de la sûreté de l'État et de la sécurité nationale. La légitimité ne peut être que présumée en l'espèce.
Le GESTEREX est un autre fichier secret-défense à la finalité plus étroite car il a été mis en place pour le travail d'une sous-section de la Direction du Renseignement de la Préfecture de Police (DR-PP) qui est chargée de la lutte contre le terrorisme et les extrémismes à potentialité violente. Le principe de la conservation d'une donnée en stricte adéquation avec la finalité du fichier conduit à présumer le bien-fondé du fichier.
Au soutien de ces présomptions de validité, il s'agit de préciser que, malgré le poids du secret-défense, ces fichiers sont soumis au droit d'accès et de rectification garanti à chaque citoyen et réalisé par le biais de la CNIL[88]. Cette éventualité pèserait nécessairement sur le respect des principes et de la finalité des fichiers.

En dehors des fichiers classés confidentiels, d'autres traitements rendus officiels servent au renseignement et à la surveillance du territoire.
Ces traitements permettent d'enrichir les enquêtes par le recoupement d'informations, notamment relatives aux habitudes des délinquants, à leur environnement, ou aux modes opératoires constatés.

[88] Art. 41 de la loi de 1978

Le Fichier des Brigades Spécialisées (FBS) et le Fichier de Travail de la Police Judiciaire (FTPJ) sont deux fichiers créés respectivement en 1991 et 1987 par les services de police sans autorisation légale. Leur commune finalité tient au recensement de toute information recueillie à l'occasion de la surveillance du territoire dans le cadre de la lutte contre la grande délinquance et le crime organisé ; l'un permettant des échanges entre services spécialisés et l'autre non. En dehors de l'absence de légalité de ces fichiers, mis en avant comme simples fichiers de travail pour remédier à la critique[89], les données collectées ainsi que la durée de conservation ne sont pas spécifiquement déterminées. La seule garantie tient une nouvelle fois au respect des principes légaux dont la proportionnalité, unique guide du comportement des policiers. Il peut apparaître illégitime que de tels fichiers, soit disant officialisés, ne rendent pas compte plus précisément des données enregistrées et des circonstances justifiant leur alimentation. On ne peut que souhaiter leur obsolescence constatée par les spécialistes.
Enfin, leurs défauts transparaissent d'autant plus face à un autre traitement, le logiciel SALVAC, encadré par la loi[90] et à la finalité précise, tenant au rapprochement des procédures judiciaires pour lutter contre la criminalité sérielle. Un service spécialisé alimente le fichier à partir des informations issues de la constatation d'infractions complexes, pour lesquelles aucun mobile n'est apparent ou mettant à jour un mode opératoire particulier. Les précisions données sur les hypothèses d'enregistrement et la finalité claire du fichier mettent sa légitimité en lumière par rapport aux fichiers précédents.

Pour finir, le renseignement s'appuie sur un dernier fichier de police davantage controversé. Le fichier EDVIRSP a connu de nombreuses péripéties et sa création a attiré l'attention de l'opinion publique suite à la médiatisation du fichier EDVIGE initialement envisagé.
A l'origine, il était prévu de ficher les personnes ayant sollicité, exercé ou exerçant un mandat, ou jouant « un rôle institutionnel, économique, social ou religieux », ainsi que celles dont l'activité individuelle ou collective est susceptible de troubler l'ordre public. De plus, EDVIGE devait contenir des données très sensibles et prévoyait le fichage des mineurs de treize ans. De nombreuses critiques se sont élevées de la part des citoyens émus de ce fichage généralisé et reposant sur des circonstances très floues. L'arbitraire des conditions

[89] Op. cit. Rapp. Bauer 2009
[90] Loi du 12 décembre 2005 relative au traitement de la récidive des infractions pénales

d'enregistrement a fortement mobilisé les associations telles la Ligue des droits de l'homme ou encore le syndicat de la magistrature qui ont signé la pétition « Non à Edvige »[91].
Aujourd'hui, le fichier EDVIRSP tente de s'écarter des critiques par un double renoncement au critère du « trouble à l'ordre public » et au fichage des personnalités sur la base d'un mandat ou de son rôle public (mais les préfectures prennent le relais par l'institution d'un répertoire des personnalités) en faveur du fichage des personnes dont « l'activité » indique qu'elles peuvent porter atteinte à la « sécurité publique ». Les circonstances justifiant l'élargissement du fichier semblent de ce fait plus objectives, c'est en tout cas ce que défendent les partisans d'EDVIRSP qui définissent la sécurité publique comme l'absence de périls pour la vie, la liberté ou le droit de propriété des individus. Cette notion apparaît à ce titre plus restrictive que le simple trouble à l'ordre public[92].
Dans un sens opposé, le fait est que ficher des personnes en raison de leur activité, qui semblerait indiquer un danger pour la société, inquiète et peut donner l'impression d'ouvrir la voie à l'arbitraire des policiers. En effet, les circonstances manquent de précision et les critères influençant les agents publics peuvent tout à fait relever de l'apparence, des vêtements ou d'autres indices à tendance discriminatoire. Dans cette perspective, certains perçoivent la survenance du « règne du soupçon » dans la création de fichiers de renseignement aussi larges qu'Edvige[93].
Le recul s'imposant face au ressenti politique, il peut être admis que la lutte contre la criminalité exige une information précise sur les risques et les menaces pesant sur la sécurité, pour permettre la surveillance et la prévention des infractions. A ce titre, on peut avancer que ces données n'ont pas vocation à être utilisées pour le prononcé de la condamnation mais servent uniquement le travail de prévention. Dès lors, pour ce qui est des circonstances à l'origine de l'alimentation du fichier, le caractère restreint de la finalité judiciaire tendrait à justifier leur proportionnalité. Encore verra-t-on plus loin que l'efficacité de ces fichiers ne fait pas l'unanimité.

[91] Consultable sur internet, http://www.nonaedvige.sgdg.org
[92] « Les fichiers du type Edvirsp sont-ils attentatoires aux libertés », entretien avec Christophe Soullez, in *Regards sur l'actualité*, mars 2009
[93] « Contre le fichier Edvirsp et le règne du soupçon », entretien avec J.P. Dubois, Président de la Ligue des Droits de l'Homme, revue *Regards sur l'actualité,* mars 2009

§ 2 Quant aux personnes enregistrées :

Deux catégories de personnes exigent une attention toute particulière quant au fichage dont elles peuvent faire l'objet, du fait de leur vulnérabilité dont on ne doit point abuser : les étrangers (A) et les mineurs (B).

A. Les étrangers

Si « l'étranger » de Camus est sans doute le premier visé de manière générale, par les fichiers de police, du fait de son herméticité aux codes de la société ; l'étranger du fait de sa nationalité mérite un éclaircissement sur les fichiers dont il fait spécifiquement l'objet.
Les étrangers ne seront que rapidement objets de précisions car les fichiers spécifiques à cette catégorie de personnes ont pour première finalité des questions de gestion administrative, de lutte contre la fraude des titres de séjour et contre l'immigration clandestine. La procédure de délivrance de visas fait à elle seule l'objet de différents traitements de données, tant au niveau européen avec le VIS (Système d'Information sur les Visas), qu'au niveau national à travers le fichier des empreintes digitales des étrangers, le fichier ADGREF (Application De Gestion des Dossiers des Ressortissants Etrangers en France), le fichier des étrangers sollicitant la délivrance d'un visa, le Réseau Mondial Visas 2 et le fichier des hébergeants.
En ce qui concerne plus particulièrement les fichiers utilisés au cours de la procédure pénale, les étrangers sont spécifiquement concernés par des registres particuliers dans le Fichier des Personnes Recherchées. Celui-ci classe les informations selon leur utilité pour les services de police entre la « police générale des étrangers », les « oppositions à résidence » ou à l'entrée en France, les « interdictions de territoire » ou « les étrangers recherchés en vue de leur extradition ». Le mécanisme de l'extradition cher au déroulement de la procédure pénale, comprenant un élément d'extranéité, justifie aussi un fichage des étrangers dans le Système d'Information Schengen (SIS) et dans le système d'Europol.
Dans cette perspective, il apparaît que le fichage des étrangers au sein de fichiers spécifiquement dédiés dans le cadre du procès, et surtout de l'enquête pénale, ne révèle aucune démesure.
Cependant, il faut rester très vigilant en la matière car le souvenir du scandale du MENS prévient des dérives possibles au sein de la procédure d'enquête et parce qu'il en est tout autrement dans les fichiers administratifs où un « fichage intégral » des étrangers est

organisé[94]. Enfin, l'étude du contenu des fichiers de police menée par la suite conduira à dénoncer l'instrumentalisation de certains fichiers concernant toute la population à des fins de stigmatisation des étrangers à travers des données relatives aux origines.

B. Les mineurs

Les mineurs sont une catégorie bien plus délicate à traiter du fait de leur vulnérabilité et du poids des dénonciations opérées à travers les fichiers. Le statut de mineur a ainsi toujours justifié un traitement particulier à leur égard. Les principaux textes sont l'Ordonnance du 2 février 1945 et la Convention internationale des droits de l'enfant[95] qui définissent toutes deux le mineur comme l'individu non émancipé âgé de moins de 18 ans. Si étranges soient-il, les principes français relatifs à la délinquance des mineurs sont limités aux fichiers judiciaires, c'est-à-dire aux registres des tribunaux comportant toutes les décisions relatives à un mineur, qui se veulent non publics. Quant aux fichiers de police, c'est davantage la Convention de 1990 qui est protectrice de l'intérêt des mineurs en défendant un régime dérogatoire pour toute procédure pénale intentée contre eux. L'article 16 de la Convention interdit toute immixtion arbitraire ou illégale dans la vie privée, la famille, le domicile ou la correspondance des enfants de moins de 18 ans, ainsi que toute atteinte à son honneur ou sa considération. Surtout, l'article 40 envisage le cas des procédures menées contre un enfant suspecté, accusé ou convaincu d'infraction à la loi pénale et exige un traitement respectueux de la dignité et des libertés fondamentales. Toutes les étapes du procès pénal doivent tenir compte de l'âge de l'enfant et avoir pour objectif de faciliter sa réintégration dans la société. Outre les garanties traditionnelles relatives à la présomption d'innocence ou aux droits de la défense, le texte envisage le respect de la vie privée de l'enfant.

Par conséquent, le « manque de maturité physique et intellectuelle » du mineur invite à être vigilant face à la volonté de plus en plus forte de le ficher au même titre que les adultes car son comportement n'est pas définitif, et ne doit pas obstruer toutes les chances d'un développement épanoui, en conformité avec les valeurs de la société. Le fait de figer les soupçons sur un être en devenir semble tout à fait opposé à cette logique d'épanouissement de l'enfant, dont les fautes peuvent être aussi formatrices pour comprendre les règles en société.

[94] Meryem Marzouki « Fichiers : logique sécuritaire, politique du chiffre ou impératif gestionnaire> », Revue *Mouvements*, 2010 n°62, p. 85 à 98.
[95] Convention de New York du 26 janvier 1990

Victor Hugo distingue fort bien ces deux logiques en ces mots, « Les soupçons ne sont autre chose que des rides ; la première jeunesse n'en a pas »[96].
Nonobstant l'unanimité du constat quant à cette fragilité naturelle, le rajeunissement de la délinquance conduit malgré tout à la nécessité de disposer d'informations sur les mineurs. Le débat renaît donc de ses cendres pour opposer virulemment les défenseurs des droits de l'enfance et les tenants du tout sécuritaire dénonçant l'explosion de la primo-délinquance. Ainsi, selon l'Observatoire national de la délinquance, le nombre de mineurs mis en cause pour des violences physiques non crapuleuses a augmenté de 200% entre 1996 et 2007, chiffre recueilli auprès des services de police et de gendarmerie, « dépendant donc de l'efficacité des services ».

Afin d'étudier la légitimité de la mise en fiche des mineurs, il convient de voir quelles garanties l'assortissent.

Pour le casier judiciaire, fichier judicaire mais utilisé aussi bien par les juges, pour décider de la peine, que par les services de police, dans le cadre de leur enquête, l'évolution s'est faite au détriment de la protection des mineurs. Avant la loi Perben II, les mesures éducatives et les condamnations à des peines d'amende ou d'emprisonnement inférieures à 2 mois étaient automatiquement effacées à l'âge de dix-huit ans[97]. Or, depuis 2004, il est seulement prévu qu'après l'écoulement d'un délai de trois ans à compter d'une décision, son effacement peut être prononcé par le Tribunal pour enfants à condition que la rééducation soit constatée. La suppression n'est donc plus automatique et les mesures peuvent rester inscrites après la majorité puisqu'elles y sont *a minima* pour trois ans.

Quant aux fichiers de police proprement dits, le mineur est concerné par les plus attentatoires et seules des garanties spécifiques peuvent justifier la légitimité de ce constat.

Pour ce qui est des fichiers d'identification, les mesures protectrices envisagées ne sont pas homogènes.
En ce qui concerne le FIJAIS, les réserves du Conseil Constitutionnel[98] ont influencées les évolutions récentes de la loi qui participent à un juste équilibre. Tout fichage des mineurs de moins de treize ans est exclu, celui des plus grands ne peut pas être automatique pour les

[96] Victor Hugo, *Les Misérables*
[97] Ancien art. 769-2 CPP abrogé par la loi du 9 mars 2004
[98] Décision n°2004-492 DC du 2 mars 2004 sur la loi du 10 août 2011portant adaptation de la justice aux évolutions de la criminalité

délits. Le principe connaît une exception dans le cas où une juridiction, ou le procureur de la république, l'ordonnent expressément[99].

Ces nuances soulignent l'instinct de réserve face aux dangers d'une mémoire stigmatisante ; l'équilibre semble être acquis.

Dans le fichier des empreintes digitales (FAED) et celui des empreintes génétiques (FNAEG), aucune attention n'est prêtée au cas des mineurs dont les données sont conservées aussi longtemps que pour les adultes, soit durant 25 ans pour le premier et jusqu'à 40 ans pour le second. Toutefois, des précisions ont été apportées pour le FNAEG et l'article 706-54 prescrivant le relevé d'ADN des « personnes condamnées ». Une note de la direction des affaires criminelles et des grâces du 23 juin 2006 précise que les « mesures » éducatives prononcées contre les mineurs ne constituent point une condamnation. Quid des« sanctions » éducatives ? Le flou maintenu au sujet de ces dernières, pourtant nettement distinguées des simples mesures dans l'ordonnance de 1945, semble laisser place à l'appréciation souveraine des juges. L'un d'eux, dénonçant « la folie du fichage » des mineurs, estime que les sanctions éducatives ne peuvent être considérées comme une condamnation au sens de l'article susvisé, de sorte qu'elles ne devraient pas justifier l'alimentation du fichier[100].

Le dilemme du fichage de l'ADN des mineurs n'est cependant pas résolu car l'article 706-54 prévoit aussi le cas d'une simple garde à vue à l'encontre d'une personne suspectée. A ce titre, le magistrat dénonce un relevé d'ADN systématique en amont, alors que la suite de la procédure conduit majoritairement à des mesures alternatives pour lesquelles ce n'est pas obligatoire, voire exclu pour les mesures éducatives. Dès lors, les procureurs devraient sans doute proscrire ces prélèvements au stade de l'enquête, sans se réfugier derrière la prévision de la loi liée à l'effacement des données, dès lors qu'ils ne répondent plus à la finalité du fichier.

Finalement, l'abstraction faite à l'égard des mineurs dans les dispositions relatives aux FNAEG aboutit nécessairement à un régime très flou. Si les garanties de principe de la loi de 1978 interviennent en leur faveur, ce n'est qu'avec la même force que pour les majeurs. Par conséquent le manque de protection est crucial. Il apparaît alors que le fichage des mineurs au FNAEG au simple stade de l'enquête soit contraire à la proportionnalité des mesures.

Au soutien de cette analyse, la décision de la Cour européenne des Droits de l'Homme à propos du fichier ADN britannique critique un système prévoyant une conservation illimitée

[99] Art. 706-53-2 CPP

[100] Côme Jacqmin « Les mineurs pris dans la folie du fichage », , juge des enfants, Revue Justice d'avril 2007

de l'ADN de mineurs non condamnés. Mettant l'accent sur la sauvegarde de la vie privée des mineurs au cours de la procédure pénale, la Cour a précisé que la conservation de données afférentes à des personnes non condamnées est particulièrement préjudiciable pour les mineurs ; le cumul de ces circonstances avec une durée illimitée conduit à la violation du principe de proportionnalité[101].

La deuxième catégorie de fichiers préoccupante pour le cas des mineurs relève des antécédents judiciaires qui frappent le passé de l'individu du sceau de la mémoire.
Entre droit à l'oubli et nécessaire individualisation des condamnations, le STIC et le JUDEX tentent d'offrir des garanties supplémentaires aux mineurs. Le droit à l'oubli est en effet préservé par la durée de conservation des données qui est raccourcie au profit des mineurs à hauteur de 5 ans en principe, contre 20 pour les majeurs. La gravité de l'infraction pourra néanmoins conduire à un délai de 10 ou 20 ans, mais la proportionnalité persiste car de semblables dérogations concernent les majeurs avec un délai maximal de 40 ans. Depuis 2004 un apurement automatique mensuel permet de traduire concrètement ces règles, de sorte que la proportionnalité des prévisions justifierait le bien-fondé du fichage des mineurs en l'espèce.

Enfin, les fichiers les plus discutés sont ceux liés au renseignement et plus précisément le traitement PASP (Prévention des Atteintes à la Sécurité Publique) qui a relancé la polémique à ce sujet. Malgré les modifications apportées au fichier d'origine, le fichage des mineurs de treize ans a été maintenu et reste polémique. Parce qu'il n'est pas conditionné par la réalisation d'une infraction, ce fichier sème des doutes sur l'avenir de jeunes jugés susceptibles de porter atteinte à la sécurité publique et prend les airs d'un casier judiciaire fondé sur le soupçon qui ne dit pas son nom. Les besoins de surveillance semblent alors confrontés à des difficultés intrinsèques quant aux critères de jugement de ces jeunes. Pour le président de la ligue des droits de l'homme, ce n'est dès lors « pas au jeune de bien se conduire, mais au policier d'oublier un soupçon discriminatoire »[102].Outre ces risques de dérives, le problème du droit à l'oubli a été avancé et le gouvernement a dû ajouter des garanties suite au scandale d'Edvige. Il défend à ce titre une adaptation du délai de conservation des données concernant les personnes âgées de moins de 18 ans, fixé à trois ans

[101] CEDH S et Marper c/ RU, 4 décembre 2008
[102] « Contre le fichier Edvige et le règne du soupçon », *Regards sur l'actualité*, mars 2009, entretien avec J.P. Dubois, Président de la Ligue des Droits de l'Homme

au lieu de dix[103]. Cette évolution dans la protection du droit à l'oubli des mineurs semble aller dans le sens d'un plus juste équilibre du fichier, mais ne fait évidemment pas l'unanimité.

Les mineurs sont donc ancrés définitivement dans le champ d'application des principaux fichiers de police et de gendarmerie. Les garanties apportées à leur épanouissement tiennent à l'exclusion des mineurs de moins de treize ans dont l'innocence est parfaitement respectée de nos jours, et à la diminution des délais de conservation des données, pour un oubli accéléré. Il est cependant permis de rester sceptique face à cette extension du fichage et l'on peut penser que cela devrait être proscrit à l'égard des données non judiciairement constatées, instaurant un soupçon difficile à ignorer pour l'avenir du mineur.

Section 2 : UN CONTENU EN VOIE D'OBJECTIVATION

Le contenu des divers fichiers de police doit par principe correspondre à des données en lien avec la finalité poursuivie. Il apparaît dès lors hétérogène, selon les nécessités, mais la limite tient au respect des droits et libertés fondamentaux, dont la vie privée en est la principale variable d'ajustement.
S'il ne s'agit guère d'énumérer les données enregistrées dans chaque fichier, il convient d'analyser leur degré de légitimité en les regroupant en différentes catégories.

Les données classiques permettant l'identification de base d'un individu sont notamment celles indiquées sur la carte d'identité. Elles ne posent pas véritablement de problème quant à leur contenu limité au strict nécessaire et relevant d'informations notoirement connues. Ainsi le nom, le domicile, la nationalité ou l'âge figurant sur la carte nationale d'identité doivent être à la portée des vérifications policières dans la vie de tous les jours. La légitimité du contenu des fichiers est donc une question intéressante, et délicate, pour les données plus intrusives à l'égard de la vie privée des personnes fichées.

Trois catégories de données se dessinent alors : celles relatives au passé judiciaire (§1), les données dites « sensibles » par la loi de 1978 elle-même (§2) et celles tenant aux caractéristiques biologiques (§3).

[103] Réponse du Ministère de l'intérieur à la question n° 07001 de J. Mahéas publiée au JO du Sénat le 15/01/2009

§1 Le passé judiciaire

Le passé judiciaire est intrusif en ce sens qu'il assimile une personne à ses antécédents délictueux et oriente son avenir en pesant sur la décision du juge comme sur le flair des enquêteurs. En réalité, il convient de distinguer les informations selon leur degré d'objectivité.

Indispensables au travail des agents de police pour connaître la personnalité de ceux à qui ils ont affaire, ces fichiers restent pleinement légitimes lorsqu'ils se fondent sur des précédents judiciairement constatés.

Ainsi le casier judiciaire encadré par les articles 768 et suivants du CPP contient des condamnations ou décisions prononcées par l'autorité judiciaire. Que les décisions concernent l'enfance délinquante, les arrêtés d'expulsions, certains jugements ou encore les compositions pénales du procureur de la République exécutées, le constat est uniforme : un juge du siège est intervenu. La seule exception tient aux sanctions disciplinaires des autorités administratives indépendantes entrainant une incapacité mais sur ce point les règles régissant ce pouvoir disciplinaire rejoignent celles de l'impartialité, de l'indépendance et du respect des droits de la défense, de telle sorte que les droits fondamentaux sont protégés.

Cette garantie tenant à l'intervention d'un juge et légitimant le contenu du casier judiciaire est mise à mal dans d'autres fichiers d'antécédents plus subjectifs.

En effet, pour le STIC et le JUDEX, la difficulté tient au fichage des suspects, c'est-à-dire d'un passé judiciaire présumé et non constaté. Comme le précise l'article 230-7 ces fichiers contiennent des informations sur les personnes « à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer comme auteur ou complice » à une infraction. Dès lors, le contenu des fichiers consiste à charger la personne concernée d'un passé délictueux incertain. Des personnes pourront être accusées et se voir attribuer le statut de « mis en cause » pour des faits qu'elles n'ont peut-être pas commis. De plus, si le cadre de la réflexion tenant à l'utilisation de ces fichiers est limité à la procédure pénale, on ne peut omettre de préciser les inconvénients d'un tel soupçon dans le cas des enquêtes administratives prévues par les décrets au sujet du STIC…

La légitimité du contenu des fichiers d'antécédents judiciaires peut donc être critiquée en ce qui concerne les informations nominatives relatives à des faits non confirmés par un magistrat mais conservées. Telle est notamment la position de Mr Brouillet, ancien officier de

gendarmerie et professeur de « Culture historique sur la sécurité et les institutions policières » à Assas[104].

§2 Les données sensibles

L'analyse est encore plus complexe face aux données dites « sensibles ».
Les tensions autour de cette catégorie de données ont déjà été étudiées dans le cadre de leur légalité. Les parlementaires exigent à leur sujet une autorisation expresse du législateur, recommandation jusque-là restée lettre morte[105].
A présent, le caractère particulièrement intrusif de ces informations par rapport aux libertés individuelles induit de nouveaux débats quant à leur légitimité.
La définition de ces informations est fixée par l'article 8 de la loi de 1978 dont il convient de rappeler qu'elle concerne « les données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci. »
A l'origine, cet article vise précisément à en interdire la collecte mais il prévoit des exceptions pour les fichiers justifiés par un intérêt public et autorisés par décret en Conseil d'Etat, donc pour les fichiers de police.
Par conséquent, il convient d'analyser le respect de la proportionnalité attendue en pareil cas entre la finalité poursuivie, les données autorisées, et l'intimité des personnes concernées.
Cela concerne en réalité quatre types d'informations : les données géographiques (A), celles relatives à l'origine raciale ou ethnique (B), aux opinions politiques, philosophiques, religieuses ou à l'appartenance syndicale (C), et celles concernant l'état de santé et la vie sexuelle (D).

[104] Professeur agrégé et docteur en histoire, chargé de cours à Sciences Po Paris et à l'IEJ d'Assas, rencontré le 9 avril 2013, ayant notamment commandé deux compagnies de gendarmerie départementale

[105] Recommandation n°10 du Rapp. AN de 2009

A. Les données géographiques

A première vue, cette notion de donnée géographique n'est pas visée par l'article 8 comme une donnée sensible et son caractère objectif vient au soutien de cette exclusion. Or, elle est en réalité contestée et le débat a été relancé avec la création du fichier PASP (fichier relatif à la Prévention des Atteintes à la Sécurité Publique) par le décret du 16 octobre 2009 prévoyant cette information en son article 3.

Les plus sceptiques y voient un effet implicite et indirect tenant à la révélation de l'origine raciale ou ethnique d'une personne, il s'agirait d'éviter la qualification de donnée « sensible ». Ainsi, l'association SOS racisme a par exemple dénoncé ce qu'elle considère comme un contournement et réclamé la suppression de cette donnée dans le fichier PASP devant le Conseil d'Etat[106].

Les rapporteurs de l'Assemblée nationale ont de même été divisés sur la question[107] entre ceux hostiles à tout risque de dérive et ceux y voyant un élément de signalement indispensable.

Enfin, les auteurs du décret à l'origine du PASP eux-mêmes participent de ce doute puisqu'ils ont inscrit cette donnée parmi celles sensibles et dérogatoires, malgré le silence de la loi de 1978.

Cependant, les garanties pratiques vont dans le sens du respect d'une stricte objectivité car le thésaurus fermé ne permet a priori d'enregistrer que le lieu de naissance des personnes, et non d'indiquer implicitement son origine raciale ou ethnique. Au soutien du maintien de l'origine géographique, une note du 18 octobre 2009 adressée aux Préfets précise que « 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 jouer un rôle déterminant ».

Finalement, l'origine géographique peut sembler opportune et efficace à la procédure pénale face à l'évolution de la criminalité et aux phénomènes de bandes. Le strict respect des prévisions reste indispensable à cette admission.

B. Les données relatives à l'origine raciale ou ethnique

De manière explicite, l'enregistrement des données relatives à l'origine raciale ou ethnique est prévu par la loi pour le STIC et le JUDEX, fichiers d'antécédents judiciaires et de

[106] Recours de l'association SOS racisme devant le CE contre le Décr. N° 2009-1249
[107] Rapp. AN de 2009

signalement. La sensibilité est immédiatement perceptible puisque le racisme flirte avec ce type de données.

Le rappel du principe permet de nuancer les critiques car une telle information n'est en principe précisée que si elle est nécessaire à l'identification des responsables. Cela participerait de la description indispensable à tout signalement. Toutefois, ce critère d'identification est fragile et le risque de racisme est inhérent à sa connotation très subjective. Sur ce point le STIC-Canonge a suscité des débats et les parlementaires ont exprimé leur hostilité face à ce type de donnée. Ce logiciel spécifique, développé dans le cadre du STIC, permet de faciliter la recherche d'auteurs d'infraction déjà connus des services de police à partir d'éléments de signalements fournis par un témoin ou la victime. Ce logiciel prévoit un filtre sur le « type » de la personne, en distinguant onze profils différents : blanc caucasien, méditerranéen, moyen-oriental, nord-africain maghrébin, asiatique eurasien, amérindien, indien, métis-mulâtre, noir, polynésien, mélanésien-canaque. Les rapporteurs parlementaires ont sollicité la suppression de cette typologie ethno-raciale pour y substituer des éléments objectifs tel un portrait-robot, la couleur des yeux, des cheveux et de la peau[108]. Cependant, cette proposition est restée sans effet et la typologie soutenue par le groupe de contrôle des fichiers de police présidée par Mr Bauer a été maintenue pour le STIC et sera présente dans le nouveau fichier TAJ. Le seul et faible changement opéré tient au retrait du type « gitan » de la liste envisagée.

Le groupe de travail de Mr Alain Bauer souligne, pour justifier la légitimité du relevé de telles données sensibles, le fait qu'il se rapporte à des « signes physiques particuliers, objectifs et permanents, en tant qu'éléments de signalement des personnes »et nécessaires à la recherche et à l'identification des auteurs des infractions inscrites dans le périmètre de l'application.

L'objectivité de l'origine ethno-raciale est donc diversement appréciée, on pourrait soutenir que la mise en place d'une typologie claire permet de réduire le risque de dérives lié à la simple qualification d' « origine raciale et ethnique ».Toutefois, comme le soulignent les associations SOS Racisme et la LICRA, cette typologie est absurde car elle est dépourvue de sens. En effet, la détermination du « type » de l'individu recherché par le témoin ou la victime participe non seulement d'une typologie raciale de l'humanité qu'il faut combattre mais elle est surtout totalement subjective selon son auteur, voire hasardeuse. Dès lors, c'est l'efficacité même du procédé qui est en cause et tend à détruire toute son utilité à la faveur de

[108] Rapport AN 2009, recommandation n°22

grands écarts entre la perception et la réalité. Ce point de vue peut être juridiquement appuyé par la décision du Conseil constitutionnel sur la loi relative à la maîtrise de l'immigration, à l'intégration et à l'asile[109] précisant que « Si les traitements nécessaires à la conduite d'études sur la mesure de la diversité des origines des personnes, de la discrimination et de l'intégration peuvent porter sur des données objectives, ils ne sauraient, sans méconnaître le principe énoncé par l'article 1er de la Constitution, reposer sur l'origine ethnique ou la race [...]. ». Il apparaît alors que de telles données ne sont pas objectives et ne doivent guider aucune distinction entre les individus. La légitimité est alors mise à mal à la fois théoriquement mais aussi en pratique du fait de l'absence de fiabilité de telle information.
Il nous semble personnellement qu'il faudrait s'en tenir à un signalement intangible tenant à la couleur des yeux, de la peau ou des cheveux.

C. Les données relatives aux opinions politiques, philosophiques ou religieuses & l'appartenance syndicale

Ce type de données se trouve dans les fichiers de renseignements généraux et de prévention des atteintes à la sécurité publique tels le PASP, issu d'Edvirsp en sa finalité judiciaire et remplaçant pour partie le fichier des Renseignements Généraux. Ces données étant extrêmement sensibles du fait de leurs atteintes très marquées à la liberté d'opinion et d'expression, le respect de la finalité du fichier prime avant tout et va définir la légitimité du contenu.
Une évolution en faveur des libertés est ici à signaler car à l'origine le décret relatif au ficher des RG du 14 octobre 1991 prévoyait la centralisation d'informations relatives aux personnes physiques ou morales ayant sollicité, exercé ou exerçant un mandat politique, syndical ou économique ou jouant un rôle significatif en ces domaines : il s'agissait du fichage des « personnalités ».
Pour le cas du fichier PASP, le décret final a renoncé au fichage des « personnalités » et aux données originellement prévues dans le cadre d'Edvige tenant aux « opinions » politiques, philosophiques ou religieuses pour y substituer celles relatives aux « activités » politiques, philosophiques, religieuses ou syndicales. En outre un garde-fou a été instauré tenant en l'impossibilité de sélectionner une catégorie particulière de personnes dans le fichier à partir de ces seules données. Ces éléments ne peuvent donc faire l'objet d'une recherche aveugle et

[109] Conseil Constitutionnel, n° 2007-557, DC du 15 novembre 2007

automatisée, ils sont mis à disposition dans le seul cadre de la consultation spécifique d'une personne.
Cette évolution vers plus d'objectivité par le biais de l'activité et non de simples opinions présumées pourrait satisfaire l'opportunité d'un tel contenu, fondé sur des actes.
La finalité préventive des fichiers de renseignements exige en effet de telles informations pour mettre fin à une activité terroriste ou repérer les troubles potentiels à l'ordre public.
Dès lors, il semble que les données permises par l'article 8 de la loi de 1978 relatives aux opinions ne soient guère légitimes puisque les tenants de la sécurité eux même y ont renoncé pour préférer la notion d'activité. Cette substitution devrait selon nous concerner tous les fichiers, y compris ceux soumis au secret-défense où de telles données doivent sûrement exister. De plus, comme le précise Mr Soullez[110], rapporteur du groupe de contrôle des fichiers de police présidé par Mr Bauer, il convient de distinguer les fichiers de renseignements tels Edvirsp, et les fichiers d'antécédents judiciaires tels le STIC et JUDEX qui ont davantage de poids dans la procédure pénale et sont donc moins enclins à accueillir de telles données. Selon lui, le renseignement n'a pour finalité que la seule prévention des troubles à l'ordre public et les données recueillies « ne vont pas jouer un rôle dans des poursuites ou dans la condamnation d'une personne » de sorte que si le doute n'est pas fondé il n'y aura aucune conséquence.
Le strict respect de la finalité des fichiers de renseignements légitimerait donc parfaitement le recueil de telles données sensibles, qui plus est factuelles.

Cependant, cette analyse met à jour les écueils de la légitimité de ce même type de données dans les fichiers STIC et JUDEX, ces derniers contenant de telles informations.
Point noir du sujet, ni le rapport du groupe de travail de Mr Bauer ni celui des parlementaires ne met l'accent sur la présence de telles données dans ces fichiers et il faut rechercher dans les textes de loi pour trouver une telle information. En effet, la création du TAJ par le décret du 6 mai 2012 confirme les doutes soulevés dès 2008 par un député face à la possibilité d'enregistrer des données sensibles dans un tel fichier[111]. L'article R 40-23 du CPP[112] prévoit que le TAJ « peut contenir des données à caractère personnel de la nature de celles

[110] Christophe Soullez « Les fichiers du type Edvirsp sont-ils attentatoires aux libertés ? », Revue *Regards sur l'actualité*, mars 2009
[111] Possibilité prévue dès l'article 1er du décret du 20 novembre 2006 quant au fichier ARIANE précédant le TAJ, in Questions parlementaires et réponses ministérielles : Les débats et documents de l'Assemblée Nationale et du Sénat : VIIe à XIIe législature, http://questions.assemblee-nationale.fr/q13/13-33627QE.htm
[112] Issu du Décret n° 2012-652 du 4 mai 2012 relatif au traitement d'antécédents judiciaires, fonctionnera le 31 décembre 2013

mentionnées au I de l'article 8 de la loi du 6 janvier 1978 dans le seul cas où ces données résultent de la nature ou des circonstances de l'infraction ou se rapportent à des signes particuliers, objectifs et permanents, en tant qu'élément de signalement des personnes » et dans le strict respect de la finalité du fichier.
Par conséquent, le futur TAJ, et les actuels fichiers d'antécédents et d'identification STIC et JUDEX, peuvent tout à fait contenir des données relatives aux opinions politiques, religieuses ou philosophiques des personnes si l'agent l'estime utile.
Cette faculté, ne serait-ce que théorique, semble bien disproportionnée au vu du but poursuivi tenant à établir les antécédents judiciaires d'une personne ! L'article règlementaire semble trop largement viser les données sensibles et l'exigence liée à un signalement objectif peut paraître insuffisante face aux potentielles dérives. La légitimité du contenu dépend alors bien davantage de la pratique que de la prévision textuelle et cela nuit à l'image de ce « super-fichier » qui inquiète les citoyens[113].

D. Les données relatives à l'état de santé et la vie sexuelle

Ces données ont été plus récemment protégées puisqu'en la matière c'est une directive européenne du 24 octobre 1995[114] qui, transposée par une loi du 6 août 2004 seulement, est venu insérer ces informations dans la catégorie des données sensibles de l'article 8 de la loi de 1978.
Quant à la légalité des fichiers sur ce point, un seul traitement pose des difficultés du fait de sa non-conformité à l'article 8 modifié. Il s'agit du fichier ESCORTE relatif à la gestion des transferts et extractions de détenus. Ce fichier est régi par un décret du 13 avril 2011 qui prévoit la collecte de données relatives aux maladies, mesures médicales ou prophylactiques, et au handicap d'une personne. La CNIL a bien expliqué à ce sujet que cette collecte n'est pas illégale mais que le décret ne précise pas que ce sont des données « sensibles » au sens de l'article 8. La légitimité n'est ici pas discutée car la connaissance de telles informations est indispensable pour la protection des détenus eux-mêmes.

Quant à la proportionnalité de ce type de donnée au vu de la finalité des autres fichiers, la question est plus complexe. En effet, il est intéressant de noter que le décret instaurant le fichier de renseignement PASP ne prévoit pas de dérogation à l'article 8 de la loi de 1978 en

[113] Article du 15 mai 2012, Le Monde « Police : Pourquoi le super-fichier TAJ inquiète » Anne-Gaëlle Rico
[114] Directive du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données

ce qui concerne les données sensibles liées à la santé et la vie sexuelle des personnes. Cette position montre le caractère très intrusif de telles informations et l'absence de toute utilité dans le cadre de la prévention des atteintes à l'ordre public.
Il semble même que le gouvernement ait la volonté d'exclure ce type d'informations de tout fichier comme l'indique la LICRA, membre du groupe de travail de Mr Bauer. On ne peut que se féliciter d'une telle décision si elle correspond réellement aux faits. Encore faut-il distinguer l'état de santé et la vie sexuelle.

Pour ce qui est de l'état de santé, sa connaissance peut tout d'abord être protectrice des personnes concernées elles-mêmes si l'on songe à la garde à vue.
Cependant l'examen médical obligatoire lors d'une garde à vue, permettant d'évaluer le possible maintien des personnes dans de telles conditions, est soumis au secret professionnel et doit être effectué à l'abri du regard et de toute écoute extérieure[115].
Il n'est donc nullement question d'enregistrer ces données dans un fichier.
Toutefois, pour les fichiers d'identification que sont le STIC, le JUDEX, et bientôt le TAJ, l'état de santé peut intéresser les agents s'il participe d'un constat objectif et permanent facilitant soit la reconnaissance d'un individu soit la connaissance de son comportement.
Ainsi, malgré la difficulté d'accéder à des informations claires et la volonté affichée du gouvernement de se débarrasser de ce genre de donnée, la lecture du décret créant le fichier TAJ et des articles règlementaires à son sujet sème doublement le doute.
D'une part, l'article R 40-24 prévoit de façon générale une dérogation à la prohibition d'enregistrer des données sensibles dans les seuls cas où elles « se rapportent à des signes physiques particuliers, objectifs et permanents, en tant qu'éléments de signalement des personnes » et dans le strict respect de la finalité du fichier. Ce premier constat montre que l'état de santé n'est pas par principe exclu.
D'autre part, l'article R 40-26 précisant les données pouvant être enregistrées sur les personnes mises en cause envisage « l'état de la personne ». Or la définition de cet « état » fait défaut et il est alors permis de le rapprocher de l'état de santé.
Par conséquent, le manque de lisibilité se fait ici doublement sentir et la prudence amène à ne pas confondre volonté du gouvernement et pratique des agents.

L'état de santé semble donc bien pouvoir être enregistré mais la légitimité de ce contenu peut être défendue si les strictes conditions des textes sont respectées car il s'agit de ne relever que des éléments objectifs et visibles puisqu'ils servent au signalement. Dès lors, le

[115] Art. 63-3 du CPP

caractère notoirement connu de cet état de santé répond à la juste mesure attendue dans le cas du fichage de tels renseignements. Le but de signalement ou même de prévention du comportement des personnes face à un agent est alors proportionnellement poursuivi.

Il en est autrement pour les données sensibles relatives à la vie sexuelle des individus, elles aussi exclues du fichier de renseignements PASP. Sur ce dernier point, le fichier TAJ est encore celui qui pose difficulté car la dérogation générale à l'article 8 de la loi de 1978 interdisant de récolter les données sensibles ouvre les portes à des dérives. Les conditions tenant à la nécessité et au respect de la finalité du fichier viennent se poser comme garde-fou mais il nous semble ici que l'élimination de la vie sexuelle aurait dû être expressément indiquée au vu de l'absence de toute utilité d'une telle donnée pour signaler une personne ou prévoir son comportement. Ce dernier type de donnée devrait selon nous être totalement exclu de tout fichier de police, à finalité judiciaire ou administrative ; la discrimination étant immédiatement perceptible.

§3 Les données biométriques

Enfin, la dernière grande catégorie de données présentes dans certains fichiers correspond à celles révélant le patrimoine biologique d'une personne. Ces données sont issues de l'empreinte digitale et de l'empreinte génétique, elles sont donc présentes dans certains fichiers d'identification judiciaire que sont le FAED et le FNAEG. Face à ce type de données, il ne s'agit plus d'examiner les conditions de l'enregistrement mais leur contenu, qu'est ce qui est exactement fiché ?

En ce qui concerne le FAED, sa finalité est double car il vise à identifier les auteurs de crimes ou de délits ainsi qu'à lutter contre les usurpations d'identité ou les identités multiples. Pour cela, il contient les traces digitales et palmaires relevées tout d'abord au cours des enquêtes, sur les lieux de crimes ou de délits et sur les personnes à l'encontre desquelles il existe des indices graves et concordants. En outre, le relevé des traces peut être ordonné par une autorité judiciaire, notamment en cas de disparition inquiétante ou suspecte d'une personne[116].

[116] Art. 3 du Décr. n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur

Enfin le contexte particulier des établissements pénitentiaires justifie cet enregistrement pour s'assurer de l'identité de la personne détenue et pour établir les cas de récidive.

Finalement les données transcrites correspondent à deux choses différentes si l'on veut être précis. Dans le cadre de la police scientifique, il s'agit en effet de distinguer les traces digitales (des doigts) et palmaires (des paumes) par rapport aux empreintes. Les premières sont les marques, visibles ou invisibles, laissées par les crêtes papillaires sur un support lorsqu'un individu manipule un objet ou un corps, alors que les secondes sont le résultat de l'apposition complète des crêtes papillaires après encrage de celles-ci. Les empreintes résultent donc de l'opération de prélèvement du policier alors que les traces sont laissées par le délinquant.

Dans les deux cas on obtient le même résultat tenant au dessin digital de l'individu qui est unique, immuable et inaltérable de sorte qu'il permet l'identification. Cette donnée manifeste donc le caractère unique de chaque être humain et concourt à son individualisation mais elle semble moins intrusive que l'ADN car elle est le fruit d'un prélèvement externe.

Les conditions d'inscription de cette donnée ayant été précisées en amont, le contenu répond bien à la finalité du FAED et semble sur ce point satisfaire aux exigences de nécessité et de proportionnalité caractérisant la légitimité.

Le FNAEG poursuit la même finalité d'identification des auteurs d'infractions et des personnes disparues mais son objet tenant à l'ADN semble plus intrusif, en ce qu'il conduit à mémoriser l'empreinte génétique des individus, située à l'intérieur des cellules.

De ce fait, la légitimité à enregistrer le patrimoine génétique tient à deux aspects, au contenu de l'information et à la méthode de prélèvement.

Cette donnée biométrique voit son contenu limité dans le FNAEG car l'article 706-54 du CPP, conforme aux exigences du Comité des ministres du Conseil de l'Europe et aux résolutions du conseil de l'Union Européenne[117], précise bien que seul l'ADN « non codant », à l'exception du segment marquant le sexe, peut être inscrit.

L'ADN codant correspond à celui qui « code » les protéines, c'est-à-dire à celui qui en commande la création en délivrant les informations nécessaires à une cellule pour créer une protéine. Cette partie de l'ADN permet notamment de connaître les maladies de l'individu et correspond à 5% du génome.

[117] Recommandation R.(92) 1 du comité des ministres du conseil de l'Europe et résolutions du 9 juin 1997 et du 25 juin 2001 du Conseil de l'UE

L'ADN non codant, seul à être enregistré, est donc celui qui ne permet pas la création des protéines et ne délivre aucune information sur l'état de santé. Il donne l'identité génétique des individus et permet de les distinguer, sauf pour les vrais jumeaux.
Par conséquent, le fait de ne retenir que cette partie du génome humain participe de la proportionnalité de la mesure et limite le risque de dérives, notons au passage que cette précision est d'une importance telle qu'elle figure dans la loi et n'a pas été assimilée aux simples modalités d'application réservées au décret.
Quant au prélèvement de cette donnée située au cœur des cellules, il s'agit d'un procédé « externe » et le conseil constitutionnel est venu préciser qu'il ne pouvait impliquer « aucune intervention corporelle interne » et donc « aucun procédé douloureux, intrusif ou attentatoire à la dignité des intéressés »[118].
Ces différentes précautions justifient le contenu des données enregistrées car il ne permet donc que l'identification des personnes, et non la fourniture d'informations sur les caractéristiques héréditaires spécifiques ; il répond au but poursuivi en respectant la dignité humaine.

La première partie du développement conduit donc à constater que la légalité des fichiers de police déroge sensiblement au principe de légalité criminelle par rapport à d'autres mesures prises dans le cadre de la procédure pénale comme la garde à vue, les perquisitions ou les auditions, du fait de son caractère éminemment règlementaire. Quant à la légitimité des fichiers, elle est discutée et certains fichiers apparaissent trop intrusifs dans les libertés et droits fondamentaux. Encore faut-il étudier la réelle efficacité des données collectées.

[118] DC Cons. Const. n° 2003-467 du 13 mars 2003, considérant 55

PARTIE II : LE CONTROLE DES FICHIERS DE POLICE POUR UN SERVICE LOYAL DE LA PROCEDURE PENALE

L'étude des fichiers de police s'inscrivant dans le contexte de la procédure pénale, il convient d'interroger l'efficacité de ces instruments au regard des objectifs qui leur sont assignés, et servant de justification, que sont la prévention et la répression des infractions. Toutefois, l'efficacité ne doit pas être synonyme de permissivité et le concept de loyauté vient plus justement illustrer les attentes des citoyens à l'égard de traitements renfermant des données personnelles par nature attentatoires aux libertés individuelles. La notion de loyauté dépassant le respect des prescriptions légales, parfois floues et dans tous les cas insuffisantes à garantir leur réel respect, elle est une exigence posée par l'article 6 de la loi de 1978. On la retrouve aussi comme limite à l'arbitraire à l'article 427 du code pénal relatif aux modes de preuve en droit pénal. Pour le doyen Bouzat, la loyauté est « une manière d'être de la recherche des preuves, conforme au respect des droits de l'individu et à la dignité de la justice »[119], l'horizon de la loi est donc dépassé pour atteindre le respect des droits fondamentaux.

Pour y parvenir, il est un préalable indispensable tenant à la fiabilité des fichiers sans lequel ces colosses aux pieds d'argile ne peuvent plus servir la procédure pénale, ou pire ne peuvent que la fausser. Divers contrôles des traitements de données sont organisés pour tenter de garantir leur fidélité (Chapitre 1). Par suite, c'est l'utilisation des fichiers qui nous renseignera sur la loyauté du service rendu à la procédure pénale et permettra de conclure sur leur efficacité (Chapitre 2).

[119] P.Bouzat « La loyauté dans la recherche des preuves », Mélanges Hugueney, Sirey 1964, p. 172

Chapitre 1 : LE CONTROLE DE LA FIABILITE DES FICHIERS

Corollaire évident de la loyauté des fichiers de police, la fiabilité des données enregistrées est un préalable considérablement important. De ce fait, nombre de vérifications ont été mises en place afin d'atteindre ce qui ne semble finalement être qu'un idéal. Deux catégories de contrôles sont alors à envisager : ceux internes au système des fichiers participant activement à l'institution judiciaire (Section 1) et ceux relevant d'acteurs externes que sont les personnes fichées et la CNIL (Section 2).

SECTION 1 : LE CONTROLE INTERNE

L'utilité des fichiers de police dépend en premier lieu de l'exactitude des données enregistrées. L'article 6 de la loi « Informatique et Libertés » énonce les conditions de licéité des fichiers de police, parmi lesquelles figure l'exigence de n'enregistrer que des données « adéquates, pertinentes et non excessives au regard des finalités » du traitement informatique ainsi qu' « exactes, complètes et, si nécessaire, mises à jour ».
Deux temps semblent alors se dessiner pour répondre au postulat de la fiabilité : celui de l'alimentation (§1) et celui des rectifications (§2).

§ 1 L'alimentation des fichiers

L'inscription des données dans les fichiers informatiques est une étape primordiale pour leur utilisation à venir dont l'efficacité dépendra de la qualité des informations.
Cette qualité dépend de plusieurs facteurs participant au contrôle interne des fichiers : de garanties personnelles tenant au niveau de formation des agents (A) comme de garanties techniques tenant aux modalités d'enregistrement (B).

A. Les garanties personnelles endogènes

Au stade de l'alimentation des fichiers, le contrôle interne est endogène en ce sens qu'il doit provenir des agents inscrivant les données eux-mêmes, et non de leurs supérieurs, opérant ce que l'on peut appeler un contrôle interne exogène lors de la vérification des données. Ce contrôle « endogène » dépend en premier lieu du niveau de formation des agents

de manière générale (1), mais aussi plus spécifiquement du statut des agents habilités pour les fichiers les plus intrusifs (2).

1) Le niveau de formation des agents

A cet égard, tous les spécialistes recommandent de renforcer la formation du personnel. Comparant les fichiers à « l'arme des policiers », le groupe de travail d'Alain Bauer argue du rôle fondamental de cet instrument dans le travail quotidien des agents pour défendre le besoin d'un niveau de préparation équivalent[120].

Cette formation est assurée pour les commissaires de police et les officiers de la gendarmerie et des guides pédagogiques sont mis à disposition.

Toutefois, cette prudence fait défaut pour les agents administratifs affectés à l'enregistrement des données dans de nombreux fichiers, alors que des connaissances en droit et procédure pénale sont éminemment attendues au vu des atteintes aux libertés individuelles encourues. Sur ce point, les parlementaires pointent du doigt une « problématique délaissée »[121] donnant lieu à un apprentissage sur le tas, dont le niveau juridique dépend du bon vouloir de l'administrateur. Le renforcement de leur formation est donc une exigence urgente[122].

L'espoir est permis du fait de la modernisation de nombreux fichiers de police qui sont autant d'occasions à saisir pour former le personnel.

2) La sélection des agents

Cette exigence générale doit être renforcée pour les fichiers de police aux conséquences attentatoires aux libertés individuelles. La question du statut de l'agent habilité à alimenter le fichier se pose alors.

Le premier fichier qui a connu une évolution à ce sujet est le FNAEG, encadré par les articles 706-54 et suivants du Code de procédure pénale, et contenant les empreintes génétiques des personnes concernées. L'extension du champ d'application du fichier, quant aux infractions et aux simples suspects, opérée depuis la loi du 18 mars 2003, s'est accompagnée d'un élargissement des personnes ayant un pouvoir d'initiative dans l'inscription des données.

---

[120] Recommandations n° 54 du rapp. AN de 2009 et n°15 du Rapp. de 2009 Bauer

[121] Rapp. AN de 2011, 3ème partie, A. 1.

[122] Recommandations n° 25 et 29 du rapp. AN 2009, n° 16 Rapp. Bauer 2009

Aujourd'hui, les empreintes génétiques des personnes déclarées coupables ou ayant fait l'objet d'une décision d'irresponsabilité pénale, pour une infraction justifiant l'alimentation du FNAEG, sont nécessairement inscrites par suite de la décision d'un magistrat.
Il en est tout autrement pour l'enregistrement des empreintes des simples suspects à l'encontre desquels il existe des indices graves ou concordants rendant vraisemblable qu'ils aient commis l'une des infractions en cause. La décision peut en ce cas émaner de l'officier de police judiciaire menant l'enquête, soit d'office, soit sur demande du procureur de la République ou du juge d'instruction. Par conséquent, c'est un pouvoir d'initiative important accordé à l'OPJ par rapport à ceux qui lui sont traditionnellement reconnus, notamment pour les perquisitions devant toujours être autorisées par le procureur dans les circonstances d'une enquête de flagrance ou préliminaire[123].
Il faut ici rappeler que le code distingue l'enregistrement de l'ADN et sa simple comparaison avec la base de donnée, qui relève elle aussi d'un pouvoir d'initiative de l'officier de police judiciaire, d'office ou à la demande des magistrats susvisés. Dès lors, l'enregistrement a des conséquences sur le long terme beaucoup plus graves que la simple comparaison, ne donnant pas lieu à alimentation du fichier, et l'on peut s'interroger sur la proportionnalité du pouvoir d'initiative des agents pour l'alimentation de la base de données. Il peut sembler que la comparaison satisfait à l'efficacité de l'enquête alors que l'enregistrement préfigure la condamnation du suspect, de sorte qu'il ne devrait pas être autorisé dans ces conditions.
Des garanties attachées à l'enregistrement décidé par un agent de police viennent nuancer le jugement. En effet, le procureur de la République peut, d'office ou sur demande de la personne concernée, ordonner l'effacement de l'empreinte dès lors que sa conservation n'est plus nécessaire. A défaut, l'intéressé peut saisir le juge des libertés et de la détention, et dispose même d'un recours devant le président de la chambre de l'instruction en cas de nouveau refus. Par conséquent, certains sont convaincus que l'extension du pouvoir d'initiative dans l'alimentation du FNAEG répond aux nécessités de l'efficacité du procès pénal.
Cependant le point de vue inverse est permis, notamment au vu des carences dans le suivi et l'effacement des données, et l'on peut rester pantois devant cette procédure[124].

[123] Art. 56 CPP pour l'enquête de flagrance et 76 pour l'enquête préliminaire
[124] Avis de Mr Brouillet condamnant cette alimentation du FNAEG

Le second fichier encadré par la loi aux articles 706-53-1 et suivants du CPP et particulièrement attentatoire aux libertés est le FIJAIS. Le FIJAIS est alimenté de plein droit ou sur décision expresse de l'autorité judiciaire uniquement suite à une condamnation, même non définitive, à l'exécution d'une composition pénale, à une mise en examen par une juridiction d'instruction, ou à un non-lieu, une relaxe ou un acquittement fondés sur l'abolition des facultés mentales, pour des infractions expressément délimitées.
L'inscription repose donc sur une décision émanant d'un juge. En outre, la loi précise que c'est le procureur de la République ou le juge d'instruction qui fait procéder à l'enregistrement des informations devant figurer dans le fichier, par l'intermédiaire d'un moyen de télécommunication sécurisé.
Ainsi, toutes les garanties sont prises au niveau de l'initiative pour garantir une alimentation légale du fichier, et donc exacte. Enfin, en cas de déclaration d'un changement d'adresse des personnes fichées, seuls les officiers de police judiciaire enregistrent la nouvelle information. C'est dire si en l'espèce la fiabilité des informations est protégée au vu des conséquences du fichier.

B. Les garanties techniques de l'alimentation

La fiabilité des fichiers au stade de leur alimentation met en jeu deux aspects techniques : si la technologie peut tout d'abord permettre de limiter le risque d'erreurs lors de la saisie des données (1), ses limites rejoignent en revanche la question de la vérité scientifique à travers les relevés d'ADN (2).

1) Les techniques de saisie des données

L'aspect positif des garanties techniques participe en premier lieu à limiter les bévues de saisie grâce à des logiciels permettant une inscription directe dans un fichier sans qu'un agent ait besoin de recopier les informations. Ainsi pour le fichier TAJ, il devrait être directement alimenté par le logiciel de rédaction des procédures de la police nationale (LRPPN, aujourd'hui NS2I). Ce transfert informatique des données simplifie le processus. De plus, comme précédemment expliqué, ce fichier fusionnant le STIC et le JUDEX les contradictions liées aux doublons entre les services de police et de gendarmerie seront évincées.

Enfin, les erreurs sont intrinsèquement limitées par le système informatique et la mise en place de thésaurus fermés. Il s'agit d'une liste de mots standards utilisés pour le classement[125] de sorte que le choix des agents est limité et normé dans le remplissage des informations collectées.

C'est encore une fois le cas dans le logiciel à l'origine du TAJ, fichier se voulant exemplaire en matière de lutte pour la fiabilité des données puisque de nombreux garde-fous techniques ont été mis en place à son égard. Il est aussi prévu que les données nominatives issues des procédures ne soient inscrites, en ce qui concerne les personnes mises en cause, qu'à la clôture de l'enquête de l'officier de police judiciaire, et non au compte-goutte comme avant. Pour autant, il est un obstacle redouté des services de police et redoutable, celui de l'usurpation d'identité. Fléau s'il en est, cette ruse amoindrit l'efficacité des fichiers d'antécédents mais le développement de la biométrie tente d'endiguer le phénomène.

2) L'ADN, la science et la recherche de la « vérité »

Nonobstant, la technologie connait ses limites et le point crucial de la fiabilité des fichiers est celui relatif à l'ADN. L'attrait pour les biotechnologies et la « vérité » scientifique n'a de cesse d'augmenter depuis les attentats du 11 septembre. La dernière version du Système d'information Schengen II, le fichier des visas délivrés au sein de l'espace Schengen, Eurodac, le FNAEG, Eurojust ou encore Europol sont autant de fichiers contenant l'identité génétique des individus.

Or, ce recours systématique à la biométrie justifié par l'insécurité et jouant avec les sentiments de peur des citoyens n'est pas infaillible. Le contrôleur européen de la protection des données dénonce lui-même ce problème de fidélité des analyses génétiques en illustrant ses propos par un exemple ayant conduit à l'emprisonnement d'un avocat pendant 2 semaines par le FBI suite à une erreur d'analyse[126].

Les principales failles du fichage de l'ADN tiennent à trois facteurs.

Tout d'abord, le premier cas d'erreur possible consiste en une inversion de prélèvements par les laborantins. La pratique montre en effet que lorsqu'il y a peu d'analyses à faire dans une enquête on regroupe les échantillons avec ceux d'un autre dossier pour former un « pool ». S'il faut un exemple pour convaincre, une affaire de meurtre en 2004 a mis en avant une telle confusion. Les empreintes génétiques relevées sur le lieu du crime identifient un homme au

[125] Dictionnaire le Larousse

[126] P.Piazza « L'Europe biométrique contre les libertés ? », in *Regards sur l'actualité*, mars 2009

profil de coupable idéal car déjà condamné pour tentative de meurtre et de viol, or celui-ci est en prison. Seul cet alibi en béton le sauva et conduisit à de nouvelles analyses l'innocentant. Les tubes entre deux affaires avaient été inversés. Le laboratoire s'excusant de la bévue a précisé qu'il était impossible d'écarter le facteur humain et donc les erreurs potentielles de manipulation des scellés. Cette première catégorie de faille montre que le risque d'erreur judiciaire perdure[127].

De surcroît, une autre maladresse est possible par le biais d'une contamination accidentelle des prélèvements. Pour cela, il suffit que le matériel scientifique, réutilisé pour différentes analyses, soit mal nettoyé et imparfaitement débarrassé des doses d'ADN d'une enquête antérieure pour que l'auteur précédent soit désigné comme suspect dans le prochain procès.
Cet incident a notamment été constaté dans une affaire de crime débutée en 2003 où les analyses effectuées sur l'ADN prélevé désignaient un suspect au profil intéressant mais habitant à plus de 850 kilomètres du drame. L'enquête a finalement révélé que les tapis de bouchons fermant les échantillons analysés et réutilisés avaient été la source d'une pollution des prélèvements. Encore une fois si l'alibi du principal et unique suspect n'avait pas pu mettre en doute de manière particulièrement évidente les résultats scientifiques, il aurait été fort probable que le suspect soit condamné.

Enfin, le G29 met en avant la multiplication des risques d'erreurs face à un fichier contenant une base de données trop importante. L'augmentation du nombre de données traitées diminuerait proportionnellement la probabilité d'identifier une personne face au manque de fiabilité des analyses[128], notamment pour les enfants ou les personnes âgées[129]. Ces avis concernent en l'espèce le VIS, fichier relatif aux visas délivrés dans l'espace Schengen et amené à contenir près de 70 millions de données biométriques, mais il fait fortement écho aux souhaits liberticides de certains politiciens de voir enregistrer l'ADN de tous les citoyens.

[127] Patrice Reviron « L'ADN : la preuve parfaite ? », AJP novembre 2012
[128] Avis n° 7/2004 du 11 août 2004 du G29 sur le VIS, p. 13
[129] Avis n° 3/2007 du 1er mars 2007 du G29 sur le VIS p.8.

« Les citoyens seraient mieux protégés si leurs données ADN étaient recueillies dès leur naissance », une telle déclaration est donc non seulement oppressante mais aussi techniquement fausse[130].

L'imperfectibilité des garanties humaines aussi bien que techniques, jusqu'à celle de la science elle-même, amènent donc à renforcer la nécessité de contrôler les données enregistrées et, comme nous le verrons dans le prochain chapitre, à rester prudent dans l'utilisation de ces informations.

§ 2 La rectification des données

De nombreuses données étant enregistrées en amont du procès pénal pour renforcer l'efficacité de l'enquête sur la base de suspicions, la mise à jour de celles-ci est indispensable pour la fiabilité des fichiers. L'article 6 en fait une condition de licéité des traitements de données en précisant que « les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées »
Les garanties propres à ce contrôle postérieur de la fiabilité des données sont à la fois personnelles, et relèvent alors d'un contrôle « exogène » car hiérarchique (A), et techniques (B).

A. Des garanties personnelles exogènes

La rectification des données est surtout sensible pour le cas de celles enregistrées en amont d'une décision sur le fond, en l'absence de la constatation des faits par un juge. Le contrôle hiérarchique s'impose alors pour la fiabilité à long terme des fichiers de police alimentés de suspicions.
Il s'agit principalement des fichiers d'antécédents judiciaires STIC et JUDEX, prochainement TAJ, servant à la constatation des infractions, au rassemblement des preuves et à la recherche des auteurs de ces infractions. Ces traitements contiennent, rappelons-le, des données recueillies au cours des enquêtes sur les mis en cause et les victimes présumées de sorte que leur temporalité est antérieure à une éventuelle décision du juge.

[130] Christian Estrosi, cité dans *Le Monde*, 16/01/2007

La solution semble alors simple et duale : il conviendrait d'effacer les données en cas de relaxe ou d'acquittement ou de non-lieu, de les corriger lorsqu'elles sont pénalement qualifiées. Les hypothèses étant en réalité plus diverses, les prévisions légales sont plus complexes. Il s'agit d'expliciter tout d'abord le fonctionnement du contrôle hiérarchique (A), ensuite les pouvoirs concrets des organes de contrôle (B).

1) Le fonctionnement du contrôle hiérarchique

Le fonctionnement du contrôle interne et hiérarchique des fichiers de police est tout d'abord une précision importante car facteur, une fois de plus, de troubles.
En effet, l'article 230-8 du CPP prévoit tout d'abord que ces fichiers sont sous le contrôle du procureur de la république territorialement compétent pouvant demander que les données soient effacées, complétées ou rectifiées.
L'article 230-9 du CPP met ensuite en place une surveillance des fichiers de police par un magistrat « chargé de suivre la mise en œuvre et la mise à jour » des traitements informatisés. Concourant à l'application de l'article 230-8 au dire du texte lui-même, les spécialistes de droit pénal, que sont Mrs Buisson et Guichard, mettent en doute l'utilité de ce « doublon »[131]. En effet, la loi prévoit que ce magistrat agit d'office ou sur requête de particuliers et dispose des mêmes pouvoirs d'effacement, de rectification ou de maintien des données personnelles dans les fichiers que son homologue le procureur. Même délai, même limitation du pouvoir, même droit d'accès aux fichiers concernés : l'identité des pouvoirs et du champ d'action est évidente. Le risque est alors de voir surgir des décisions contradictoires entre les deux magistrats, et même pire d'attenter à l'égalité des citoyens devant la loi. Le fonctionnement du contrôle hiérarchique met donc à jour une première faille pratique du fait du défaut d'utilité de sa dualité.

En outre, une seconde faille relative au statut des magistrats en cause discrédite ce contrôle interne d'un point de vue juridique. La recommandation R.(87) et la jurisprudence de la Charte des droits fondamentaux de l'Union Européenne exigeant la mise en place d'un contrôle des traitements de données personnelles par une « autorité indépendante »[132], le doute de la conformité du droit français en la matière des fichiers de police est permis[133].

[131] Serge Guinchard et Jacques Buisson, Manuel de procédure pénale, Lexis Nexis, 2012
[132] Article 8 Charte des droits fondamentaux intitulé « protection des données à caractère personnel »
[133] Charles Morel « Droit des fichiers, droit des personnes », 2ème partie, Gazette du Palais du 13 janvier 2004

Le contrôle du second magistrat prévu par la loi pourrait peut-être remédier à cette faille et recouvrer une utilité pour le moins théorique mais encore faut-il signaler qu'il n'est pas précisé si ce dernier relève du parquet ou du siège, voire de l'ordre administratif !
Pour le FNEAG, l'article R 53-16 prévoit expressément que le fichier est placé sous le contrôle d'un magistrat du parquet hors hiérarchie, en sus de celui du Procureur de la République compétent, nommé pour trois ans par arrêté du Garde des sceaux.
La carence de la loi est flagrante et fragilise d'autant plus le fonctionnement de ce contrôle.

Ces deux critiques fragilisent donc le contrôle hiérarchique prévu pour contrôler la fiabilité des fichiers et pourrait conduire à des décisions contradictoires quant aux mises à jour nécessaires au vu des pouvoirs de décision des magistrats en concurrence. C'est précisément ce pouvoir décisionnel de ces magistrats qu'il s'agit d'analyser à présent pour évaluer la fiabilité des fichiers de police et de gendarmerie à l'aune des garanties personnelles.

2) *La portée du contrôle hiérarchique* :

A la lecture de l'article 6 de la loi de 1978, la mise à jour des données et leur effacement répondent aux principes de l'exactitude et de la nécessité des données par rapport à la finalité du fichier. Dès lors, deux situations se présentent selon l'intervention postérieure d'un juge ou du législateur.

L'INTERVENTION DU JUGE

Suite à l'intervention d'un juge, trois hypothèses sont à distinguer : le cas de l'approbation des données par un juge ou de leur requalification judiciaire, le cas de la négation, et celui de l'indifférence aux données.

En cas d'approbation ou de requalification judiciaire, il est logique que les données soient conservées ou rectifiées. C'est le cas en pratique puisque la rectification est de droit pour le STIC et le JUDEX[134].

Si les données sont démenties, par suite d'une décision de relaxe ou d'acquittement devenu définitive, la logique voudrait que les soupçons pesant sur une personne disparaissent. Or, pour le STIC et le JUDEX, il est prévu que les données sont en principe effacées mais que le procureur peut en prescrire le maintien pour des raisons liées à la finalité du fichier s'il

[134] Art. 230-8 du CPP

prévient l'intéressé et que mention en est faite dans le fichier[135]. Pour le FNAEG l'effacement n'est même pas exigé par principe.

Enfin, dans l'hypothèse où les données ne donnent lieu à aucune suite judiciaire, il est prévu que les décisions de non-lieu et les classements sans suite, si ces derniers sont motivés par une insuffisance de charges, font en principe l'objet d'une simple mention sauf si le magistrat instructeur décide de leur effacement pour le STIC. Les autres décisions de classement sans suite (fondées sur une mesure alternative par exemple) font l'objet d'une mention mais ne peuvent pas être effacées par le procureur[136].

Dès lors, les principes régissant la mise à jour des données pour les fichiers d'antécédents semblent, en apparence, à la mesure de chaque suite donnée à la procédure. Les exceptions à l'effacement des données n'ayant donné lieu à aucune condamnation sont portées à la connaissance des agents, de sorte que la fiabilité du fichier paraît sauvegardée.

Cette logique est cependant critiquable, pourquoi conserver des données suspectant une personne d'avoir commis une infraction si celle-ci est innocentée ?

Malgré la mention qui est faite de la décision de justice pour répondre en apparence au critère de la fiabilité, cette solution biaise l'exactitude des renseignements puisqu'elle laisse perdurer des constatations officieuses et contredites par un magistrat. Dès lors, nombreuses sont les oppositions à ce droit de rétention. Le rapport parlementaire de 2009 présente ainsi des conclusions partagées sur le droit du procureur de maintenir les données en cas de relaxe ou d'acquittement[137]. Pour les décisions de classement sans suite ou de non-lieu, les parlementaires ont unanimement dénoncé le silence de la loi pour celles non motivées par une insuffisance de charges, sur lesquelles aujourd'hui le procureur ne peut pas s'appuyer pour prononcer un effacement des données.

Quant au fichage des suspects dans le FNAEG, aucune disposition ne fait obligation au procureur d'effacer les données, même en cas de décision de non-lieu, classement sans suite, relaxe ou d'acquittement non fondées sur l'absence de facultés mentales. Ce silence laisse entier le pouvoir de décision du procureur dont la seule limite générale tient à l'obligation d'effacer toute donnée qui n'est plus nécessaire à la finalité du fichier. C'est s'en remettre à un critère flou, qui laisse place à l'arbitraire, et il aurait été bien plus objectif de faire de telles décisions des critères d'effacement. Enfin, notre position peut être en partie justifiée par l'arrêt S et Marper contre Royaume-Uni de la Cour européenne des droits de

[135] Article 230-8 CPP

[136] Article 21 III de la loi du 18 mars 2003, Décr. du 6 mai 2012 article R. 40-31 et R.40-32

[137] Recommandation n° 38 pour et 38bis contre

l'homme du 4 décembre 2008 où elle juge que le refus d'effacer des empreintes digitales de personnes soupçonnées mais ayant bénéficié d'un classement sans suite, en outre mineurs, et sans délai maximum fixé, est manifestement disproportionné par rapport au but poursuivi et au regard de l'atteinte à la vie privée. L'absence de distinction claire entre les personnes condamnées et ceux ayant bénéficié d'une décision favorable, du point de vue de la conservation des données, semble donc critiquable.

L'INTERVENTION DU LEGISLATEUR

Il s'agit à présent d'étudier la négation du caractère délictueux des faits imputés aux personnes fichées par le législateur, c'est-à-dire l'amnistie et la réhabilitation.
Le Code pénal distingue la grâce, définie en son article 133-7 comme une simple dispense d'exécuter la peine, et l'amnistie, définie par l'article 133-9 comme l'effacement des condamnations prononcées. Hormis leur absence commune d'effet préjudiciable envers les tiers, les conséquences des décisions ne sont pas du tout les mêmes puisque la grâce ne conteste pas l'existence de l'infraction. L'amnistie, quant à elle, fait perdre le caractère délictueux des faits commis, de sorte qu'elle entraine l'effacement des condamnations constatant les infractions, la remise des peines, et l'extinction de l'action publique, à compter de la promulgation de la loi et durant la période envisagée.
Qu'elle soit acquise de plein droit ou judiciairement, la réhabilitation, définie aux articles 133-12 et suivants du code pénal, présente la même conséquence d'effacement pour « les incapacités et déchéances » résultant des condamnations. Or, il est prévu que les articles 133-10 et 133-11 relatifs à l'amnistie s'appliquent pour la réhabilitation. Il ne s'agit donc pas de renvoyer à l'article 133-9 prévoyant l'effacement de toutes les peines mais seulement celui des peines accessoires ou complémentaires.

La précision importante du code tient précisément à l'article 133-11 qui fait interdiction à toute personne qui, dans l'exercice de ses fonctions, a connaissance de condamnations pénales effacées par amnistie ou réhabilitation, d'en rappeler l'existence sous quelque forme que ce soit ou d'en laisser la mention dans un document quelconque. Cette interdiction, qui semble générale, laisse penser que les mentions de telles condamnations sur un fichier de police devraient être effacées.
En effet, cela peut être justifié par la disparition du caractère délictueux des faits amnistiés qui, emportant disparition de toute atteinte à la société, met fin à la fois à la nécessité

d'enregistrer de telles informations mais aussi à la fiabilité des données enregistrées sous une qualification pénale amnistiée. Les fichiers alimentés suite à une condamnation pénale devraient doublement être concernés par l'effacement des condamnations qui ont pour but de « remettre le condamné dans une situation d'innocence »[138], de lui « rendre un statut de citoyen ordinaire comme s'il n'avait jamais été frappé par la justice ». Enfin, la loi pose des exceptions seulement pour les minutes de jugements, arrêts et décisions de sorte qu'à la lecture de l'article 133-11 du code pénal, il est entendu que les fichiers doivent être rectifiés suite à une amnistie.

Toutefois, le premier obstacle à la rectification des données des fichiers de police est lié à l'absence de sanction prévue par le dit article. La jurisprudence a ainsi dû intervenir pour pallier le défaut de la loi et elle juge de manière constante que, malgré l'absence de prévision de la nullité par les textes, elle doit être prononcée lorsqu'une décision a été prise en considération d'une condamnation amnistiée. C'est dire que, si une décision est influencée par une condamnation amnistiée au vu de ces motifs, la chambre criminelle de la Cour de cassation l'annulera[139]. Cette première garantie jurisprudentielle est cependant insuffisante pour faire obstacle au maintien des données dans les fichiers.

Le second obstacle tient aux prévisions de la loi elle-même qui, pour certains fichiers, prévoit expressément qu'en cas d'amnistie ou de réhabilitation les règles propres à l'effacement des condamnations ne s'appliquent pas.

A ce titre, l'article 706-53-4 relatif au FIJAIS exclue la prise en compte de telles décisions pour apurer le fichier, alors même que celui-ci renferme des qualifications pénales. Les dispositions relatives au FNAEG restent silencieuses.

Face au défaut de clarté de la loi, une circulaire[140] accompagnant une loi d'amnistie de 2002 va dans le sens d'une distinction entre les fichiers. Elle précise que l'amnistie n'empêche pas le maintien des mentions relatives à des faits constatés dans un fichier de police judiciaire en amont de toute décision de justice car les simples faits, non pénalement qualifiés, ne sont pas effacés par la loi. Dès lors, il semble que toute prévision contraire comme celle envisagée dans les dispositions règlementaires relatives au STIC soit caduque.

---

[138] Mr Mayaud, Ouvrage de « Droit pénal général »,Edition Puf, 2010, p. 607 et 608

[139] Ch. Crim. du 12 mars 1985, Bull. crim. N°201 ; après la réforme du code Ch. Crim. 8 novembre 1995, Bull. crim. N° 343

[140] Bulletin officiel du Ministère de la justice n° 88, circulaire de la direction des affaires criminelles et des grâces, commentaire de la loi du 6 août 2002 portant amnistie

Cependant, le débat est plus complexe et de nombreuses propositions de loi accompagnent chaque décision d'amnistie pour obtenir l'effacement des données recueillies dans le FNAEG et dans le STIC pour les simples mis en cause, malgré l'absence de condamnation pénale attachée. Il est alors défendu que certes, l'amnistie ne concerne que la qualification pénale et non les faits, mais que l'alimentation des fichiers étant justifiée par des soupçons pesant sur la personne d'avoir commis une infraction amnistiée, l'effacement des informations les concernant semble raisonnable. Cette proposition a été adoptée par le Sénat le 27 février 2013[141] suite à la loi d'amnistie des faits commis à l'occasion de conflits sociaux et cet exemple montre qu'il est logique que l'amnistie concerne tous les fichiers, en ce sens que la philosophie même de la loi d'amnistie est d'apaiser les tensions et de privilégier l'oubli.

En conséquence, l'effacement des données suite à une amnistie ou une réhabilitation apparaît comme indispensable dans le cadre des fichiers alimentés par suite d'une décision de justice et, sur ce point, le casier judiciaire montre l'exemple[142].
De plus, il semblerait que la logique de la loi d'amnistie, si elle n'efface pas les faits commis dépourvus de la qualification pénale concernée, puisse conduire à l'apurement de tous les fichiers du fait du soupçon jeté sur les personnes à propos d'une infraction qui a disparu.
Les revendications du syndicat de la magistrature et le vote des lois récentes d'amnistie viennent au soutien de cette analyse[143].

Toutefois, les débats théoriques concernant le contrôle des fichiers de police se révèlent bien maigres face à la réalité technique de celui-ci, mettant à jour des carences incroyables.

[141] Article 11 de la Proposition de loi portant amnistie des faits commis à l'occasion de mouvements sociaux et d'activités syndicales et revendicatives, adoptée au sénat le 27 février 2013, 174 voix pour et 171 contre
[142] Art. 769 alinéa 3 CP, pour le seul cas de l'amnistie
[143] Article sur le site internet du SM « FNAEG : ne vous en fichez pas » revendique l'enregistrement des seules personnes concernées et, à tout le moins, le retrait des données suite à toute forme de réhabilitation

B. Les garanties techniques de rectification

Les procédés techniques permettant la mise à jour et l'effacement des données qui ne répondent plus aux principes guidant les fichiers de police correspondent à divers leviers : le délai maximal de conservation (1) et les procédés de transmission automatisée des suites judiciaires (2).

1) Le délai de conservation des données

En règle générale, le principe du respect de la finalité du fichier est techniquement garanti par un effacement automatique des données à l'issue du délai légal de conservation propre à chaque fichier.

Cette première garantie conduit à préserver le droit à l'oubli, voire la présomption d'innocence, en empêchant toute pré-orientation des enquêtes à la vue de données négatives. Les recommandations européennes rejoignent cette exigence en estimant que toute donnée ne répondant plus aux fins poursuivies par le fichier doit être effacée. Pour définir la durée de conservation, quelques indices sont précisés par le Conseil de l'Europe tels le prononcé d'une décision définitive, la prescription, l'âge de la personne concernée ou la sensibilité des données[144].

La durée oscille donc selon les fichiers et leur danger pour les libertés fondamentales ; il s'agit ici de s'intéresser aux principaux fichiers servant la procédure pénale.

Pour les fichiers d'identification, le relevé des empreintes génétiques ou digitales est un premier cas d'atteinte à l'intimité qui a soulevé des débats sur la durée de conservation des données.

Si l'on omet l'absence de tout débat démocratique que révèle le renvoi par la loi à un décret en Conseil d'Etat pris après avis de la CNIL pour décider du délai assimilé à une simple « modalité d'application », il convient de s'attacher aux critères de définition de celui-ci. L'article R 53-14 du CPP prévoit que les données enregistrées dans le FNAEG sont effacées à l'expiration d'un délai de 40 ans à compter de la condamnation définitive ou d'un délai réduit à 25 ans pour les simples suspects. En cas de classement sans suite, de décision de non-lieu,

[144] Recommandation R(87) 15 sur les données à caractère personnel dans le secteur de la police exigeant que les données « soient effacées si elles ne sont plus nécessaires aux fins pour lesquelles elles ont été enregistrées »

de relaxe ou d'acquittement exclusivement fondée sur l'existence d'un trouble mental les données sont conservées pendant 40 ans à compter de ladite décision.

Dès lors, la problématique tenant à l'enregistrement des empreintes génétiques en cas de simples suspicions rejaillit au sujet du délai de conservation de ces données. Si l'on s'éloigne du principe même de l'enregistrement de l'ADN de simples suspects pour lesquels aucune suite judiciaire n'est venu confirmer les doutes, il ressort des dispositions règlementaires qu'aucune distinction n'est faite selon l'âge du condamné, son passé judiciaire ou encore la gravité de l'infraction. Or, si le délai de 40 ans pouvait être un justifié à l'origine en raison de la spécificité de son objet réservé aux infractions sexuelles[145], l'extension du fichier et de la liste des infractions concernées a introduit une hétérogénéité de son champ d'application. Par conséquent, l'évolution du fichier nécessite une adaptation du délai de conservation et il semble que tous les acteurs en soient conscients. En effet, la loi prévoit tout d'abord que la durée de conservation doit être précisée par décret et laisse donc une marge de manœuvre au gouvernement pour adapter le délai, mais surtout les juridictions suprêmes semblent faire pression sur le gouvernement pour modifier les délais.

La cour européenne des droits de l'homme, saisie de recours de la part des faucheurs OGM, a notamment soulevé le problème de la durée de conservation des données et du respect de l'article 8 de la Convention relatif à la vie privée. Les poursuites n'ont pas abouti car les plaignants ont violé l'obligation de confidentialité imposée durant la phase de négociation à l'amiable, scandalisés par ce qu'ils dénoncent comme une tentative d'achat et de contournement d'une décision sur le fond[146]. Le rejet de la recevabilité des requêtes basé sur des considérations de forme devrait favoriser une prise de conscience du problème, consolidée par l'intervention du Conseil Constitutionnel.

Ce dernier a eu l'occasion de se prononcer sur la durée de conservation du FNAEG suite à sa saisine par le biais d'une question prioritaire de constitutionnalité. Par une décision du 16 septembre 2010, le conseil a émis une réserve sur le renvoi par la loi au décret pour fixer la durée de conservation des données. Il rappelle qu' « il appartient au pouvoir règlementaire de proportionner la durée […] compte tenu de l'objet du fichier, à la nature ou à la gravité des infractions concernées tout en adaptant ces modalités aux spécificités de la délinquance des

[145] Circ. du 10 octobre 2000 du Garde des Sceaux

[146] Requête n°47447/08 Deceuninck contre France du 13 décembre 2011, suite aux articles de Libération « Des faucheurs ni à ficher ni à acheter » du 22 novembre 2011 et du Syndicat de la magistrature « FNAEG : ne vous en fichez pas ! » du 21 novembre 2011

mineurs » ; sous cette réserve la loi est conforme à l'article 9 DDHC relatif à la présomption d'innocence[147].

Par conséquent, les dispositions règlementaires en vigueur semblent inadaptées aux exigences de proportionnalité attendues, il nous semble que trois critères devraient commander la durée de conservation des données.

L'état de minorité devrait en premier lieu moduler la durée comme l'exige le Conseil Constitutionnel et la Cour européenne. Cette dernière a eu l'occasion d'appuyer ce critère dans l'affaire S et Marper contre le Royaume-Uni du 4 décembre 2008 en insistant sur les conséquences psychologiques pour les mineurs, l'atteinte à la vie privée étant encore plus grande dans ce cas.

L'état de simple « mis en cause », que nous assimilons à celui de suspect, doit ensuite être pris en compte et à cet égard les prévisions françaises semblent respecter les exigences de proportionnalité si l'on admet le principe même de leur fichage. La Cour européenne a, dans le même arrêt, condamné le fichier britannique des empreintes génétique car il est prévu un fichage général, indifférencié et illimité des personnes même suspectes. La conservation à vie des empreintes ne préfigure d'aucune proportionnalité et conduit donc à une atteinte excessive à la vie privée. A l'égard de ces personnes, le Conseil de l'Europe recommande une conservation proportionnée, justifiée par la mise en cause de la « sûreté de l'état », critère on ne peut plus flou[148].

Enfin, la nature de l'infraction devrait être un facteur de mesure du délai car elle contribuerait à une personnalisation de la durée du fichage, adaptée à la dangerosité des actes de l'auteur. C'est aujourd'hui encore un facteur occulté.

En définitive, le FNAEG connait une durée de conservation qui n'est pas contestable dans son principe, mais il existe des lacunes dans son adaptation aux différentes circonstances justifiant son alimentation. L'indifférence au statut du mineur est particulièrement critiquable, il est urgent que le gouvernement concrétise une prise de conscience croissante du problème.

Pour les empreintes digitales, le FAED pourrait indiquer une solution intéressante et en conformité avec la recommandation européenne. La durée de conservation prévue est de 25 ans maximum pour les empreintes et correspond, pour les traces, au temps de la

[147] Jean Danet « LE FNAEG au Conseil Constitutionnel : deux réserves, une confortation générale », , AJP décembre 2010, DC 16 septembre 2010 n° 2010-25-QPC

[148] Recommandation R. (92)1 du Conseil de l'Europe sur l'utilisation de l'acide désoxyribonucléique dans la justice pénale

prescription de l'action publique (3 ans pour les délits et 10 ans pour les crimes). Au vu des moindres risques de dérives pour les empreintes digitales et de l'utilité du fichier au sein de la procédure pénale pour lutter contre les usurpations d'identité ou les identités multiples, la mesure envisagée n'induit pas de critique particulière.

Le dernier fichier d'identification crucial dans la procédure pénale est le FIJAIS, dont les conséquences sur la vie privée sont particulièrement flagrantes du fait des obligations qui en découlent, et des sanctions pénales qui y sont attachées. C'est ici la loi qui fixe la durée de conservation par le biais de l'article 706-53-4 du CPP à 30 ans pour les crimes ou les délits punis de plus de 10 ans d'emprisonnement, 20 ans dans les autres cas.
En l'espèce, la présence d'une condamnation définitive ou d'une décision d'irresponsabilité pénale fondée exclusivement sur l'existence d'un trouble mental font intervenir un juge du siège constatant les faits, la durée est donc bien proportionnée à la nature particulièrement grave des infractions concernées. Cependant, la qualité de mineur n'est pas prise en compte pour moduler la durée de conservation, de sorte qu'à leur égard le dispositif peut sembler disproportionné si l'on songe aux conséquences qui en découlent et à leur vulnérabilité.

Enfin, pour les fichiers d'antécédents judiciaires que réunit dorénavant le TAJ, la durée de conservation des données est de 20 ans pour les majeurs, avec des variations allant de 5 ans pour les délits les moins graves comme les délits routiers à 40 ans pour les infractions les plus redoutées. Pour les mineurs, le délai est de 5 ans en règle générale, avec des exceptions pouvant le porter à 10 ou 20 ans selon la nature des faits.
Les victimes sont quant à elles fichées durant 15 ans en principe.
Les nuances étant de mise au sein du TAJ, la gradation du délai d'enregistrement des données semble correspondre au principe de proportionnalité.

Toutes ces indications concernent cependant l'effacement automatique des données, intervenant à l'expiration du délai de conservation du fichier qui est un délai maximum. Cette première indication correspond donc à une garantie de dernier secours et interdit une intrusion *ad vitam aeternam* dans la vie des personnes.
La nuance doit être cependant de mise car certains fichiers n'ont aucun délai maximal de conservation prévu. Le fichier des Mains Courantes Informatisées (MCI) ou le fichier des

Brigades Spécialisées (FBS), ainsi que tous les fichiers de renseignements, sont soumis au principe de la nécessité mais aucun délai maximal n'est fixé.
Heureusement, d'autres procédés existent pour que les données ne servant plus la finalité des fichiers dans la procédure pénale soient effacées ou modifiées en temps utile et non à l'expiration du délai. L'objectif est d'instaurer un traitement en temps réel des données.

2) ***Le traitement en temps réel des ordres de rectification :***

Cette exigence de rapidité a été prise en compte très récemment face au constat de la difficulté croissante à avoir des données fiables. Ainsi, pour la réponse aux demandes d'effacement des données par les mis en cause auprès du procureur pour le STIC et le JUDEX, la loi Loppsi II du 14 mars 2011[149] a modifié l'article 230-8 du Code de procédure pénale pour réduire le délai de réponse du magistrat de 3 à 1 mois.
Les parlementaires ont proposé que soit mise en place une procédure d'urgence en cas de risque d'inexactitude de données relatives à des personnes et de préjudice immédiat et sérieux pour la personne demandant la rectification[150]. Cette proposition est à l'origine du doublon instauré par l'article 230-9 instaurant un magistrat ayant les mêmes prérogatives que le procureur mais, aucun pouvoir d'urgence ne lui étant attribué, les parlementaires ne sont pas satisfaits des suites données à leur recommandation.
Outre la rapidité des réponses aux demandes de rectification, le traitement en temps réel doit être renforcé pour la transmission des ordres de mise à jour du parquet aux gestionnaires des fichiers de police.
En effet, la CNIL a constaté en 2009 une double difficulté : pour la transmission des suites judicaires mais aussi pour le respect des demandes du procureur à leur réception.

En premier lieu, la CNIL constate une « absence quasi-systématique de transmission des suites judiciaires » nécessaires à la mise à jour du STIC. La CNIL rappelle à cette occasion que si la finalité principale du fichier est judiciaire, il est aussi consulté à des fins administratives et concerne ainsi plus d'un million d'embauches. La fiabilité du fichier est donc cruciale pour le respect des droits des citoyens. Or, l'enquête menée par l'autorité administrative indépendante auprès de 34 Tribunaux de Grande Instance représentant

[149] Art. 11 de la loi du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure
[150] Recommandation n°37 du rapport de 2009

50% de l'activité pénale en France montre que 21,50 % des classements sans suite, 0,47 % des décisions de non-lieu, 6,88% des acquittements et 31,17% des décisions de relaxe seulement ont été transmis en 2007. Les carences sont plus que flagrantes et leurs conséquences désolantes. Il en de même des cas de requalification pénale pour lesquelles « la situation est tout aussi préoccupante » au dire de la CNIL qui a comparé les qualifications inscrites dans le STIC et celles finalement retenues par les juridictions pour 645 personnes et a constaté l'inexactitude du fichier dans près d'un tiers des cas.[151]

En second lieu, le bât blesse aussi quant au respect des demandes de mise à jour effectuées par le procureur. En effet, le ministère de l'intérieur refuse de manière récurrente d'effacer les données malgré l'ordre judiciaire dans certains cas, tels la levée de la garde à vue ou les classements sans suite, au motif qu'ils sont justifiés par la faute de la victime ou que les faits sont avérés.
De fait, le pouvoir de contrôle des magistrats est alors totalement inefficace et souvent ils ne sont pas informés du respect ou non de leurs prescriptions, de sorte que se dessine un contrôle fictif du STIC. Les propositions de la CNIL étaient donc déjà urgentes dès 2009 pour améliorer la mise à jour des fichiers de police.
Depuis ce rapport et sa médiatisation très forte autour du chiffre rendu officiel portant à 17% le nombre de fiches de personnes exactes, des efforts ont été engagés.
L'interconnexion entre le logiciel CASSIOPEE du ministère de la justice et le TPJ « Traitement des Procédures Judiciaires », devrait permettre dans un futur proche une mise à jour obligatoire et en temps réel du fichier TAJ[152].

La fiabilité des fichiers de police subit donc les très mauvais résultats concernant le STIC, bientôt le TAJ. Il semble que l'informatisation des procédures aille dans le sens d'un renforcement de la fiabilité des informations, par le recours à des thésaurus fermé en amont et grâce à des procédés d'effacement ou de transmission des mises à jour automatiques en aval. Le contrôle interne repose donc à la fois sur des garanties techniques et humaines, ce deuxième aspect ne pouvant atteindre la perfection du fait, pour le moins, des manques de moyens. Pour pallier le défaut de garantie quant à la fiabilité des fichiers, le contrôle externe donne une part d'initiative aux citoyens pouvant actionner la mise à jour des fichiers.

[151] « Conclusions du contrôle du STIC », Rapp. CNIL remis au premier ministre le 20 janvier 2009, p. 18
[152] Rapp. d'activité de la CNIL de 2011 page 70

SECTION 2 : LE CONTROLE EXTERNE

« Le prix de la liberté c'est la vigilance éternelle », ainsi Thomas Jefferson[153] appelait de ses vœux un contrôle permanent des mesures menaçant la liberté et les droits fondamentaux.
Ce contrôle externe est le fruit de l'intervention de deux acteurs extérieurs à l'alimentation des fichiers : les simples citoyens (§1) et la CNIL (§2).

§ 1 Le contrôle citoyen

L'action des personnes fichées a pour préalable évident leur information, c'est seulement par la suite qu'elles pourront protester. Après avoir constaté qu'une telle évidence ne semble pas partagée par les organisateurs des fichiers (A), il s'agira d'exploiter les moyens d'action permettant aux individus de concourir à la fiabilité des traitements que sont leur droit d'accès et leur droit de modification (B).

A. Le défaut de droit à l'information

Le droit à l'information peut a priori sembler indispensable afin que les personnes fichées puissent vérifier l'exactitude des données qui leur sont attachées.
A ce titre, il convient de préciser qu'en principe l'article 7 de la loi de 1978 exige le consentement des personnes fichées mais qu'il ouvre immédiatement une exception en matière de fichiers. Il faut ici se rappeler que pour les prélèvements des empreintes digitales ou génétiques, le consentement est la règle, mais le délit de refus de s'y soumettre la sanction.
En outre, l'article 32 de la loi prévoit le droit à l'information des individus fichés.
Cependant, il est aussitôt précisé au VI que ces dispositions ne s'appliquent pas aux traitements de données « ayant pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales », bref, à tous les fichiers judiciaires servant la procédure pénale.
Ce n'est donc pas la loi de 1978 qui vient garantir ce préalable pourtant essentiel à l'action citoyenne, le droit à l'information est aujourd'hui toujours « inexistant »[154].

[153] Président des Etats Unis de 1801 à 1809 et rédacteur Constitution de Virginie de 1776
[154] Rapp. AN de 2011

D'un point de vue global, ce défaut de « droit » à l'information peut être justifié par l'efficacité de la procédure pénale et des enquêtes, l'inverse serait à la fois lourd formellement et dangereux pour le travail des agents car une information systématique pourrait entrainer la destruction des preuves ou la fuite des auteurs. Pour le cas particulier de la garde à vue, si les directions générales de la police et de la gendarmerie se satisfont d'un affichage dans les commissariats, les parlementaires ont sonné le signal d'alarme face à une telle carence dans la protection des droits et le respect du contradictoire au sein de la procédure pénale. Ils recommandent notamment une information personnalisée et écrite par le biais d'un document, informant toutes les personnes placées en garde à vue de leur possible inscription dans le STIC et le JUDEX[155].

Cependant, ces vœux sont restés lettre morte et le droit d'information absent, c'est seulement en cas de décision du procureur ou d'un juge que la personne sera informée de l'éventuel maintien des données dans le fichier. Ce premier obstacle peut sembler excessif car il risque de fermer définitivement la voie au droit d'accès, l'immense majorité des individus n'ayant pas conscience de l'étendue du fichage. L'effacement serait alors « le nouveau mythe de Sisyphe »[156] si l'on compare le nombre de personnes enregistrées, plus de 5 millions de mis en cause et plus de 28 millions de victimes en 2008, aux 2516 demandes d'accès effectuées la même année auprès de la CNIL.

B. Le droit d'accès et de modification

Ce droit d'accès est quant à lui défendu par la loi « Informatique et libertés » à l'article 39 qui prévoit que toute personne justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel afin de savoir s'il contient des données le concernant, leur catégorie, les moyens de les contester, les finalités et les destinataires du fichier. Le caractère régalien des fichiers de police et de gendarmerie justifiant toujours la mise en place d'exception, l'article 41 précise les modalités spécifiques de ce droit d'accès dont la mise en œuvre est indirecte. En effet, la demande doit être adressée à la CNIL et non aux responsables du fichier, à sa réception un magistrat de la CNIL appartenant ou ayant appartenu au Conseil d'État, à la Cour de Cassation ou à la Cour des

[155] Recommandation n° 27
[156] Virginie Bianchi « L'effacement des fichiers ou le nouveau mythe de Sisyphe », AJP 2007 p. 420

Comptes est désigné pour mener les investigations utiles et faire procéder, le cas échéant, aux modifications nécessaires.
C'est seulement si la commission constate que la communication des données ne met pas en cause la finalité du fichier, la sûreté de l'Etat et la défense ou la sécurité publique que l'on donnera satisfaction à la demande. La Cour européenne est favorable à cette approche.

L'étendue de ce droit d'accès a connu une évolution assez remarquable, la communication du contenu des données enregistrées ayant été obtenue non sans peine.
A l'origine, les articles 39 et 41 étaient interprétés strictement par le Conseil d'Etat considérant qu'ils permettaient certes de savoir si des données relatives à un individu étaient enregistrées mais non le contenu de celles-ci.
Par suite d'un arrêt du 6 novembre 2002, le Conseil d'Etat[157] a permis aux citoyens signalés dans le système d'information Schengen d'accéder au contenu des données afin de pouvoir réellement les contester. Dès lors, il faut en conclure que ce n'est pas la nature du fichier qui empêche la communication des données mais seulement la nature des données elles-mêmes, dans le cas où leur publication remet en cause la finalité du traitement ou la sécurité. C'est ensuite la loi du 18 mars 2003 qui a modifié l'article 39 pour en arriver au droit positif.
La conséquence théorique majeure est que, dorénavant, la loi autorise tout citoyen à accéder aux données contenues dans les fichiers des renseignements généraux, l'accord du ministère de l'intérieur venant simplement se rajouter à la communication de ces données par la CNIL. Ainsi, les fichiers CRISTINA et GESTEREX classés secret défense ainsi que le fichier de renseignements Edvirsp restent soumis au droit d'accès tel qu'envisagé par l'article 41. La suite logique de ce droit d'accès largement ouvert est alors la possibilité de demander une mise à jour des données.

Le droit de demander la modification des données est quant à lui envisagé à l'article 40 de la loi permettant aux personnes physiques de solliciter la rectification ou l'effacement des informations les concernant. Ce droit de mise à jour des fichiers est aussi étendu que le droit d'accès puisqu'il concerne les fichiers classés secret-défense. La décision finale appartiendra à l'autorité gérant le fichier et plus particulièrement au procureur contrôlant les fichiers judiciaires. Dès 2006, le rapport Bauer pointait du doigt l'absence de recours contre une décision de refus du procureur pour le STIC et le risque de condamnation par la Cour

[157] Assemblée du Contentieux CE, 6 novembre 2002, n° 194296, Mme Moon

européenne des droits de l'homme[158]. La situation est en réalité diverse. Pour les fichiers d'identification que sont le FIJAIS et le FNAEG, les dispositions règlementaires prévoient une demande directement adressée au magistrat contrôlant le fichier et un recours devant le juge des libertés et de la détention en cas de refus.
Pour les fichiers d'antécédents judiciaires et d'analyse sérielle, on a déjà précisé les apports de la loi Loppsi II quant à un doublon des magistrats décidant des demandes de rectifications mais ne permettant toujours aucun recours.

Les droits des citoyens restent cependant insuffisants pour véritablement jouer sur la fiabilité des fichiers du fait du manque de moyens pour répondre dans un délai raisonnable à leur demande. En 2011, le constat est à « l'immobilisme » pour le droit d'accès aux antécédents judiciaires, le délai moyen de réponse pour une personne effectivement inscrite dans un fichier étant d'un an.[159]
La CNIL explique ce déficit de traitement des réponses par l'insuffisance des moyens et l'augmentation corrélative des demandes d'accès et de modification, de 12% ne serait-ce qu'entre 2010 et 2011[160].

Une dernière précision concerne le droit d'accès pour les fichiers européens de police judiciaire. En ce qui concerne EUROPOL, fichier ayant pour finalité la lutte contre la criminalité transfrontalière, le droit d'accès et de faire contrôler, rectifier ou effacer les données est reconnu aux personnes[161]. Pour autant, les analystes mettent en garde contre l'effectivité de ce droit car Europol doit consulter les autorités compétentes de chaque Etat membre concerné, un Etat pouvant à lui seul faire obstacle à la demande.
Ce même droit d'accès et de rectification est prévu pour le nouveau Système d'information Schengen, SIS II mais il est renvoyé à la compétence de l'Etat membre et à sa procédure d'accès et de mise à jour, de sorte que l'égalité d'accès sur le territoire de l'Union n'est pas assurée[162].

[158] Recommandation n°11 du rapport de 2007 du groupe de travail présidé par Bauer, « Fichiers de police et de gendarmerie : Comment améliorer leur contrôle et leur gestion ? »
[159] Rapp. AN de 2011, en 2010 sur 2796 demande en cours de traitement, une centaine datent de 2007
[160] Rapp. d'activité de la CNIL de 2011, page 69, 2099 demandes d'accès indirect en 2011, les deux tiers concernent le STIC et le JUDEX
[161] Art. 19 et 20 de la décision d'Europol de 2009
[162] Art. 41 du Règlement n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération

Enfin, pour le système Eurojust, le droit d'accès et de modification est prévu aux articles 19 et 20 de la Décision Eurojust[163] et il semble bien plus concret car la demande est gérée par l'organisme de contrôle d'Eurojust dont la décision définitive est obligatoire pour les gestionnaires du fichier. Les rapports de cet organisme montrent cependant une quasi-absence de contrôle de la fiabilité du fichier puisqu'en 2010 aucune demande d'accès n'a été portée devant l'organe de contrôle, en 2011 seules deux demandes ont été traitées. Ce constat bien faible remet à jour le problème de l'information des personnes fichées[164].

Pour conclure, le contrôle externe exercé à l'initiative des citoyens est quasi-absent pour les fichiers européens trop peu connus mais semble concourir à la fiabilité des fichiers d'identification que sont le FNAEG et le FIJAIS pour lesquels il existe un recours direct auprès des organismes de gestion des données. En revanche, pour le STIC, le JUDEX et le fichier issu d'Edvige PASP, le recours étant indirect, son efficacité subit le manque des moyens alloués à la CNIL. La fiabilité des fichiers est donc mise en danger pour ces fichiers judiciaires précisément.

§ 2 Le contrôle des autorités indépendantes

Il s'agit enfin d'analyser le rôle des autorités indépendantes dans l'effort de fidélité des données des fichiers de police en dehors de toute saisine par les citoyens. Ce contrôle externe fait intervenir en premier lieu la CNIL au niveau national (A), mais aussi diverses autorités européennes (B).

A. L'action de la CNIL

La CNIL dispose d'un pouvoir autonome de contrôle explicité aux articles 44 et suivants de la loi de 1978. A cette fin, elle dispose en principe d'un pouvoir de visite des lieux sous le contrôle d'un juge du siège et d'un droit à communication de tous les documents nécessaires à sa mission. Cependant, ces prérogatives permettant une réelle enquête sont mises à mal pour le cas des fichiers dispensés de publication de l'acte règlementaire les autorisant, c'est à dire pour les fichiers de renseignement classés secret-défense.

[163] Décision 2002/187/JAI instituant Eurojust en vue de renforcer la lutte contre les formes graves de criminalité, nommée la « Décision Eurojust »
[164] Rapport d'activité de l'Organe de contrôle commun d'Eurojust de 201, http://eurojust.europa.eu

Enfin, l'autorité administrative dispose d'un pouvoir de sanction en cas de non-respect des obligations légales, notamment en cas d'erreurs dans l'alimentation et la mise à jour des fichiers.

Une procédure contradictoire doit être mise en œuvre et débute par un avertissement, qui a le caractère d'une sanction. En principe, le président de la commission peut mettre en demeure le responsable du fichier d'agir et si celle-ci reste sans effet la CNIL peut prononcer une sanction pécuniaire, décider de l'interruption du traitement ou du verrouillage de certaines données. Toutefois, de telles sanctions sont écartées pour le cas des fichiers de police mis en œuvre par l'Etat. A leur égard, la CNIL peut prononcer un avertissement ou informer le Premier ministre des violations constatées. En cas d'atteinte grave et immédiate aux droits et libertés fondamentaux, le président de la commission peut demander à la juridiction compétente, par la voie du référé, de prendre toute mesure de sécurité nécessaire à la sauvegarde des droits et libertés.

Ce contrôle autonome de la commission reste au final modéré puisqu'elle a compétence pour contrôler tous les traitements de données à caractère personnels existants en France, dont les fichiers de police ne sont qu'une goutte dans l'océan. En 2011, la CNIL a contrôlé de sa propre initiative l'établissement pénitentiaire pour mineurs de Marseille, la direction de la protection judiciaire de la jeunesse des Bouches du Rhône, la direction départementale de la sécurité publique du Val d'Oise et la Préfecture de police du Val de Marne[165].

B. Les autorités européennes

Quant aux fichiers européens, leur contrôle relève d'une multitude d'instances.

De manière générale, le G29[166] promeut l'application uniforme des principes généraux relatifs à la protection des données dans l'Union Européenne, conseille la Commission sur les mesures nationales portant atteinte aux droits et aux libertés, et émet des recommandations. Il ne contrôle donc pas directement la fiabilité des fichiers et ne dispose d'aucun pouvoir de sanction.

[165] Rapp. d'activité 2011 CNIL

[166] Groupe de travail établi par l'article 29 de la directive n° 95/46/CE relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel et à la libre circulation de ces données

Le CEPD, Contrôleur Européen de la Protection des Données[167], est une institution indépendante qui contrôle quant à lui les fichiers de l'administration de l'UE et donne des avis sur les textes à adopter. Il est néanmoins notable que la Décision Europol de 2009 a omis de reconduire le contrôle du CEPD sur ce fichier de sorte qu'une telle carence vient limiter son rôle. Cette instance participe à la fiabilité des données mais l'immensité de son champ de travail laisse sceptique.

Surtout, des ACC, Autorités Communes de Contrôle, ont été instaurées dans le domaine de la coopération policière pour chaque traitement européen que sont Europol, Schengen et le Système d'information douanier. En matière de coopération judiciaire aussi, pour Eurojust, il existe un Organe de contrôle commun.

Enfin, des entités internes à chaque organisme gestionnaire d'un fichier bénéficient d'un statut indépendant de « délégué à la protection des données » et veillent au respect des règles entourant l'alimentation et l'utilisation du traitement.

Précision faite que les autorités nationales de contrôle des fichiers compétentes coopèrent avec ces diverses autorités, il reste que ce contrôle externe européen est trop faible et ne saurait être un facteur efficace de fiabilité des fichiers.

En outre, la multitude des textes et des avis des divers organismes compétents aboutit à une illisibilité totale et décourageante dénoncée par les spécialistes eux mêmes[168].

Le contrôle du contenu des fichiers de police fait donc tout d'abord preuve de diversité pour tenter de corriger les traitements automatisés mais, outre le risque de perdre en clarté, l'absence d'information des citoyens tend à le rendre fictif. Pour les fichiers nationaux, le contrôle de l'exactitude des données dépend de leur finalité mais de communs efforts sont à souligner dans cette recherche de vérité.

Nonobstant, la fiabilité des données reste incertaine et pose alors le problème plus large de l'utilité des fichiers. Comme l'a si justement dit un fonctionnaire de police « le STIC est tellement peu fiable qu'on ne peut rien en faire »[169]. Dès lors, de la fiabilité des fichiers à leur utilisation il n'y a qu'un pas, au support bien fragile.

[167] Créé par le Règlement n° 45/2001 relatif à la protection des personnes physiques à l'égard des traitements des données à caractère personnel des institutions et organes communautaires et à la libre circulation de ces données

[168] Sylvia Preuss-Laussinotte « Base de donnée personnelles et politiques de sécurité : une protection illusoire ? », , Identifier et surveiller. Les technologies de sécurité, *Cultures et Conflits* n°64, 2006 p.83

[169] Rapport parlementaire de 2011, Troisième partie, B. 3.

Chapitre 2 : LA LOYAUTE DE L'UTILISATION DES FICHIERS

L'article 6 de la loi de 1978 exige que les données collectées soient traitées de manière « loyale et licite », toujours dans le respect de la stricte finalité du fichier.
La licéité exige une utilisation des données s'inscrivant dans le prolongement des prévisions légales ou règlementaires, elle ne s'aurait être imprévisible.
De surcroît, la notion de loyauté, plus difficile à cerner, consiste en l'honnêteté de la manipulation des informations. Cette notion rejoint plus facilement l'idée de morale, de bonne foi dans l'usage des fichiers de sorte que l'analyse peut varier d'un individu à l'autre et que cette exigence de la loi de 1978 emprunte au flou du droit dénoncé par Mme Delmas Marty comme porte ouverte à l'arbitraire[170].

Dès lors, il n'est pas surprenant de constater des dérives en la matière (Section1), dont il faudra savoir tirer les leçons (Section 2) pour cerner l'efficacité du service réellement rendu à la procédure pénale par les fichiers de police.

SECTION 1 : LE CONSTAT DE DERIVES

Les dérives constatées ne doivent pas être simplement décrites, pour produire une réflexion aboutie il convient au préalable de s'intéresser aux précautions légales entourant l'utilisation des fichiers (§1), afin de mieux cerner les failles ouvrant la voie aux dérives (§2).

§1 L'encadrement de l'utilisation

Parce que la faillibilité humaine fait obstacle à l'avènement d'une société de risque zéro, le système juridique et social des fichiers de police ne peut se satisfaire de l'ordre de la loi et de la bonne foi des agents de police pour garantir une utilisation infaillible des données. De ce fait, diverses solutions ont été envisagées pour tenter d'empêcher les dérives relatives à la consultation des fichiers de police, par le biais des autorisations (A) et du contrôle (B).

[170] Mireille Delmas-Marty, ouvrage « Le flou du droit » PUF, 2004

A. L'habilitation à consulter les fichiers

La consultation des fichiers de police doit strictement respecter la finalité assignée au traitement de données, ce dont il ressort qu'elle est réservée à certains agents de police. Seuls les professionnels habilités peuvent accéder aux données contenues dans chaque fichier. Le principe est celui de l'habilitation individuelle et spéciale des agents, dont la fonction est en lien direct avec la finalité du fichier. Ainsi, la spécificité du droit d'accès aux données devrait permettre d'éviter les dérives.

Cela se manifeste parfaitement pour les fichiers à la finalité bien particulière comme le fichier des passagers aériens (FPA) consulté par les services de police aux frontières et certains services spécialisés.

Toutefois, si l'on considère comme acquis l'utilité des différents fichiers de police au sein de la procédure pénale, cela conduit à une consultation de données extrêmement diverses par les agents de police. La formule selon laquelle la consultation du fichier est ouverte aux «agents des services de la police nationale (ou les militaires de la gendarmerie), dans le cadre de leurs attributions légales, individuellement désignés et spécialement habilités », semblant restreindre les hypothèses, se retrouve en réalité pour des fichiers très différents. On la trouve notamment pour le fichier des possesseurs et propriétaires d'arme (AGGRIPA), le Fichier National Transfrontière (FNT), le Fichier National du Faux-Monnayage (FNFM), ou le Fichier des Véhicules et des Objets Signalés (FVOS). Ces fichiers ne posent pour autant pas de grave problème du fait de leur objectivité et de la stricte délimitation de leur champ d'application infractionnel.

Pour les fichiers plus sensibles, à commencer par ceux servant à l'identification biométrique d'une personne, la comparaison d'un état civil avec la base de données peut être faite par un Officier de Police Judiciaire pour ne pas procéder inutilement à une analyse ; pour ce qui est de la consultation des fichiers, seuls les services gestionnaires y sont autorisés. Ainsi, pour le FAED et le FNAEG, ce sont les fonctionnaires et militaires individuellement habilités des services d'identité judiciaire de la Direction Centrale de la Police Judiciaire (DCPJ) qui peuvent consulter les fichiers à la demande d'un magistrat ou des services d'enquête.

Cette concentration des pouvoirs de consultation entre les mains d'un service spécialiste du fichier satisfait le respect de la finalité du fichier car les services d'enquête doivent justifier leur demande d'accès aux données.

Ce schéma d'une consultation indirecte et argumentée se retrouve au sein du fichier PASP dont la consultation est réservée en principe aux fonctionnaires de la Direction centrale de la sécurité publique et à ceux des préfectures de police en charge du renseignement.

Toute autre est la situation pour les fichiers d'antécédents judiciaires que sont le STIC et le JUDEX, où ce sont les personnels de la police et de la gendarmerie nationale et des services des douanes, exerçant une mission de police judiciaire et désignés, qui consultent les fichiers. Les magistrats du parquet et instructeurs peuvent également accéder aux données relatives aux infractions dont ils sont saisis. Enfin, sont concernés les organismes de coopération internationale en matière de police judiciaire et les services de police étrangers dans le cadre des engagements internationaux[171].

Par conséquent, les agents habilités sont au cœur de la procédure pénale, parfois internationalisée, mais ils n'ont pas à recevoir une quelconque autorisation et sont peu contrôlés.

Il est en outre indispensable de préciser que le TAJ, tout comme ses prédécesseurs, fera aussi l'objet d'une consultation à des fins administratives par des agents spécialement habilités et dans un cadre restreint à l'identité d'une personne enregistrée en tant que mis en cause[172].

L'extension de la consultation du fichier ouvre donc la voie à une utilisation plus large, que l'on ne peut que redouter en connaissance du nombre d'erreurs, dans le fichier STIC en particulier.

Au 1er janvier 2008, 97 597 agents étaient habilités à consulter le STIC, plus de 13,8 millions de consultations ont été enregistrées en 2007[173].

Le nombre important de personnel concerné peut faire naître des doutes quant au respect d'une utilisation loyale des fichiers. Dans cette perspective, le témoignage d'un ancien policier Mr Pichon, se révèle riche d'enseignements quant aux dérives entourant le STIC, et vient corroborer nos hésitations. Ce dernier explique en effet qu'à la fin de sa carrière, il fut affecté à Meaux avec comme seule affectation professionnelle l'encadrement de dix personnes chargées de l'extraction des détenus. Sa mission ne relevant ni d'une mission de police judiciaire ni de la police administrative au sens des instructions régissant l'utilisation du fichier STIC, son habilitation à consulter le fichier lui a toujours semblé non conforme aux

[171] Art. 24 de loi sur la sécurité intérieure pour le STIC, art. R. 40-28 du décret du 6 mai 2012 pour le TAJ
[172] Art. R. 40-29 issu du Décret du 6 mai 2012
[173] Rapp. Bauer de 2009, page 55

principes[174]. De manière toujours plus surprenante, il dénonce les habilitations données à foison à un gardien de la paix chargé des archives du service ou à un brigadier chargé du matériel et de l'entretien des locaux[175].
La dose d'exhaustivité injectée dans la définition des agents habilités à consulter les fichiers de police ne peut pas suffire à garantir une interrogation loyale des bases de données.

B. Le contrôle de l'utilisation des fichiers

Subséquemment, le maniement des fichiers est sécurisé par des procédés techniques soutenant une possible répression des abus.

Le premier instrument de protection technique des données tient à l'enregistrement des consultations, afin de responsabiliser les agents et de permettre un contrôle hiérarchique.
A titre d'exemple, toute consultation du fichier PASP fait l'objet d'un enregistrement quant à l'identifiant du consultant, la date et l'heure durant un délai de deux ans ; pour le TAJ il est ajouté la nature judiciaire ou administrative de la consultation, et le délai est de cinq ans[176].

Le second instrument entourant la consultation des données consiste à limiter les critères de la recherche. En ce sens, la loi prévoit que pour certains fichiers l'accès aux données ne peut être le fruit d'une recherche aveugle mais doit partir de l'identité d'une personne pour arriver aux informations la concernant. L'objectif est de rendre impossible une recherche à partir d'un type de donnée pour arriver à l'identité de toutes les personnes fichées comme telles.
Cette réserve a néanmoins été instaurée à l'égard du seul fichier PASP contenant des données sensibles pour lequel il est interdit de sélectionner dans le traitement une catégorie particulière de personnes à partir de ces seules données[177].

Enfin, la dernière garantie relève de la répression des comportements déviants. Cette responsabilité peut être professionnelle et disciplinaire, pour non-respect des règles

[174]Philippe Pichon et Frédéric Ocqueteau, *Une mémoire policière sale : le fichier STIC,* JC Gawsewitch Editeur, 2010, p. 84
[175] Rapport de Philippe Pichon à Jean François Muller, chef de service contrôlant les habilitations du STIC, le 22 février 2007
[176] Art. R. 40-30 du décret du 6 mai 2012
[177] Art. 3 in fine du Décr. 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

déontologiques, mais aussi pénale puisque la loi de 1978 renvoie aux articles 226-16 à 226-24 du code pénal au titre des dispositions assurant son respect.
Les dispositions du code de déontologie de la Police nationale, ainsi que le règlement général d'emploi de la Police nationale, prévoient en effet que tout usage non conforme des données peut être qualifié de faute professionnelle de nature à justifier une sanction disciplinaire. Or, il n'est pas précisé quelle est la sanction encourue en cas de consultation non autorisée d'un fichier de police, de sorte que l'arbitraire peut encore s'infiltrer dans la répression ou l'absence de répression des comportements fautifs[178].
Dans cette perspective, l'article 226-21 sanctionne le fait de détourner les informations de la finalité du traitement d'une peine de cinq ans d'emprisonnement et de 300 000 euros d'amende. L'article 226-22 punit quant à lui des même peines le fait de porter à la connaissance d'un tiers, dépourvu de qualité pour les recevoir et sans autorisation de l'intéressé, des données dont la divulgation a pour effet de porter atteinte à la vie privée ou à la considération de la personne. Les poursuites sont pour ce dernier cas soumises à la plainte de la victime. La professeure de droit Mme Lepage a ainsi souligné l'efficacité plus grande de l'article 226-21 n'exigeant pas de résultat dommageable ni l'expression de la volonté individuelle de la victime pour réprimer les manquements[179]. On peut alors penser qu'elle englobe la seconde et la rend peu utile puisque la communication à un tiers non habilité vaut détournement. Toutefois le deuxième alinéa de l'article 226-22 prévoit le cas d'une divulgation à un tiers par imprudence ou négligence de sorte que le champ d'application est différent, l'infraction recouvre tout son intérêt.
Ces multiples garanties peuvent donc laisser penser qu'il existe un strict contrôle de la consultation des fichiers mais les témoignages éteignent vite cet espoir.

§2 Les dérives

L'efficacité de ces procédés est aujourd'hui à relativiser car les missions de contrôle effectuées sur place ont révélé des failles importantes dans la consultation des fichiers, notamment pour le STIC.

[178] Décr. n°86-592 du 18 mars 1986 portant code de déontologie de la police nationale JORF du 19 mars 1986 page 4586, article 114-3 de l'Arrêté du 6 juin 2006 portant règlement général d'emploi de la police nationale
[179] Commentaire de l'arrêt CA d'Aix en Provence du 30 juin 2009 par Mme Agathe Lepage, « Détournement de finalité de données à caractère personnel contenues dans le STIC », in *Communication Commerce électronique* n° 3, Mars 2010

Des petites entorses aux prescriptions légales aux dérives attentatoires aux libertés, les dangers du fichage mettent en garde quant à l'utilisation des données. Il s'agit dès lors d'analyser en premier lieu les défaillances du système, pour mieux cerner les dérives qui en découlent. L'occasion se présente alors de dénoncer les abus, qui concernent non seulement les fichiers d'antécédents (A) mais aussi ceux moins attendus d'identification (B)

A. Des fichiers d'antécédents aux dérives incontrôlables

L'utilisation quotidienne des fichiers de police a mis en exergue divers manquements à la loi, surtout pour le STIC qui a un rôle fondamental dans la procédure pénale et qui est ainsi surnommé « le casier judiciaire bis »[180]. La pratique a tout d'abord montré que les agents inscrivent leur mots de passe et identifiant sur des post-it à proximité des postes de travail de sorte que l'utilisation strictement personnelle de l'habilitation n'est pas garantie. De plus, les consultations administratives étaient en 2007 quasi-systématiquement effectuées à partir du module de police judiciaire alors que le module administratif ne permet d'avoir accès qu'à des données restreintes. L'enjeu est ici considérable pour la vie privée et l'accès à l'emploi, les données ayant connu des suites favorables aux personnes concernées tels un classement sans suite, un non-lieu, une relaxe ou acquittement ainsi que toutes celles relatives aux victimes étant exclues des consultations administratives. Enfinn les inspecteurs ont démontré que les responsables hiérarchiques n'utilisent majoritairement pas la traçabilité des consultations pour contrôler leurs subordonnés.
Les conséquences sont alors explicites et d'autant plus fatales en matière administrative qu'elles peuvent priver une personne de l'accès à un emploi : l'accès aux informations est souvent indu et l'utilisation des données non contrôlée[181].

Ces défaillances sont autant de portes ouvertes aux dérives qui viennent fragiliser l'efficacité, voire la légitimité, des fichiers de police.
Les arrêts sanctionnant le détournement de la consultation des données par rapport à la finalité du fichier expliquent les différents motifs persuadant certains fonctionnaires de violer la loi : l'amitié[182], l'argent[183], un conflit personnel[184] ou la simple curiosité, tout est bon pour biaiser la loyauté des êtres humains.

[180] Op. cit. CNIL
[181] Rapp. de la CNIL du 20 janvier 2009 « Conclusions du contrôle du STIC »
[182] CA Aix en Provence, 30 juin 2009 ; JurisData N° 2009-014406

Le professeur de droit Mme Lepage, commentant une de ces affaires, rappelle la nécessité d'un contrôle strict des consultations des fichiers de police face à la définition officielle de leur finalité qui « désarme la vigilance » et « permet sans doute de porter plus facilement atteinte aux libertés et à la vie privée ».

Ce doute traversant l'esprit de vigilance de toute personne extérieure au système a été confirmé lors de plusieurs scandales dévoilant les dangers du fichage.

La phrase de Bernanos selon laquelle « Il faut beaucoup d'indisciplinés pour faire un peuple libre » rejoint parfaitement un premier exemple de dérive dénoncé dans un livre par Mr Philippe Pichon, policier de profession et « mis à la retraite d'office » pour avoir détourné des données du STIC afin d'en dénoncer l'illégalité. Assimilant le STIC à « un casier judiciaire parallèle qui défie les lois et les valeurs de notre démocratie »[185], ce citoyen averti a voulu frapper fort en divulguant les fiches STIC de Jean Philippe Smet et de Jamel Debbouze, par ailleurs réciproquement consultées 543 et 610 fois sans susciter de poursuites. Le but est assumé : dénoncer l'idéologie sécuritaire et le fichage de masse, ses erreurs et ses dérives indissociables. « Monstruosité policière », « ennemi public numéro un », « bombe à retardement liberticide à l'égard de tous les citoyens », les adjectifs ne manquent pas à l'ancien policier pour critiquer un fichier alimenté de suspicions ; pas plus que les témoignages et les exemples de détournement de la finalité des informations contenues dans le STIC. Le commissaire de police Martial Berne, délégué du syndicat des commissaires de la police nationale prévenait dès 2008[186] que « les cabinets d'intelligence économique pourraient constituer la principale source de revenus des fonctionnaires de police souhaitant commercialiser les informations figurant dans les fichiers policiers, si l'on en croit certains services spécialisés, notamment de renseignements ». L'affaire Monge, en attente du délibéré mais aux faits avérés et avoués, met ainsi à jour la corruption d'un commissaire ayant perçu entre 30 et 400 euros par fiche divulguée[187].

S'il faut un dernier exemple d'actualité, deux journalistes radiophoniques ont même réussi à obtenir les fiches STIC de deux chanteurs de rap connus, simplement par téléphone, en se

---

[183] Décision mise en délibéré avec aveu du Commissaire Moigne, http://www.lessor.org/prison-ferme-requise-contre-un-ancien-commissaire-de-police-pour-corruption/

[184] http://bugbrother.blog.lemonde.fr/2009/12/02/un-policier-condamne-pour-espionnage/

[185] « Une mémoire policière sale : le fichier STIC », Philippe Pichon et Frédéric Ocqueteau, J.C. Gawsewitch Editeur, 2010, page 16

[186] Revue professionnelle *La tribune du commissaire* n° 110 de décembre 2008

[187] Préc.

faisant passer pour un commandant[188] ! La sécurisation de l'accès aux données semble alors détruite au profit des intentions malveillantes.

B. Des fichiers d'identification aux dérives inavouables

Ces initiatives déloyales ne concernent pas seulement le STIC mais aussi les autres fichiers et notamment le FNAEG. Alors que le patrimoine génétique doit être strictement protégé si l'on ne veut dériver vers un état totalitaire digne de la science-fiction, les agents de la police nationale sont tentés, et sont récemment passé à l'action, de contourner les règles relatives à la consultation du FNAEG. Ces abus sont inavouables car ils font honte dans un Etat de droit égalitaire et doivent donc être en principe fermement proscrits, en réalité ils ne sont pas toujours reconnus comme tels.

Au stade de la simple tentation, une première dérive consiste à déterminer les caractères physiques ou l'origine ethno-géographique d'une personne à partir des résultats d'analyse de son ADN. Cette dérive n'est pas une fiction mais bien une réalité, qui plus est constatée par le Garde des Sceaux lui-même dans une circulaire adressée aux procureurs généraux près les cours d'appel[189].
Le délégué aux fonctions du ministre dénonce cette proposition faite à des magistrats et officiers de police judiciaire d'identifier de telles informations à partir d'un ADN non identifié, recueilli sur la scène d'une infraction pénale. S'appuyant sur le principe de la liberté de la preuve, les défenseurs du procédé soutenaient que leur proposition concourait à la manifestation de la vérité mais la circulaire s'y oppose. De fait, cette méthode ne vise pas l'identification d'une personne comme le prévoit la loi pour le FNAEG mais l'examen des caractéristiques génétiques d'un individu, prohibé par l'article 16-10 hors la poursuite de finalités strictement médicales ou scientifiques. Cela relève même d'une infraction pénale prévue à l'article 226-25 du code pénal. Par conséquent, cette réaction à des intentions illicite rassure et tente de protéger le respect des prévisions légales. Le Conseil constitutionnel avait par ailleurs prévu cette dérive dans sa décision du 16 septembre 2010, suite à une question prioritaire de constitutionnalité relative au FNAEG, en précisant que « la disposition contestée

[188] « Obtenir la fiche Stic d'un rappeur, mode d'emploi », Nouvel Observateur, le 4 janvier 2013, par Elena Brunet
[189] Référence : CRIM-PJ N°08-28.H5 tome 4, dépêche du 29 juin 2011

n'autorise pas l'examen des caractéristiques génétiques des personnes […] mais seulement leur identification », ainsi est-elle conforme à la Constitution[190].
La vigilance doit donc l'emporter sur l'utilisation illimitée des nouvelles technologies au sein de la procédure pénale.

La seconde initiative contestable, mais quant à elle réalisée, correspond à une technique utilisée pour la première fois en 2011 dans l'affaire du viol et du meurtre de « la banquière de Péronne » agressée en 2002.
L'idée est alors d'une « familial search », recherche familiale de l'ADN, qui consiste non plus à rechercher l'identité de celui dont l'empreinte a été relevée sur le lieu de l'infraction mais à identifier la présence d'un de ses parents dans la base de données. Ce procédé est rendu possible grâce à une composante « familiale » de l'identité génétique correspondant à un allèle paternel et un allèle maternel que chaque enfant possède et qui correspond à la transmission d'une part de l'identité génétique de ses parents. A partir de ce parent, il ne reste plus qu'à comparer l'empreinte relevée et les ADN des membres de la famille, frères et sœurs compris. Ce procédé existait déjà en matière civile, en cas de catastrophes telles le crash du Concorde ou l'incendie sous le Mont Blanc, pour identifier avec certitude les victimes mais en aucun cas le FNAEG n'intervenait. Si le feu vert a été donné par la chancellerie au moment des faits, la loi ne prévoit pas cette hypothèse de sorte que le débat oppose ceux pour qui le vide juridique est signe de permission et ceux dénonçant un procédé illicite.
Le point certain tient au danger des conséquences d'une telle technique, élargissant considérablement le nombre des personnes fichées, de deux millions d'individus on passerait à cinq si l'on considère le taux moyen de natalité de deux enfants par couple[191]. La maîtrise des informations stockées dans le FNAEG semble en tout cas fragilisée.
Aux dires de la magistrate Evelyne Sire-Marin, le «familial search» est «un détournement total de procédure», elle rappelle que « La Cour européenne des droits de l'Homme a condamné la Grande-Bretagne pour ses fichiers trop larges. Je serai curieuse de savoir ce qu'elle dirait dans ce cas.»[192]

Colosse aux pieds d'argile, on peut effectivement douter de la licéité de cette consultation du FNAEG pour diverses raisons.

---

[190] Cons. Constit. QPC n° 2010-25 du 16 septembre 2010
[191] Pierre Alonso « L'ADN d'un Français sur six est fiché », Article de Slate du 20 février 2013
[192] Vice-présidente du TGI de Paris, auteur d'un chapitre sur le fichage dans l'ouvrage *Contre l'arbitraire du pouvoir*, Ed. La fabrique, 2012.

En premier lieu, l'hypothèse soutenue par Mme Sire-Martin d'une possible condamnation par la Cour européenne peut être renforcée si l'on songe à son exigence éminente de prévisibilité[193] dans les atteintes aux droits. En l'espèce, le procédé a été appliqué de manière tout à fait novatrice en 2011 et il n'y a toujours pas de loi ni de jurisprudence reconnaissant cette technique, l'argument pourrait peser dans la balance. Cependant la nuance doit être de mise car cette exigence s'applique aux peines, en vertu de l'article 7 de la Convention européenne des droits de l'homme, ce que n'est pas le fichage de l'ADN. Il reste que l'article 8 relatif à la vie privée exige que toute ingérence soit non seulement nécessaire et proportionnée mais avant tout prévue par la loi.

En outre, on peut s'interroger sur le respect du consentement, ici biaisé puisque l'on se contente du consentement d'un membre de la famille pour atteindre le patrimoine génétique d'une personne qui n'en est pas informée. Il convient de rappeler à ce titre que l'article 706-56 CPP en son alinéa 5 prévoit la possibilité d'un prélèvement sans l'accord de la personne sur réquisitions écrites du procureur de la République pour les cas de crime ou de délit puni de plus de dix ans d'emprisonnement. Le consentement présidant le cadre juridique du prélèvement ADN serait donc totalement bafoué pour les autres cas mais pas en l'espèce.

Enfin, la force du principe de légalité va à l'encontre de ce type de contournement s'appuyant sur un soit disant « vide juridique ». A l'instar de la citation de Lacordaire selon qui « C'est la liberté qui opprime, la loi qui affranchit », l'intervention d'une loi pour encadrer le FNAEG prouve la sensibilité du fichier et l'indispensable autorisation parlementaire pour empiéter sur le principe du respect de la vie privée et des libertés individuelles. Nous ne pouvons accepter l'argument d'un vide juridique alors que le principe tient à l'interdiction générale de violer les droits fondamentaux sans autorisation légale. Faut-il rappeler les conseils de Portalis selon qui « L'office de la loi est de fixer, par de grandes vues, les maximes générales du droit ; d'établir des principes féconds en conséquences, et non de descendre dans le détail des questions qui peuvent naître sur chaque matière. »[194]

[193] Arrêts CEDH Cantoni c/ France 15 novembre 1996 requête n°17862/91 et Soros c/ France du 6 octobre 2011, requête n°50425/06

[194] Discours préliminaire sur le projet de code civil, Jean-Etienne-Marie PORTALIS, présenté le 1er pluviôse an IX

Le législateur ne peut, ni ne doit, prévoir toutes les entraves et dérives possibles à des prescriptions légales. Ce serait là un travail dangereux car autorisant les autres dérives mais surtout impossible face à l'infinitude de l'imagination humaine.
Dès lors, l'atteinte aux droits fondamentaux, puisque c'est cela dont il s'agit lorsqu'on élargit le champ d'application du FNAEG, exige nécessairement une loi et non la simple autorisation de la Chancellerie.
Ces considérations nous amène à douter de la licéité de la recherche familiale de l'ADN.

SECTION 2 : LES ENSEIGNEMENTS DERIVES

L'analyse des dysfonctionnements au sein des fichiers de police a pour finalité de nourrir la réflexion quant à l'utilisation (§1) et quant à l'efficacité même des fichiers (§2).

§1 L'utilisation des fichiers de police

Les critiques relatives à la fiabilité des fichiers ne sauraient rester lettre morte et descriptives mais visent à en tirer les leçons quant à leur utilisation.
Deux dimensions sont à traiter relativement à l'usage des données policières, la première se limite au cadre traditionnel des fichiers isolément envisagés (A), la seconde tient à l'interconnexion des fichiers de police (B).

A. L'utilisation traditionnelle des fichiers de police

La subjectivité des données enregistrées, conjuguée au risque d'erreurs avéré, sont autant de vecteurs de nuance appelant une manipulation prudente des fichiers.
De ce fait, les fichiers consultés au cours de la procédure pénale ne doivent pas définitivement l'orienter à eux seuls, ce non seulement au stade de l'enquête menée par les policiers(1), mais aussi au stade de la décision et de l'individualisation de la peine par le magistrat (2).

1) Au stade de l'enquête

La nécessité de corroborer toute information issue d'un fichier par d'autres éléments de preuve matériels devrait faire l'unanimité. De nombreux textes et spécialistes rappellent autant que faire se peut l'inexistence d'une « reine des preuves », notamment attachée aux

fichiers et à l'empreinte digitale. En outre, le respect du contradictoire est un aspect de l'utilisation des fichiers qui semble quelque peu oublié.

Ainsi Mr Renaud Vedel, conseiller juridique du directeur général de la police nationale en 2007, et favorable au développement des fichiers de police permettant selon lui un « redressement rapide du taux d'élucidation des affaires constaté au cours des années récentes » (sans aucune source ni chiffre), insiste aussi sur le fait que l'activité de police « ne saurait se fier aveuglément et intégralement » aux fichiers. Les limites intrinsèques à la technique, liées à la dimension humaine et psychologique de la tenue des fichiers, empêchent leur triomphe[195]. Pourtant il ne faut pas être dupe et la consultation aujourd'hui systématique du STIC oriente nécessairement, même inconsciemment, le jugement d'un policier face à un individu suspecté d'avoir fait les « quatre cents coups ». La pratique le montre et le « flair » légendaire des agents de sécurité est en grande partie orienté, voire biaisé, par les données issues des fichiers de police. De surcroît, la politique du chiffre et les attentes des magistrats instructeurs de voir leurs affaires résolues sont des facteurs de stress et d'empressement ajoutant à la tentation déjà grande de recourir aux fichiers pour faciliter le travail.
A titre d'exemple, la garde à vue est par principe motivée par l'existence d' « une ou plusieurs raisons plausibles de soupçonner » que la personne a commis ou tenté de commettre un crime ou un délit puni d'emprisonnement. L'article 62-2 du CPP exige que ce soit l'ultime moyen de procéder efficacement à l'enquête, d'assurer la représentation de la personne ou de faire cesser le trouble. Dès lors, elle peut être fondée uniquement sur une information issue d'un fichier de police indiquant, lors d'un contrôle routier, que le véhicule est volé ou que la personne n'est plus titulaire d'un permis de conduire. Or, de nombreuses gardes à vue fondées sur de telles informations erronées ont entrainé la rétention des personnes pendant toute une nuit. Le rapport de la Commission nationale de déontologie de la sécurité dénonce ces effets pervers dus à des erreurs contenues dans les fichiers de police consultés lors des contrôles routiers et émet des réserves quant à la mise en place systématique d'une garde à vue sur ce seul fondement. Le travail des policiers ne serait pas davantage entravé si un passager est titulaire du permis et si la personne suspectée de conduire sans permis présente des garanties de représentation.

[195] Renaud Vedel « Le rôle des fichiers dans l'action opérationnelle des services de sécurité intérieure », AJP 2007 p. 64

Si la mesure est indispensable, la commission estime que les policiers peuvent mettre fin à la garde à vue dès que les éléments prouvant l'absence d'infractions sont réunis et qu'il n'est pas opportun de prolonger la mesure infondée jusqu'à la communication au parquet des suites de l'affaire[196].

Il en va de même par rapport aux empreintes ADN trouvées sur les lieux délictueux qui ne doivent pas orienter l'enquête des agents de police dans un seul sens et laisser de côté les autres pistes. Les failles dénoncées précédemment auraient toutes pu conduire à des erreurs judiciaires dramatiques en l'absence d'un alibi indiscutable si seul l'ADN avait été pris en compte. Les agents de la brigade criminelle, en charge des crimes les plus complexes sur le territoire de la capitale, sont les premiers à répéter ce caractère partiel de la découverte d'une empreinte ADN car, au-delà du risque d'erreur, rien ne dit qu'elle est celle de l'auteur du crime sans la présence d'éléments corroborant l'hypothèse[197].

Au même titre que l'aveu durant les années précédentes, la preuve ADN ne doit pas être considérée comme la « reine des preuves ». Elle est certes un outil efficace pour les policiers et les magistrats mais elle ne doit convaincre de rien envisagée de manière isolée.

L'autre préoccupation dans l'utilisation des fichiers de police au cours de la procédure d'enquête tient selon nous au respect du contradictoire. L'efficacité du travail des agents et la réticence à tout formalisme ralentissant l'enquête sont depuis toujours perçues comme des raisons supérieures permettant de faire obstacle au respect du contradictoire. L'absence de statut protecteur au stade de l'enquête de police est un problème d'autant plus important que les pouvoirs de police ont augmenté. Ce défaut transparaît à travers l'article 11 du CPP imposant le secret de l'enquête et de l'instruction. Pourtant, il est bien précisé « sans préjudice des droits de la défense » de sorte que l'on peut revendiquer davantage de contradictoire dans l'alimentation des fichiers de police. L'analyse de la Cour européenne des droits de l'homme vient au soutien de tels propos en exigeant que les modes de présentation des preuves revêtent un caractère équitable, corollaire de l'obligation de loyauté dans la réunion policière et judiciaire des preuves[198]. Il semble donc que la loyauté des fichiers de police et leur utilisation dans la procédure pénale plaident pour la reconduction des principes du contradictoire et des droits de la défense vis-à-vis des données enregistrées. Or, comme vu

[196] Rapport de la Commission nationale de déontologie de la sécurité de 2010, consultable à l'adresse http://www.cnds.fr/rapports/rapport_annuel_2010.pdf .
[197] Documentaire « Des enquêteurs d'élite : 6 mois au cœur de la Crim' », émission *Les docs de l'info* sur M6
[198] Arrêt du 6 décembre 1988 CEDH Barbara, Massegue et Jabardo c/ Espagne, série A n°146.

plus en amont, l'information des personnes concernées par l'alimentation des fichiers n'est aujourd'hui pas systématiquement assurée au nom des impératifs de sécurité. Seule l'ouverture d'une information judiciaire ou d'un procès permettront à la personne d'acquérir un statut plus protecteur, tardiveté notamment critiquée par Mr Rebut dans son cours de procédure pénale.
Il s'agit donc à présent de se pencher sur l'utilisation des fichiers de police par les magistrats.

2) Au stade de la condamnation

Pour les magistrats, cet impératif est particulièrement important et exigé à l'article 10 de loi « Informatique et Libertés » selon lequel aucune décision de justice impliquant l'appréciation du comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer des aspects de la personnalité. Dans cette perspective, il s'agit de s'intéresser non pas au juge d'instruction soumis aux mêmes préventions que les policiers mais au magistrat jugeant le fond de l'affaire et la culpabilité des personnes, plus particulièrement pour le prononcé de la peine. Soumises au principe d'individualisation au nom de l'article 8 de la Déclaration des Droits de l'Homme et du Citoyen, les peines doivent en effet être définies en fonction des circonstances de l'infraction et de la personnalité de son auteur, critères visés à l'article 132-24 du code pénal, dans le but de concilier à la fois la protection effective de la société, la sanction du coupable et les intérêts de la victime tout en favorisant la réinsertion et prévenant la récidive. Large programme donc, présidant la détermination de la nature et du quantum d'une peine. A ce stade, la loi de 1978 interdit au juge de se reporter aux fichiers « destinés à évaluer certains aspects de la personnalité ». Cette finalité est néanmoins floue car on peut penser qu'il ne s'agit pas de renoncer à la consultation du casier judiciaire relatant objectivement le passé d'un individu, mais en même temps l'histoire de chacun participe à la construction de notre personnalité, en partie au moins. En tout cas, il s'agit sûrement de prohiber le recours aux fichiers d'antécédents subjectifs comme le STIC ou aux fichiers de renseignements tel le PASP. Ce serait attenter à la présomption d'innocence que de se fier à des suspicions non confirmées, voire infirmées par un jugement définitif mais non rectifiées.

Par conséquent, l'absence de fiabilité absolue et l'existence d'utilisations déloyales des fichiers de police et de gendarmerie conduisent à nuancer leur importance dans la procédure

pénale qui, si elle peut s'appuyer sur, ne doit pas dépendre des données recueillies au risque de perdre toute efficacité.

B. L'interconnexion des fichiers de police

L'interconnexion a été définie par le Conseil d'Etat 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 »[199].Par suite, la CNIL a mis en évidence trois critères caractérisant l'interconnexion de fichiers : une mise en relation de différents fichiers, qui soient au moins au nombre de deux, et dans le cadre d'un processus automatisé[200]. Cette appréhension juridique de l'interconnexion n'est peut-être pas exhaustive car l'exigence du caractère automatique exclu le recoupement ponctuel d'informations par des agents mais elle rend compte de l'évolution des technologies et de l'aspect systématique du procédé de sorte que l'on s'en satisfera.

Le danger est donc apparent, celui de ne plus respecter le cloisonnement des fichiers, inhérent à la distinction de leur finalité. Malgré cette conséquence extensive et liberticide des connaissances policières, les demandes en faveur d'une interconnexion des fichiers sont récurrentes. La CNIL elle-même ne s'y montre pas toujours franchement hostile puisqu'elle admet un recoupement des données figurant dans les fichiers d'identification avec celles des fichiers d'antécédents du fait de la similitude de leur cadre, celui de l'enquête judiciaire. Le TAJ prévoirait ainsi une recherche automatique dans le FNAEG et le FAED lors de chaque inscription d'une personne dans le fichier, le but étant de fiabiliser les données[201].
En revanche, elle s'y oppose entre le fichier des personnes recherchées et les fichiers d'identification au nom d'une dissension des buts poursuivis.
Cette analyse peut nous laisser amer, tout d'abord parce que le décret instituant le TAJ reste silencieux sur la question, ensuite parce qu'il n'est pas certain que l'inverse soit empêché, c'est à dire que la simple vérification d'identité débouche sur la consultation des antécédents de la personne. Assurément, la finalité du fichier est étendue et la prudence de la CNIL face au même schéma pour les personnes recherchées montre qu'il est dangereux de tout justifier par la lutte contre l'usurpation d'identité.

[199] CE, 19 juillet 2010, Base élèves
[200] Fiche pratique « Comment déterminer la notion d'interconnexion ? », 5 avril 2011 sur le site www.cnil.fr
[201] Audition du 29 juin 2011 de M. Yann Padova, secrétaire général de la Commission nationale de l'informatique et des libertés par les parlementaires

Surtout, l'interconnexion des fichiers est sans doute l'avenir de la coopération européenne, voire mondiale, au nom de la lutte contre le terrorisme.
Le Traité de Prüm sur l'approfondissement de la coopération transfrontalière signé le 27 mai 2005 entre sept pays de l'Union dont la France, puis étendu à tous en 2008, a pour objectif d'approfondir la coopération policière et judiciaire des Etats membres. Ce traité instaure un principe de libre accès aux données relatives à l'ADN dans un but répressif, et aux empreintes digitales dans un but préventif et répressif[202]. En outre, il réaffirme le principe de « disponibilité des informations » figurant dans les normes européennes[203].
Il est donc évident qu'au sein de l'Union Européenne, la lutte contre la criminalité a conduit au passage du principe de protection des données à celui de libre disposition des données. S'il est toujours indiqué que la consultation est soumise au droit national de l'Etat membre, il reste que ce dernier est tenu par le principe de coopération et que la consultation se fait par voie automatique. La frontière entre une coopération renforcée et une interconnexion des fichiers n'est donc pas officiellement franchie mais dans la pratique le résultat est le même.
Or, le plus gros défaut du système est l'absence de sanction en cas de violation des traités et de consultation injustifiée. Ici, le vide juridique ouvre la voie aux dérives les plus dangereuses pour la vie privée.

Enfin, il est un fichier très intéressant du point de vue de l'interconnexion, de son avenir et de ses dangers, le fichier des Passagers Aériens (FPA). Entendons-nous bien, ce fichier est alimenté par les données dont disposent les agences de transport privées mais il peut servir d'exemple car sa finalité est doublement policière : il vise à lutter contre l'immigration clandestine et le terrorisme, et il est mis en relation avec des fichiers de police répertoriant les personnes recherchées que sont le SIS de Schengen et le fichier des personnes recherchées français (FPR). Au départ expérimenté dans le cadre de sept pays européens, la prorogation du fichier en 2011 vise à l'étendre à 31 pays, membres de l'Union ou non. La CNIL a dénoncé dans son avis relatif à la prorogation du fichier l'absence de sécurisation des données dans un certain nombre de compagnies, ainsi que le nombre élevé d'erreurs.
Pourtant, le gouvernement envisageait déjà l'élargissement des données pour atteindre le

[202] Décision du Conseil 2008/615/JAI du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière, articles 2 et 8
[203] Programme de la Haye adopté par le Conseil européen des 4 et 5 novembre 2004

volume de celles utilisées aux Etats Unis, qui correspondent aux données PNR, c'est-à-dire celles relatives aux réservations.

Ainsi, l'avenir du fichier est clairement dessiné par le Ministre de l'Intérieur en 2011 : « À terme, dans le cadre de l'Union européenne, la France devra se doter d'un outil plus ambitieux, capable de traiter les données PNR et de prendre en compte l'ensemble des pays extérieurs à l'espace Schengen »[204].

Cette perspective est en œuvre depuis l'Accord de Washington du 28 mai 2004 entre l'Union Européenne et les Etats-Unis, prévoyant la communication de trente neufs données personnelles contenues dans le fichier passager des systèmes de réservation des transporteurs aériens (le fameux PNR, Passenger Name Record). Or, le point crucial tient aux concessions faites par l'Union aux Etats Unis dans l'accord, celle-ci ayant accepté en 2004 que l'accès aux données obéisse aux exigences de la loi des Etats-Unis, de sorte que les coordonnées bancaires ou l'adresse électronique obtenues dans le PNR seront autant de données transmises. Cela revient à autoriser l'accès à toutes les données personnelles[205] ! L'accord de Washington a été annulé par la Cour Européenne de justice au vu de ses failles mais un nouveau texte a été immédiatement mis en place et approuvé par le Parlement européen le 19 avril 2012[206].

La lecture du texte est plus qu'inquiétante ; il est seulement précisé que sont communiquées les informations contenues dans le dossier passager de sorte qu'elles s'étendent aux coordonnées, numéro de téléphone et adresse de messagerie, aux moyens de paiement, aux goûts alimentaires ou encore au comportement dans l'aéroport… Les présentations officielles[207] s'éloignent de manière grotesque de la réalité puisque, pour les données dites sensibles, soi-disant écartées du fichier, l'accord lui-même reconnaît en son article 6 qu'elles sont divulguées par les informations visées, tout en précisant qu'elles seront automatiquement masquées sauf circonstance exceptionnelle tenant à une grave mise en péril d'une personne. En outre, la durée de conservation est de 15 ans mais par suite les informations sont seulement rendues anonymes et non effacées. Dès lors, l'adoption de cet accord a fait l'objet d'un débat

[204] Question à l'Assemblée Nationale n°91193, Réponse publiée au JO le : 07/06/2011 page : 6077

[205] Droit de l'administration électronique, article « Interopérabilité internationale, interconnexion des fichiers et protection des libertés : interrogation sur le devenir des données transférées dans le cadre de la lutte contre le terrorisme », Jean-Jacques Lavenue

[206] Résolution législative du Parlement européen du 19 avril 2012 sur le projet de décision du Conseil relative à la conclusion de l'accord entre les États-Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers et leur transfert au ministère américain de la sécurité intérieure 17433/2011 – C7-0511/2011 – 2011/0382(NLE)

[207] http://www.vie-publique.fr/actualite/alaune/donnees-personnelles-passagers-aeriens-accord-entre-etats-unis-europe.html

houleux et nombreux sont ceux qui dénoncent ce transfert d'informations portant atteinte aux droits fondamentaux et aux règles européennes[208].

Par conséquent, la coopération renforcée des Etats autour de la lutte contre le terrorisme est un facteur de dangers imminents pour la protection des données et pour le respect de la vie privée. Au nom de l'efficacité de la prévention et de l'enquête pénale, des données révélatrices de notre vie privée peuvent être diffusées avec la seule garantie d'une utilisation fidèle au principe de nécessité et de finalité. Toutefois, l'interconnexion des données met en évidence le problème de la perte de tout contrôle sur les données une fois transférées dans un état étranger, la loyauté de leur utilisation dans une procédure pénale est difficilement garantie. Nombreux sont les spécialistes mettant en garde dans le prolongement de l'analyse de Goethe selon qui « C'est du volume de données dont elle dispose que notre époque tire le sentiment immérité de sa supériorité alors que le véritable critère porte sur le degré auquel l'homme sait pétrir et maîtriser les informations dont il dispose »[209]. La perte de maîtrise des données transmises dans le cadre du droit pénal pourrait conduire à une utilisation à des fins commerciales ou industrielles des informations dans le futur. Certains poussent même le vice jusqu'à prévenir un possible détournement des données par les Etats-Unis à des fins de chantage et de contrôle des personnes dans un pays tiers en temps de guerre[210].

[208] Débats sur l'accord et opposition de nombreux parlementaires français et étrangers http://www.europarl.europa.eu/sides/getDoc.do?type=CRE&reference=20120419&secondRef=ITEM-004&language=FR&ring=A7-2012-0099

[209] Cité sur le site du Ministère de la Défense, fiche n°40 du Centre d'enseignement militaire supéireur AIR, revue*Droit et institutions*, octobre 2009, http://www.cesa.air.defense.gouv.fr/IMG/pdf/QA40.pdf

[210] Analyse de la professeur de droit privé Mme Laure Marino, lors du colloque annuel de la Semaine juridique du 19 octobre 2012 présidé par Mme Agathe Lepage sur « Le secret à l'ère de la transparence »

§2 L'efficacité des fichiers

La faillibilité des fichiers, corroborée par une utilisation parfois déloyale, conduit finalement à interroger l'efficacité elle-même.

La nécessité des fichiers de police ne peut être critiquée de manière générale face à une criminalité elle-même de plus en plus organisée et en proie aux nouvelles technologies. Notre société étant sujette à une mobilité permanente des personnes et des biens, il est indispensable de pouvoir détenir des informations, les comparer, les sauvegarder, pour que l'enquête de police vienne au soutien d'une procédure pénale qui ne soit pas démunie. Cependant, l'opposition entre l'extension des fichiers de police et la préservation des libertés individuelles amène à prendre du recul face à une course effrénée aux données. *In medio stat virtus*, il ne faudrait pas y perdre plus que l'on n'y gagne. Tel est aussi le premier message du Président Obama aux américains après les attentats du 11 septembre, citant Benjamin Franklin : « Une société qui abandonne un peu de liberté pour obtenir un peu de sa sécurité, ne mérite ni l'une ni l'autre et les perdra tous les deux ».

Dès lors, l'efficacité des fichiers de police venant soutenir leur existence est un sujet sensible mais important. Effectivement, si le droit à la sécurité doit venir justifier le développement des fichiers, les citoyens sont en mesure d'attendre des résultats concrets. Mais évidemment, aucune statistique ne vient indiquer le taux d'élucidation d'affaires pour lesquelles un fichier aurait eu un rôle déterminant...

Sans tomber dans les excès défendus des deux côtés, il semble que les fichiers de police soient plus ou moins efficients au sein de la procédure pénale selon leurs répercussions et le type de criminalité envisagée.

On ne peut que rejoindre ici la critique du professeur Mr Brouillet qui, tout en reconnaissant l'utilité des fichiers de police dans le cadre de la délinquance sérielle ou sexuelle, pointe du doigt la grande différence existant entre les fichiers stigmatisant les personnes et ceux plus anodins.

Cette distinction n'est pas sans rappeler les analyses faites tout au long de l'exposé, plus ou moins critiques selon qu'un fichier contienne des informations objectives ou subjectives, constatées ou suspectées. La distinction faite plus en amont peut donc ici être reprise à travers le prisme de l'efficacité des fichiers entre ceux relevant d'une vocation judiciaire (A), des renseignements (B), du passé judiciaire (C) ou de l'identification (D).

A. Les fichiers à vocation judiciaire

Tout d'abord, il est une catégorie de fichiers de police techniquement neutres qui sont les fichiers à vocation judiciaire. Il s'agit du Fichier des Objets et des Véhicules Signalés (FOVeS), de l'Application de Gestion du Répertoire Informatisé des Propriétaires et Possesseurs d'armes (AGRIPPA), du fichier des Permis de Conduire ou le Fichier National des Interdictions de Stade (FNIS). L'efficacité du FOVes et du fichier relatif au permis de conduire est généralement admise, leurs données sont objectives et sans conséquences directes sur les personnes, elles facilitent le travail des agents. Quant à ceux plus circonscrits que sont AGRIPPA et le FNIS, s'ils concernent directement des personnes, ils restent objectivement alimentés suite à des mesures administratives ou judiciaires. Surtout, ils permettent de prévenir les agents quant à la dangerosité potentielle des individus.

B. Les fichiers de renseignements

Ensuite, les fichiers de renseignements, dont l'emblème est le fichier PASP (issu d'Edvirsp), sont une catégorie bien plus délicate. D'un côté, ficher des personnes en raison de leur seule activité « indiquant qu'elles peuvent porter atteinte à la sécurité publique » est totalement intrusif et attentatoire aux libertés individuelles. La sécurité serait alors l'excuse légitimant et justifiant la proportionnalité de l'atteinte. Pour Mr Brouillet, de tels fichiers sont inutiles et relèvent d'une pure violation des libertés. En effet, comment définir un comportement potentiellement dangereux ? Le simple fait d'être salafiste ne peut selon lui être un prétexte au fichage, non seulement illicite mais en outre inutile. La question s'élargit alors aux fichiers CRISTINA et GESTEREX classés secret-défense. D'un autre côté, le renseignement est perçu par beaucoup de spécialistes comme indispensable pour l'ordre public. Ce débat a été relancé avec l'affaire Mérah, certains mettant sur le dos des services de renseignements une faute inexcusable liée au défaut de surveillance du jeune homme. Ces arguments répondant à la clameur populaire et à la peur entretenue en ces temps de lutte contre la délinquance sont en réalité à analyser avec du recul. Il ne semble pas qu'en réalité les fichiers de renseignements servent le travail des policiers et la limitation de leur consultation le démontre. L'attentat de Boston vient ici prouver l'efficacité de l'action policière, même face à un acte terroriste, sans avoir recours à des fichiers de renseignement. Il peut dès lors sembler qu'ils relèvent davantage d'une surveillance généralisée, substitut homéopathique à la crainte générale entretenue. Sur ce point, les remarques d'un gendarme

confortent notre point de vue très dubitatif face à l'efficacité des fichiers de renseignement, sans parler de son extension aux mineurs de treize ans.

C. Les fichiers d'antécédents

Les fichiers d'antécédents judiciaires sont quant à eux à diviser en deux parts entre ceux enclins au subjectivisme et ceux offrant davantage d'objectivité.
Le TAJ, fusionnant le STIC et le JUDEX à l'oraison fin 2013, est le plus gros fichier de police relatif aux antécédents judiciaires. L'analyse concise de ce fichier opérée tout au long de la réflexion a mis en avant son important taux d'erreur (27% pour le STIC) et le nombre de dérives dont il fait l'objet. A son égard, de nombreux commentateurs restent partagés, voire y sont fortement hostiles. En réalité il faut nuancer nos propos selon les données enregistrées.

Premièrement, pour les données concernant les « personnes à l'encontre desquelles sont réunis des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer à la commission de l'infraction », des soupçons, d'un certain degré en principe, suffisent à alimenter le traitement. Sur ce point, outre le fait que les mises à jour ne soient pas souvent respectées et que les erreurs soient fréquentes, il peut apparaître bien peu utile de sauvegarder de telles données. Elles présentent un intérêt certain durant la procédure pénale suivant les faits, mais encore faut-il qu'il y en ait une. Si tel est le cas et qu'elle sont finalement contredites, il pourrait sembler plus opportun d'effacer les données. Par suite, pour les enquêtes relatives à d'autres faits, il semble que de telles données nominatives ne fassent qu'orienter le travail d'enquête des agents et biaiser le respect de la présomption d'innocence. Le casier judiciaire est un élément de travail bien plus objectif qui pourrait suffire au travail des agents.

Deuxièmement, pour les données « non nominatives qui concernent les faits objets de l'enquête, les lieux, dates de l'infraction et modes opératoires » ainsi que celles relatives à des objets, le fichier semble recouvrer toute son utilité. En effet, ces informations conjuguent une absence de tout soupçon pesant sur une personne identifiée et une utilité certaine dans le travail des services de police. De ce fait, les analystes qui n'osent critiquer le fichier STIC pour son premier aspect admettent pourtant que les fichiers d'antécédents « sont tout particulièrement utiles pour la lutte contre les délinquants d'habitude »[211]. Cette remarque

[211]Renaud Vedel « Le rôle des fichiers dans l'action opérationnelle des services de sécurité intérieure », AJP 2007

montre que le fichier TAJ présente surtout une efficacité grâce à ce type d'informations, bien objectives, et pour une criminalité ciblée, la délinquance sérielle. C'est dire si les deux critères mis en avant par Mr Brouillet sont révélateurs de la productivité des fichiers de police au sein de la procédure pénale.

Quant aux fichiers entièrement objectifs, pour ce qui est de la procédure pénale au stade de l'enquête, il s'agit principalement du fichier SALVAC et du FIJAIS. Le FIJAIS comporte l'identité et notamment l'adresse des individus reconnus coupables d'infractions graves, notamment à caractère sexuel. Le SALVAC (Système d'analyse et de liens de la violence associée au crime) est un logiciel opérant des rapprochements entre les modes opératoires des infractions sexuelles ou des homicides à caractère sériel. Des éléments relatifs au comportement verbal, physique et sexuel de l'auteur sont enregistrées, ou encore le lieu, les armes, les véhicules de l'agression ou le mode opératoire. Ces fichiers participent pleinement des enquêtes, au point que des chiffres officiels sont donnés et portent à 24 le nombre de séries qui se sont révélées exactes depuis 2003, 130 dossiers ayant été résolus grâce à ces recoupements. Les parlementaires parlent du SALVAC comme d'une « précieuse aide à l'enquête en matière de crimes et délits sexuels à caractère sériel »[212].

Pour en finir avec les fichiers d'antécédents, il convient de préciser qu'au stade du jugement et de la fixation de la peine, le casier judiciaire est sans aucun doute efficace pour les magistrats en ce qu'il permet d'évaluer la personnalité d'un individu. Cependant le droit à l'oubli doit toujours être mis en parallèle avec une « dangerosité » impossible à évaluer.

D. Les fichiers d'identification

Enfin, les fichiers d'identification remplissent un rôle important même si leur finalité est plus réduite. Outils d'une puissance imparfaite mais importante, le FNAEG et le FNAED sont aujourd'hui utilisés dans toute enquête pénale pour identifier les personnes ayant été présentes sur le lieu de l'infraction. S'ils ne doivent évidemment pas se substituer au travail d'enquête et à l'examen consciencieux de toutes les pistes possibles, ils restent indéniablement une aide à la procédure pénale. A ce titre, leur caractère objectif permet une investigation à charge comme à décharge comme le montrent les résultats de l'association « Innocence Project » aux Etats-Unis qui a sauvé plus de 250 personnes du couloir de la mort

[212] Rapp. AN 2009

suite à la révélation d'erreurs judiciaires par le biais de l'identité biologique. A leur égard ce n'est donc pas tant l'efficacité qui fait l'objet de critiques mais l'utilisation, devant rester prudente.

Les derniers fichiers participant de l'identification des personnes sont ceux relatifs aux personnes recherchées, le FPR et le SIS dans le cadre de Schengen. Ces fichiers sont aussi très utiles pour retrouver des personnes faisant notamment l'objet d'un mandat européen, de mandats d'arrêt ou de recherche pour l'exécution d'un jugement.

Quotidiennement utilisé par les agents de police, le FPR est consulté à chaque contrôle d'identité, arrestation, interpellation ou garde à vue de sorte que dix millions de requêtes sont effectuées tous les ans par les forces de police et de gendarmerie[213]. Cette utilisation du fichier ne pose pas de problème en ce qu'elle ne porte aucune conséquence pour la personne concernée et ne peut qu'informer les agents du comportement à avoir en cas de recherche effective.

Le long cheminement emprunté à travers l'étude des fichiers de police amène donc à dresser un constat en demi-teinte pour chaque thème abordé tenant à la légalisation, la légitimité et la loyauté des traitements informatisés de données personnelles. Leur utilisation au cours de la procédure pénale est d'autant plus délicate au stade de l'enquête que le flair des enquêteurs ne doit pas totalement être guidé par des informations dont il est raisonnable de se méfier. Pour conclure sur une note nuancée, il semble qu'une approche distinguant les fichiers porteurs uniquement de soupçons et ceux au contenu plus tangible pourrait être la clé de voûte de toute l'organisation des fichiers de police. Si des progrès sont encore à faire de manière générale pour la légalisation ou la fiabilité des fichiers, ce critère pourrait commander encore plus fortement l'existence même des fichiers de police, à défaut leur contenu tout autant que leur durée de conservation, leur champ d'application personnel comme leur utilisation.

[213] Audition par les parlementaires le 7 avril 2011 de Mr Brendel, chef du service central de documentation de la police nationale et du colonel Hubert pour la gendarmerie

Conclusion

Les citoyens étant trop peu avertis et les politiques trop peu aguerris, il semble que la logique des fichiers de police l'ait emporté et ce ne sont pas les évolutions technologiques et leur gain de certitude qui risquent de freiner la course aux données. L'espoir est cependant permis grâce à la Cour européenne des droits de l'homme qui sait parfois redonner un véritable sens aux droits fondamentaux et notamment à la vie privée. A ce titre, l'arrêt M. K. contre France du 18 avril 2013[214] vient à point soutenir nos propos en condamnant la France pour la conservation des empreintes digitales de « personnes soupçonnées d'avoir commis une infraction mais non condamnées », « atteinte disproportionnée au droit du requérant au respect de sa vie privée et [qui] ne peut passer pour nécessaire dans une société démocratique ».

Une telle conclusion illustre parfaitement la distinction souhaitée ci-dessus car les juges analysent les différentes garanties entourant le FAED, notamment le recours offert à la personne fichée et le délai de conservation. La Cour insiste lourdement sur la circonstance tenant au fait que le requérant, ayant bénéficié d'un classement sans suite, n'a pas été reconnu coupable de l'infraction à l'origine reprochée et, si elle évite de parler de soupçons, elle estime qu'il ne faut pas que le requérant ait « l'impression de ne pas être considéré comme innocent ». Critiquant la « prétendue garantie » de protection contre l'usurpation d'identité soutenue par le procureur ayant refusé l'effacement des empreintes, condamnant par avance le fichage de l'intégralité de la population comme « assurément excessif et non pertinent » et assimilant la durée de conservation de 25 ans à « une conservation indéfinie ou du moins une norme plutôt qu'un maximum », les juges dressent un bilan très sévère à l'égard du FAED. Il suffit de songer au FNAEG prévoyant une durée de conservation égale pour les simples suspects ou au futur TAJ variant entre cinq et quarante ans pour espérer un retentissement important de cette jurisprudence.

Le droit européen, tel qu'appliqué par la Cour des droits de l'homme, apparaît être la réelle autorité gardienne des droits fondamentaux sur laquelle on peut aujourd'hui compter, reste à voir si les juridictions internes feront écho à cette décision renouant avec la philosophie humaniste chère à notre droit pénal à l'aune de sa dernière codification.

[214] Arrêt CEDH 18 avril 2013 M. K. contre France, requête n°19522/09

ANNEXE : TABLEAU RECAPITULATIF DES FICHIERS DE POLICE

FICHIERS	TEXTE DE REFERENCE	ADMINISTRATION GESTIONNAIRE	FINALITE	TYPE DE DONNEES	MINEURS + 13 ans	MIS EN CAUSE	DELAI maximal
1° ***Les fichiers à vocation judiciaire***							
FPA Fichier des Passagers Aériens	Loi du 23 janvier 2006 (n°2006-64) transposant la Directive du 29 avril 2004	Direction centrale de la police aux frontières	-Améliorer le contrôle aux frontières -Lutter contre l'immigration clandestine -Lutter contre le terrorisme.	Classiques	oui	non	5ans ou 24h selon le but
CNI Carte Nationale d'Identité	Décr. du 22 octobre 1955 n°55-1397	Ministère de l'intérieur	-Limiter les risques de contrefaçon et d'usurpation d'identité -Contrôler les mouvements aux frontières	Classiques	oui	non	15 ans
FNPC Fichier National des Permis de Conduire	Arrêté du 20 décembre 1972, art. L 225-1s. c. route	Ministère de l'intérieur (DLPAJ)	-Enregistrer et gérer toutes les informations relatives aux permis de conduire	Classiques et mesures relatives au permis	non	non	aucun
FNT Fichier National Transfrontière	Arrêté du 29 août 1991	Direction centrale de la police aux frontières	-Contrôle aux frontières -Lutter contre l'immigration clandestine ; -Lutter contre le terrorisme	Classiques et relatives aux voyages	oui	non	3 ans
SDRF Fichier de Suivi des titres de circulation remis aux personnes Sans Domicile ni Résidence fixe	Arrêté du 22 mars 1994	Gendarmerie	Suivi des titres de circulations	Classiques, signalement, mention « sédentaire », photo	A partir de 16 ans	non	Jusqu' aux 80 ans de la personne max
MCI	Arrêté du 24	Direction	-Gestion des déclarations et	Classiques	oui	oui	aucun

Fichier des Mains Courantes Informatisées	février 1995	générale de la police nationale	plaintes -Statistiques				
FNFM Fichier National du Faux Monnayage	Règlement (CE) du 28 juin 2001 n°1338/2001 pour la protection de l'euro	Police & gendarmerie	Lutte contre le faux-monnayage : -Identifier les malfaiteurs récidivistes -Rapprocher les affaires	Classiques, signalement et signes particuliers	oui	oui	Aucun
Registre des fourrières et immobilisations	Projet d'acte-cadre en cours	Police nationale					
Fichier de suivi du contrôle judiciaire	Projet d'acte-cadre en cours	Préfecture de police					
Fichier de suivi des assignations à résidence	Projet d'acte-cadre en cours	Préfecture de police					
Fichier de suivi des permissions de sortir	Projet d'acte-cadre en cours	Préfecture de police					
Fichier des appels à témoins	Projet d'acte-cadre en cours	Préfecture de police					
FNIS Fichier National des Interdits de Stade	Arrêté du 28 août 2007	Direction générale de la police nationale	Lutter contre les violences lors des manifestations sportives	Classiques, club de supporter, photo	non	non	5 ans après la fin de la mesure
AGGRIPA Application de Gestion du	Arrêté du 15 novembre 2007	Ministère de l'intérieur (DLPAJ)	Enregistrement et suivi des autorisations administratives de port d'arme	Classiques Celles relatives à l'arme	oui	non	20 après la fin du

Répertoire Informatisé des Propriétaire et possesseurs d'Armes							port d'arme
FVV Fichier des Véhicules Volés	Arrêté du 15 mai 1996	Police & gendarmerie	Vérifier si un véhicule est signalé Indiquer la conduite à tenir	Classiques et signalement du véhicule	non	non	aucun
FOS Fichier des Objets Signalés	Aucun texte	Police & gendarmerie	Vérifier si un objet a été déclaré signalé ou volé, conduite à tenir	Classiques et signalement des objets	non	non	aucun
Les 2 fichiers doivent avoir fusionné pour donner le FOVeS (Fichier des Objets et Véhicules Signalés) avec les mêmes caractéristiques. 2° ***Les fichiers relatifs au passé judiciaire***							
STIC Système de Traitement des Infractions Constatées	Décr. du 5 juillet 2001 n°2001-583	Direction générale de la police nationale	-Faciliter la constatation des infractions à la loi pénale -Rassembler des preuves -Recherche les auteurs -Consultations administratives	Données sensibles si résultent de l'infraction ou se rapportent à des signes physiques objectifs et permanents, en tant qu'éléments de signalement	oui	oui	De 5 à 40 ans pour les majeurs De 5 à 20 ans pour les mineurs
JUDEX Système Judiciaire de Documentation et d'Exploitation	Décr. du 20 novembre 2006 n°2006-1411	Gendarmerie nationale	-Faciliter la constatation des infractions à la loi pénale -Rassembler des preuves -Recherche les auteurs	Pareil que le STIC	oui	oui	Pareil que le STIC

ANNEXE : TABLEAU RECAPITULATIF DES FICHIERS DE POLICE

Casier judiciaire			-Mémoriser les condamnations	Passé judiciaire	oui	non	40 ans
SALVAC Système d'Analyse des Liens de la Violence Associée aux Crimes	Loi du 12 décembre 2005 n°2005-1549	Fichier commun à la police et la gendarmerie	Lutter contre la délinquance sérielle par le rapprochement d'informations entre procédures	Données classiques et sensibles	oui	oui	40 ans
3° ***Les fichiers d'identification***							
FNAEG Fichier National Automatisé des Empreintes Génétiques	Loi du 17 juin 1998 n°90-1131	DCPJ, fichier commun à la police & gendarmerie	-Lutte contre la récidive par l'identification des auteurs d'infractions -Identifications des personnes disparues et des cadavres inconnus	Données biométriques	oui	oui	40 ans pour les condam-nés / 25 pour mis en cause
FIJAIS Fichier Judiciaire des Auteurs d'Infractions Sexuelles	Loi du 9 mars 2004 n°2004-204	Ministère de la Justice	-Prévenir la récidive d'infractions sexuelles ou violentes -Faciliter l'identification des auteurs	Données classiques et passé judiciaire	oui	non	20 ou 30 ans selon l' infracti-on
FAED Fichier Automatisé des Empreintes Digitales	Décr. du 8 avril 1987 n°87-249	DCPJ, fichier commun à la police & gendarmerie	-Rechercher et identifier les auteurs d'infraction -Lutter contre l'usurpation d'identité	Données biométriques	oui	oui	25 ans
SIS Système d'Information Schengen	Accords de Schengen du 9 juin 1990, Décr. Du 6 mai 1995	Direction générale de la police nationale (DCPJ)	-Coopération internationale pour lutter contre la criminalité (mandats d'arrêts, personnes recherchées…)	Données classiques et biométriques	oui	oui	aucun
FPR	Décr. du 28 mai	Police &	-Rechercher les personnes suite à	Données	oui	oui	aucun

Fichiers des Personnes Recherchées	2010 n°2010-569	gendarmerie	une demande judiciaire, administrative ou militaire	classiques, photo et conduite à tenir			
4° Les fichiers de renseignement							
FRG Fichier des Renseignements Généraux	Décr. du 14 octobre 1991 n°91-1051	Direction générale de la police nationale	-Protéger la sûreté de l'Etat et la sécurité nationale	Données sensibles	oui	oui	aucun
CRISTINA Centralisation du Renseignement Intérieur pour la Sécurité du Territoire et les Intérêts Nationaux	Décr. du 27 juin 2008 non publié au JO	DCRI	-Protéger la sûreté de l'Etat et la sécurité nationale	Données sensibles,	oui	oui	aucun
GESTEREX Gestion du Terrorisme et des Extrémismes à potentialité violente	Aucun texte	Préfecture de police de Paris	-Lutter contre le terrorisme et les extrémismes à potentialité violente	Données sensibles	oui	oui	aucun
PASP Prévention des Atteintes à la Sécurité Publique	Décr. du 16 octobre 2009 n°2009-1249	Police nationale	-Surveiller les personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique	Données sensibles, photo, antécédents judiciaires	oui	oui	Aucun 3ans pour mineurs
FTPJ	Pas de texte,	Direction	-Collecter des informations sur	Données sensibles,	oui	oui	aucun

Fichier de Travail de la Police Judiciaire	déclaré à la CNIL en 1991	générale de la police nationale	l'environnement et les habitudes des délinquants spécialisés ; -Favoriser la coopération des services	tout renseignement recueilli lors de la surveillance			
FBS Fichier des Brigades Spécialisées	Pas de texte	Direction générale de la police nationale	-Collecter des informations sur l'environnement et les habitudes des délinquants spécialisés ; -Favoriser la coopération des services	Données sensibles, tout renseignement recueilli lors de la surveillance	oui	oui	aucun

BIBLIOGRAPHIE

I/ Ouvrages :

A) Morale, philosophie et sociologie

BERLIERE J.M. et FOURNIER P. *Fichés ? Photographie et identification 1850-1960,* Editions Perrin 2011

LA BOETIE, *Le discours de la servitude volontaire*

MATTELARD Armand, *La globalisation de la surveillance, aux origines de l'ordre sécuritaire,* Editions La Découverte, 2007

NOIRIEL Gérard, *L'identification. Genèse d'un travail d'Etat,* Ed. Paris, Belin, 2007.

PICHON Philippe et OCQUETEAU Frédéric, *Une mémoire policière sale : le fichier STIC,* JC Gawsewitch Editeur, 2010

SHMITT Carl, *La notion de politique*, Editions Champs classiques

B) Juridiques

BUISSON et GUINCHARD, *Procédure pénale*, Ed. Litec, 2010

DELMAS-MARTY Mireille, *Le flou du droit* PUF, 2004

MAYAUD Yves, *Droit pénal général* PUF, 2010

II/ Articles :

Chroniques :

BIANCHI Virginie « L'effacement des fichiers ou le nouveau mythe de Sisyphe », *AJP* 2007 p. 420

BLANCO Agnès « Le système français de lutte contre le terrorisme et la garantie de l'Etat de droit » in la Revue *Regards sur l'actualité*, mars 2009 p.45

BOTTINI F. « A quand une QPC sur le cadre législatif des fichiers de police ? » *SJA* du 2 mai 2011

CEYHAN Ayse, « Technologie et sécurité : une gouvernance libérale dans un contexte d'incertitudes », *Cultures & Conflits*, n°64 (2006), pp. 11-32

CEYHAN Ayse , « Enjeux d'identification et de surveillance à l'heure de la biométrie », *Cultures &Conflits*, n° 64 (2006) p. 33-47

CÔME Jacqmin, juge des enfants, « Les mineurs pris dans la folie du fichage » *Revue Justice* avril 2007

DENIS Vincent, « Comment le savoir vient aux policiers : l'exemple des techniques d'identification en France, des Lumières à la Restauration », in la *Revue d'histoire des sciences humaines*, n°19, Histoire des savoirs policiers en Europe, 2008

DUBOIS J.P., Président de la Ligue des Droits de l'Homme « Contre le fichier Edvirsp et le règne du soupçon », revue *Regards sur l'actualité*, mars 2009

FOREST « Politique et technique : des problématiques consubstantielles », in la revue *Expertises des systèmes d'information*, avril 2008.

GAUTRON Virginie « Usages & mésusages des fichiers de police : la sécurité contre la sûreté ? », *AJP* 2011 p. 266

GRUNDLER Tatiana, « Le droit au recours confronté au secret » *AJDA*, N°42, 14 décembre 2009

LAVENUE J.J., « Anormalité, surveillance et fichiers de police » in *Vidéo-surveillance et détection automatique des comportements anormaux.* Editions du Septentrion Juillet 2011 pp. 9-31.

LAVENUE Jean-Jacques « Interopérabilité internationale, interconnexion des fichiers et protection des libertés : interrogation sur le devenir des données transférées dans le cadre de la lutte contre le terrorisme », in *Droit de l'administration électronique*

MAROT Pierre-Yves, « Fonctions et mutations des fichiers de police » *AJP* 2007 p. 61

MARZOUKI Meryem « Fichiers : logique sécuritaire, politique du chiffre ou impératif gestionnaire> », Revue *Mouvements*, 2010 n°62, p. 85 à 98.

MOREL Charles « Droit des fichiers, droit des personnes » 2ème partie, *Gazette du Palais* du 13 janvier 2004

PIAZZA Pierre « L'Europe biométrique contre les libertés ? » in *Regards sur l'actualité*, mars 2009, n° 349

PIAZZA P. « L'extension des fichiers de sécurité publique » *Revue Hermès* n°53 d'avril 2009

PREUSS-LAUSSINOTTE Sylvia « Base de donnée personnelles et politiques de sécurité : une protection illusoire ? », Identifier et surveiller. Les technologies de sécurité, *Cultures et Conflits* n°64, 2006 p.83

REVIRON Patrice « L'ADN : la preuve parfaite ? », *AJP* novembre 2012

SOULLEZ Christophe « Les fichiers du type Edvirsp sont-ils attentatoires aux libertés » in *Regards sur l'actualité*, mars 2009

TÜRK A. « Cnil : autoportrait d'un président énervé », interview dans la revue *Expertises des systèmes d'information* d'octobre 2008

VEDEL Renaud « Le rôle des fichiers dans l'action opérationnelle des services de sécurité intérieure » *AJP* 2007 p. 64

Notes de jurisprudence :

DANET Jean « Le FNAEG au conseil constitutionnel : deux réserves, une confortation générale », Cons. Const. 16 septe 2010, *AJP* 2010 p. 545

GUERRIER Claudine « Les fichiers génétiques britannique et français à l'aune des droits de l'homme », revue *Lamy Droit de l'Immatériel,n°56, 2010 p.77-86*

LEPAGE Agathe, « Détournement de finalité de données à caractère personnel contenues dans le STIC », in *Communication Commerce électronique* n° 3, Mars 2010 : commentaire de l'arrêt de la Cour d'Appel d'Aix en Provence du 30 juin 2009.

Journaux :

« Police : Pourquoi le super-fichier TAJ inquiète », *Le Monde,* Article du 15 mai 2012

« Obtenir la fiche Stic d'un rappeur, mode d'emploi », *Nouvel Observateur*, le 4 janvier 2013, par Elena Brunet

III/ Travaux divers (rapports, discours, documentaires, films, colloques)

Rapport de 2004 de M. Pascal Lemoine, conseiller référendaire à la Cour de Cassation sur « La loyauté de la preuve » (à travers quelques arrêts récents de la chambre criminelle), Publication de la Cour

Rapport du groupe de travail sur le contrôle des fichiers de police et de gendarmerie présidé par Mr Bauer « Fichiers de police et de gendarmerie : comment améliorer leur fonctionnement ? » de 2007

Rapport du groupe de travail sur le contrôle des fichiers de police et de gendarmerie présidé par Mr Bauer « Mieux contrôler les fichiers de police pour protéger les libertés » de 2009

« Conclusions du contrôle du STIC », rapport de la Cnil remis au Premier ministre le 20 janvier 2009

Rapport d'information n°441 du Sénat, « Le respect de la vie privée à l'heure des mémoires numériques » du 27 mai 2009

Communiqué de l'AEDH« Une motion de rejet du Parlement européen pour dénoncer le déni de démocratie dans la mise en place du nouvel Office européen de police Europol », Bruxelles, le 2 décembre 2009

Rapport définitif du 25 novembre 2010 rendu par la CNIL sur le MENS

Rapport du groupe de travail sur l'amélioration des fichiers de police et de gendarmerie présidé par Mr Bauer « Fichiers de police et de gendarmerie en France : une nouvelle étape vers une transparence nécessaire » de 2011

Rapport d'information déposé à l'Assemblée Nationale le 21 décembre 2011 par la commission des lois constitutionnelles, de la législation et de l'administration générale de la république dirigée par Mme Delphine Batho et Mr Jacques Alain Bénisti

Rapport d'activités de la CNIL de 2011

Rapport du Président Dean Spielmann de la Cour européenne des droits de l'homme sur « La protection des données dans la jurisprudence de la Cour européenne des droits de l'homme » du lundi 28 janvier 2013

Rapport sur la valeur scientifique de l'utilisation des empreintes génétiques dans le domaine judiciaire, par Mr Christian Cabal, AN n° 3121 et au Sénat n°364

Travaux parlementaires de la loi du 14 mars 2003, Rapport n°508 de l'assemblée nationale, première lecture

IV/ Sites internet

www.assemblée-nationale.fr

www.senat.fr

www.cnil.fr

www.vie-publique.fr

TABLE DES MATIERES