

UNIVERSITE PARIS 1
PANTHEON-SORBONNE
FACULTE DE DROIT

MEMOIRE DE DEA DROIT PENAL ET POLITIQUE CRIMINELLE EN
EUROPE

Sous la direction
du Professeur Christine Lazerges

LES FICHIERS DE POLICE : AU CŒUR DE LA DERIVE SECURITAIRE

Présenté par :
Maud Kornman

École Doctorale de Droit Comparé

Année universitaire 2003-2004

Plan Général

PARTIE 1 : LES FICHIERS DE POLICE : DES OUTILS TOUJOURS PLUS PERFORMANTS AU SERVICE DE LA SECURITE 9

Chapitre 1 : Autonomie policière et caractéristiques des fichiers de police 10

Section 1 : Soustraction des caractéristiques des fichiers de police au pouvoir d'influence de la CNIL..... 11

§ 1 : La CNIL, une autorité influente sur les caractéristiques des fichiers de police 12

§ 2 : La CNIL, une simple autorité morale 15

Section 2 : Les caractéristiques des fichiers de police : efficacité au détriment des libertés22

§ 1 : Un encadrement des finalités insuffisant à circonscrire l'étendue les fichiers de police 23

§ 2 : Le principe de finalité insuffisant à circonscrire la mémoire et l'usage des fichiers de police 29

Chapitre 2 : Autonomie policière dans la collecte de l'information destinée à alimenter les fichiers de police..... 35

Section 1 : Élargissement des pouvoirs de police dans la collecte des données de signalisation..... 36

§ 1 : Encadrement du recours aux procédés de signalisation de nature à limiter les risques d'abus au stade de la recherche d'identité..... 36

§ 2 : Autonomie policière restreinte dans le cadre de la vérification d'imputabilité 39

Section 2 : Élargissement des pouvoirs de police dans la collecte du matériel biologique nécessaire à l'établissement de l'empreinte génétique..... 47

§1 : Accroissement des possibilités de prélèvement 48

§ 2 : La problématique du consentement au prélèvement : tension entre sécurité et respect de l'intégrité physique..... 52

PARTIE 2 : VERS DE NOUVEAUX ACTEURS DE LA REGULATION DES FICHIERS DE POLICE ? 62

Chapitre 1 : Une régulation citoyenne : ouverture des fichiers de police à la société civile 63

Section 1 : Les moyens de la régulation citoyenne : le droit d'accès aux fichiers de police 64

§ 1 : Le droit d'accès aux fichiers de police : entre transparence et secret 64

§ 2 : Consécration d'un droit d'accès indirect aménagé au détriment d'un droit d'accès direct..... 72

Section 2 : Les conditions d'une régulation citoyenne des fichiers de police par le droit d'accès..... 80

§ 1 : Limite au droit d'accès : sous utilisation et défaut d'information ou utilisation et information : le préalable nécessaire à une régulation citoyenne des fichiers de police.. 81

§ 2 : Les prolongements nécessaires du droit d'accès : un droit de rectification des données..... 84

Chapitre 2 : Vers une régulation judiciaire des fichiers de police ? 88

Section 1 : Les contraintes structurelles en matière de judiciarité des fichiers de police 88

§ 1 : Les contraintes constitutionnelles et les exigences de judiciarité 88

§ 2 : Les contraintes européennes et les exigences de judiciarité : incitation à la mise en place de garanties procédurales propres à prémunir contre les abus..... 94

Section 2 : Les fichiers de police et judiciarisation..... 97

§ 1 : Le rôle du Ministère public dans le contrôle des fichiers de police..... 97

§ 2 : Les limites du contrôle du Ministère public et ses relais 104

INTRODUCTION

La sécurité est devenue une préoccupation politique primordiale destinée à répondre à un sentiment d'insécurité exacerbé par les médias. En témoigne la consécration par le législateur du droit fondamental à la sécurité par la loi du 21 janvier 1995¹, redéfini par la loi du 15 novembre 2001² et réaffirmé par la loi du 18 mars 2003³ comme un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives.

C'est ce courant sécuritaire, plus soucieux d'améliorer l'efficacité de la politique criminelle que de la préservation des libertés individuelles qui a inspiré les récentes réformes législatives qui s'abattent comme une tornade sur la procédure pénale.

L'une des grandes orientations de ce courant sécuritaire est la tendance à accroître la place accordée à l'enquête de police en conférant aux forces de sécurité plus de pouvoirs et des outils toujours plus performants.

C'est ainsi, alors que la doctrine dénonce le glissement perceptible d'activité de la phase judiciaire au bénéfice de la phase policière, que l'accent est mis par le législateur sur l'information policière, sa collecte, sa centralisation, et surtout sa conservation⁴. En effet, la police ne peut assurer pleinement la mission de maintien de l'ordre public, de recherche et de poursuite des auteurs d'infraction qui lui est impartie que par une maîtrise de l'information. L'information et sa maîtrise apparaissent comme des conditions essentielles de l'accomplissement des missions de police. A cette fin, l'information va être collectée par la police et cette collecte va donner lieu à une conservation sous forme de fiches. Dès lors, l'existence de fichiers policiers apparaît comme inhérente à l'exercice même de la fonction de police.

¹ Loi n° 95-73 du 21 janvier 1995, Loi d'orientation et de programmation relative à la sécurité

² Loi n° 2001-1062 du 15 novembre 2001, Loi relative à la sécurité quotidienne

³ Loi n° 2003-339 du 18 mars 2003, Loi pour la sécurité intérieure

⁴ En ce sens, J. DANET, « Le droit pénal et la procédure pénale sous le paradigme de l'insécurité », *Archives de politique criminelle*, n° 24, 2003, p. 49

Le développement des technologies a permis de les associer à celui des instruments policiers de conservation de l'information. Parmi ces technologies figure en première ligne l'informatique qui permet de stocker des quantités infinies d'informations dans un espace réduit. Ainsi, l'informatique va être mise au service de l'information policière qui va faire l'objet de traitements automatisés. L'automatisation de l'information policière en permet une conservation quasi illimitée et une exploitation plus efficace. Mais les informations ainsi conservées sont le plus souvent nominatives, c'est à dire relatives à des personnes physiques dont elles peuvent directement ou indirectement permettre l'identification. Dès lors, si les fichiers informatisés de la police vont apparaître comme générateurs de davantage de sécurité, car nécessairement plus performants, ils recèlent des risques formidables pour les libertés individuelles.

De plus en plus nombreux, de plus en plus centralisés et de plus en plus généraux, les fichiers de police font craindre la transformation de la société libérale en un État policier qui utiliserait la technologie de l'information pour surveiller les citoyens au détriment des libertés individuelles.

Si la seule considération de la fonction policière conduirait à admettre la collecte et la conservation de l'information par la police sans aucune limitation, dans une société démocratique, les exigences fonctionnelles de la police sont limitées par les libertés individuelles⁵. Dès lors, il s'agit de placer le curseur à juste distance entre sécurité et libertés⁶. Toute la difficulté réside dans la nécessité de conjuguer efficacité de l'action policière et, par là même, des outils mis au service de cette action de nature à l'optimiser, et les libertés individuelles.

Si la nécessité et le principe même de la collecte et de la conservation de l'information sur support informatique par la police apparaissent difficilement contestables, il convient d'encadrer ces fichiers de telle sorte que ne soit pas institué un régime policier de surveillance généralisée.

⁵ En ce sens, E. PICARD, « La police et le secret des données d'ordre personnel en droit français », *Rev. Sc. Crim.*, avr-juin 1993, p. 276

⁶ CNIL, 19^{ème} Rapport d'activité 1998, p. 67

Il est apparu que cette conciliation ne pouvait être opérée qu'au terme d'un stricte encadrement des conditions de fonctionnement des fichiers de police et par le contrôle du respect de la mise en œuvre de ces règles. En d'autres termes, une stricte soumission au droit et une grande transparence s'avèrent nécessaires en la matière pour assurer une juste conciliation.

A cette fin, le législateur avait mis en place un système original de régulation des fichiers de police par la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés⁷.

La loi du 6 janvier 1978, née de la prise de conscience des risques que faisait peser un usage incontrôlé de l'informatique suite au scandale provoqué par la révélation dans la presse du projet gouvernemental, baptisé « SAFARI », d'étendre l'utilisation du Numéro d'Identification au Répertoire National d'Identification des Personnes Physiques⁸ afin de faciliter l'interconnexion des fichiers publics, n'était pas spécifique aux fichiers de police mais avait vocation à régir tous les traitements automatisés de données nominatives. C'est donc en tant que traitements automatisés de données nominatives que les fichiers de police y étaient soumis.

Le système mis en place par la loi du 6 janvier 1978 se révélait original à plusieurs titres et semblait être à même d'assurer un équilibre entre sécurité et libertés. Tout d'abord, la loi créait la première autorité administrative indépendante, la Commission nationale de l'informatique et des libertés (CNIL) à laquelle elle confiait le soin de veiller au respect des dispositions qu'elle prévoyait⁹. A ce titre, elle lui conférait un réel pouvoir d'influence sur les caractéristiques des fichiers de police en la dotant d'un pouvoir de contrôle *a priori* sur ces fichiers. Mais encore, de la tentative de conciliation entre sécurité, efficacité des fichiers et droits de la personne fichée, elle ménageait une timide, mais non pas moins innovante, ouverture des fichiers de police à la société civile.

⁷ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JO* du 7 janvier 1978

⁸ dit numéro de sécurité sociale

⁹ Art. 6 de la loi n° 78-17 du 6 janvier 1978

Mais les récentes interventions législatives, portées par un courant sécuritaire, semblent avoir remis en cause ce fragile équilibre mis en place par la loi du 6 janvier 1978, telle qu'interprétée par la doctrine exigeante de la CNIL.

Soucieux d'améliorer l'efficacité des forces de sécurité dans l'identification et la recherche des auteurs d'infraction¹⁰, le législateur a modifié le fragile équilibre par un renforcement de l'autonomie policière.

Cette modification est passée par une réforme d'ampleur de la loi du 6 janvier 1978 par une loi du 6 août 2004¹¹ transposant dans l'ordre interne une directive communautaire de 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.

Ainsi, le pouvoir exécutif se voit plus libre de déterminer les conditions de fonctionnement de ces fichiers par la remise en cause de l'effectivité du pouvoir de contrôle de la CNIL et la police voit une extension prodigieuse de ses pouvoirs d'alimentation des fichiers et de conservation des données, alors même que la transmission de ces données est largement autorisée.

Paradoxalement, un autre mouvement est perceptible. Un mouvement de plus grande ouverture à la société civile et de judiciarisation. Cependant, il reste à savoir si cette contrepartie est de nature à apporter de réelles garanties en permettant un contrôle exigeant des fichiers de police.

Pour retracer la lutte perpétuelle entre la sécurité et les libertés comme valeurs sous-jacentes à la politique criminelle suivie en matière de fichiers de police, il convient, dans un premier temps, d'examiner la portée du courant sécuritaire sur les conditions de fonctionnement des fichiers de police (Partie 1), pour, dans un deuxième temps, s'interroger

¹⁰ Exposé des motifs du projet de loi pour la sécurité intérieure, déposé au Sénat le 23 octobre 2002

¹¹ Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JO*, 7 Août 2004

sur l'effectivité des contreparties mises en place sur la régulation des fichiers de police (Partie 2).

Partie 1 : Les fichiers de police : des outils toujours plus performants au service de la sécurité

Guidé par l'objectif prioritaire de rétablir la sécurité¹² face à un sentiment d'insécurité, réelle ou supposée, le législateur a renforcé les pouvoirs policiers. Ce renforcement des pouvoirs policiers allait passer en premier lieu par celui de l'efficacité des outils destinés à améliorer l'efficacité de l'action policière, en première ligne desquels figurent les fichiers de police.

Deux grandes tendances sont alors perceptibles. Afin de laisser une plus grande latitude dans l'action policière, l'encadrement juridique des fichiers de police a été profondément remanié (chapitre 1) et la collecte de l'information, destinée à l'alimentation de ces fichiers, facilitée (chapitre 2).

Chapitre 1 : Autonomie policière et caractéristiques des fichiers de police

Un mouvement d'autonomisation de la police dans le traitement de l'information sous forme de traitements de données nominatives informatisés est perceptible. Il s'est traduit par deux mouvements distincts. Tout d'abord, le pouvoir de contrôle *a priori* dont jouissait la Commission nationale de l'informatique et des libertés (CNIL.), autorité administrative indépendante, instituée par le législateur en même temps qu'émergeait un corpus de règles destiné à protéger le citoyen face aux risques que le développement de l'informatique faisait courir sur le droit au respect de la vie privée, sur les caractéristiques des fichiers de police a été remis en cause (Section 1). Mais encore, le mouvement de réforme d'ampleur opéré par la loi du 18 mars 2003, pour la sécurité intérieure, a bouleversé l'encadrement juridique des conditions de fonctionnement de ces fichiers, dans le sens d'une plus grande performance de ces fichiers. C'est ainsi que ces fichiers sont devenus les principaux appuis d'une politique sécuritaire plus soucieuse de sécurité que de liberté (Section 2).

¹² Exposé des motifs du projet de loi pour la sécurité intérieure, déposé au Sénat le 23 octobre 2002

Section 1 : Soustraction des caractéristiques des fichiers de police au pouvoir d'influence de la CNIL

La loi de 1978 avait fait reposer l'équilibre entre libertés et sécurité en matière de fichiers de police sur le principe d'un contrôle en amont de la création de ces fichiers par une autorité administrative indépendante, la Commission nationale informatique et libertés (CNIL.). C'est ainsi, que préalablement à la constitution d'un fichier de police, la CNIL devait être saisie. Ce contrôle *a priori* des fichiers de souveraineté apparaissait comme l'une des garanties essentielles offertes par la loi¹³. Selon la valeur normative de l'acte constitutif, la CNIL. était dotée de pouvoirs plus ou moins étendus. La loi du 6 août 2004¹⁴ sur la protection des personnes physiques, à l'égard des traitements de données nominatives, n'a pas remis en cause le principe d'un contrôle préalable à la constitution des fichiers de police. Cependant, l'effectivité de ce contrôle a été remise en cause. En effet, l'efficacité d'une procédure consultative ne peut se mesurer qu'à l'aune de la latitude qu'elle laisse à l'autorité qui la consulte dans l'édition de l'acte¹⁵. L'effectivité de la procédure n'étant réelle que si l'organe consulté peut apparaître comme coauteur de l'acte¹⁶. Pour comprendre le recul opéré par la loi du 6 août 2004 en matière de sauvegarde des libertés, il convient d'examiner le pouvoir d'influence dont était doté la CNIL sous l'empire de la loi de 1978, avant sa révision par la loi de 2004 et de le confronter au droit positif.

¹³ V. J. FAUVET, « La commission nationale de l'informatique et des libertés vingt ans après ... », Mélanges Jacques Robert, Libertés, Monchrétien, 1998, p. 122

¹⁴ Loi n° 2004-801 du 6 août 2004

¹⁵ V. J. BEER-GABEL, « Le contrôle de l'administration par la commission nationale de l'informatique et des libertés », *Rev. Dr. Publ.*, 1980, p. 1055

¹⁶ V. J. BEER-GABEL, « Le contrôle de l'administration par la commission nationale de l'informatique et des libertés », *Rev. Dr. Publ.*, 1980, p. 1055

§ 1 : La CNIL, une autorité influente sur les caractéristiques des fichiers de police

La loi de 1978 avait opté, en matière de fichiers de police, pour une plus grande transparence et soumission au droit. C'est ainsi, qu'une obligation de consignation du fichier, destinée à assurer sa publicité, était mise en place auprès de la CNIL. Cette dernière étant dotée par la loi d'un pouvoir d'influence sur les caractéristiques du fichier de police.

Ainsi, lorsque la création du fichier de police avait lieu par voie réglementaire, la CNIL était dotée d'un pouvoir d'influence sur les caractéristiques du fichier dont l'étendue était fonction de la nature des données collectées. En effet, l'idée s'était imposée que la collecte de données d'une certaine nature et leur traitement s'averraient plus dangereux pour les libertés que d'autres. Mettant à bas les tentations de la raison d'État, la loi de 1978 soumettait les fichiers de police, relevant des fichiers dits de souveraineté, en grande partie au droit commun des fichiers publics et ne ménageait que quelques dispositions dérogatoires au droit commun.

Ainsi, selon la nature des données collectées, la CNIL était dotée soit d'un pouvoir d'influence, soit d'un réel pouvoir de codécision. En effet, la loi de 1978 mettait en place deux types de procédure : une procédure d'autorisation préalable (A) et une procédure d'avis conforme de la CNIL. (B).

A : Un pouvoir d'influence grâce au système d'autorisation préalable

La procédure d'autorisation préalable était mise en place par l'article 15 de la loi du 6 janvier 1978. Elle était la procédure de droit commun pour les fichiers du secteur public, les fichiers du secteur privé étant soumis à une simple procédure de déclaration préalable. Cette distinction entre fichiers du secteur public et fichiers du secteur privé reposait sur la méfiance plus grande à l'égard des fichiers du secteur public et sur la crainte de citoyens transparents à l'égard de l'administration grâce aux possibilités d'interconnexion des fichiers de l'administration, que les progrès de l'informatique permettaient de réaliser. Les fichiers de police étant mis en œuvre par le secteur public, ils relevaient, par principe, de ce régime d'autorisation préalable. C'est ainsi, que l'article 15 de la loi du 6 janvier 1978 disposait que les traitements automatisés d'information nominative opérés pour le compte du secteur public ne pouvaient être décidés par voie réglementaire, qu'après un avis motivé de la CNIL. La demande d'avis adressée par le gouvernement à la CNIL devait être accompagnée, en vertu de

l'article 19 de la loi du 6 janvier 1978, d'un certain nombre d'informations nécessaires à la CNIL pour opérer son contrôle des caractéristiques du fichier¹⁷. La CNIL avait développé plusieurs sortes d'avis. Il pouvait être implicitement ou explicitement favorable, assorti de réserves ou négatif. L'article 15 alinéa 2 de la loi du 6 janvier 1978 disposait que si l'avis de la CNIL était défavorable, il ne pouvait être passé outre que par un décret pris sur avis conforme du Conseil d'État. Cependant, cette procédure ne fut pas utilisée pendant les trente années d'application de la loi du 6 janvier 1978. L'avis de la CNIL fonctionnait en fait comme une sorte de veto. La procédure de dépassement de l'avis de la CNIL, par un avis conforme du Conseil d'État, paraissait trop lourde à mettre en œuvre et le gouvernement préférait le plus souvent négocier avec la CNIL¹⁸. Ainsi, si de fait la CNIL était dotée d'un pouvoir de codécision en matière de fichiers de police, elle disposait de ce pouvoir en droit lorsque les fichiers avaient vocation à collecter certaines données de nature particulière, qualifiées de sensibles.

B : Un pouvoir d'influence grâce à la procédure de codécision

L'article 31 de la loi du 6 janvier 1978, dans sa rédaction antérieure à la loi du 6 août 2004, posait le principe de l'interdiction de mise en mémoire ou de la conservation des données nominatives dites sensibles. Ces données étaient celles qui faisaient apparaître directement ou indirectement les origines raciales, les appartenances syndicales ou les mœurs des personnes. Mais il ménageait une exception à ce principe en cas de motifs d'intérêt public sur proposition ou avis conforme de la CNIL par décret en Conseil d'État. La CNIL était ici dotée d'un véritable pouvoir de codécision qui donnait lieu à une navette avec le Conseil d'État et le Gouvernement. Il y avait un réel partage du pouvoir réglementaire entre la CNIL et le pouvoir exécutif. La CNIL pouvait s'opposer et interdire la collecte de telles données au Gouvernement. Or, en matière de fichiers de police, les enquêteurs travaillent le plus souvent

¹⁷ L'art. 19 imposait la communication d'un dossier très complet lors de la demande d'avis mais son alinéa 3 avait ménagé pour les fichiers de sécurité publique des possibilités d'allègement quant aux informations à communiquer à la Commission. Le décret n° 79-1160 du 28.12.1979 avait prévu les mentions minimum que devaient comporter les demandes d'autorisation relatives à ces traitements.

¹⁸ Guy BRAIBANT, *Données personnelles et société de l'information*, Rapport au Premier ministre, Doc. Fr., 1998 : « *les gouvernements hésitent à faire en quelque sorte " appel " de la CNIL au Conseil d'Etat et à se trouver ainsi enfermés entre deux avis d'autorités qui dans les deux cas et de façon inhabituelle dans notre droit, le lient ; ils préfèrent continuer à négocier avec la CNIL pour aboutir à un compromis hypothétique* ».

sur la base du signalement et de l'état civil des personnes¹⁹. Cette disposition permettait donc une protection satisfaisante des droits et libertés des personnes à l'égard des fichiers de police, car elle avait vocation à s'appliquer le plus souvent en la matière et garantissait que le fichier de police ne serait mis en œuvre que sur avis favorable de la CNIL. Cette garantie s'est trouvée accrue du fait du contrôle opéré par la CNIL sur la notion de donnée sensible et celle d'intérêt public. Elle allait donner une interprétation extensive de la notion de donnée sensible et une interprétation restrictive de celle d'intérêt public²⁰. Par une interprétation extensive de la notion de donnée sensible, elle allait accroître les domaines dans lesquels elle était dotée d'un pouvoir de codécision. Cette extension prenant tout son sens en matière de fichiers de police. C'est ainsi, que la CNIL va considérer dans sa délibération du 8 novembre 1988, relative à la création du fichier des personnes recherchées²¹, que « l'information relative à la nationalité des personnes peut indirectement faire apparaître leur origine raciale ». Est-il utile de préciser que les fichiers de police mentionnent le plus souvent la nationalité des personnes ? Dès lors, la CNIL s'est octroyée un pouvoir de codécision en la matière et la possibilité de s'opposer à la mention de la nationalité des personnes dans les fichiers. Son interprétation extensive de la notion s'est poursuivie par la considération que « les informations relatives au signalement des personnes mises en cause, permettant aux enquêteurs de noter de l'aspect physique et les signes distinctifs tels que le port ostensible de signes religieux, est de nature à faire apparaître les origines raciales ou les convictions religieuses des personnes concernées. »

La CNIL a également exercé son contrôle sur la notion d'intérêt public. C'est ainsi, qu'elle pouvait circonscrire les dérogations accordées. Dans sa délibération du 19 décembre 2000 relative au Système de traitement des infractions constatées (STIC)²², la CNIL a limité la collecte des données sensibles « *aux seules informations qui résultent de la nature ou des circonstances de l'infraction ou à celles qui se rapportent à des signes physiques particuliers, objectifs et permanents en tant qu'élément de signalement des personnes dès lors que ces éléments de signalement sont nécessaires à la recherche et à l'identification des auteurs d'infraction.* ». En d'autres termes, les données sensibles ne pourront être collectées qu'à la

¹⁹ V., D.MARTIN, *Les fichiers de police*, coll. Que sais-je ?, PUF, 1999, p. 49

²⁰ V., J. FRAYSSINET, *Informatique, fichiers et libertés*, Litec, 1992, p. 62

²¹ Délibération n° 88-120 du 8 novembre 1988 portant sur la mise en œuvre conjointe par le Ministère de l'Intérieur et de la Défense du traitement automatisé d'informations nominatives relatif au fichier des personnes recherchées

²² Délibération n° 00.064 du 19 décembre 2000, Rapport annuel d'activité, 2001

condition qu'elles résultent de la nature de l'infraction (ex : crime raciste ou pédophile) ou qu'elles soient nécessaires à la recherche et à l'identification des auteurs.

§ 2 : La CNIL, une simple autorité morale

La loi du 6 août 2004 relative à la protection des personnes physiques à l'égard de traitements de données personnelles a maintenu le principe de la consultation de la CNIL préalablement à la constitution du fichier de police, mais a ôté toute effectivité à cette procédure. En effet, les avis de la CNIL ne sont pas juridiquement contraignants (A) et leur publicité n'est pas de nature à assurer un même niveau de garantie (B).

A : Un contrôle préalable des caractéristiques du fichier de police par la CNIL dénué de porté contraignante

Il convient, dans un premier temps, d'examiner la procédure de constitution des fichiers de police mise en place par la loi du 6 août 2004 modifiant la loi du 6 janvier 1978 (1) pour, dans un deuxième temps, s'interroger sur la conformité de cette procédure au regard des engagements internationaux souscrits par la France (2).

1. La procédure de constitution des fichiers de police, une procédure dérogatoire au droit commun des fichiers dangereux pour les libertés

Alors qu'un régime d'autorisation préalable par la CNIL est mis en place pour les traitements dangereux pour les libertés (a), les fichiers de police sont soustraits à ce régime (b).

a) Un régime d'autorisation par la CNIL pour les traitements dangereux pour les libertés

A la différence de la loi du 6 janvier 1978, qui opérait une distinction entre les fichiers selon que le responsable du traitement appartenait au secteur public ou au secteur privé, la loi du 6 août 2004 a retenu un critère horizontal, préconisé par la directive du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques, à l'égard

du traitement des données à caractère personnel et à la libre circulation des données²³. Ainsi, les traitements du secteur public et du secteur privé sont, par principe, soumis au même régime juridique. Le régime de droit commun est celui de la simple déclaration préalable des traitements et par exception, l'article 25 de la loi du 6 janvier 1978 modifiée met en place une procédure d'autorisation préalable pour les traitements qui présentent des dangers pour les libertés. En effet, la directive communautaire imposait une procédure d'autorisation pour les traitements les plus dangereux pour les libertés, mais elle laissait les États libres d'en fixer la liste²⁴. La directive n'a d'ailleurs pas vocation à s'appliquer aux fichiers de police, car elle ne s'applique qu'aux traitements qui relèvent de la compétence du droit communautaire, ce qui exclut les traitements d'informations par la police²⁵. C'est ainsi, que le législateur a opté pour la soumission des fichiers de police à un régime juridique dérogatoire par rapport à celui des fichiers considérés comme dangereux pour les libertés. En effet, alors que les fichiers considérés comme dangereux pour les libertés sont soumis à l'autorisation préalable de la CNIL, les fichiers de police ne le sont pas. Il s'agit d'un paradoxe. Alors même que les législateurs communautaire et interne considèrent comme une garantie nécessaire l'autorisation préalable des traitements dangereux pour les libertés, par une autorité indépendante spécialisée en la matière, cette garantie n'est pas accordée aux citoyens à l'égard des fichiers de police.

b) Les fichiers de police soustraits au régime d'autorisation par la CNIL

L'article 25 de la loi du 6 janvier 1978 modifiée, qui énumère les traitements considérés comme les plus dangereux soumis à un régime d'autorisation, prend soin d'exclure de son champ d'application les traitements dits de souveraineté, à savoir les traitements mis en œuvre pour le compte de l'État et qui intéressent la sûreté de l'État, la défense ou la sécurité publique ; les traitements qui ont pour objet la prévention, la recherche, la constatation ou la

²³ Directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données

²⁴ Art. 20 paragraphe 1 de la Directive 95/46/CE

²⁵ Art. 3 paragraphe 2 de la Directive 95/46/CE : « *La présente directive ne s'applique pas au traitement de données à caractère personnel mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telle que celles prévues aux titres V et VI du traité sur l'Union européenne, (...) et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'Etat et les activités de l'Etat relatives à des domaines du droit pénal.* »

poursuite des infractions pénales. Une distinction est donc opérée entre les traitements relatifs à la sûreté de l'État, la défense ou la sécurité publique et ceux qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales. Cette distinction apparaît comme une consécration de la doctrine de la CNIL qui, s'efforçant de soustraire les fichiers de police au régime dérogatoire mis en place par la loi de 1978 en la matière, considérait que des fichiers de police pouvaient ne pas intéresser la sécurité publique. En effet, cette distinction semble signifier que des fichiers qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ne relèvent pas nécessairement de ceux qui intéressent la sûreté de l'État, la défense ou la sécurité publique. Cependant, cette consécration va dans le sens, non pas d'un renforcement du niveau de garanties, mais bien dans celui d'un affaiblissement du niveau de garanties. En effet, ces fichiers sont soumis aux règles dérogatoires prévues par la loi alors que tel aurait pu ne pas être le cas sous l'empire de la loi antérieure.

Pour les traitements ne comportant pas de données dites sensibles, la loi du 6 janvier 1978, dans sa rédaction issue de la loi du 6 août 2004, prévoit en son article 26 qu'ils sont autorisés par arrêté ministériel pris après avis motivé et publié de la CNIL. Cette procédure d'avis consultatif remplace le système de l'autorisation préalable qui leur était applicable avant la modification de la loi du 6 janvier 1978 par la loi du 6 août 2004. Ainsi, l'examen préalable par la CNIL des caractéristiques du traitement n'est pas sanctionné juridiquement, puisque son avis est dénué de toute portée contraignante. Ce régime est pourtant classé par la loi dans une section intitulée « autorisation ». Il a été qualifié par un auteur²⁶, non sans ironie, « d'autorisation par soi-même ». En effet, la CNIL est consultée, mais l'autorisation n'émane pas de la Commission mais du responsable du fichier lui-même.

Un régime plus protecteur demeure pour les fichiers de souveraineté comportant des données sensibles en vertu du paragraphe 2 de l'article 26 de la loi informatique et libertés dans sa nouvelle rédaction. En effet, comme en l'état antérieur du droit, le principe de l'interdiction de la collecte des données sensibles a été maintenu et des exceptions ménagées. Ainsi, le paragraphe 3 de l'article 8 de la loi informatique et libertés prévoit une exception au profit des traitements justifiés par l'intérêt public. La liste de ces données diffère par ailleurs de celle établie sous l'empire de l'ancienne loi. En effet, l'article 8 de la loi informatique et libertés modifiée par la loi du 6 août 2004 interdit « *la collecte ou le traitement des données à*

²⁶ E. DROUARD, « Projet de loi de modification de la loi « informatique et libertés »... Ou comment s'en débarrasser ? », *Expertises*, octobre 2001, p. 342

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. ». Les données justifiant une protection accrue sont élargies, conformément aux dispositions de la directive. Les traitements de souveraineté comportant des données sensibles doivent désormais être autorisés par un décret en Conseil d'État, pris après avis motivé et publié de la CNIL. Cette procédure contraint certes le Gouvernement à solliciter l'avis de deux autorités : celui de la CNIL puis celui du Conseil d'État, mais ni l'un ni l'autre ne s'averre juridiquement contraignant. La CNIL a perdu le pouvoir qu'elle avait de s'opposer à la création de tels fichiers et le Gouvernement demeure libre de sa décision finale.

2. La procédure de constitution des fichiers de police, une procédure problématique au regard du droit international

Le nouveau dispositif mis en place prévoit que les fichiers seront constitués soit par le responsable du traitement lorsqu'il ne comporte pas de données sensibles, soit par le Gouvernement lorsqu'il comporte des données sensibles. Dans ces deux cas de figure, le pouvoir exécutif n'est pas soumis au respect d'un avis juridiquement contraignant. Un problème de conformité à nos engagements internationaux peut dès lors se poser.

a) Constitution des fichiers de police et droit communautaire

Tout d'abord, la directive impose pour les traitements, qui font courir des risques pour les libertés, un examen préalable par l'autorité de contrôle indépendante dont elle contraint à la mise en place à l'article 28. Ces dispositions ne sont certes pas applicables aux traitements dits de souveraineté, parmi lesquels figurent les fichiers de police, cependant l'esprit qui anime la directive incite à ce contrôle préalable²⁷. L'esprit qui anime la Charte européenne des droits de l'homme est identique. En effet, en son article 8 relatif à la protection des données personnelles, la Charte des droits fondamentaux consacre en son article 8 le principe du

²⁷ V., Recours dirigé contre la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés par plus de soixante députés adressé au Conseil constitutionnel le 20 juillet 2004

contrôle des données par une autorité indépendante. Elle ne précise certes pas si ce contrôle doit être opéré en amont ou en aval de la création du fichier de police.²⁸

b) Constitution des fichiers de police et le droit du Conseil de l'Europe

Mais c'est surtout la jurisprudence de la Cour européenne des droits de l'homme, rendue sur le terrain de l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CESDH), en matière de mesures de surveillance secrète qui semble inciter à un contrôle préalable par une autorité indépendante. En effet, de la jurisprudence rendue par la Cour en matière de mesures de surveillance secrète sur le terrain de l'article 8, il résulte une exigence de judiciarité, entendue au sens large, comme l'intervention d'une autorité indépendante. Dès lors, un fichier de police, qui aurait été créé par arrêté ministériel, peut poser des problèmes en terme de respect du droit à la vie privée tel qu'il est garanti par l'article 8 de la CESDH. En effet, sur le fondement du contrôle de la nécessité de la mesure dans une société démocratique à la poursuite d'un but légitime au regard de l'article 8 § 2, la Cour européenne incite les États à mettre en place des garanties procédurales propres à prémunir contre les abus. Ainsi, un contrôle en amont de la mesure de surveillance est exigé par la Cour européenne des droits de l'homme. Cette procédure de contrôle doit respecter les valeurs d'une société démocratique, parmi lesquelles figurent la prééminence du droit, qui implique un contrôle efficace de l'ingérence du pouvoir exécutif²⁹. La Cour marque sa préférence pour le contrôle d'une autorité judiciaire car il est de nature à apporter des garanties nécessaires d'indépendance et d'impartialité. Cependant, si la Cour marque sa préférence pour un contrôle de l'autorité judiciaire, elle admet que l'autorité de contrôle ne soit pas un juge si cette autorité répond à certaines exigences. La Cour exige que cette autorité soit indépendante par rapport à l'autorité de surveillance, qu'elle soit dotée de

²⁸ Art. 8 de la Charte des droits fondamentaux de l'union européenne :

« Protection des données :

Toute personne a droit à la protection des données à caractère personnelle la concernant.

Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »

²⁹ Cour EDH, KLASS c. RFA6 septembre 1978, requête n° 5029/71 : § 55 ; Cour EDH ROTARU c. Roumanie, 4 mai 2000, obs. O. De SCHUTTER, *RTDH*, 2001, pp. 145-183 : § 59

pouvoirs et d'attributions suffisants pour exercer un contrôle efficace et permanent, qu'elle doit avoir une composition équilibrée.³⁰

Alors que sous l'empire de la loi ancienne, l'avis de la CNIL liait le gouvernement, la loi nouvelle lui a ôté toute portée contraignante. La contrepartie mise en place par le législateur est la publication de l'avis de la CNIL en même temps que l'acte autorisant la création du traitement, mais cette contrepartie n'apparaît pas de nature à assurer de sérieuses garanties.

B : Le contrôle préalable des caractéristiques du fichier de police par la CNIL : entre publicité et secret

La publicité des avis de la CNIL en matière de fichiers de police n'apparaît pas de nature à assurer un niveau de protection suffisant des libertés (1) et cela d'autant plus qu'une possibilité de secret non conforme à nos engagements internationaux est prévue (2).

1. La publicité des avis de la CNIL en matière de fichiers de police

L'article 26 de la loi du 6 janvier 1978 prévoit qu'en matière de fichiers de police l'avis de la CNIL quant à la création d'un fichier de police doit être publié concomitamment à l'acte réglementaire créant le fichier. La publication de l'avis de la CNIL et de l'acte réglementaire constitutif s'imposant que le traitement comporte des données dites sensibles ou pas. Cette publication a été présentée comme la contrepartie à l'absence de portée contraignante des avis de la CNIL. Mais, il apparaît difficile de considérer que la publication d'un avis défavorable puisse comporter le même niveau de garanties qu'un avis obligatoire favorable pour la mise en œuvre du traitement³¹. De plus, il n'en résulte pas d'avantage de transparence ou de publicité en la matière, comme le laisse entendre les travaux parlementaires, car la publication des avis de la CNIL était d'ores et déjà assurée par l'intermédiaire de celle de son rapport

³⁰ Cour EDH, KLASS c. RFA : examen par la Cour du contrôle opéré par la commission G 10 en matière d'écoutes téléphoniques ; Cour EDH, LEANDER c. Suède, 26 mars 1987, requête n° 9248181, obs. L.-E. PETTITI et F. TEITGEN, *Chronique des droits de l'homme, Rev. Sc. Crim.*, juill-sept. 1987, pp. 749-750 : § 65

³¹ V., E. DROUARD, « Projet de loi de modification de la loi « informatique et libertés »... Ou comment s'en débarrasser ? », *Expertises*, octobre 2001, p. 342

annuel³². Pourtant, la CNIL, dans son avis sur le projet de loi modifiant la loi du 6 janvier 1978³³, a estimé que « *la publication de l'avis rendu par la CNIL paraît de nature à assurer le maintien d'un haut niveau de garantie* ». Mais elle émettait tout de suite une réserve. En effet, elle soulignait que si cette publication devait apparaître comme la contrepartie de la suppression du caractère contraignant de son avis, il était quelque peu contradictoire de prévoir la possibilité de déroger au principe de publication. Et cela d'autant plus que, comme sous l'empire du droit antérieur, le législateur a pris soin de ménager une exception au principe de la publication de l'acte réglementaire créant le traitement et à celui de l'avis de la CNIL. En effet, le paragraphe 3 de l'article 26 de la loi du 6 janvier 1978 modifiée dispose que les traitements dits de souveraineté « *peuvent être dispensés par décret en Conseil d'État, de la publication de l'acte réglementaire qui les autorise* », seule la publication du décret autorisant la dispense de publication de l'acte et le sens de l'avis émis par la CNIL étant alors assurée. Il s'agit de la reprise de l'ancien article 20 alinéa 3 de la loi du 6 janvier 1978. Toutefois, le domaine de l'exception au principe de publicité a été élargi. En effet, alors qu'antérieurement seuls pouvaient être dispensés de publication les traitements concernant la sûreté de l'État, la défense ou la sécurité publique, désormais peuvent également être dispensés d'une telle publication les traitements qui ont pour objet la prévention, la recherche ou la répression des infractions pénales.

2. Un secret critiquable au regard des exigences européennes

En ménageant une possibilité de dispense de publication de l'acte constitutif du traitement et en faisant la part belle au secret, le législateur met la France en porte à faux avec les exigences européennes développées par la Cour européenne des droits de l'homme et des libertés fondamentales sur le terrain de l'article 8 de la CESDH. En effet, il est de jurisprudence constante³⁴ que le traitement d'informations nominatives est une atteinte au droit au respect de

³² Art 23 de la loi du 6 janvier 1978 : « *La commission présente chaque année au Président de la République et au Parlement un rapport rendant compte de l'exécution de sa mission. Ce rapport est publié* »; Art. 11 de la loi : « *La commission présente chaque année au Président de la République, au Premier ministre et au Parlement un rapport public rendant compte de l'exécution de sa mission* »

³³ Avis de la CNIL sur le projet de loi modifiant la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés du 26 septembre 2000

³⁴ Alors que la Cour admettait l'applicabilité de l'article 8 de la CESDH dès lors qu'étaient mémorisées dans un fichier de police des données relatives à la vie privée d'un individu, elle a amorcé une évolution de jurisprudence

la vie privée, garanti par l'article 8 de la Convention³⁵. Par conséquent, s'impose en la matière le respect des exigences de l'article 8§2 de telle sorte que l'ingérence soit prévue par la loi et nécessaire dans une société démocratique à la poursuite d'un but légitime. Ainsi, s'impose l'exigence de légalité. Cette exigence de légalité impose que la loi prévoyant l'ingérence dans le droit au respect de la vie privée soit d'une certaine qualité³⁶. Cette exigence renvoie essentiellement à des conditions d'accessibilité de la loi et de prévisibilité propres à limiter le risque d'arbitraire. L'accessibilité de la loi suppose que l'individu puisse disposer de renseignements suffisants et publics sur les normes juridiques applicables. Assurément, l'exigence d'accessibilité de la loi ne saurait être remplie par la seule publication du décret dispensant l'acte constitutif du traitement de publication et le sens de l'avis de la CNIL. Si toutefois, une solution inverse devait être retenue, les exigences de prévisibilité de la loi ne seraient en aucun cas remplies, car elles supposent que la loi soit claire et précise pour indiquer à tous de manière suffisante en quelles circonstances et dans quelles conditions elle habilite la puissance publique à recourir à des mesures attentatoires à la vie privée³⁷.

Les caractéristiques des fichiers de police sont donc désormais soustraites de l'influence de la CNIL et il ne sera possible de s'en remettre qu'au résultat du rapport de force entre l'opinion publique et le pouvoir exécutif, qui pourrait naître de la publicité des avis de la CNIL pour s'assurer d'un encadrement juridique équilibré des fichiers de police.

Section 2 : Les caractéristiques des fichiers de police : efficacité au détriment des libertés

Le mouvement législatif récent est revenu sur l'encadrement juridique des fichiers de police afin d'assurer une plus grande efficacité à ces fichiers au détriment des libertés. Cet

la conduisant à considérer que le fait de recueillir de manière systématique des données et de les mémoriser alors même que ces données sont publiques peut soulever des questions liées à la vie privée : ROTARU c. Roumanie, 4 mai 2000 : §§ 43-44 ; AMANN c. Suisse, 16 février 2000 : §§ 65-67 ; PERRY c. RU, 17 juillet 2003 : § 38

³⁵ Pour plus de détails et sur l'évolution de la notion de vie privée dans la jurisprudence de la Cour européenne des droits de l'homme voir l'excellent article d'Olivier DE SCHUTTER, « Vie privée et protection de l'individu vis-à-vis des traitements de données à caractère personnel », *Rev. Trim. Dr. H.*, 2001, pp. - 183

³⁶ V. par exemple : Cour EDH, KLASS c. RFA, 6 septembre 1978 ; Cour EDH, DOERGA c. Pays-Bas, 27 avril 2004

³⁷ V. en matière de registre secret tenu par la police : Cour EDH, LEANDER c. Suède, 26 mars 1987 : § 51

encadrement s'est relâché à la faveur d'une plus grande latitude dans l'action policière, ce qui témoigne en la matière de la fragilité de l'équilibre entre sécurité et liberté. C'est sur le principe de finalité, considéré comme la colonne vertébrale³⁸ de la protection des données que repose l'encadrement des fichiers. Ce principe repose sur l'idée que les dangers pour les droits et libertés du citoyen ne résident pas tant dans l'existence même du fichier que dans la finalité de l'utilisation des données qu'il contient. Il impose que, dès l'origine les finalités du traitement soient précisées et ce sont ces finalités qui guideront les caractéristiques du traitement. Il est destiné à circonscrire l'étendue et l'usage du fichier. Ce principe a montré ses limites quant à l'encadrement des conditions de fonctionnement des fichiers de police.

§ 1 : Un encadrement des finalités insuffisant à circonscrire l'étendue les fichiers de police

Si les finalités attribuées aux fichiers de police ont été précisées (A), cet encadrement n'a pas été de nature à limiter le domaine des fichiers de police (B).

A : Les fichiers de police : des finalités insuffisamment circonscrites

Il convient, dans un premier temps, d'examiner la valeur juridique du principe de finalité (1), pour, dans un deuxième temps, examiner les finalités des fichiers de police (2).

1. Le principe de finalité

Le principe de finalité signifie que la collecte des données s'effectue dans un but déterminé et que leur utilisation ne peut se faire que conformément à ce but. Le respect du principe de finalité est imposé par les engagements internationaux souscrits par la France et par le droit national. Ainsi, en vertu de l'article 5 b) de la Convention 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel³⁹ impose que les données à caractère personnel faisant l'objet d'un traitement automatisé soient enregistrés pour des finalités déterminées et légitimes et ne soient pas

³⁸ J. FRAYSSINET, op. citée, p. 73

³⁹ Convention 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *JO* du 20 novembre 1985

utilisées de manière incompatible avec ces finalités. Cependant, l'article 9 de la Convention autorise les États contractants à déroger à cette obligation lorsqu'une telle dérogation serait prévue par la loi et constituerait une mesure nécessaire dans une société démocratique à la protection de l'État, à la sûreté publique, aux intérêts monétaires de l'État ou à la répression des infractions pénales. Aux conditions que la Convention énumère, les États seraient donc libres de ne pas respecter le principe de finalité en matière de fichiers de police. Le principe de finalité est également énoncé par la directive de 1995. Mais, la directive n'est pas applicable en matière de fichiers de souveraineté. Cependant, cette exigence résultait déjà implicitement des dispositions de la loi du 6 janvier 1978, dans sa rédaction antérieure à la loi du 6 août 2004⁴⁰. Désormais, elle figure explicitement à l'article 6 2° de la loi du 6 janvier 1978 modifiée qui dispose que les données « sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec les finalités initiales de la collecte des données ». Cette formulation est la transposition fidèle de la Directive du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données⁴¹. Le but de la collecte et du traitement doit être précisé dès la création du traitement en vertu de l'article 29 1° de la loi du 6 janvier 1978 modifiée. Le législateur n'a pas décidé d'y soustraire les fichiers de police, comme semblait l'y autoriser le droit international.

2. Les finalités des fichiers de police

Pour être de nature à sauvegarder les libertés et à garantir le citoyen contre une surveillance généralisée propre aux États totalitaires, les finalités des fichiers de police devraient être limitées. Or, si le principe de finalité est bien énoncé, une large marge d'appréciation demeure pour le responsable du traitement. La loi de 1978 ne circonscrit pas, en effet, les finalités poursuivies par les fichiers de police. La définition de la finalité doit être précise pour couvrir toutes les applications mais elle ne doit pas être trop large ni formulée de manière ambiguë ou équivoque. C'est au vu des finalités du fichier que la CNIL apprécie la cohérence des

⁴⁰ L'article 20 alinéa 1 de la loi du 6 janvier 1978 disposait que le règlement portant création d'un traitement automatisé de données personnelles devait en préciser obligatoirement la finalité. De plus, conformément à l'article 19 alinéa 1 de la loi du 6 janvier 1978, la finalité du traitement devait être spécifiée dans la demande d'avis adressée à la CNIL.

⁴¹ Voir art. 6 paragraphe 1 b) de la Directive du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

informations, la qualité des destinataires et la durée de conservation des données. Mais ce principe n'est pas de nature à constituer une garantie réelle⁴². La plupart du temps les finalités du fichier, si elles sont précisées au moment de sa constitution, le sont de manière large, afin de ne pas entraver l'action policière. Elles le sont le plus souvent par rapport aux missions du service qui utilise le traitement et il est rare qu'elles soient plus limitées. Initialement, le gouvernement avait tout de même choisi de ne pas préciser les finalités des fichiers de police judiciaire dans le projet de loi pour la sécurité intérieure, ce qui témoignait de sa volonté de laisser une large marge d'appréciation à l'autorité de police. Toutefois, à l'initiative du Sénat, les finalités des fichiers de police judiciaire ont été précisées. C'est ainsi que l'article 21 de la loi du 18 mars 2003 précise que les finalités des fichiers de police judiciaire sont de faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leur auteur. La finalité des fichiers de police est énoncée de manière large par rapport aux missions de la police judiciaire. En effet, l'énoncé de ces finalités est la reprise des termes de l'article 14 du Code de procédure pénale qui définit en des termes généraux les missions de la police judiciaire comme « *la constatation le rassemblement des preuves et la recherche des auteurs des infractions à la loi pénale tant qu'une information n'est pas ouverte* ». Cette précision des finalités des fichiers n'apparaît dès lors pas de nature à apporter une réelle garantie. De même, le fichier national des empreintes génétiques (FNAEG) a pour finalité de faciliter l'identification et la recherche des auteurs d'infractions mentionnées à l'article 706-55 CPP. Ses finalités sont plus circonscrites que les fichiers de police judiciaire puisqu'elles sont limitées à des infractions déterminées. Mais il est un réel outil policier alors qu'il n'était antérieurement qu'un instrument spécifique, lié à la lutte contre les infractions sexuelles⁴³. Mais encore, de par ses finalités⁴⁴, le fichier judiciaire national automatisé des auteurs d'infraction sexuelles s'apparente plus à un fichier de police qu'à un fichier judiciaire⁴⁵. La vocation de ce fichier est, en effet, de doter les services d'enquête d'un mécanisme destiné à éviter la récidive et à faciliter l'identification des auteurs d'infraction sexuelles limitativement énumérées par l'article 706-47 CPP.

⁴² D. MARTIN, op. citée, p. 74

⁴³ V., Y. PADOVA, « Droit des fichiers, droit des personnes ; Première partie : droit des fichiers », *Gaz. Pal.*, n° 9, 9 janvier 2004, p. 3 ; C. CHARBONNEAU, F.-J. PANSIER, « Présentation de la loi du 18 mars 2003 pour la sécurité intérieure : de la LSQ à la LSI », *Gaz. Pal.*, n° 85, 26 mars 2003, p. 7

⁴⁴ Art. 706-53-1 CPP issu de la loi du 9 mars 2004

⁴⁵ V. Clément SCHOULER, « Les nouveaux sables mouvants de la procédure pénale », *Justice*, n° 178, mai 2004, p. 15

B : Extension des fichiers de police : vers une surveillance généralisée ?

Les fichiers de police ont vu s'étendre de manière importante leur possibilité d'alimentation dans deux sens. Tout d'abord, le domaine des infractions justifiant une mention dans les fichiers de police a été élargi (1). Mais encore, les critères d'inscription dans ces fichiers ont été étendus (2).

1. Extension du domaine des infractions concernées par les fichiers de police

Les récentes interventions législatives ont amorcées un mouvement d'extension des possibilités de traitement de l'information par la police en accroissant le domaine des infractions concernées par ces fichiers. Afin de circonscrire l'étendue des fichiers et d'éviter une surveillance généralisée, l'idée semblait s'être imposée de limiter les infractions pouvant justifier la mémoire policière, mais progressivement, le domaine des infractions permettant une mention dans les fichiers de police s'est élargi.

L'extension du domaine des infractions pouvant justifier la collecte, le traitement et la conservation dans un fichier automatisé vont être examinés à travers celles du fichier FNAEG (a) et des fichiers de police judiciaire (b).

a) Extension du domaine des infractions pouvant justifier une mention dans le FNAEG

Le fichier national automatisé des empreintes génétiques est le fichier qui a connu la plus importante extension du domaine des infractions justifiant une signalisation dans ce fichier. Initialement créé par la loi du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs⁴⁶, il ne comportait en effet que les seules empreintes génétiques des personnes ayant commis certains crimes ou délits relatifs à des infractions sexuelles⁴⁷. Une partie de la doctrine⁴⁸ et des praticiens⁴⁹ considérait que le

⁴⁶ Loi n° 98-468, JO 18 juin 1998

⁴⁷ Ces crimes et délits étaient limitativement énumérés par l'article 706-47 CPP dans sa rédaction issue de la loi du 17 juin 1998 : meurtre ou assassinat d'un mineur précédé ou accompagné d'un viol, de tortures ou d'actes de barbarie ; viol de 222-23 ; exhibition sexuelle de 222-32 CP ; mise en péril des mineurs des articles 227-22 à 227-27 du CP.

⁴⁸ V. J. PRADEL, J.-L. SENON, « De la prévention et de la répression des infractions sexuelles. Commentaire de la loi n° 98-468 du 17 juin 1998 », *Rev. Pén. Dr. Pén.*, p. 236

fichier était conçu de manière trop étroite et appelait de ses vœux une augmentation du domaine des infractions justifiant le signalement dans le fichier. Le domaine du FNAEG a été élargi par les lois du 15 novembre 2001⁵⁰ et du 18 mars 2003 à des infractions relatives à des atteintes aux biens. Cette extension du domaine des infractions concernées correspond à une transformation des finalités du fichier. En effet, ce fichier était initialement destiné à « *faciliter l'identification et la recherche des auteurs d'infraction sexuelle* ». Cette limitation aux seules infractions sexuelles reposait sur l'idée erronée que la récidive serait particulièrement forte dans ce domaine. L'article 56 de la loi du 15 novembre 2001 relative à la sécurité quotidienne a amorcé le mouvement d'extension du fichier en ajoutant trois nouvelles catégories d'infractions. Cependant ce mouvement d'expansion du fichier est demeuré limité aux infractions de nature criminelle⁵¹. La loi du 18 mars 2003 a étendu le domaine des infractions pouvant justifier une inscription dans le FNAEG aux délits mais en déterminant un nombre restreint de délits. Le FNAEG est donc susceptible de comprendre les empreintes de personnes ayant commis ou suspectées d'avoir commis des infractions passibles de peines très variables et d'une gravité plus ou moins grande. En effet, il peut s'agir de celles de personnes condamnées pour crime contre l'humanité, punies de réclusion criminelle ou bien de celles de personnes ayant commis des violences volontaires simples au sens de l'article 222-13 du Code pénal, passibles de trois ans d'emprisonnement. L'augmentation du seul domaine des infractions devrait permettre une extension du fichier de 212.293 empreintes⁵². Le seuil de gravité des infractions justifiant une inscription dans le fichier est abaissé, mais le pouvoir d'appréciation de l'autorité de police chargée de l'inscription est tout de même limitée car la liste des infractions est précisée. Ce constat n'est pas identique quant au domaine des fichiers de police judiciaire.

⁴⁹ V. M. BONNIEU, Juge d'Instruction, in « Le juge d'instruction et les empreintes génétiques à l'aube du troisième millénaire », *Rev. Pén. Dr. Pén.*, 2000, p. 211, n° 20

⁵⁰ Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, *JO* 16 novembre 2001

⁵¹ Pouvaient justifier la présence dans le FNAEG la commission de crimes d'atteintes volontaires à la vie de la personne, de torture et actes de barbarie et de violences volontaires ; les crimes de vols, d'extorsions et de destructions, dégradations et détériorations dangereuses pour les personnes ; les crimes constituant des actes de terrorisme.

⁵² Y. PADOVA, op. citée, pp. 6-7

b) Extension du domaine des infractions pouvant justifier une mention dans les fichiers de police judiciaire

La loi du 18 mars 2003 pour la sécurité intérieure prévoit que les fichiers de police judiciaire peuvent traiter « *tout crime ou tout délit* » ainsi que « *les contraventions de cinquième classe sanctionnant un trouble à la sécurité ou à la tranquillité publique ou une atteinte aux personnes, aux biens ou à l'autorité de l'État* ». Le domaine des infractions justifiant une inscription dans le fichier est plus étendu que celui que prévoyait le droit en vigueur puisque le décret du 5 juillet 2001⁵³ relatif au STIC n'incluait, outre les crimes et délits, que six contraventions de la cinquième classe. La généralité des infractions pouvant donner lieu à fichage est à souligner. Il s'agit de la quasi totalité des infractions à l'exception des contraventions des quatre premières classes. De plus, il suffit que l'information concerne la commission d'une infraction, c'est à dire qu'elle soit en rapport avec l'infraction, ce qui permet de ficher des informations relatives à des faits connexes à l'infraction⁵⁴.

Il appartiendra au pouvoir réglementaire de fixer avec précision la liste des contraventions qui pourront justifier une inscription dans les fichiers de police judiciaire⁵⁵. Mais l'extension proposée devrait conduire à une augmentation substantielle des données figurant dans le fichier⁵⁶.

2. Des critères d'inscription élargis

Les personnes susceptibles de figurer dans les fichiers de police sont de trois types : les simples suspects, les personnes définitivement condamnées et les victimes. Mais en aucun cas les simples témoins ne peuvent faire l'objet d'une signalisation dans les fichiers de police.

L'alimentation des fichiers de police repose sur la notion de personne suspecte. Le législateur a adopté successivement des formulations voisines, mais non identiques telles que « *personnes contre laquelle il existe des indices graves et concordants de nature à motiver leur inculpation* », expression retenue pour l'alimentation du fichier automatisé des empreintes digitales⁵⁷, ou encore « *les personnes à l'encontre desquelles sont réunies (...) des*

⁵³ Décret n° 2001-583 du 5 juillet 2001

⁵⁴ V. C. CHARBONNEAU, F-J. PANSIER, « Présentation de la loi du 18 mars 2003 pour la sécurité intérieure : de la LSQ à la LSI », *Gaz. Pal.*, n° 85, 26 mars 2003, p. 5

⁵⁵ Art. 21 alinéa 3 de la loi du 18 mars 2003

⁵⁶ Y. PADOVA, *op. citée*, p. 11

⁵⁷ Art. 3 2° du décret n° 87-249 du 8 avril 1987

indices ou des éléments graves et concordants attestant leur participation à la commission d'une infraction », expression retenue pour l'alimentation du STIC⁵⁸. La loi du 18 mars 2003⁵⁹ retient comme critère « *la personne à l'encontre de laquelle il existe des indices graves ou concordants rendant vraisemblable la commission de l'infraction* ». Le lien ainsi établi entre l'infraction et la personne fichée apparaît assez lâche⁶⁰. Les critères d'inscription dans les fichiers de police judiciaire et le FNAEG sont unifiés. Ils témoignent d'un glissement vers une plus large place à l'appréciation subjective du policier. En effet, la notion de vraisemblance ne repose pas sur la base d'indices qui est un signe apparent et objectif mais sur celle de l'apparence de la réalité beaucoup plus subjective⁶¹. Cette notion laisse place à la subjectivité ce qui la rend moins contraignante pour l'action policière⁶². Aucune limitation d'âge n'est prévue. La minorité n'est pas un obstacle à l'inscription dans les fichiers de police judiciaire ou dans le FNAEG. Le Conseil constitutionnel, saisi de la constitutionnalité de ce dispositif, n'a pas considéré qu'il méconnaissait les principes constitutionnels applicables à la responsabilité pénale des mineurs⁶³. Il a toutefois enjoint au pouvoir réglementaire de déterminer une durée de conservation conciliant la nécessité d'identifier les auteurs d'infraction et celle de rechercher le relèvement éducatif et moral des mineurs délinquants⁶⁴. Les victimes d'infraction font l'objet d'un signalement dans les fichiers de police judiciaire mais en aucun cas elles ne peuvent faire l'objet d'un signalement dans le FNAEG.

§ 2 : Le principe de finalité insuffisant à circonscrire la mémoire et l'usage des fichiers de police

Il convient d'examiner, dans premier temps, les conditions de conservation des données récoltées par la police et mises en mémoire informatique (A) pour, dans un deuxième temps, mettre ces durées de conservation en parallèle avec l'ouverture des fichiers de police à un usage à des fins administratives (B). Les fichiers de police ne peuvent, dès lors, manquer

⁵⁸ Art. 2 du Décret n° 2001-583 du 5 juillet 2001

⁵⁹ Art. 21 paragraphe 2 et art. 29 de la loi du 18 mars 2003

⁶⁰ V. C. CHARBONNEAU, F.-J. PANSIER, op. citée, p. 6

⁶¹ V., M. Bertrand, M. VERPEAUX, in *Petites affiches*, 18 septembre 2003, n° 187, p. 9

⁶² V., M. SCHWENDENER, Signalement et identification, Rép. Pén. Dalloz, octobre 2003, n° 42, p. 8

⁶³ Décision n° 2003-467 DC du 13 mars 2003, Loi pour la sécurité intérieure, Considérant 37

⁶⁴ Décision n° 2003-467 DC du 13 mars 2003, Loi pour la sécurité intérieure, Considérant 38

d'apparaître comme des « casiers judiciaires parallèles » dont les conditions de fonctionnement n'apportent pas les mêmes garanties.

A : Un droit à l'oubli menacé : quelle limite à la mémoire policière ?

La problématique de la durée de conservation des données en matière pénale n'est pas nouvelle. Elle se rapproche de la notion de prescription de l'action publique. Pour justifier l'existence de cette prescription, la doctrine avance qu'elle repose sur l'idée qu'au bout d'un certain temps dans un intérêt de paix et de tranquillité sociale, il vaut mieux oublier l'infraction que d'en raviver le souvenir ou encore qu'en raison du risque de dépérissement des preuves, l'exercice d'une action trop longtemps après les faits accroît les risques d'erreur judiciaire. Mais l'informatisation du traitement de l'information par la police en permet une conservation illimitée et nécessite une procédure de destruction de l'information⁶⁵ sous peine de porter atteinte au droit à l'oubli, « *droit indispensable pour que le poids du passé n'écrase pas un homme en lui faisant perdre le sentiment de sa liberté et en l'empêchant d'amender sa personnalité* »⁶⁶. Ainsi, les données collectées par la police ne devront pas être conservées indéfiniment. Le principe est leur effacement, dès qu'elles ne sont plus pertinentes au regard de la finalité du traitement. L'article 6 de la loi du 6 janvier 1978 modifiée prévoit que les données ne doivent pas être conservées sous une forme permettant l'identification des personnes pendant une durée supérieure à celle nécessaire aux finalités du fichier. La loi du 6 janvier 1978, dans sa rédaction antérieure, imposait implicitement la fixation de la durée de conservation des informations lors de la création du traitement, puisqu'elle devait figurer dans la demande d'autorisation adressée à la CNIL. Cette disposition n'a pas été reprise par la loi du 6 août 2004, ce qui pourrait signifier que le responsable du traitement ne serait pas tenu de fixer la durée de conservation des données lors de la création du traitement et de la sollicitation de l'autorisation de la Commission. Il s'agit d'un « oubli » fâcheux du législateur. Cependant, les exigences européennes devraient conduire à fixer initialement cette durée de conservation. De plus, aucun critère n'est imposé par la loi du 6 janvier 1978 modifiée

⁶⁵ V. C. CHARBONNEAU, F-J. PANSIER, « Le système de traitement des infractions constatées ou les faits infractionnels à l'épreuve de la « memory STIC » », *Les petites affiches*, 24 août 2001, p. 3

⁶⁶ P. KAYSER, *La protection de la vie privée par le droit*, Protection du secret de la vie privée, Economica, 3^{ème} éd., 1995, 605 p.

permettant de fixer cette durée. Lorsque l'on recherche un critère pertinent de fixation de la durée de conservation des données dans les fichiers de police, des difficultés apparaissent. La seule considération de la fonction policière nous conduirait à admettre des durées de conservation illimitées. Cependant, la préservation du droit à l'oubli impose une durée limitée.

Un premier critère pertinent serait de distinguer une durée de conservation selon que la personne faisant l'objet d'un signalement est une personne suspectée ou une personne définitivement condamnée. Si seules les personnes condamnées définitivement sont fichées, le critère pertinent pourrait être celui de la durée de conservation des données du bulletin n° 1 du casier judiciaire. Cette durée est fixée par l'article 769 alinéa 3 CPP à 40 ans mais est également prévu le retrait dans les cas d'amnistie, de réhabilitation judiciaire et légale, les condamnations non avenues et les contraventions n'y figurent que trois ans. Mais encore, des règles spécifiques plus favorables de retrait des fiches du bulletin n° 1 sont prévues pour les mineurs délinquants par l'article 769-2 CPP. Ce qui est certain, c'est qu'en aucun cas, la durée de conservation des données des fichiers de police ne devrait être supérieure à celle prévue pour le casier judiciaire. Il faut donc vérifier si les fichiers de police permettent une durée de conservation plus longue que celle du casier judiciaire. Il apparaît qu'aucun fichier de police ne permet une durée de conservation supérieure à 40 ans. Ainsi, le FNAEG, avant son extension aux personnes mises en cause, permettait une conservation des données de 40 ans. La CNIL n'avait alors pas manqué de relever que seules les personnes condamnées y figuraient⁶⁷. Mais encore, le décret du 5 juillet 2001 relatif au STIC n'autorise que pour les infractions les plus graves dont la liste est annexées au décret une durée de conservation des données de 40 ans. Mais toute la difficulté réside dans le fait que ne sont pas seulement fichées les personnes ayant fait l'objet d'une condamnation devenue définitive. Le critère pertinent de durée de conservation étant alors, à mon sens, celui de la prescription de l'action publique⁶⁸. Cependant ce critère n'a pas été retenu pour le STIC. En effet, la durée de conservation des données collectées dans ce fichier semble plutôt s'aligner sur celui de la prescription de la peine⁶⁹. En effet, la durée de conservation de principe est de 20 ans mais

⁶⁷ CNIL, Rapport d'activité pour l'année 2000

⁶⁸ Articles 7 à 9 CPP : 10 ans pour les crimes, 3 ans pour les délits et 1 an pour les contraventions

⁶⁹ Articles 133-2 à 133-4 CP : 20 ans pour les crimes, 5 ans pour les délits et 3 ans pour les contraventions

peut être portée à 5 ans pour certaines infractions⁷⁰ et à titre exceptionnel atteindre celle de 40 ans. Les durées de conservation des données du FNAEG sont fonction de la qualité de personne mise en cause ou de la personne définitivement condamnée. En effet, la durée de conservation de principe est de 40 ans, mais les informations relatives aux simples suspects ne peuvent être conservées pour une durée de plus de 25 ans, à moins que la personne n'ait fait l'objet d'une décision de classement sans suite, de non lieu, de relaxe ou d'acquittement exclusivement fondée sur l'existence d'un trouble mental en application de 122-1 alinéa 1 CPP⁷¹. Le décret n'a pas prévu des durées de conservation variant en fonction de la gravité de l'infraction alors que la CNIL l'avait appelé de ses vœux⁷².

Mais encore, il devrait être impératif de moduler la durée de conservation en fonction de la gravité de l'infraction, de l'âge du condamné ou du suspect et de ses antécédents judiciaires.⁷³ C'est le système prévu par le décret relatif au STIC. En effet, la durée de conservation des données varie en fonction de l'âge de la personne et la gravité de l'infraction. Pour les majeurs, la durée de droit commun est de vingt ans mais peut atteindre quarante ans pour les délits les plus graves. En tout état de cause, la modulation de la durée de conservation par la prise en considération de la minorité de la personne apparaît comme une exigence constitutionnelle⁷⁴.

Les durées de conservation des données des fichiers de police sont donc extrêmement longues. Les arguments avancés en cette faveur sont liés à la finalité des fichiers de police qui doivent permettre de faciliter les enquêtes grâce aux recoupements. Cependant, il est certain que la durée de conservation des données doit varier selon que seules des personnes condamnées ou non y figurent et ne doit pas mettre en cause le droit à l'oubli, au respect de la

⁷⁰ délits du Code de la route, les infractions involontaires des articles 221-6 et 222-19 CP, infractions de détournement de gage ou d'objet des articles 314-5 et 314-6 CP, le vol simple de 311-3 CP, le délit d'entrave aux libertés constitutionnellement protégées de 431-1 CP, le délit de participation à un rassemblement interdit de 431-4 CP, le délit d'abandon de famille, et les contraventions visées à l'article 2 du décret du 5 juillet 2001

⁷¹ R 53-14 CPP dans sa rédaction issue du Décret n° 2004-470 du 25 mai 2004 art. 12, *JO* du 2 juin 2004

⁷² CNIL, 19^{ème} rapport d'activité 1998, p. 65 ; CNIL, 24^{ème} rapport d'activité 2003, p. 32 : « Elle a toutefois demandé (...) que la durée de conservation puisse (...) être modulée en fonction de la gravité et de la nature de l'infraction concernée »

⁷³ V. Y. PADOVA, « Droit des fichiers, droit des personnes ; Première partie : droit des fichiers », *Gaz. Pal.*, n° 9, 9 janvier 2004, p. 8 ; CNIL, 19^{ème} rapport d'activité 1998, p. 65 ; CNIL, 24^{ème} rapport d'activité 2003, p. 32 à propos du FNAEG

⁷⁴ Décision n° 2003-467 DC du 13 mars 2003, Loi pour la sécurité intérieure, Considérant 38

présomption d'innocence. Ces exigences apparaissant d'autant plus impératives que le législateur a prévu un accès large aux fichiers de police.

B : Un accès aux fichiers de police élargi à des fins d'enquête administrative

La CNIL s'est toujours fermement opposée à l'utilisation des fichiers de police judiciaire à des fins étrangères à l'orientation des enquêtes et à l'identification des auteurs d'infraction. Elle a toujours refusé leur utilisation à des fins d'enquête administrative dite de moralité. En effet, la CNIL a relevé le risque de faire jouer aux fichiers de police un rôle de « casier judiciaire parallèle » s'ils pouvaient être consultés à des fins d'enquête de moralité alors même qu'ils n'offrent pas les mêmes garanties sur la certitude de la culpabilité, la durée limitée des informations et l'effacement des données⁷⁵. Ces consultations sont des contournements des règles strictes, mises en place par le législateur pour la délivrance d'un bulletin numéro 2 du casier judiciaire aux administrations⁷⁶. De plus, les informations contenues dans ces fichiers ne bénéficient pas des mêmes garanties de fiabilité que celles contenues dans le casier judiciaire. Sont susceptibles d'y figurer des informations erronées, des informations relatives à de simples soupçons des policiers et qui ont donné lieu à fichage. Néanmoins, le législateur est intervenu afin de lever cet obstacle juridique posé par la CNIL à la suite des attentats du 11 septembre 2001. En effet, l'article 28 de la loi du 15.11.2001 autorise de manière temporaire la consultation des fichiers de police judiciaire dans le cadre d'enquêtes administratives de moralité. Mais cette possibilité avait été alors doublement limitée. Limitée d'une part quant aux emplois dont l'accès permettait la consultation des fichiers et d'autre part à « la stricte mesure exigée par la protection de la sécurité des personnes et la défense des intérêts fondamentaux de la nation ». Cette possibilité a été pérennisée et étendue dans une large mesure par la loi du 18 mars 2003. La loi du 18 mars 2003 a pérennisé ces dispositions et élargi leur domaine d'application. Les consultations des fichiers de police à des fins d'enquête administratives sont soit obligatoires, soit facultatives. Les instructions de demandes d'acquisition de nationalité française, de délivrance et de renouvellement des titres de séjours des étrangers, et de nomination et promotion à des ordres

⁷⁵ CNIL, Rapport d'activité pour l'année 1998 p. 63 ; 21^{ème} rapport d'activité pour l'année 2000 p. 77 ; 23^{ème} rapport d'activité pour l'année 2002 p. 25

⁷⁶ Art. 776 CPP pose les conditions de délivrance du bulletin n° 2 du casier judiciaire, moins expurgé que le bulletin n° 3, aux administrations qu'il énumère limitativement.

nationaux devront donner lieu à la consultation des fichiers de police. Ainsi, il est désormais inscrit dans la loi un usage des fichiers de police contraire à leur finalité initiale au mépris de nos engagements internationaux et de la position réaffirmée à plusieurs reprises de la CNIL. Eu égard à ce détournement de finalité, on aurait pu penser que le Conseil constitutionnel, saisi des dispositions de la loi du 18 mars 2003, n'aurait pas hésité à souligner l'importance du principe de finalité quant aux fichiers de police⁷⁷, comme il l'avait fait à plusieurs reprises dans des décisions antérieures relatives à des traitements informatisés d'informations⁷⁸. Pourtant, il s'est borné à relever qu' « aucune norme constitutionnelle ne s'oppose par principe à l'utilisation à des fins administratives de données recueillies dans le cadre d'activité de police judiciaire ». Cependant, il a assorti sa décision de deux réserves d'interprétation, au prix desquelles a été acquise la conformité de la consultation des fichiers de police judiciaire à des fins administratives à la Constitution. Il a, en effet, considéré que cette « utilisation méconnaîtrait les exigences résultant des articles 2, 4, 9 et 16 de la Déclaration de 1789 si, par son caractère excessif, elle portait atteinte aux droits ou aux intérêts légitimes des personnes concernées ». Ainsi, le Conseil constitutionnel vise l'article 2 de la loi du 6 janvier 1978 dans sa rédaction antérieure qui dispose que « Aucune décision administrative ou privée impliquant une appréciation d'un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé » et décline cette réserve sous deux aspects différents. C'est ainsi que, sur la consultation des fichiers de police judiciaire, lors des procédures d'acquisition de la nationalité française ou de renouvellement de titres de séjour, le Conseil constitutionnel va estimer que cette consultation ne saurait remettre en cause « l'acquisition de la nationalité française lorsque celle-ci est, en vertu de la loi, de plein droit, ni le renouvellement d'un titre de séjour lorsque celui-ci est, en vertu de la loi, de plein droit ou lorsqu'il est commandé par le respect du droit de chacun à mener une vie familiale normale⁷⁹ ». Si le Conseil a refusé de remettre en cause la possibilité de consultation des fichiers de police pour l'instruction de telles demandes, il la prive de tout effet lorsque la délivrance du titre de séjour ou l'acquisition de la nationalité française sont de plein droit ou subordonne les conclusions que l'administration pourrait en tirer au droit au respect de la vie

⁷⁷ V., J. BOYER, « Fichiers de police judiciaire et normes constitutionnelles : quel ordre juridictionnel ? », *Les petites affiches*, 22 mai 2003, pp. 4-19

⁷⁸ Décisions n°98-405 du 29.12.1998, n°99-416 du 23.07.1999, n°99-419 du 9.11.1999

⁷⁹ Décision n° 2003-467 DC du 13 mars 2003, Considérant 35

privée et familiale⁸⁰. La loi du 9 mars 2004 prolonge ce mouvement d'ouverture des fichiers aux enquêtes de police administrative. En effet, l'article 706-53-7 du CPP prévoit un accès direct au fichier des délinquants sexuels aux préfets et aux administrations étatiques dont la liste sera fixée ultérieurement par décret. Cette consultation ne pourra avoir lieu que pour une finalité déterminée par la loi qui est l'examen des demandes d'agrément concernant des activités ou professions impliquant un contact avec des mineurs. Elle ne pourra être opérée que sur le critère de l'identité de la personne concernée par la demande d'agrément. Le Conseil constitutionnel a considéré que, en raison des garanties mises en place par le législateur et en raison du motif assigné à ces consultations, ces dispositions ne portaient ni atteinte à la vie privée ni à la présomption d'innocence⁸¹.

Le mouvement de renforcement de l'autonomie policière quant aux caractéristiques des fichiers de police a trouvé un prolongement dans celui de la collecte de l'information par les forces de l'ordre des données destinées à alimenter les fichiers de police.

Chapitre 2 : Autonomie policière dans la collecte de l'information destinée à alimenter les fichiers de police

Les forces de l'ordre se sont vu conférer par les réformes successives de la procédure pénale d'importants pouvoirs en matière de collecte de l'information. La collecte de l'information destinée à alimenter les fichiers policiers n'a pas échappé à ce mouvement et y figurait même en première ligne. Ce mouvement d'accroissement des pouvoirs de police étant le plus perceptible quant à la collecte des données destinées à permettre l'identification des personnes, il sera examiné travers la collecte des données de signalisation (Section 1) et celle du recueil du matériel biologique destiné à l'établissement de l'empreinte génétique (Section 2).

⁸⁰ En ce sens, . J. BOYER, op. citée, p. 13

⁸¹ Décision n° 2004-492 du 2 mars 2004, Considérant 88

Section 1 : Élargissement des pouvoirs de police dans la collecte des données de signalisation

La police est amenée à prélever des empreintes digitales et des photographies, qui demeurent les procédés de signalisation les plus courants, dans le cadre de la recherche de l'identité d'une personne, afin d'établir son identité de manière certaine (§1), et dans le cadre de la recherche de l'auteur d'une infraction, afin d'établir l'innocence ou la culpabilité d'une personne déterminée par la comparaison de ses empreintes avec les traces laissées sur les lieux de la commission de l'infraction (§2).

§ 1 : Encadrement du recours aux procédés de signalisation de nature à limiter les risques d'abus au stade de la recherche d'identité

Le recours aux procédés de signalisation est rendu possible, dans le cadre des vérifications d'identité, par l'article 78-3 du Code de procédure pénale. Ce recours est strictement encadré. D'une part, il présente un caractère subsidiaire (A) et d'autre part, des garanties ont été mises en place (B)

A : Subsidiarité du recours aux procédés de signalisation

Il convient d'examiner, en premier lieu, la distinction entre la vérification d'identité sommaire et la vérification d'identité technique (1) pour, dans un deuxième temps, examiner les conditions du recours à la vérification technique (2).

1. Distinction entre vérification d'identité sommaire et technique

Lorsqu'une personne refuse ou se trouve dans l'impossibilité de justifier son identité, des vérifications d'identité peuvent être mises en œuvre en vertu de l'article 78-3 alinéa 1 du C.P.P. Ces vérifications d'identité ont pour objet de retrouver l'identité de la personne. La recherche de l'identité de l'individu peut alors être opérée de deux manières. Soit par une vérification sommaire qui est la recherche de l'identité par des moyens non techniques, soit par une vérification technique qui est la recherche de l'identité d'une personne par les moyens

de l'identité judiciaire⁸². Seule cette dernière vérification, dite technique, permet le relevé d'empreintes digitales et la prise de photographies.

2. Le recours à la vérification technique et alimentation des fichiers de police

Le recours à la vérification technique présente un caractère subsidiaire. En effet, elle ne peut être mise en œuvre qu'après l'échec d'une vérification sommaire. Elle ne peut être employée qu'en cas d'impérative nécessité à la double condition que l'intéressé ait une attitude négative, c'est à dire s'oppose à l'établissement de son identité et qu'elle soit l'unique moyen d'établir l'identité de la personne. Ainsi, cette mesure doit constituer l'unique moyen d'établir l'identité d'une personne et est par là même *l'ultima ratio* pour établir l'identité d'une personne⁸³. Ces dispositions ont pour conséquence l'interdiction d'une vérification technique systématique des individus. Les policiers et gendarmes ont perdu le pouvoir, exercé de manière systématique, d'établir une fiche d'identité judiciaire. L'alimentation des fichiers de police aurait dû s'en trouver ralentie et être principalement assurée par la signalisation pénitentiaire. Le recours à l'identité judiciaire ne devrait plus apparaître comme une commodité à la disposition des enquêteurs⁸⁴.

B : Accroissement encadré des pouvoirs policiers

Le domaine du recours aux procédés de signalisation dans le cadre de la vérification d'identité a été élargi (1), mais en contrepartie des garanties ont été mises en place (2).

1. Extension du domaine du recours aux procédés de signalisation

Alors que sous l'empire de la loi du 10 juin 1983, les prises d'empreinte digitales et de photographies ne pouvaient être pratiquées que dans le cadre d'une enquête pour crime ou délit flagrant ou d'une enquête préliminaire ou de l'exécution d'un ordre de recherche délivré

⁸² J. BUISSON, Contrôles et vérifications d'identité, Art. 78-1 à 78-6 : fasc. 20, sept. 2000, n° 30, p. 7

⁸³ J. PRADEL, « Les recherches d'identité et la poursuite des délits flagrants depuis la loi du 10 juin 1983 », Dalloz, 1984, Chron., XIII, p. 77

⁸⁴ J. BUISSON, Contrôles et vérifications d'identité, Art. 78-1 à 78-6 : fasc. 20, sept. 2000, n° 43, p. 9

par une autorité judiciaire, ce qui *a contrario* excluait le recours à de telles mesures en matière administrative, la loi du 3 septembre 1986 est venue étendre cette possibilité à toute opération de vérification d'identité.

L'extension des possibilités de recours aux procédés de signalisation s'est accompagnée de la mise en place de garanties.

2. Mise en place de garanties

Le recours aux procédés de signalisation ne peut avoir lieu sans autorisation de l'autorité judiciaire (a), ne peut être accompagné du recours à la coercition (b) et donne lieu à une alimentation limitée des fichiers de police (c).

a) Le contrôle de l'autorité judiciaire

Le recours aux procédés de l'identité judiciaire n'est possible que sur autorisation d'un magistrat, seul juge de l'opportunité de la mesure. En effet, la loi du 3 septembre 1986 est venue subordonner le recours aux procédés de signalisation à l'autorisation préalable d'un magistrat, alors que cette autorisation était exclue sous l'empire des lois précédentes en cas d'enquête ou d'ordre de recherche judiciaire. Ainsi, le policier doit au préalable obtenir l'autorisation du procureur de la République ou du Juge d'Instruction. Les forces de l'ordre apparaissent donc strictement subordonnées à l'autorité judiciaire et ne disposent, en théorie, d'aucune autonomie. Cette formalité doit être accomplie à peine de nullité.

b) L'interdiction du recours à la coercition

Le législateur a incriminé le refus de consentement d'une personne de se soumettre à une prise d'empreintes ou de photographies⁸⁵. Il a donc choisi pour s'assurer du consentement de la personne soumise à une vérification technique d'identité, de créer un délit spécial. En incriminant un tel comportement, il s'agit d'une reconnaissance implicite de la possibilité pour la personne concernée de se soustraire aux mesures de l'identité judiciaire. Le recours à la coercition pour l'exécution de ces mesures est donc strictement prohibé.

⁸⁵ Art. 78-5 C.P.P

c) Une alimentation encadrée des fichiers de police

La collecte des données de signalisation aboutit, selon les suites données à la vérification d'identité, à la conservation et à la mise en mémoire sur fichier. En effet, lorsque la vérification s'insère dans une procédure judiciaire, les données collectées pourront donner lieu à une mise en mémoire sur fichiers, mais lorsqu'elle n'est suivie d'aucune procédure judiciaire elle ne peut donner lieu à une mise en mémoire sur fichier⁸⁶.

Par conséquent, le cadre juridique du recours aux empreintes digitales et aux photographies est strict dans le cadre des vérifications d'identité et paraît de nature à préserver contre des abus éventuels. Toutefois, il convient d'établir la distinction entre le relevé d'empreintes digitales et la prise de photographies dans le cadre de la vérification technique, dont nous venons d'examiner le cadre juridique, de ce que M. BUISSON qualifie de « vérification d'imputabilité ». La vérification d'imputabilité diffère, en effet, de la vérification technique par sa finalité. Alors que la première a pour finalité d'établir avec certitude l'identité d'une personne déterminée, la seconde tend à établir la culpabilité ou à l'inverse l'innocence d'une personne, déterminée par la comparaison de ces empreintes digitales avec les traces trouvées sur les lieux de la commission d'une infraction ou par la présentation d'une photographie aux témoins ou aux victimes permettant d'identifier l'agresseur. La jurisprudence fait la distinction entre vérification d'identité et d'imputabilité concernant par exemple la prise de photographies et d'empreintes digitales concernant une personne gardée à vue dans le cadre d'une enquête préliminaire.⁸⁷

§ 2 : Autonomie policière restreinte dans le cadre de la vérification d'imputabilité

Dans le cadre de la vérification d'imputabilité, les forces de l'ordre disposent d'une autonomie qui s'accorde mal avec l'importance des pouvoirs qui leur sont octroyés. Il

⁸⁶ Art. 78-3 al. 8 C.P.P. : « Si elle n'est suivie à l'égard de la personne qui a été retenue d'aucune procédure d'enquête ou d'exécution adressée à l'autorité judiciaire, la vérification d'identité ne peut donner lieu à une mise en mémoire sur fichiers et le procès verbal ainsi que toutes les pièces se rapportant à la procédure sont détruits dans un délai de six mois sous le contrôle du procureur de la République. »

⁸⁷ TGI Marseille, 1^{ère} ch., 23.03.1995, Claude R. / le ministre de la Justice, obs. J. Frayssinet, *D.* 1996, Jur. p. 41 et s.; Expertises, juillet/août 1995, p. 280-282

convient, dans un premier temps, d'examiner l'incitation européenne à un mouvement de prééminence du droit en matière de collecte de données de signalisation (A) pour, dans un deuxième temps, s'interroger sur la conformité du droit national au droit européen (B).

La vérification d'imputation était pratiquée jusqu'à la loi du 18 mars 2003 sans reposer sur une base textuelle expresse autorisant les forces de l'ordre à y recourir. Selon, M. BUISSON, en l'absence de régime juridique spécifique, il convenait de rattacher cette vérification aux constatations effectuées sur les personnes⁸⁸ auxquelles elle devait emprunter son régime juridique. Elle pouvait donc, selon lui, être mise en œuvre de manière coercitive lorsqu'elle prenait place en flagrance ou sur commission rogatoire ou avec l'accord de l'intéressé au sein d'une enquête préliminaire. Cependant, ce point de vue ne semble pas s'accorder avec les exigences européennes.

A : Les exigences européennes de prééminence du droit

1. Les procédés de signalisation : des procédés attentatoires au droit au respect de la vie privée

Le recours à des procédés de signalisation, tels que la prise d'empreintes digitales et de photographies, apparaît attentatoire au droit au respect de la vie privée, tel qu'il est garanti par l'article 8 de la Convention européenne des droits de l'homme. Plusieurs affaires ont donné l'occasion à la Commission et à la Cour européenne des droits de l'homme de se prononcer sur la conformité de telles mesures à la Convention. C'est ainsi que les affaires *Mc Veigh*, *O'Neill et Evans*⁸⁹ ont donné à la Commission l'occasion de se prononcer sur la légalité de telles mesures. Dans cette affaire, des personnes soupçonnées de terrorisme avaient été régulièrement détenues et leurs empreintes digitales prises de force alors même que par la suite les intéressés n'aient pas été accusés ou reconnus coupables d'infraction pénale. La Commission a considéré que la prise d'empreintes digitales et de photographies des requérants, au cours de leur détention, était constitutive d'une ingérence dans leur droit au

⁸⁸ J. BUISSON, Contrôles et vérifications d'identité, Art. 78-1 à 78-6 : fasc. 20, J.-Cl. Procédure pénale, sept. 2000, n° 37, p. 8 ; J. BUISSON, Crimes et délits flagrants, Art. 53 à 73 : fasc. 20, J.-Cl. Procédure pénale, décembre 2003, n° 127, p. 25

⁸⁹ Commission EDH, 18 mars 1981, Requêtes n° 8022/77 ; 8025/77 et 8027/77

respect de la vie privée, mais que les conditions de l'article 8 § 2 étaient respectées⁹⁰. La Cour européenne s'est prononcée dans un sens identique par un arrêt Murray contre Royaume-Uni du 28 octobre 1994⁹¹. Dans cette affaire, la requérante, soupçonnée de participation à la collecte de fonds pour l'achat d'armes destinées à l'IRA, est arrêtée par l'armée et détenue dans un centre de détention militaire. Bien que refusant de se laisser photographier, elle est photographiée lors de son séjour sans son consentement et à son insu (§14). Elle soutenait que la prise de photographie avait été faite en violation de son droit au respect de la vie privée, tel que garanti par l'article 8 de la Convention. La Cour conclut à la non violation de l'article 8 de la CESDH. Cependant, elle reconnaît que ces mesures sont constitutives d'une ingérence dans l'exercice par les requérants de leur droit au respect de leur vie privée (§86). Si, dans cette affaire, la cour conclut à la non violation du droit au respect de la vie privée de la requérante, c'est parce que cette ingérence remplit les conditions énoncées au paragraphe 2 de l'article 8. En effet, la mesure était prévue par la loi et s'averrait nécessaire dans une société démocratique à la poursuite légitime du but de prévention des infractions (§ 89). Elle reconnaît en cette matière une large marge nationale d'appréciation, car était en cause la prévention des infractions terroristes (§91). Ces affaires sont à rapprocher d'un arrêt récent. En effet, dans une affaire Perry contre le Royaume Uni du 17 juillet 2003, une personne, soupçonnée d'avoir commis plusieurs infractions pénales, avait refusé de participer aux parades d'identification, et avait été filmée à son insu dans un commissariat de police afin de présenter un montage du film aux témoins pour voir s'ils le désignaient comme l'auteur des agressions. La Cour européenne des droits de l'homme retient, dans cette affaire, la violation de l'article 8 de la CESDH, alors que le gouvernement invoquait, pour sa défense, une affaire dans laquelle la Commission avait jugé légitime l'utilisation de photographies figurant dans des fichiers anthropométriques. La Cour prend alors soin de distinguer l'affaire invoquée avec le cas de l'espèce, en se basant sur le fait que les photographies avaient été volontairement remises aux autorités à l'occasion de demandes de passeport, alors qu'en l'espèce le film avait été réalisé sans l'accord de l'intéressé. *A contrario*, il est possible d'en déduire que la prise de photographies sans l'accord de l'intéressé serait constitutive d'une atteinte au droit au respect de la vie privée, tel que garanti par l'article 8 de la Convention.

⁹⁰ § 224 : « la Commission est convaincue que ces mesures (...) se justifiaient sur le terrain de l'article 8, paragraphe 2, comme étant prévue par la loi et nécessaire dans une société démocratique à la prévention des infractions pénales. »

⁹¹ V. F. MASSIAS, *Chronique internationale, Rev. Sc. Crim.*, 1995, avril/juin, p. 392-393

2. Incitation européenne à un mouvement de prééminence du droit

Si les opérations de signalisation, telle que la prise d'empreintes digitales et de photographies sont constitutives d'une ingérence au sens de l'article 8 § 1 CESDH, les conditions de l'article 8 § 2 doivent être respectées. Pour reprendre la terminologie de la Cour, cette ingérence doit être justifiée. La Cour européenne des droits l'homme ne considère cette ingérence comme justifiée qu'à la double condition que cette ingérence soit prévue par la loi et que des garanties contre les abus aient été mises en place. C'est ainsi que l'opération de signalisation doit avoir une base en droit interne. Mais surtout, cette base doit être dotée d'une certaine qualité pour la rendre compatible avec l'exigence de prééminence du droit. Ainsi, la loi doit être accessible et prévisible mais surtout claire et précise. Ces exigences renvoient à l'idée que le pouvoir d'appréciation de l'autorité responsable de la mesure doit être limité. Cette limitation passe par un rapport fort à la loi et au juge. Des exigences européennes résultent une incitation à la légalisation et à la judiciarisation. Il est ainsi permis d'affirmer que si les instances de Strasbourg font preuve de compréhension à l'égard du recours aux procédés de signalisation, même lorsqu'il est fait usage de la force par la police pour collecter l'information nécessaire à l'alimentation de ses fichiers en amont du procès pénal⁹², elles encadrent le recours à ces pratiques.

B : Confrontation du droit national aux exigences européennes

1. Le recours aux procédés de signalisation : absence de base légale avant la loi du 18 mars 2003

Avant la loi du 18 mars 2003, le pouvoir de prélever des empreintes digitales et de prendre des photographies ne reposait sur aucune base de nature à satisfaire aux exigences européennes (a), alors même que la jurisprudence interne admettait la légalité de ces procédés (b).

⁹² Alain BACCIGALUPO, « Polices d'investigations et droits de l'homme, Etude de droit comparé Canada/France », Dir. M. DELMAS-MARTY, Paris I, 1999, p. 426

a) La recherche d'une base légale formelle avant la loi du 18 mars 2003

Avant la loi du 18 mars 2003, plusieurs bases textuelles pouvaient être invoquées sans qu'aucune ne paraisse satisfaisante au regard du droit conventionnel européen. La circulaire du 13 août 1983, pour la mise en œuvre de la loi du 10 juin 1983 portant abrogation ou révision de certaines dispositions de la loi du 2 février 1981 et complétant certaines dispositions du code pénal et du Code de procédure pénale⁹³, était la seule disposition à prévoir expressément la possibilité pour les forces de l'ordre de recourir aux procédés de signalisation. En effet, elle précisait que « les nouvelles dispositions concernant les contrôles et vérification d'identité n'interdisaient pas qu'il soit procédé à des relevés anthropométriques ou à des prises de photographies lorsque ces opérations, réalisées pour les besoins d'une procédure judiciaire, tendent, non à l'identification d'une personne, mais à l'établissement de sa culpabilité ou à sa mise hors de cause. » Cependant, une circulaire n'est pas dotée d'une force juridique suffisamment contraignante pour satisfaire aux exigences européennes d'une base légale textuelle. Cette base légale ne pouvait, dès lors, apparaître suffisante au regard des exigences européennes⁹⁴. C'est ainsi que dans les affaires Khan⁹⁵, PG et JH⁹⁶, Armstrong⁹⁷ et Hewiston⁹⁸, la Cour européenne des droits de l'homme a refusé d'admettre que des pratiques attentatoires au droit au respect de la vie privée reposaient sur une base légale, alors qu'elles relevaient d'une directive émanant du Ministère de l'Intérieur. Cependant, la jurisprudence nationale admettait la légalité de ces procédés.

b) Appréciation de la légalité par la jurisprudence interne

La jurisprudence interne s'est penchée sur la légalité de la collecte d'empreintes digitales et de photographies par des policiers dans le cadre d'une enquête préliminaire sur une personne gardée à vue. Tout d'abord, dans un jugement en date de 1995, le Tribunal de grande instance

⁹³ Circulaire CRIM. 83- 23 S.D.L.C.-F. 1 / 13 août 1983

⁹⁴ En ce sens D. MARTIN, *Les fichiers de police en France : dérive sécuritaire ou sécurité à la dérive ?*, thèse de doctorat, Droit privé, Paris X, 1996, p. 401 ; Contra M. SCHWENDENER, *Signalement et identification*, Rép. Pén. Dalloz, octobre 2003, n° 27, p. 6

⁹⁵ Cour EDH, KHAN c. RU, 12 mai 2000, obs. O. BACHELET, *JDI*, 2001, p. 205

⁹⁶ Cour EDH, PG et JH c. RU, 25 septembre 2001, n° de requête : 44787/98

⁹⁷ Cour EDH, ARMSTRONG c. RU, 16 juillet 2002, n° de requête : 48521/99

⁹⁸ Cour EDH, HEWISTON c. RU, 27 mai 2003, n° de requête : 50015/99

de Marseille⁹⁹ reconnaissait la légalité du procédé en admettant qu'il pouvait avoir pour base légale les articles 14¹⁰⁰ et 427¹⁰¹ du C.P.P. combinés. Si ces deux articles combinés étaient de nature à fonder de tels pouvoirs de police en droit interne, cette base légale ne paraît pas pouvoir remplir les conditions de qualité de la loi imposées par la jurisprudence européenne. Mais encore, dans un arrêt rendu par la deuxième chambre civile en date du 18 décembre 2003¹⁰², la Cour de cassation a examiné la légalité au regard de l'article 9 du Code civil de la prise de photographies anthropométriques et du relevé d'empreintes digitales d'une personne gardée à vue. Le requérant, s'estimant victime d'une atteinte à la vie privée, saisit le président du tribunal de grande instance d'une requête tendant à ce que soit ordonnée la destruction de ces photographies et de ce relevé d'empreintes. La Cour de cassation va considérer que ces procédés ne sont pas attentatoires au droit au respect de la vie privée « *dès lors que ces photographies et relevés sont conservés par les services de police judiciaire et ne servent qu'à leurs enquêtes dans les conditions prévues par la loi* ». Dès lors, un parallèle ne peut manquer d'être fait avec la jurisprudence nationale et européenne rendue en matière d'écoutes téléphoniques, telles qu'elles étaient pratiquées antérieurement à la loi du 10 juillet 1991. En effet, la jurisprudence interne¹⁰³ admettait la légalité d'écoutes téléphoniques ordonnées par le juge d'Instruction dans le cadre d'une information en se fondant sur l'article 81 alinéa 1 du CPP qui dispose que « *le Juge d'Instruction procède conformément à la loi à tous les actes d'information qu'il juge utiles à la manifestation de la vérité* ». Donc, la Cour de cassation s'était appuyée sur une disposition unique qui énonce en des termes généraux les pouvoirs du juge d'Instruction pour admettre la légalité d'un tel procédé. Cependant, dans les arrêts

⁹⁹ TGI Marseille, 1^{ère} ch., 23.03.1995, Claude R. / le ministre de la Justice, obs. J. Frayssinet, D. 1996, Jur. p. 41 et s.; *Expertises*, juillet/août 1995, p. 280-282

¹⁰⁰ Art. 14 CPP : La police judiciaire « *est chargée, suivant les distinctions établies au présent titre, de constater les infractions à la loi pénale, d'en rassembler les preuves et d'en rechercher les auteurs tant qu'une information n'est pas ouverte. Lorsqu'une information est ouverte, elle exécute les délégations des juridictions d'instruction et défère à leurs réquisitions.* »

¹⁰¹ Art. 427 CPP : « *Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction. Le juge ne peut fonder sa décision que sur des preuves qui lui sont apportées au cours des débats et contradictoirement discutées devant lui.* »

¹⁰² Cour de cassation, 2^{ème} civ., 18.12.2003, n° de pourvoi : 02610237, obs. P. REMILLIEUX, *AJ Pénal*, mars 2004, p. 120

¹⁰³ Crim. 13 juin 1989, Derrien, *JCP*, 1990, jurisprudence, n° 21418

Kruslin et Huvig¹⁰⁴, rendus à propos de la pratique des écoutes téléphoniques judiciaires antérieurement à la loi du 10 juillet 1991, la Cour européenne des droits de l'homme avait considéré comme insuffisante, au regard des exigences européennes, la qualité de la loi. En effet, si elle avait estimé la base textuelle de l'article 81 C.P.P. suffisante, elle avait jugé que la précision de la loi faisait défaut.

2. Légalisation du recours aux procédés de signalisation par la loi du 18 mars 2003

La loi du 18 mars 2003 pour la sécurité intérieure est intervenue afin d'autoriser dans le cadre des enquêtes de flagrance, des enquêtes préliminaires et au cours de l'information judiciaire les opérations « *prélèvements externes nécessaires à la réalisation d'examens techniques et scientifiques de comparaison avec les traces et indices prélevés pour les nécessités de l'enquête* » ainsi que « *les opérations de signalisation nécessaires à l'alimentation et à la consultation des fichiers de police selon les règles propres à chacun de ces fichiers* ». Ce faisant, elle a insuffisamment précisé l'étendue des pouvoirs policiers (a) et opéré un durcissement de la procédure pénale en accompagnant ce nouveau pouvoir d'une incrimination floue de nature à en assurer le respect (b).

a) Imprécision de l'étendue des pouvoirs policiers

La loi du 18 mars 2003 a autorisé le recours à des « prélèvements externes » et à des « opérations de signalisation » sans préciser le sens de ces deux notions. Le législateur est à nouveau intervenu par la loi du 9 mars 2004 avec le souhait d'apporter une clarification de la notion de « signalisation ». C'est en effet sur amendement sénatorial que la notion « d'opérations de signalisation » a été remplacée par celle d'« opérations signalétiques et notamment de prise d'empreintes digitales, palmaires ou de photographies nécessaires à l'alimentation et à la consultation des fichiers de police ». Si le législateur est venu éclairer la notion en l'illustrant, il n'en résulte pas un encadrement plus strict des conditions dans lesquelles des opérations de relevé signalétique peuvent être accomplies, à l'inverse de ce qui

¹⁰⁴ Cour EDH, KRUSLIN c. France, 24 avril 1990, obs. G. COHEN-JONATHAN, *RUDH*, 1990, p. 185-191; obs. PRADEL, *Dalloz* 1990, jurisprudence, p. 353 ; Cour EDH, HUVIG c. France, 24 avril 1990, obs. G. COHEN-JONATHAN, *RUDH*, 1990, p. 185-191

est soutenu dans les travaux parlementaires¹⁰⁵. En effet, l'introduction de l'adverbe « notamment » indique que la liste de l'article 55-1 alinéa 2 C.P.P. n'est pas limitative mais seulement indicative. Ainsi, il sera loisible aux policiers de recourir à des procédés de signalisation autres que ceux énumérés par le législateur. Cette absence de précision des termes législatifs, alors même qu'ils déterminent l'étendue des pouvoirs de police, est de nature à laisser aux forces de l'ordre une latitude dans l'action qui est condamnable alors même que ces procédés sont attentatoires au droit au respect de la vie privée de la personne sur laquelle ils sont exercés.

b) Durcissement de la procédure pénale et incrimination floue

Mais le législateur ne s'est pas contenté d'octroyer de nouveaux pouvoirs aux policiers, car un mouvement de pénalisation de la procédure pénale les a accompagné.

Dans un premier temps, le législateur avait incriminé le seul refus de se soumettre aux opérations de prélèvement externe sans prévoir une incrimination similaire en matière de refus de soumission aux opérations de signalisation. Dès lors, l'imprécision de la notion de prélèvement externe était de nature à émettre des doutes sur le respect de l'exigence constitutionnelle de clarté et de précision des incriminations pénales. Notamment, se posait la question de savoir si la notion de « prélèvement externe » incluait celle de « signalisation » ou si les deux notions recouvraient des procédés différents. Un refus de se soumettre aux opérations de signalisation pouvait-il être poursuivi au titre du refus de se soumettre à des opérations de prélèvement externe ? Dans une décision du 13 mars 2003¹⁰⁶, le Conseil constitutionnel a indiqué ce qu'il fallait entendre par « prélèvement externe » en reprenant les observations du gouvernement et les travaux parlementaires. Il a considéré que cette notion faisait référence à un prélèvement qui n'implique aucune intervention corporelle interne et qui ne comporte aucun procédé douloureux, intrusif et attentatoire à la dignité des intéressés.¹⁰⁷ Cependant, il n'a pas précisé si la prise d'empreintes digitales et de photographies devaient être inclus dans la notion de « prélèvement externe ». De l'examen des travaux parlementaires, il ressort que le législateur entendait par « prélèvement externe », la prise de photographies et la prise d'empreintes digitales, la notion de signalisation étant alors comprise dans celle de prélèvement externe. De la même manière, les observations du gouvernement

¹⁰⁵ Rapport du Sénat sur le projet de loi portant adaptation de la justice aux évolutions de la criminalité

¹⁰⁶ Décision n° 2003-467 DC du 13 mars 2003

¹⁰⁷ Décision n° 2003-467 DC du 13 mars 2003, Loi pour la sécurité intérieure, considérant 55

sur les recours dirigés contre la loi du 18 mars 2003 devant le Conseil constitutionnel indiquaient que les prélèvements externes pouvaient être définis comme des « *opérations de prélèvement indolores réalisées de manière non invasive - c'est-à-dire ne créant aucune lésion - et qui ne sont susceptibles de mettre en cause ni l'intégrité physique ni la dignité de la personne humaine* », tels que les prélèvements de salive, aux fins d'une expertise par empreinte génétique, d'empreintes digitales, de photographies, voire de prélèvements de spécimens d'écriture. Cette interprétation a été confirmée par la circulaire de présentation des dispositions de procédure pénale de la loi du 18 mars 2003 pour la sécurité intérieure¹⁰⁸.

Dans un deuxième temps, le législateur¹⁰⁹ est à nouveau intervenu pour préciser que le refus de se soumettre aux opérations de signalisation était passible de sanction pénale, tout comme celui de se soumettre à des prélèvements externes.

L'élargissement des pouvoirs de police dans la collecte des données de signalisation s'est accompagné d'un élargissement similaire dans la collecte du matériel biologique nécessaire à l'établissement de l'empreinte génétique.

Section 2 : Élargissement des pouvoirs de police dans la collecte du matériel biologique nécessaire à l'établissement de l'empreinte génétique

L'identification par le recours aux empreintes génétiques suppose au préalable un matériel biologique. Ce matériel biologique existe soit indépendamment de la volonté de la personne, car il a été relevé sur le lieu de l'infraction et il n'y a pas de prélèvement à effectuer sur la personne ; soit les enquêteurs cherchent à établir le profil génétique d'une personne déterminée et il faudra alors effectuer un prélèvement sur cette personne. Se pose alors inévitablement la question de l'encadrement juridique des conditions de collecte du matériel biologique destiné à établir un profil génétique aux fins d'alimentation du fichier national automatisé des empreintes génétiques (FNAEG). Dans un premier temps, il convient d'observer que les possibilités de prélèvement du matériel biologique, destiné à l'établissement d'une empreinte génétique ont été accrues, conférant par là même plus de

¹⁰⁸ Circulaire de présentation des dispositions de procédure pénale de la loi du 18 mars 2003 pour la sécurité intérieure, NOR : JUSDO330126C, CRIM 2003-12 E8/31.07.2003, BO du Ministère de la justice, n° 91, 31 juillet/1^{er} septembre 2003

¹⁰⁹ Art 55-1 alinéa 3 CPP dans sa rédaction issue de l'article 109 de la loi du 9 mars 2004

pouvoir aux enquêteurs dans leurs moyens de recherches destinés à établir la vérité (§1) pour, dans un deuxième temps, s'interroger sur le point de savoir si au nom de la manifestation de la vérité, il est admissible de porter une atteinte à l'intégrité physique de la personne qui refuserait de se soumettre à un prélèvement (§2).

§1 : Accroissement des possibilités de prélèvement

A : L'absence de pouvoir policier autonome de collecte du matériel biologique antérieurement à la loi du 18 mars 2003

A l'origine, les conditions de recours aux empreintes génétiques dans le cadre du procès pénal étaient très peu précisées. Lorsque l'on recherchait une base légale au prélèvement du matériel biologique nécessaire à l'établissement d'une empreinte génétique, on ne pouvait manquer d'être frappé par l'absence d'encadrement législatif du recours aux empreintes génétiques et, par là même au prélèvement de l'échantillon de matériel biologique. La loi du 29 juillet 1994¹¹⁰ est venue en partie combler ce vide juridique en autorisant, à titre d'exception, l'identification d'une personne par ses empreintes génétiques, dans le cadre de mesures d'enquêtes ou d'instruction diligentées lors d'une procédure judiciaire¹¹¹. Si l'acceptation large de la notion de procédure judiciaire implique qu'il soit possible d'identifier une personne par ses empreintes génétiques dans le cadre d'une enquête de police, il convient de rechercher quel est le cadre procédural permettant aux policiers de recourir à ce type d'investigation. Pour un auteur¹¹², si le recueil des traces et la détermination des traces de

¹¹⁰ Loi n° 94-653 du 29 juill. 1994

¹¹¹ Art. 16-11 al. 1 C. civ. : « L'identification d'une personne par ses empreintes génétiques ne peut être recherchée que dans le cadre de mesures d'enquête ou d'instruction diligentées lors d'une procédure judiciaire ou à des fins médicales ou de recherche scientifique »

¹¹² V. E. MOLINA, *La liberté de la preuve des infractions en droit français contemporain*, Presses universitaires d'Aix-Marseille, 2001, n° 170, p. 175-176 ; Dictionnaire permanent Bioéthique et Biotechnologies, Empreintes génétiques, Feuilles 12, 1996, n° 17, p. 844 : au stade de l'enquête, « il est exclu qu'un témoin ou que le suspect soit soumis, à la demande d'un OPJ ou du Parquet à un examen génétique. La protection de l'inviolabilité et de l'intimité de la personne s'y opposent. » ; Contra l'opinion minoritaire de V. LESCLOUS, C. MARSAT, « Du procès pénal et du juge à propos des empreintes génétiques », *Chronique des parquets et de l'instruction, Droit pénal*, juin 1998, p. 6 ; J. Cl Civil, *Respect et protection du corps humain*, Fasc. 32, 1997, n° 136, p. 21 : « les textes semblent conférer aux OPJ pouvoir de mettre en œuvre la recherche d'identité génétique »

personnes inconnues pouvaient s'inscrire dans le cadre procédural du Code de procédure pénale en cas de flagrance ou dans le cadre de l'enquête préliminaire, les OPJ n'avaient, en revanche, pas compétence pour prendre la décision d'ordonner une mesure attentatoire à l'inviolabilité et à l'intimité de la personne. En effet, le Code de procédure pénale autorise le recours rapide aux techniciens dans ses articles 60, pour l'enquête de flagrance et, 77-1 pour l'enquête préliminaire, mais il ne s'agit que de textes généraux qui fondent le recours à des personnes qualifiées et, non pas la possibilité d'opérer un prélèvement sur une personne. A l'inverse, une doctrine minoritaire¹¹³ trouvait dans l'article 16-11 du Code civil une base légale suffisante au recours aux empreintes génétiques durant la phase d'enquête en s'appuyant sur la distinction qu'opèrerait l'article 16-11 du Code civil entre l'enquête et l'instruction. Cette interprétation semble avoir été démentie par la jurisprudence. En effet, il est possible de déduire, par une lecture *a contrario* d'un arrêt rendu par la Cour d'appel de Grenoble le 7 mai 1999, que le Code de procédure pénale ne conférait pas le pouvoir aux policiers d'effectuer un prélèvement ou de requérir une personne qualifiée pour opérer ce prélèvement. En effet, dans une affaire où un supplément d'information avait été demandé aux fins de recueil du matériel génétique sur une personne poursuivie pour exhibition sexuelle, la Cour d'appel rejeta la demande en invoquant le fait que « *seuls le procureur de la République ou le Juge d'Instruction ont compétence pour ordonner les examens nécessaires.* ». Une base textuelle pouvait être trouvée dans l'article R 53-21 du Code de procédure pénale introduit par le Décret du 18 mai 2000¹¹⁴ quant au prélèvement de matériel biologique sur les personnes définitivement condamnées, mais semblait insuffisante pour fonder un prélèvement lors de la phase policière.¹¹⁵

B : Des pouvoirs policiers de prélèvement insuffisamment encadrés

La loi du 18 mars 2003 est intervenue afin d'accorder de nouveaux pouvoirs aux officiers de police judiciaire (O.P.J.) en matière de prélèvement de matériel biologique destiné à

¹¹³ V. Vincent LESCLOUS, « Empreintes génétiques et procédure pénale », in *Les empreintes génétiques en pratique judiciaire*, La Documentation française, Paris, 1998, p. 115

¹¹⁴ Décret n° 2000-413 du 18 mai 2000, JO du 19 mai 2000

¹¹⁵ Si l'Art. R. 53-21 al. 1 CPP dispose que « *lorsqu'elle n'a pas été réalisée au cours de la procédure d'enquête, d'instruction ou de jugement, l'analyse d'identification par empreintes génétiques d'une personne définitivement condamnée (...) est ordonnée par le procureur de la République* », ce qui fonde une possibilité de prélèvement lors de l'enquête, il semble être une bien mince assise pour fonder un tel pouvoir de l'OPJ.

l'établissement de profil génétique sans suffisamment les encadrer. Il convient d'observer, dans un premier temps, que le degré de subordination policière à l'autorité judiciaire est fonction du cadre de l'enquête (1) pour, dans un second temps, observer que le rapport à la loi n'est pas de nature à apporter des garanties contre les risques d'abus (2).

1. Un rapport à l'autorité judiciaire déterminé par le cadre de l'enquête

Le degré de l'autonomie policière varie en fonction du cadre de l'enquête.

Ainsi, dans le cadre de l'enquête de flagrance, l'O.P.J. dispose d'un pouvoir propre d'ordonner le prélèvement destiné à obtenir le matériel biologique. En effet, l'article 55-1 du C.P.P., introduit par l'article 30 de la loi du 18 mars 2003, autorise « *l'OPJ à procéder ou à faire procéder sous son contrôle, sur toute personne susceptible de fournir des renseignements sur les faits en cause ou sur toute personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis ou tenté de commettre l'infraction aux opérations de prélèvement externes nécessaires à la réalisation d'examen techniques et scientifiques de comparaison avec les traces et indices prélevés pour les nécessités de l'enquête.* ». Il dispose donc d'un pouvoir autonome, qu'il peut mettre en œuvre sans autorisation préalable de l'autorité judiciaire, alors même que ce pouvoir met en cause le droit à l'intimité de sa personne, voire à l'intégrité physique. Par contre, dans le cadre de l'enquête préliminaire, ce pouvoir est encadré car il s'agit soit d'un pouvoir propre du procureur de la République, soit d'un pouvoir de l'OPJ exercé sous contrôle du procureur de la République¹¹⁶. Dans le cadre de l'information, ce pouvoir est également conféré à l'OPJ par l'article 154-1 CPP, mais il est strictement subordonné à l'autorité judiciaire car il s'exerce sur commission rogatoire et est donc soumis à un formalisme strict. De manière plus spécifique, l'article 706-56 I alinéa 1 du CPP, dans sa rédaction issue de la loi du 18 mars 2003¹¹⁷, autorise l'OPJ à procéder ou à faire procéder sous son contrôle à un prélèvement biologique destiné à permettre l'analyse d'identification de leur empreinte génétique des personnes condamnées, des personnes à l'encontre desquelles il existe des indices graves et concordants, rendant vraisemblable qu'elles aient commis l'une des infractions énumérées à l'article 706-55 CPP, des personnes à l'encontre desquelles il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis un crime ou un délit. De manière plus spécifique,

¹¹⁶ Art.76-2 C.P.P.

¹¹⁷ Art. 29 de la loi du 18 mars 2003

car les personnes pouvant faire l'objet d'un prélèvement sont plus limitées dans ce cadre car en sont exclues les simples personnes susceptibles de fournir des renseignements à l'enquête et que le prélèvement est, dans ce cadre, spécifiquement destiné à l'alimentation du fichier.

2. Un rapport faible à la loi

L'autonomie policière atteint son paroxysme en raison de l'absence d'encadrement par le législateur des personnes sur lesquelles le prélèvement peut être opéré (a) et des moyens par lesquels le policier récolte le matériel biologique destiné à établir le profil génétique (b).

a) Absence d'encadrement des personnes pouvant faire l'objet d'un prélèvement

Les personnes pouvant faire l'objet d'un prélèvement sont très largement définies puisqu'il peut s'agir de toute personne susceptible de fournir des renseignements à l'enquête et du suspect. Il est même possible d'affirmer qu'il n'y a pas d'encadrement législatif des personnes pouvant faire l'objet d'un prélèvement puisque autoriser un tel prélèvement sur toute personne revient à ne rien encadrer.

b) La notion de « prélèvement externe », une notion floue

Mais plus encore, c'est la notion de « prélèvement externe » qui pose le plus de difficulté. En effet, la loi se garde bien de la définir alors qu'il aurait été opportun en terme de légalité de le faire car elle conditionne un pouvoir important de l'O.P.J. Le Conseil constitutionnel a considéré que la notion de prélèvement externe faisait référence à un prélèvement qui n'implique aucune intervention corporelle interne et qui ne comporte aucun procédé douloureux, intrusif et attentatoire à la dignité des intéressés.¹¹⁸ Cependant, cette décision laisse entier le problème de savoir ce qu'il faut entendre par « intervention corporelle interne ». Les travaux parlementaires, s'appuyant sur la circulaire du 4 décembre 2000 de présentation des dispositions relatives au fichier des empreintes en France, précisent que « les prélèvements visés peuvent être de tous ordres. Il peut également s'agir de prélèvements buccaux (...), d'empreintes digitales ou de prélèvements quelconques, y compris de spécimen d'écriture.»¹¹⁹. ». Faut-il admettre, avec les travaux parlementaires et la circulaire de la chancellerie qu'un prélèvement buccal soit inclus dans la notion de « prélèvement externe » ?

¹¹⁸ Décision n° 2003-467 DC du 13 mars 2003, Loi pour la sécurité intérieure, considérant 55

¹¹⁹ Rapport sur le projet de loi n° 0508

Ce procédé est, en effet, le plus utilisé mais il nécessite le frottement d'un écouvillon sur la paroi interne des joues par un mouvement de bas en haut répété au minimum dix fois et six écouvillons sont nécessaires pour obtenir le matériel biologique suffisant à la réalisation des empreintes¹²⁰. Dès lors, il semble difficile d'admettre que ce procédé ne soit ni intrusif, ni douloureux et non attentatoire à la dignité des personnes. Pourtant saisi de la constitutionnalité de l'article 30 de la loi 18 mars 2003, permettant à l'OPJ de procéder ou de faire procéder à un prélèvement, le Conseil constitutionnel a considéré que cet article ne portait aucune atteinte à des principes constitutionnellement reconnus. Il a, en effet, admis le recours à de tels prélèvements en estimant que l'atteinte au principe d'inviolabilité du corps humain n'était pas constituée alors que le prélèvement est externe et qu'il ne comporte aucun procédé douloureux ou intrusif ou attentatoire à la dignité des personnes. Cette déclaration de constitutionnalité peut laisser perplexe le commentateur qui ne peut manquer d'observer que le Conseil constitutionnel laisse indéterminée la question des procédés qui seraient attentatoires à la dignité de la personne mais qui ne seraient ni intrusifs ni douloureux¹²¹.

§ 2 : La problématique du consentement au prélèvement : tension entre sécurité et respect de l'intégrité physique

Lorsque l'on veut établir l'empreinte génétique d'une personne déterminée, il faut nécessairement un produit ou un élément du corps humain qui peut être un échantillon de sang, ou une simple racine de cheveu, mais son obtention passe nécessairement par une atteinte, même si elle n'est que minime, à l'intégrité physique. Dès lors se pose la question du consentement de la personne concernée au prélèvement. Ce consentement s'averre-t-il nécessaire ou peut-on sacrifier l'intégrité physique de la personne au bénéfice de l'efficacité de la procédure pénale ?

¹²⁰ J.M. LECOUNA, « 1990-2000 : dix ans d'empreintes génétiques en pratique judiciaire : impact sur les prélèvements », in *10 ans d'empreintes génétiques*, Dir. C. DOUTRMEPUICH, Doc. Fr., p. 145-146

¹²¹ M. BERTRAND, M. VERPEAUX, commentaire de la décision n° 2003-467 DC du 13 mars 2003, in *Petites affiches*, 18 septembre 2003, n° 187, p. 10

A : Incertitudes face à un refus de prélèvement

Il convient d'examiner au préalable les différents systèmes concevables face à un refus de prélèvement opposé par la personne dont on cherche à établir le profil génétique (1) pour ensuite examiner le système français antérieurement à la loi du 9 mars 2004 (2).

1 Les différents systèmes concevables

Face à un refus de prélèvement qui serait opposé par la personne dont on cherche à établir le profil génétique, trois systèmes sont en théorie concevables¹²². En effet, une première option consiste à incriminer le refus et à le sanctionner d'une peine d'emprisonnement et/ou d'amende. Cette solution a été retenue pour sanctionner le refus d'une personne de se soumettre au dépistage d'imprégnation alcoolique. Une deuxième solution consiste à laisser le juge libre de tirer les conséquences d'un tel refus au regard de la preuve de l'infraction. Cette solution, critiquable au regard de la présomption d'innocence est admise par la Cour européenne des droits de l'homme. La troisième solution consiste à recourir à la contrainte pour obtenir le prélèvement. La force employée devant alors être proportionnelle à l'objectif poursuivi et à la gravité de l'infraction. Cette dernière solution n'apparaît pas contraire à la jurisprudence européenne. En effet, bien que la Cour européenne reconnaisse que le droit de se taire et de ne pas contribuer à sa propre incrimination est un droit lié au principe de la présomption d'innocence reconnu par l'article 6 § 2, elle ne semble pas considérer que ce droit puisse s'étendre à l'usage de données que l'on peut obtenir par voie coercitive de l'accusé¹²³. La Commission européenne s'est par ailleurs prononcée sur une requête relative à un prélèvement obligatoire en matière civile de sang. Sur le fondement de l'article 8 § 2, elle a considéré que l'ingérence était prévue par la loi et nécessaire dans une société démocratique

¹²² J.-P. TAK, G. A. van EIKEMA HOMMES, " Le test ADN et la procédure pénale en Europe", *Rev. Sc. Crim.*, oct.-déc., 1993, p. 689

¹²³ Cour EDH, SAUNDERS c. RU, 17 décembre 1996, n° 19187/91 : « le droit de ne pas s'incriminer soi-même concerne en premier lieu le respect de la détermination d'un accusé à garder le silence (...) il ne s'étend pas à l'usage, dans une procédure pénale, de données que l'on peut obtenir de l'accusé en recourant à des pouvoirs coercitifs mais qui existent indépendamment de la volonté du suspect, par exemple les documents recueillis en vertu d'un mandat, les prélèvements d'haleine, de sang et d'urine ainsi que de tissus corporels en vue d'une analyse de l'ADN. »

au but recherché.¹²⁴ Par conséquent, il apparaît que les contraintes internationales ne font pas obstacles par principe au recours à la contrainte pour l'obtention d'un prélèvement. La recommandation du Conseil de l'Europe sur l'utilisation des analyses ADN, dans le cadre de la justice pénale prévoit alors que « lorsque le droit interne admet que des échantillons soient prélevés sans le consentement du suspect, un tel prélèvement ne devrait être effectué que si les circonstances de l'affaire exigent une telle mesure. »¹²⁵. Mais comme l'a justement souligné André GIUDICELLI, rien n'empêche le droit interne de prévoir des solutions plus protectrices¹²⁶.

2 Le système français avant la loi du 9 mars 2004

Antérieurement à la loi du 9 mars 2004, le système retenu semblait avoir opté en faveur de la prohibition du recours à la contrainte, au prix d'une distinction entre le consentement à l'identification génétique et au prélèvement du matériel biologique nécessaire à cette identification (a) et du recours au droit pénal (b).

a) Incertitudes doctrinales et distinction entre consentement à l'identification et consentement au prélèvement

En droit interne, l'hésitation était permise quant à la possibilité de recourir à la force pour l'obtention d'un échantillon biologique, que ce soit sur la personne d'un suspect ou d'un condamné, jusqu'à la loi du 9 mars 2004. Cette loi est venue clore le débat doctrinal en faveur du recours à la contrainte pour l'obtention d'un prélèvement sur la personne des condamnés et non pas sur les simples suspects. L'hésitation était permise en raison du silence législatif sur le cadre juridique du récolement du matériel biologique sur les personnes. En effet, le Code civil pose le principe de l'inviolabilité du corps humain¹²⁷, celui de la nécessité du consentement de la personne pour toute atteinte à son intégrité corporelle et précise que le consentement de l'individu doit être recueilli préalablement à la réalisation de l'étude de ses caractéristiques génétiques ou à son identification par ses empreintes génétiques, que ce soit à des fins médicales, de recherche scientifique, ou dans le cadre d'une procédure civile. En

¹²⁴ Commission EDH, 13 décembre 1979, n° 8378/78

¹²⁵ Recommandation n° R (92) 1 du Comité des Ministres aux Etats membres sur l'utilisation des analyses de l'acide désoxyribonucléique (ADN) dans le cadre du système de justice pénale, adoptée le 10 février 199, principe 4.

¹²⁶ A. GIUDICELLI, *Rev. Sc. Crim.*, juill.-sept. 2001, p. 609

¹²⁷ Art. 16-3 C. civ.

revanche, le législateur n'a pas précisé si le recueil du consentement de la personne était nécessaire « dans le cadre de mesures d'enquête ou d'instruction diligentées dans le cadre d'une procédure judiciaire ». Pour une partie de la doctrine, ce silence du législateur devait s'interpréter comme permettant de passer outre un refus de consentement et donc une atteinte à l'intégrité corporelle.¹²⁸ A l'inverse pour la doctrine majoritaire¹²⁹, le silence législatif ne pouvait s'interpréter comme permettant de passer outre un refus de prélèvement et de recourir à la contrainte. Pour un auteur¹³⁰, il apparaissait possible de distinguer selon que le prélèvement devait s'effectuer sur un simple suspect ou sur une personne définitivement condamnée. Cette distinction s'appuyait sur les termes de l'article R. 53-21 du C.P.P. qui rend l'analyse obligatoire pour le procureur de la République. Cependant, l'analyse de la doctrine majoritaire se trouva confortée par la circulaire de présentation des dispositions du FNAEG¹³¹. En effet, la circulaire opérait une distinction entre consentement à l'identification génétique et consentement au prélèvement biologique, plus conforme à la lettre et à l'esprit du texte. Ainsi, le consentement à l'identification par empreintes génétiques n'était pas requis alors que celui au prélèvement devait l'être. Le recours à la contrainte étant proscrit, y compris sur les personnes définitivement condamnées car contraire aux principes généraux de notre droit garantissant l'inviolabilité du corps humain. C'est également la solution qui semble se dégager implicitement de l'arrêt rendu par la chambre criminelle de la Cour de

¹²⁸ En ce sens, N.-J. MAZEN, « Tests et empreintes génétiques : du flou juridique au pouvoir scientifique », *Petites affiches*, 14 décembre 1994, n° 149 : « Plus remarquables par leur importance sont les exceptions prévues par le législateur « dans le cadre de mesures d'enquête ou d'instruction diligentées lors d'une procédure judiciaire » (...) On se doit de souligner le caractère novateur de cette mesure : jusqu'alors, aucune atteinte ne pouvait être réalisée de manière contraignante sur la personne d'un témoin, d'un suspect ou d'une personne mise en examen. »

¹²⁹ V. J. C. GALLOUX, « L'empreinte génétique : la preuve parfaite ? », *J.C.P.*, 1991, I, 3497, n° 25, p. 108 ; J. L. CROIZIER, « Le consentement aux analyses génétiques », in *Les empreintes génétiques en pratique judiciaire*, Doc. Fr., Paris, 1998, p. 52 ; Vincent LESCLOUS, « Empreintes génétiques et procédure pénale », in *Les empreintes génétiques en pratique judiciaire*, Doc. Fr., Paris, 1998, p. 119 ; H. MATSOPOULOU, *Les enquêtes de police*, coll. Bibliothèque des sciences criminelles, L.G.D.J., 1995, p. 737, n° 911 ; E. MOLINA, *La liberté de la preuve des infractions en droit français contemporain*, Presses universitaires d'Aix-Marseille, 2001, n° 177, p. 182

¹³⁰ A. GIUDICELLI, *op. cit.*, p. 610

¹³¹ Circulaire « Présentation des dispositions relatives au fichier national automatisé des empreintes génétiques et au service central de préservation des prélèvements biologiques » du 10 octobre 2000, Ministère de la justice, direction des affaires criminelles et des grâces, n° CRIM 2000-08 F1/10-10-2000

cassation du 30 avril 1998¹³². Dans cette affaire, des policiers, agissant sur commission rogatoire, avaient entendu un témoin et procédé à la saisie de son mégot de cigarette fumée lors de son audition. Une expertise génétique avait ainsi pu être réalisée. Le requérant invoquait l'annulation du procès verbal d'audition et l'annulation de la saisie subséquente au motif qu'il n'avait pas été informé que la saisie était destinée à une analyse d'A.D.N. La Chambre de cassation rejeta le pourvoi au motif que l'intéressé avait consenti à la saisie du mégot de cigarette. Il est ainsi possible d'affirmer que la Cour de cassation n'exige pas que l'intéressé consente à ce qu'une analyse génétique soit effectuée.

b) Incrimination du refus de prélèvement : prohibition du recours à la coercition

La loi du 15 novembre 2001 et du 18 mars 2003 sont venues apporter des premiers éléments de réponse en optant pour le recours au droit pénal afin d'assurer l'efficacité de la procédure pénale par celle du consentement au prélèvement des personnes concernées. La loi du 15 novembre 2001 n'avait incriminé que le refus opposé par une personne définitivement condamnée. La loi du 18 mars 2003 a poursuivi ce mouvement en incriminant le refus de prélèvement opposé par le simple témoin¹³³ ou le simple suspect aux opérations de prélèvement dans le cadre de l'enquête préliminaire, de flagrance ou de l'information. La personne opposant ce refus encourant alors une peine fonction de son état de personne définitivement condamnée ou non et variant du simple au double. Certains auteurs¹³⁴ ont estimé que ces peines ne s'averraient pas suffisamment incitatives en raison de leur *quantum* assez faible au regard de la peine encourue en cas de reconnaissance de culpabilité. Ces dispositions, bien que témoignant d'un durcissement de la procédure pénale, semblaient pouvoir signifier que l'intéressé se voyait implicitement reconnaître la possibilité de refuser de consentir au prélèvement. Mais le législateur est à nouveau intervenu par la loi du 9 mars 2004 pour préciser les conditions du prélèvement.

¹³² Cassation Crim. 30 avril 1998, n° 98-80741, Inédit, obs. A. GIUDICELLI, *Rev. Sc. Crim.*, juill.-sept. 2001, pp. 607-610

¹³³ L'art. 109 de la loi du 9 mars 2004 a supprimé l'incrimination du refus opposé par le simple témoin

¹³⁴ P. TABEL, « ADN et preuve pénale », *Revue de la gendarmerie nationale*, n° 208, 3^{ème} trimestre 2003, p. 51

B : La loi du 9 mars 2004, un encadrement insuffisant et critiquable

L'article 49 de la loi du 9 mars 2004¹³⁵ est venu modifier l'article 706-56 du Code de Procédure pénale afin de permettre d'une part d'identifier l'empreinte génétique d'une personne à partir de matériel biologique qui se serait naturellement détaché du corps de l'intéressé et, d'autre part, le recours à la contrainte pour obtenir un prélèvement sans l'accord de l'intéressé sur réquisitions écrites du procureur de la République sur les personnes condamnées pour crime ou délit puni de dix ans d'emprisonnement. Cette disposition a été introduite par la voie d'un amendement sénatorial.

1. Le recours à la contrainte sur les personnes définitivement condamnées

a) La constitutionnalité du recours à la contrainte

Initialement, il était prévu que seuls les condamnés pour crime puissent faire l'objet d'un prélèvement forcé mais, en deuxième lecture, l'Assemblée nationale, à l'initiative du rapporteur de la commission des Lois, a prévu la possibilité d'effectuer des prélèvements forcés d'empreintes génétiques non seulement sur les auteurs de crimes, mais également sur les auteurs de délits punis de dix ans d'emprisonnement. Cette nouvelle disposition n'a fait l'objet d'aucun débat parlementaire mais, au contraire, d'un large consensus politique¹³⁶, de telle sorte que l'inconstitutionnalité de cette disposition n'a pas été soulevée. Toutefois, il est permis de penser que la constitutionnalité du recours à la contrainte pour obtenir du matériel biologique n'est pas douteuse. En ce sens, peut être invoquée la décision du Conseil constitutionnel du 13 mars 2003 dite sécurité intérieure. En effet, le Conseil constitutionnel, saisi de la constitutionnalité de la disposition permettant de recourir à la contrainte pour pratiquer une prise de sang sur une personne contre laquelle il existe des indices graves et concordants d'avoir commis une agression sexuelle, afin de déterminer si l'intéressé n'est pas atteint d'une maladie sexuellement transmissible, avait estimé que « *la contrainte à laquelle est soumise la personne concernée n'entraîne aucune rigueur qui ne serait pas nécessaire au regard des autres exigences constitutionnelles en cause et, plus particulièrement, conformément au onzième alinéa du Préambule de la Constitution de 1946, de la protection*

¹³⁵ Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice à l'évolution de la criminalité

¹³⁶ Voir Séance du 2 octobre 2003, lors de l'examen en première lecture au Sénat du projet de loi portant adaptation de la justice aux évolutions de la criminalité

*de la santé de la victime ; que l'examen médical et le prélèvement sanguin ne portent atteinte ni aux droits de la défense, ni aux exigences du procès équitable, ni à la présomption d'innocence »*¹³⁷.

b) Un recours à la force problématique en terme de proportionnalité

Il semble que permettre le prélèvement forcé sur une personne qui a été définitivement condamnée est problématique en terme de proportionnalité. En effet, à ce stade le prélèvement a pour unique objet l'alimentation du fichier de police. Il repose sur l'idée que la personne déjà condamnée est un récidiviste potentiel et, qu'en cas de récidive, il pourra être confondu grâce aux traces recueillies sur le lieu de l'infraction. S'il apparaît plus respectueux de la présomption d'innocence de bannir le prélèvement forcé en amont du procès pénal, il apparaît que ce prélèvement n'apparaît plus nécessaire pour mener à bien une enquête déterminée lorsqu'il est opéré dans la phase d'exécution des peines. Dès lors la proportionnalité nécessaire entre la mesure employée et le but poursuivi apparaît douteuse.

c) Un cumul exécution forcée / peine inconstitutionnel ?

De plus, la possibilité de recourir à la contrainte pour obtenir le matériel biologique d'une personne définitivement condamnée s'accompagne de la possibilité de sanctionner pénalement le refus de prélèvement. En effet, la loi du 15 novembre 2001 relative à la sécurité quotidienne a introduit une peine d'emprisonnement et d'amende pour la personne définitivement condamnée qui refuserait de se soumettre à un prélèvement biologique¹³⁸. Le quantum de la peine encourue était alors fonction de la gravité de l'infraction ayant motivé la condamnation donnant lieu à l'inscription dans FNAEG. La loi du 18 mars 2003 a poursuivi ce mouvement de pénalisation en doublant le quantum de la peine encourue qui passait de six mois à un an d'emprisonnement. Mais le législateur, en ménageant une possibilité de recours à la contrainte, n'est pas revenu sur cette incrimination. Un cumul est donc possible entre l'exécution forcée du prélèvement et la sanction pénale en raison d'un refus au prélèvement. Or, ce cumul apparaît problématique au regard des exigences constitutionnelles de proportionnalité de la peine. En effet, le Conseil constitutionnel, dans sa décision du 9 mars 2003, saisi de la constitutionnalité de l'incrimination de refus de prélèvement introduite par

¹³⁷ Décision n° 2003-467 DC du 13 mars 2003, Loi pour la sécurité intérieure, Considérant n° 49

¹³⁸ Ancien art. 706-56 issu de la loi du 15 novembre 2001 : « Le fait pour une personne définitivement condamnée pour une des infractions visées à l'article 706-55, de refuser de se soumettre à un prélèvement biologique destiné à permettre l'analyse d'identification de son empreinte génétique est puni de six mois d'emprisonnement et de 7 500 euros d'amende. Lorsque la personne a été condamnée pour crime, la peine est de deux ans d'emprisonnement et 30 000 euros d'amende »

l'article 30 de la loi 18 mars 2003, avait admis la proportionnalité de la peine notamment en raison de l'absence de voies d'exécution d'office du prélèvement¹³⁹. Un raisonnement par analogie nous conduit donc à affirmer qu'il est probable que le Conseil constitutionnel n'aurait pas admis la constitutionnalité d'un tel cumul. Et cela d'autant plus que la loi du 9 mars 2004 a prévu que la commission d'une telle infraction par une personne condamnée entraînait de plein droit toutes les réductions de peine, dont elle aurait pu bénéficier, et interdisait l'octroi de réductions de peine¹⁴⁰.

2. Le prélèvement sur les simples suspects

Le consentement au prélèvement du matériel biologique nécessaire pour établir l'empreinte génétique des simples suspects est en principe requis. Cependant, la nécessité du consentement comporte deux limites. Tout d'abord, l'identification de l'empreinte génétique peut se faire à partir de matériel génétique qui se serait naturellement détaché du corps humain (a). Mais encore, le refus de prélèvement est passible de sanction pénale (b).

a) Consentement au prélèvement et recours à la ruse

Si le législateur de mars 2004 ne l'a pas expressément spécifié, il n'est désormais plus possible de s'interroger sur la possibilité de recourir à la contrainte pour obtenir un prélèvement sur une personne non définitivement condamnée. Pour ces dernières, la loi incite à réaliser l'identification de l'empreinte génétique à partir de matériel biologique qui se serait naturellement détaché du corps humain. Cette formulation est empruntée à celle employée par la circulaire de présentation des dispositions du FNAEG¹⁴¹. Il existe donc des possibilités de contourner un refus de prélèvement. Avec un auteur, il est possible d'affirmer que la loi incite les enquêteurs à « recourir à la ruse »¹⁴², dans la mesure où le recours à la contrainte se trouve limité. Il apparaît même que la loi incite à recourir à des procédés déloyaux. Est-il admissible qu'un enquêteur ou un magistrat offre un verre d'eau ou une cigarette à celui qui refuse un

¹³⁹ Décision n° 2003-467 DC du 13 mars 2003, Loi pour la sécurité intérieure, Considérant n° 57

¹⁴⁰ Art. 706-56 III° C.P.P issu de la loi du 9 mars 2004

¹⁴¹ Circulaire « Présentation des dispositions relatives au fichier national automatisé des empreintes génétiques et au service central de préservation des prélèvements biologiques » du 10 octobre 2000, Ministère de la justice, direction des affaires criminelles et des grâces, n° CRIM 2000-08 F1/10-10-2000

¹⁴² Hervé ANCEL, « La preuve biologique », *in* « Les transformations de l'administration de la preuve pénale : perspectives comparées », G. GIUDICELLI-DELAGE (dir.), à paraître.

prélèvement pour ensuite saisir ces objets et procéder à une analyse de comparaison ? La pratique se développerait, en effet, de l'utilisation de stratagèmes par les enquêteurs pour obtenir le matériel biologique souhaité. Des risques de dérive sont donc aisément perceptibles tant il apparaît difficile de discerner l'échantillon extorqué par provocation de celui obtenu en bonne et due forme¹⁴³. Cette incitation législative apparaît des plus problématiques alors même que la jurisprudence de la Chambre criminelle tend à faire prévaloir l'efficacité de la procédure pénale par la liberté de la preuve des infractions¹⁴⁴. Ainsi, il n'est pas possible de recourir à la contrainte pour obtenir un prélèvement sur les personnes non définitivement condamnées.

b) Consentement au prélèvement et incrimination

Du fait de l'incrimination du refus de prélèvement qui s'accompagne de sanctions assez lourdes sur les personnes non définitivement condamnées, on peut s'interroger sur le caractère libre et éclairé d'un tel consentement¹⁴⁵. Le Conseil constitutionnel dans sa décision du 13 mars 2003 relative à la loi pour la sécurité intérieure a toutefois validé une telle incrimination¹⁴⁶.

En soustrayant les fichiers de police à un contrôle a priori effectif de la CNIL, le législateur a entendu pouvoir se soustraire à la doctrine exigeante qu'elle avait mis en place dans son interprétation de la loi du 6 janvier 1978. Dès lors, les fichiers de police pourront apparaître comme des outils dont les conditions de fonctionnement et d'alimentation sont entièrement tournés vers une seule et même finalité : l'efficacité de ces outils et cela, quitte à oublier au passage certains des grands principes de la procédure pénale. Mais de nouveaux acteurs sont

¹⁴³ D. THOMAS (Dir.), « Les transformations de l'administration de la preuve pénale : perspectives comparées », Recherche réalisée par l'Université de Montpellier I, Equipe de Recherche sur la Politique criminelle, avec le soutien de la Mission de recherche Droit et Justice, Juin 2004, non publié, synthèse disponible sur www.gip-recherche-justice.fr

¹⁴⁴ V. Cassation Crim. 30 avril 1998, n° 98-80741, Inédit, obs. A. GIUDICELLI, *Rev. Sc. Crim.*, juill.-sept. 2001, pp. 607-610

¹⁴⁵ En ce sens, D. THOMAS (Dir.), « Les transformations de l'administration de la preuve pénale : perspectives comparées », op. citée.

¹⁴⁶ Décision n° 2003-467 DC du 13 mars 2003, Loi pour la sécurité intérieure, Considérant n° 57

apparus dans le champ de la régulation des fichiers de police. En effet, une timide ouverture des fichiers de police à la société civile est perceptible de même qu'un mouvement de judiciarisation. Cette apparition est-elle de nature à rétablir un équilibre ?

PARTIE 2 : Vers de nouveaux acteurs de la régulation des fichiers de police ?

De nouveaux protagonistes sont apparus dans le champ de la régulation des fichiers de police. En effet, les citoyens se voient dotés de droits dont l'exercice leur permettrait d'exercer un certain contrôle sur le contenu des fichiers et, par là même, sur le respect des conditions d'encadrement (Chapitre 1). Mais encore, sous l'effet de l'impulsion des contraintes régionales et constitutionnelles, un mouvement de judiciarisation est amorcé. Ces deux mouvements parallèles sont-ils de nature à apporter de réelles garanties dans le contrôle des conditions de fonctionnement des fichiers ? Peuvent-ils apparaître comme des contreparties suffisantes pour compenser le relâchement de l'encadrement juridique des fichiers de police ? Ces nouveaux acteurs sont-ils à même de remplir le rôle qui leur est confié ? Sont-ils doter des moyens juridiques ou pratiques de nature à rendre ce contrôle exigeant ?

Nous tenterons de répondre à ces questions en examinant dans un premier temps l'ouverture des fichiers de police à la société civile (Chapitre 1) et, dans un deuxième temps, le mouvement de judiciarisation (Chapitre 2).

Chapitre 1 : Une régulation citoyenne : ouverture des fichiers de police à la société civile

Le système initialement mis en place par la loi de 1978 était original car il marquait une timide ouverture des fichiers de police à la société civile, en dotant la personne fichée d'un droit d'accès aux informations les concernant contenues dans ces fichiers. Le droit d'accès consiste, dans la prérogative donnée à toute personne qui pense figurer dans un fichier, de connaître le contenu des informations le concernant. Il apparaît comme le moyen de contrôle à la disposition du citoyen des fichiers de police. Par l'exercice de ce droit, la responsabilité de veiller à la préservation de ses droits incombe à la personne fichée. Cette ouverture des fichiers de police à la société civile est apparue lors de l'entrée en vigueur de la loi comme brisant la tradition du secret entretenu par l'administration en la matière. Mais il apparaît désormais que ce mouvement d'ouverture devrait être prolongé afin de faire du droit d'accès un outil citoyen de contrôle des fichiers de police.

Section 1 : Les moyens de la régulation citoyenne : le droit d'accès aux fichiers de police

C'est sur ce droit d'accès, qui pourrait être un puissant instrument de l'action policière par le citoyen, que s'est cristallisée une partie du débat et qu'apparaît avec le plus de véhémence la tension inhérente à l'objet de cette étude entre sécurité et liberté. Cette tension a atteint son paroxysme à travers le conflit entre l'interprétation dynamique de la CNIL du droit d'accès applicable aux fichiers de police et celle du Conseil d'État plus soucieux de la raison d'État (§1). La doctrine de la CNIL a influé sur le droit d'accès aux fichiers de police de telle sorte qu'un droit d'accès indirect aménagé aux fichiers de police a été consacré, mais au détriment d'un droit d'accès direct (§2).

§ 1 : Le droit d'accès aux fichiers de police : entre transparence et secret

En matière de droit d'accès aux données les concernant dans les fichiers de police, le droit international n'apparaît pas de nature à influencer les systèmes juridiques nationaux dans le sens d'une plus grande ouverture de ces fichiers à la société civile (A), le droit interne a opté pour le principe d'un droit d'accès mais ce droit d'accès est aménagé de manière spécifique (B).

A : Le droit supranational en matière de droit d'accès : de faibles contraintes structurelles¹⁴⁷ quant au droit d'accès aux fichiers de police

Il convient d'examiner si le droit international est de nature à apporter des garanties aux citoyens en matière d'accès aux données les concernant contenues dans les fichiers de police. Autrement dit, le droit international est-il de nature à imposer une plus grande ouverture des fichiers de police à la société civile ? Afin de répondre à cette question, seront plus particulièrement examinées la jurisprudence de la Cour européenne des droits de l'homme (1),

¹⁴⁷ Au sens entendu par Mireille DELMAS-MARTY, *in* Les grands systèmes de politique criminelle, coll. Thémis, PUF, 1992, p. 329, c'est à dire comme les principes qui limitent les choix possibles de politique criminelle en imposant certaines contraintes.

la Convention 108 du Conseil de l'Europe¹⁴⁸ (2) et, la recommandation R (87) 15 relative à la réglementation de l'utilisation de données à caractère personnel dans le secteur de la police¹⁴⁹ (3).

1. La Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales

Il convient d'examiner les dispositions de la CESDH, telles qu'interprétées par la Cour européenne des droits de l'homme, afin de déterminer s'il en résulte des garanties applicables en matière d'accès par les citoyens aux données les concernant contenues dans les fichiers de police.

Dans l'arrêt LEANDER contre Suède du 25 février 1987¹⁵⁰, la Cour se penche sur une affaire dans laquelle un requérant s'était vu refuser l'accès à un emploi en raison des informations relatives à sa vie privée contenues dans un registre secret de la police. Elle a alors eu l'occasion de se prononcer sur le droit d'accès aux fichiers de police sous l'angle de plusieurs droits garantis par la Convention.

Tout d'abord, sous l'angle de l'article 8 de la CESDH, qui garantit le droit au respect de la vie privée, la Cour note « *que tant la mémorisation que le refus d'accorder la faculté de réfuter des données relatives à la vie privée portaient atteinte au droit au respect de la vie privée de l'individu* »¹⁵¹. Toutefois, la Cour a toujours refusé de consacrer un tel droit d'accès sur le fondement de l'article 8.

Mais, il peut se déduire de l'arrêt ROTARU contre Roumanie¹⁵² que le droit d'accès constitue un aspect du droit au recours effectif de l'article 13 de la Convention qui garantit le droit à un recours effectif. En effet, dans cet arrêt, la violation de l'article 13 est déduite de ce que le système juridique examiné par la Cour ne permettait pas à l'individu de contester la détention par les services de renseignements de données sur la vie privée du requérant ou de réfuter ces

¹⁴⁸ Convention 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel, *JO* du 20 novembre 1985

¹⁴⁹ Recommandation du Conseil de l'Europe R (87) 15 relative à la réglementation de l'utilisation de données à caractère personnel dans le secteur de la police, 17 septembre 1987

¹⁵⁰ Cour EDH, LEANDER c. Suède, 26 mars 1987, requête n° 9248181

¹⁵¹ Cour EDH, LEANDER c. Suède, 26 mars 1987: § 48

¹⁵² Cour EDH, ROTARU c. Roumanie, 4 mai 2000, obs. O. DE SCHUTTER, *RTDH*, 2001, pp. 145-183

informations¹⁵³. La Cour admet toutefois, que les États puissent substituer à un contrôle des données par l'exercice du droit d'accès de l'individu un mécanisme de contrôle qu'elle qualifie « d'objectif » lorsque l'efficacité du traitement de données personnelles est liée au caractère secret des données qu'il contient. Ainsi, dès lors que le caractère secret des données collectées par la police est une condition de leur efficacité, c'est à dire que ces données perdraient tout leur intérêt pour la police, si elles venaient à être connues de la personne qu'elles concernent, la Cour laisse une large marge d'appréciation à l'État et admet que soit substitué au droit d'accès un autre mécanisme de contrôle des données. Autrement dit, le droit d'accès n'est pas garanti par la Convention dès lors qu'il compromet les finalités du fichier et qu'une autre procédure de contrôle des données est prévue.

Enfin, le requérant avait également tenté de se fonder sur l'article 10 de la Convention qui reconnaît une liberté de recevoir des informations pour faire admettre une violation de la Convention, du fait du refus d'accès qui lui avait été opposé par le Gouvernement aux informations le concernant contenues dans un registre de la police. Mais la Cour européenne des droits de l'homme rejette son grief au motif qu'elle considère que l'article 10 de la Convention n'accorde pas à l'individu le droit d'accéder à un registre où figurent des informations sur sa propre situation, ni n'oblige le gouvernement à les lui communiquer.

Il semblerait donc que la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales n'est pas de nature à apporter des garanties spécifiques au citoyen en matière d'accès aux données le concernant dans les fichiers de police.

2. La Convention 108 du Conseil de l'Europe

La Convention 108 du Conseil de l'Europe¹⁵⁴ pose le principe du droit d'accès en son article 8 mais permet, en vertu de son article 9 paragraphe deux, aux États membres de prévoir dans leur législation une exception au droit d'accès lorsqu'une telle dérogation est prévue par la loi et constitue une mesure nécessaire dans une société démocratique à la protection de la sécurité de l'État, à la sûreté publique, aux intérêts monétaires de l'État ou à la répression des

¹⁵³ En ce sens, O. DE SCHUTTER, « Vie privée et protection de l'Individu vis-à-vis des traitements de données à caractère personnel », *Rev. Trim. Dr. H.*, 2001, p. 176

¹⁵⁴ Convention 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel, *JO* du 20 novembre 1985

infractions pénales. La Convention ne contient donc pas de dispositions qui seraient de nature à apporter des garanties plus poussées que celles mises en place par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales en la matière.

3. La Recommandation R (87) sur l'utilisation de données personnelles dans le secteur de la police

A l'inverse des conventions précédemment examinées, la recommandation sur l'utilisation de données personnelles dans le secteur de la police apporte des garanties spécifiques en matière de droit d'accès aux données contenues dans les fichiers de police. En effet, elle dispose en son article 6.2 que la personne concernée devrait pouvoir obtenir l'accès à un fichier de police à des intervalles raisonnables et sans délais excessifs conformément aux modalités du droit interne. La recommandation admet toutefois que ce droit d'accès puisse faire l'objet de restrictions dans la mesure où une telle restriction serait indispensable pour l'accomplissement d'une tâche légale de la police ou nécessaire pour la protection de la personne concernée ou des droits et libertés d'autrui. Ce texte écarte la possibilité pour les États de prévoir dans leur législation une exception systématique au principe du droit d'accès¹⁵⁵. Cependant, la recommandation est dénuée de toute portée contraignante.

Le droit interne a opté pour le principe d'un droit d'accès des individus aux données les concernant, contenues dans un fichier de police mais a ménagé un droit d'accès dérogatoire au droit commun.

A : Un droit d'accès dérogatoire au droit commun

La loi du 6 janvier 1978 a ménagé dans ses dispositions un droit d'accès dérogatoire au droit commun pour les traitements intéressant la sûreté de l'État, la défense et la sécurité publique qui a donné lieu à une interprétation audacieuse et controversée de la CNIL.

¹⁵⁵ V. D. MARTIN, *op. citée*, p. 264

1. Le principe d'un droit d'accès indirect

Pour les traitements intéressant la sûreté de l'État, la défense et la sécurité publique, l'article 39 de la loi du 6 janvier 1978, dans sa rédaction antérieure à la loi du 6 août 2004, conserve le principe du droit d'accès, mais aménage des modalités particulières d'exercice du droit d'accès aux fichiers de police.

Le droit d'accès de droit commun était prévu par les articles 34 et 45 de la loi du 6 janvier 1978. C'était un droit d'accès direct, car il s'exerçait directement contre le responsable du fichier. De plus, il avait pour corollaire le droit de communication des informations contenues dans le fichier. Au regard des caractéristiques du droit d'accès de droit commun, la loi de 1978 avait mis en place un mécanisme de droit d'accès aux fichiers intéressant la sûreté de l'État, la défense et la sécurité publique doublement dérogatoire.

En effet, le droit d'accès à ces fichiers, aménagé par l'article 39 était indirect et ne permettait pas au requérant d'accéder aux informations contenues par ces fichiers. Le droit d'accès était indirect car il devait s'exercer obligatoirement par l'intermédiaire de la CNIL. En effet, le titulaire du droit d'accès devait adresser une demande à la Commission. Elle devait alors désigner l'un de ses membres magistrat pour mener les investigations utiles. Le droit d'accès était indirect car il ne comportait pas le droit d'obtenir communication des données enregistrées dans le fichier. En effet, l'article 39 prévoyait que lorsqu'il avait été procédé aux vérifications, il devait être notifié au requérant que les vérifications avaient été opérées¹⁵⁶. Par conséquent, le requérant n'accédait pas aux informations le concernant. Il n'avait pas même la possibilité de savoir si des renseignements le concernant figuraient bien dans le fichier. Ce mécanisme imposait au requérant de faire confiance à la Commission pour veiller à la préservation de ses droits. Il ne pouvait dès lors qu'être source de frustrations pour les citoyens l'exerçant¹⁵⁷.

¹⁵⁶ Ancien art. 39 alinéa 3 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JO* 7 janvier 1978

¹⁵⁷ D. LOCHAK, « Informatique, police et libertés », *Après-demain*, n° 327, oct.-nov. 1990, p. 16 : ce professeur de droit décida elle-même d'exercer son droit d'accès aux fichiers des renseignements généraux et fini par obtenir la communication de son dossier.

2. L'interprétation de l'article 39 par la CNIL : une interprétation audacieuse et controversée

La CNIL a œuvré en faveur d'une plus grande transparence et d'une plus grande ouverture des fichiers de police à la société civile. Elle s'est en effet réservée le pouvoir d'interpréter la notion de « traitement intéressant la sûreté de l'État, la défense et la sécurité publique », visée à l'article 39 de la loi du 6 janvier 1978, qui conditionnait l'applicabilité du droit d'accès indirect. Elle en contrôlait l'invocation par l'administration et en appréciait le bien fondé¹⁵⁸. C'est ainsi, qu'elle a contesté l'application automatique de l'article 39 aux fichiers de police soit en ne l'appliquant pas à un traitement (a), soit en l'appliquant de manière distributive (droit d'accès mixte) (b).

a) Des fichiers de police soumis au droit d'accès direct

La CNIL, par son interprétation de la notion de « sécurité publique », a pu soustraire des fichiers de police du droit d'accès indirect mis en place par l'article 39 de la loi du 6 janvier 1978 dans sa rédaction antérieure.

C'est ainsi, qu'elle a considéré que le droit d'accès indirect de l'article 39 ne devait pas être appliqué au fichier national des empreintes digitales. En effet, dans sa délibération en date du 14 octobre 1986¹⁵⁹ relative au projet de décret portant création du fichier national des empreintes digitales, elle considère que « *la communication aux intéressés des informations les concernant – informations dont le caractère strictement objectif – n'est pas susceptible de porter atteinte à la sécurité publique.* ». C'est pourquoi, l'article 6 du décret du 8 avril 1987 relatif au fichier automatisé des empreintes digitales¹⁶⁰ prévoit que le droit d'accès s'exerce conformément à l'article 34 de la loi de 1978.

Il faut en déduire que l'un des critères d'applicabilité du droit d'accès direct est le caractère subjectif ou objectif des informations contenues dans le fichier. Ainsi, les données subjectives relèveraient du droit d'accès indirect, alors que les données objectives relèveraient du droit d'accès direct. Mais encore, la Commission semble lier le caractère objectif ou subjectif des données collectées à l'origine de la collecte. Ainsi, lorsque les données ont été collectées directement auprès des individus, elles sont objectives et lorsque les données n'ont pas été

¹⁵⁸ V. CNIL, Rapport 1986, p. 111

¹⁵⁹ Délibération 86-102 du 14 octobre 1986 concernant un projet de décret relatif au fichier automatisé des empreintes digitales géré par le Ministère de l'Intérieur

¹⁶⁰ Décret n° 87-249 du 8 avril 1987

collectées auprès des individus, elles sont subjectives. Les données collectées auprès des individus relevant alors du droit d'accès direct et celles recueillies à leur insu relevant du droit d'accès indirect. L'analyse de cette délibération donnerait à penser que les fichiers de signalisation devraient relever du droit d'accès direct et les fichiers d'antécédents du droit d'accès indirect. Cette interprétation semble confirmée par le fait que le pouvoir exécutif a ménagé un droit d'accès direct au fichier FNAEG¹⁶¹.

S'il peut sembler paradoxal d'admettre un droit d'accès direct, plus protecteur pour des données objectives et de le dénier pour des données subjectives, plus dangereuses pour le citoyen fiché, cette doctrine semble être dans la droite ligne de la jurisprudence européenne¹⁶².

b) Des fichiers de police soumis au « droit d'accès mixte »

Dans une délibération en date du 1^{er} avril 1980 portant adoption d'une recommandation relative à la mise en œuvre du droit individuel d'accès aux fichiers automatisés¹⁶³, la CNIL posait deux principes importants quant au droit d'accès aux traitements intéressant la sûreté de l'État, la défense et la sécurité publique. Tout d'abord, elle posait le principe de divisibilité des fichiers en considérant que le droit d'accès devait s'apprécier par rapport aux informations contenues par le traitement et non par rapport au traitement lui-même apprécié dans son ensemble. Mais encore, elle posait le principe selon lequel l'appréciation du caractère communicable des informations contenues dans le fichier serait apprécié par le commissaire chargé de procéder aux investigations aux termes de ces dernières. La CNIL posait ainsi le principe d'un droit d'accès mixte et la possibilité pour le Commissaire chargé d'exercer le droit d'accès indirect d'apprécier *in concreto* le caractère communicable des données contenues dans le fichier. Cette possibilité paraissait audacieuse et de nature à accroître sensiblement la transparence en la matière. Pourtant elle n'a que partiellement appliqué cette délibération. En effet, elle s'est bornée à faire application du principe de divisibilité des fichiers lors de l'examen des caractéristiques du traitement, à l'occasion de la sollicitation de son autorisation émanant du pouvoir exécutif. Cela signifie qu'elle examinait les informations contenues dans le fichier et adaptait le droit d'accès en considération de ces informations. Par

¹⁶¹ Art. R 53-15 C.P.P

¹⁶² Voir infra A) Le droit supranational en matière de droit d'accès : de faibles contraintes structurelles quant au droit d'accès aux fichiers de police

¹⁶³ Délibération en date du 1^{er} avril 1980 portant adoption d'une recommandation relative à la mise en œuvre du droit individuel d'accès aux fichiers automatisés, 5^{ème} rapport d'activité, p. 86

conséquent, lorsque le traitement portait à la fois sur des informations non protégées et sur des informations non communicables, pouvaient être communiquées au requérant les informations non protégées. Certains auteurs¹⁶⁴ ont estimé que cette doctrine de la CNIL était *contra legem*. Deux raisons pouvaient être invoquées en ce sens. La première, ayant le plus de poids, est que l'article 39 faisait référence aux traitements intéressant la sécurité publique et non pas aux informations dont la communication serait susceptible de menacer la sécurité publique. La deuxième est qu'en prévoyant expressément que le membre de la CNIL qui procède au contrôle du traitement « notifie au requérant qu'il a été procédé aux vérifications », le législateur aurait entendu soustraire au droit de communication l'ensemble des informations enregistrées dans les fichiers. Il est certain que la CNIL prit le parti de faire prévaloir l'esprit du texte sur sa lettre, dans un souci de plus grande transparence. Entre la logique du secret et celle de la transparence, pour la CNIL, cette dernière devait, prévaloir. Mais la doctrine majoritaire devait plutôt saluer cette initiative et la juger propre à concilier les couples antagoniques sécurité/secret et liberté/transparence¹⁶⁵. Cependant, le Conseil d'État devait adopter une interprétation exactement à l'inverse de celle défendue par la CNIL. En effet, dans un arrêt en date du 27 avril 1988, Madame Lochak¹⁶⁶, le Conseil s'est prononcé sur l'interprétation de l'article 39 de la loi du 6 janvier 1978. Il va considérer que l'appréciation du traitement doit se faire dans son ensemble. C'est à dire que l'article 39 s'applique par rapport au traitement et non en fonction des informations qu'il contient. Par conséquent, dès lors qu'un fichier intéresse la sûreté de l'État, la défense ou la sécurité publique, il ne peut faire l'objet que d'un droit d'accès indirect. Autrement dit, la moindre information intéressant la sûreté, la défense ou la sécurité publique contenue dans un fichier était susceptible de le faire relever du droit d'accès indirect de l'article 39. Cette interprétation avait pour conséquence de faire échapper à la communication un nombre important d'informations n'ayant aucune raison d'être couvertes par le secret¹⁶⁷. Alors qu'entre la

¹⁶⁴ V., D. MARTIN, op. citée, p. 297-298 : cet auteur a une lecture originale de la délibération du 1^{er} avril 1980 sus mentionné puisqu'il va jusqu'à affirmer que « *Dès l'origine, la CNIL a indiqué qu'elle entendait ne pas appliquer l'article 39 de la loi.* »

¹⁶⁵ V. D.LOCHAK, « Secret, sécurité et liberté », in *Information et transparence administrative*, CURAPP, P.U.F, 1988, p. 65 ; J. FRAYSSINET, « Droit d'accès et de communication aux données figurant dans les fichiers des services des Renseignements généraux », *AJDA*, Jurisprudence, p. 145 : il qualifie cette position « d'équilibrée »

¹⁶⁶ CE, 27 avril 1988, Mme Lochak : Rec. CE, p. 173

¹⁶⁷ D.LOCHAK, op. citée, p. 65

logique de la transparence et celle du secret, la CNIL avait choisi celle de la transparence, le Conseil d'État devait faire le choix opposé, en faisant prévaloir la logique du secret.

§ 2 : Consécration d'un droit d'accès indirect aménagé au détriment d'un droit d'accès direct

Le droit d'accès indirect aux fichiers de police, s'il avait témoigné en son temps d'un progrès de l'État de droit sur la raison d'État, apparaît pour l'observateur contemporain comme le témoin des tensions entre les valeurs antagoniques, transparence et raison d'État. Une plus grande ouverture des fichiers de police s'imposait, mais entre la petite révolution opérée par le juge administratif (A) et la petite évolution finalement consacrée (B) la part faite au secret est encore trop belle.

A : Ouverture des fichiers de police à la société civile : l'impulsion du juge administratif

Le juge administratif a, par un formidable revirement de jurisprudence, ouvert les fichiers de police à la société civile en permettant un droit d'accès direct et une communication des informations contenues dans ces fichiers. Il marquait l'émergence de la juridictionnalisation de l'exercice du droit d'accès.

1. La jurisprudence Moon : droit d'accès direct et communicabilité des données du fichier de police

Par deux arrêts d'assemblée rendu le 6 novembre 2002¹⁶⁸, le Conseil d'État opérait un remarquable revirement de jurisprudence quant à son interprétation de l'article 39 de la loi du 6 janvier 1978. Les requérants avaient effectué une demande d'accès auprès de la CNIL aux informations les concernant contenues dans le fichier Schengen. Le droit d'accès à ce fichier est régi par l'article 109 de la Convention Schengen qui renvoie aux dispositions du droit

¹⁶⁸ Conseil d'Etat, Ass. 26 novembre 2002, Moon, obs. F. DONNAT, D. CASA, *AJDA*, 2002, Jurisprudence, p. 1337

interne relatives au droit d'accès aux fichiers¹⁶⁹. En vertu du décret du 6 mai 1995 relatif au système informatique national du système Schengen, le droit d'accès à ce fichier s'exerce donc auprès de la CNIL dans les conditions définies à l'article 39 de la loi du 6 janvier 1978. Dans cette espèce, la CNIL, après avoir réalisé les investigations nécessaires, avait notifié aux requérants qu'il a été procédé aux investigations. Cette réponse n'ayant pas satisfait les requérants, ils décident d'exercer un recours en excès de pouvoir à l'encontre de cette décision. Le Conseil d'État devait en premier lieu reconnaître sa compétence. Pour ce faire, il va assimiler la notification de la CNIL selon laquelle il avait été procédé aux vérifications à une décision de refus d'accès aux informations concernant le requérant qui seraient intégrées dans le système d'information Schengen. Dès lors, le Conseil d'État va admettre que le fichier Schengen qui intéresse la sûreté, la défense ou la sécurité publique peut comprendre des informations dont la communication est susceptible de compromettre les finalités du fichier et d'autres dont la communication ne mettrait pas en cause ces mêmes fins. Alors que pour les informations dont la communication serait susceptible de mettre en cause les finalités du fichier, la Commission saisie par la personne visée par les informations se bornera à indiquer qu'il a été procédé aux vérifications nécessaires, pour les informations dont la communication n'est pas susceptible de mettre en cause les finalités du fichier, il appartiendra au responsable du fichier ou à la CNIL, saisis par cette personne, de lui donner communication, avec, pour la Commission, l'accord du responsable du traitement. Le Conseil d'État opère donc par cet arrêt un double revirement de jurisprudence par rapport à sa jurisprudence traditionnelle¹⁷⁰.

En premier lieu, le Conseil d'État revient sur son interprétation du droit d'accès indirect aux traitements de souveraineté résultant de l'article 39 de la loi du 6 janvier 1978. Il revient sur sa lecture qui le conduisait à une approche globale des fichiers, pour juger qu'un fichier intéressant la sûreté de l'État, la défense et la sécurité publique peut comprendre des informations de nature différente. Mais le Conseil d'État a opéré, par cet arrêt, un revirement sur un autre point. Alors qu'il n'admettait pas que la personne concernée puisse saisir directement le responsable du fichier d'une demande de vérification, le filtre de la CNIL s'imposant en tout état de cause, il considère que peuvent être communiquées à l'intéressé,

¹⁶⁹ Art. 109 de la Convention Schengen : « Le droit de toute personne d'accéder aux données la concernant qui sont intégrées dans le système d'information Schengen s'exerce dans le respect du droit de la partie contractante auprès de qui elle le fait valoir. Si le droit national le prévoit, l'autorité nationale de contrôle prévue à l'article 114 paragraphe 1 décide si des informations sont communiquées et selon quelles modalités »

¹⁷⁰ CE, ass., 19 mai 1983, Bertin : Rec. CE, p. 173 ; CE, 27 avril 1988, Mme Lochak : Rec. CE, p. 173 ; CE, 29.12.1997, Thorel : Rec. CE, tables, p. 650 et 824

qui en fait la demande, les informations dont la communication n'est pas susceptible de mettre en cause les fins assignées au traitement. Il crée *ex nihilo* une possibilité de communication directe des informations contenues dans le fichier¹⁷¹. Il appartiendrait alors au responsable du fichier déniait le caractère communicable des informations contenues dans le fichier de renvoyer le requérant vers la CNIL qui pourrait décider du caractère communicable avec l'accord du responsable du traitement. Le Conseil d'État, par cet arrêt, adopte la même position que celle adoptée par la CNIL adoptée dans sa délibération du 1^{er} avril 1980, portant adoption d'une recommandation relative à la mise en œuvre du droit individuel d'accès aux fichiers automatisés¹⁷² à une nuance près : le Commissaire ne peut communiquer les informations contenues dans le fichier qu'avec l'accord du responsable du traitement. *In fine*, le responsable du traitement dispose d'un droit de veto. Il s'agit de la reprise du dispositif ménagé par le décret¹⁷³ relatif au fichier des renseignements généraux à une nuance près. En effet, le décret relatif aux fichiers des renseignements généraux ne prévoit qu'un droit d'accès indirect et non la possibilité, pour le requérant, de s'adresser directement au responsable du fichier. Depuis, cette jurisprudence a été confirmée à plusieurs reprises. Elle a notamment donné lieu à une intéressante application aux fichiers des renseignements généraux. En effet, dans un arrêt du 30 juillet 2003¹⁷⁴, confirmé par la suite¹⁷⁵, rendu dans une affaire Raoust, le Conseil d'État s'est penché sur une espèce où le requérant, membre de l'Eglise de scientologie, avait demandé à la CNIL l'accès aux données le concernant, contenues dans le fichier des renseignements généraux. La CNIL lui fit savoir que l'un des membres de la Commission avait procédé aux vérifications nécessaires en application de l'article 39 de la loi du 6 janvier 1978. Il contesta cette décision qui équivalait à un refus de communication des informations le concernant. Or, le décret relatif au fichier des renseignements généraux ménage des modalités spécifiques d'accès à ces fichiers. En effet, une possibilité de communication des informations est prévue lorsque les informations ont été enregistrées pour

¹⁷¹ V. F. DONNAT, D. CASA, *AJDA*, 2002, Jurisprudence, p. 1337

¹⁷² Délibération en date du 1^{er} avril 1980 portant adoption d'une recommandation relative à la mise en œuvre du droit individuel d'accès aux fichiers automatisés, 5^{ème} rapport d'activité, p. 86

¹⁷³ Décret n° 91-1051 du 14 octobre 1991 portant application aux fichiers informatisés, manuels ou mécanographiques gérés par les services des renseignements généraux des dispositions de l'article 31, alinéa 3, de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, *JO* du 15 octobre 1991

¹⁷⁴ Conseil d'Etat, 20 juillet 2003, requête n° 242812, *AJDA* n° 39, 17 novembre 2003, p. 2101 avec les conclusions du Commissaire du Gouvernement Christine Maugué ; obs. C.M., Dr. Adm., 2003, Comm. n° 244

¹⁷⁵ Conseil d'Etat, 28 avril 2004, 3 arrêts, requêtes n° 251396, n° 251397, n° 243417, inédits au Recueil Lebon

des finalités précisées par le décret¹⁷⁶ mais pour les données enregistrées au titre des autres finalités¹⁷⁷, le décret prévoit expressément que le droit d'accès s'exerce conformément aux dispositions de l'article 39 de la loi du 6 janvier 1978¹⁷⁸. En l'espèce, les informations avaient été enregistrées au titre des finalités ouvrant un droit d'accès dans les conditions définies par l'article 39 de la loi du 6 janvier 1978. La Cour administrative d'appel de Paris en avait déduit que la communication directe aux demandeurs des informations les concernant, figurant dans les fichiers des renseignements généraux ne pouvait éventuellement avoir lieu que lorsque ces informations étaient enregistrées au titre des finalités pour lesquelles le décret l'avait expressément prévu. Le Conseil d'État, en vertu de sa jurisprudence Moon¹⁷⁹, ne pouvait que considérer que des informations, concernant le requérant et recueillies au titre des finalités ouvrant un droit d'accès dans les conditions définies à l'article 39, pouvaient lui être communiquées à la condition que leur communication ne porte pas atteinte à la sûreté de l'État, la défense et la sécurité publique et annuler l'arrêt rendu par la Cour d'appel de Paris qui lui avait été déféré.

Cette jurisprudence marque les progrès de la démocratie et de la transparence de l'administration à l'égard des administrés dans un domaine où la politique criminelle est parfois plus soucieuse de son efficacité que de la préservation des libertés.

2. La juridictionnalisation de la procédure : exercice du droit d'accès sous le contrôle du juge administratif

Le droit d'accès s'exerce désormais sous le contrôle du juge administratif.

a) Le contrôle du juge sur l'exercice du droit d'accès

La jurisprudence Moon marque les progrès de l'État de droit, car le juge administratif se considère compétent pour apprécier le caractère communicable ou non communicable des informations contenues dans le fichier en tout état de cause.

Le Conseil d'État exerce sur les refus de communication opposée par la CNIL ou le Ministre concerné un contrôle entier. De plus, l'administration devra établir que la communication des informations au requérant serait dans le cas concret de nature à porter atteinte à la sûreté de

¹⁷⁶ Au titre du 2° ou du 3° de l'article 3 du décret n° 91-1051 du 14 octobre 1991

¹⁷⁷ Au titre du 1° de l'article 3 du décret n° 91-1051 du 14 octobre 1991

¹⁷⁸ Art. 7 du décret n° 91-1051 du 14 octobre 1991

¹⁷⁹ Conseil d'Etat, Ass. 26 novembre 2002, Moon

l'État, la défense et la sécurité publique. Ainsi, dans l'affaire Raoust, le Conseil d'État a considéré que la réponse qui lui avait été faite par le Ministre de l'intérieur pour justifier le refus de communication des données le concernant au requérant n'était pas de nature à justifier un tel refus. Le Ministre se contentait en effet de la seule appartenance du requérant à l'Église de scientologie, pour refuser la communication des données. La réponse du Ministre péchait par sa généralité. En effet, elle ne précisait ni des agissements imputables au requérant ou ni des informations relatives à l'Église de scientologie qui auraient été de nature à conforter ce refus de communication. Aucun des éléments soumis à l'appréciation du juge ne permettait d'établir que la décision de refus de communication des informations au requérant serait susceptible de porter atteinte à la sûreté de l'État ou à la sécurité publique.

b) Les moyens de contrôle du juge

Il convient d'examiner sur la base de quelles informations la juridiction administrative examine le caractère communicable des informations contenues dans le fichier de police.

Le juge doit-il demander à la CNIL la communication des constatations de son commissaire ? Mais comment, dès lors, respecter le principe du contradictoire sans au final donner un accès direct au requérant à ses données via la communication du dossier ?

Le Conseil d'État a opté pour une solution plus en retrait quant à ses moyens de contrôle sur les diligences de la CNIL, mais témoignant de son attachement au respect du principe du contradictoire¹⁸⁰. Alors que son commissaire du gouvernement l'invitait à enjoindre la communication des documents dont le refus constitue l'objet du litige, afin d'apprécier le caractère communicable ou non communicable des informations, ce qui aurait conduit à une entorse au principe du respect du contradictoire. Le Conseil d'État a préféré ordonner à l'administration de lui produire les éléments de nature à l'éclairer sur les pièces en cause et sur les raisons qui la pousse à les considérer comme protégées par le secret. Cette solution a l'avantage de respecter totalement le principe du contradictoire qui suppose que le juge ne dispose pas de documents auxquels n'auraient accès les parties, mais il limite le contrôle du juge sur les diligences de la CNIL¹⁸¹.

¹⁸⁰ V. C.M., obs. CE 30 juillet 2003, *Dr. Adm.* 2003, comm. 244

¹⁸¹ V. C.M., *Dr. Adm.* 2003, comm. 43

B : L'influence de la doctrine de la CNIL sur le droit d'accès aux fichiers de police

La doctrine de la CNIL, relative au droit d'accès aux informations contenues dans les fichiers de police, a conduit le pouvoir exécutif (1) puis le pouvoir législatif (2) à ménager des modalités particulières d'accès à ces fichiers, mais c'était sans compter sur la nouvelle interprétation du Conseil d'État quant au droit d'accès indirect de l'article 39 de la loi du 6 janvier 2004.

1. Influence sur le pouvoir exécutif

Sous l'impulsion de la CNIL, le pouvoir exécutif a mis en place des modalités particulières d'accès au fichier des renseignements généraux et du STIC qui correspondent à un droit d'accès indirect aménagé. Cette appellation semble s'imposer, car le droit d'accès demeure indirect dans le sens que le filtre de la CNIL s'impose en toutes occasions. Autrement dit, le requérant ne pourra pas s'adresser directement au responsable du fichier pour avoir communication des données le concernant. C'est en tous cas ce que souhaitait le pouvoir exécutif lorsqu'il concédait ces modalités d'accès aux fichiers des renseignements généraux et du STIC. C'était sans compter sur le revirement de jurisprudence du Conseil d'État dans les affaires Moon qui devait le conduire à admettre un tel droit d'accès direct. Mais lors des négociations intervenues entre la CNIL et le gouvernement, à l'occasion de l'élaboration des décrets relatifs aux fichiers des renseignements généraux et du STIC, il était déjà « révolutionnaire »¹⁸² qu'une possibilité de communication des informations soit ménagée. Nous allons examiner plus en détail les droits d'accès au fichier des renseignements généraux et au STIC.

a) Les fichiers des renseignements généraux

Le décret du 14 octobre 1991¹⁸³ est venu organiser un droit d'accès particulier en aménageant l'article 39 qui demeure applicable dans son principe¹⁸⁴. Il est prévu que lorsque des informations sont enregistrées conformément à des finalités qu'il définit, la CNIL pourra en accord avec le responsable du traitement constater que les informations ne mettent pas en

¹⁸² expression employée par Madame MOUEGIER Bérengère, juriste à la CNIL, responsable du droit d'accès indirect, lors de notre entretien téléphonique en date du 5/08/2004

¹⁸³ Décret n° 91-1051 du 14 octobre 1991

¹⁸⁴ Article 7 du décret n° 91-1051 du 14 octobre 1991

cause la sûreté de l'État, la défense ou la sécurité publique et lui communiquer les informations. Lorsque le requérant n'est pas connu du service des renseignements généraux, la CNIL peut le lui indiquer, avec l'accord du Ministère de l'Intérieur. Ce dispositif assurait une plus grande transparence tout en préservant la sécurité publique, puisque la communication ne peut, au final, intervenir qu'avec l'accord du Ministre de l'Intérieur. Ces modalités d'accès permettaient de satisfaire plus largement les besoins d'information des requérants. Elles reposent toutefois dans une large mesure sur la bonne volonté ministérielle. Il est remarquable que, ces dernières années, la CNIL ne se soit vu opposer aucun refus de communication par le Ministère de l'Intérieur¹⁸⁵. Cet état de fait pourrait s'expliquer par le caractère raisonnable des demandes de la CNIL ou, autrement dit, par son autolimitation quant aux demandes effectuées au ministère. Mais tel ne semble pas être le cas. En effet, la CNIL n'a jugé en 2003 non communicables que 11 % des dossiers des personnes fichées aux renseignements généraux, ayant fait une demande d'accès, soit 26 dossiers sur 243¹⁸⁶.

b) Le STIC

L'article 8 du décret du 5 juillet 2001¹⁸⁷ pose le principe du droit d'accès indirect en son alinéa 1, mais son alinéa 2 ménage un droit d'accès particulier. En effet, la CNIL peut constater, en accord avec le Ministère de l'Intérieur, que des informations nominatives enregistrées ne mettent pas en cause la sûreté de l'État, la défense ou la sécurité publique et qu'il y a lieu de communiquer les informations sous réserve que la procédure judiciaire soit close et après accord du procureur de la République. Mais il convient de souligner que plus de trois années après l'entrée en vigueur du décret, cette disposition n'est toujours pas appliquée¹⁸⁸. Des négociations sont actuellement en cours entre la CNIL et le Ministère de l'Intérieur. De plus, suite à l'intervention de la loi du 18 mars 2003¹⁸⁹, le gouvernement devrait présenter un nouveau projet de décret.

¹⁸⁵ CNIL, 24^{ème} rapport d'activité pour l'année 2003, p. 53

¹⁸⁶ CNIL, 24^{ème} rapport d'activité pour l'année 2003, p. 53

¹⁸⁷ Décret n° 2001-583 du 5 juillet 2001 pris pour l'application des dispositions de l'article 31, alinéa 3, de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et portant création du système de traitement des infractions constatées, *JO* du 6 juillet 2001

¹⁸⁸ CNIL, 24^{ème} rapport d'activité pour l'année 2003, p. 52

¹⁸⁹ Loi n° 2003-239

2. Influence sur le pouvoir législatif

La loi du 18 mars 2003¹⁹⁰ a modifié l'article 39 de la loi du 6 janvier 1978. Aucune modification n'a été apportée au droit d'accès en matière de fichiers de police par la loi du 6 août 2004¹⁹¹. Cet article confirme le principe, qui régnait sous l'empire de l'ancienne rédaction, selon lequel lorsque le traitement intéresse la sûreté de l'État, la défense ou la sécurité publique, le droit d'accès s'exerce par l'intermédiaire de la CNIL et qu'à l'issue des investigations le requérant n'a pas communication des données le concernant. Cependant, le nouveau texte prévoit que la CNIL peut constater, en accord avec le responsable du fichier, que la communication des données qui y sont contenues ne met pas en cause ses finalités, ce qui donnera droit au requérant d'en obtenir la communication. De plus, le nouveau texte prévoit que les actes réglementaires portant création des fichiers peuvent prévoir que les informations seront directement communiquées au requérant par le gestionnaire du fichier directement saisi. A première vue, cette rédaction semble d'inspiration plus libérale et de nature à permettre une plus grande accessibilité des fichiers de police. Mais cette loi ne renforce en aucune façon le droit d'accès des citoyens aux données les concernant, contenues dans les fichiers de police. Elle ne vient que consacrer la doctrine de la CNIL et la jurisprudence du Conseil d'État. Les droits des personnes fichées ne sont en aucune manière renforcés par l'intervention législative, qui n'est en quelque sorte que de la poudre aux yeux. En insérant dans le projet de loi initial une disposition relative au droit d'accès, dont la rédaction peut laisser penser qu'elle permettra un droit d'accès élargi par rapport au droit en vigueur, le législateur a tenté de faire croire, à qui pouvait s'y tromper, que le renforcement des droits d'accès des personnes fichées était la contrepartie nécessaire du nouvel encadrement juridique des fichiers de police, porté par le courant sécuritaire. Allons même plus loin. Il apparaît que l'intervention législative opère un recul par rapport à l'état du droit existant, tel qu'interprété par le Conseil d'État dans ses récents arrêts¹⁹². En effet, un droit d'accès direct aux données du fichier de police ne sera plus possible que si l'acte réglementaire constitutif prévoit une telle possibilité. Il apparaît donc que la porte ouverte par le Conseil d'État dans sa jurisprudence Moon a été refermée par le législateur. En effet,

¹⁹⁰ Art. 22 de la loi du 18 mars 2003

¹⁹¹ Art. 41 de la loi du 6 janvier 1978 modifiée

¹⁹² Conseil d'Etat, Ass. 26 novembre 2002, MOON, obs. F. DONNAT, D. CASA, *AJDA*, 2002, Jurisprudence, p. 1337

comme nous l'avons vu, le Conseil d'État avait admis un droit d'accès direct quant aux informations contenues dans le fichier qui ne compromettaient pas les finalités du fichier et cela en dehors même d'une telle possibilité ménagée par l'acte réglementaire portant création du traitement. L'article 41 en prévoyant que l'acte réglementaire peut prévoir un droit d'accès direct permet qu'un même traitement puisse comporter des informations relevant d'un droit d'accès direct et des informations relevant d'un droit d'accès indirect. Cependant, cette possibilité d'accès direct n'est désormais possible que si elle est ménagée par l'acte réglementaire constitutif et non plus lorsque l'acte réglementaire ne prévoit pas cette possibilité¹⁹³.

Un parallèle entre les nouvelles dispositions relatives au droit d'accès aux fichiers de police et celles relatives aux pouvoirs *a priori* de la CNIL dans l'autorisation de la création des traitements, on ne peut manquer de s'interroger sur le sort qui sera fait au droit d'accès direct aux informations contenues dans un fichier de police qui ne compromettraient pas les finalités du fichier.

La CNIL a certes influencé le législateur qui a consacré un droit d'accès indirect « aménagé »¹⁹⁴ ou « renforcé »¹⁹⁵ mais la transparence n'y a pas gagné.

Section 2 : Les conditions d'une régulation citoyenne des fichiers de police par le droit d'accès

La régulation des fichiers de police, qui repose désormais presque entièrement sur les citoyens par l'exercice du droit d'accès, n'est possible que si les citoyens disposent d'une information suffisante sur les conditions d'exercice de ce droit. Il faut au préalable qu'ils sachent qu'ils font l'objet d'un fichage (§1). Mais encore, la régulation citoyenne des fichiers de police n'est possible que si l'exercice du droit d'accès permet un contrôle réel sur les données du fichier,

¹⁹³ Cette interprétation des dispositions de la loi du 18 mars 2003 est conforme à celle de Christine Maugué, Commissaire du gouvernement, voir ses conclusions sous les arrêts RAOUST, *JCP*, 14 janvier 2004, p. 81

¹⁹⁴ expression utilisée par Madame MOUEGIER, juriste à la CNIL, responsable du droit d'accès indirect, lors de notre entretien téléphonique en date du 5/08/2004

¹⁹⁵ C. MOREL, « Droit des fichiers, droit des personnes ; Seconde partie : droit des personnes », *La Gazette du Palais*, n° 11, 11 janvier 2004, p.

ce qui suppose également un droit de rectification des mentions inexactes susceptibles de figurer dans le fichier (§2).

§ 1 : Limite au droit d'accès : sous utilisation et défaut d'information

Le droit d'accès ne peut être effectif dans la régulation des fichiers de police qu'à la condition qu'il soit exercé, ce qui suppose au préalable une information suffisante du citoyen sur les conditions de la collecte des données personnelles par la police et sur ses droits.

A : Une information insuffisante des citoyens

Une régulation citoyenne des fichiers de police n'est possible qu'à la double condition que les citoyens aient conscience et connaissance de la collecte policière de leur données personnelles par la police et de leur traitement sous forme de fichiers informatisés et d'autre part qu'ils soient informés sur leurs droits en la matière.

La loi du 6 janvier 1978, dans sa rédaction issue de la loi du 6 août 2004, prévoit en son article 32 des obligations d'information à la charge du responsable du fichier à l'égard de la personne dont les données sont collectées, que ces données aient fait l'objet d'une collecte directement auprès de la personne concernée ou non. Toutefois, les paragraphes III et IV de l'article 32 ménagent une exception générale aux obligations d'information que cet article impose aux traitements de données ayant pour objet la prévention, la recherche et la constatation ou la poursuite d'infractions pénales. Le pouvoir réglementaire, à qui il appartient de fixer les conditions de fonctionnement des fichiers de police, n'est donc pas tenu, en vertu des dispositions générales de la loi du 6 janvier 1978, de mettre en place une procédure de nature à assurer ni l'information des citoyens sur les conditions du fichage des informations par la police, ni sur leurs droits à l'égard de ces traitements d'informations par la police. Et cela même, alors qu'à l'occasion de l'examen du projet de décret relatif à la légalisation du fichier STIC, la CNIL avait demandé¹⁹⁶ au pouvoir exécutif que des mesures soient prises pour assurer l'information des personnes sur leurs droits et tout particulièrement sur leurs droits d'accès, de rectification, de mise à jour ou d'effacement des données. Il est

¹⁹⁶ V., les réserves émises dans sa délibération n° 00-064 du 19 décembre 2000 relative à un projet de décret en Conseil d'Etat portant création du « STIC » et application des dispositions du troisième alinéa de l'article 31 de la loi du 6 janvier 1978

vrai qu'aucune disposition garantissant « une information claire et précise », telle qu'exigée par la CNIL, n'est finalement présente dans le décret du 20 juillet 2000. La CNIL avait demandé que les ministères concernés, soit les ministères de la Justice et de l'Intérieur l'informent des mesures prises à cet effet. A notre connaissance, aucun effort n'a été fait en ce sens. Cependant, pour le fichier Judex, le pendant du fichier STIC mis en œuvre par la gendarmerie nationale, une procédure originale semblait avoir été mise en place par le pouvoir réglementaire. En effet, dans une délibération en date du 9 janvier 2003¹⁹⁷, la CNIL fait état du projet de décret relatif au fichier Judex. Était ainsi prévu par ce projet de décret, l'information des personnes de la collecte des informations les concernant par une mention sur le service télématique et sur le site web de la gendarmerie nationale, par un affichage dans le local d'accueil du public de la gendarmerie nationale et par une mention sur l'attestation du dépôt de plainte par la victime, ce qui devrait être de nature à lui permettre d'exercer le droit d'opposition que lui confère la loi. Ce dispositif serait de nature à apporter une information suffisante des citoyens. La CNIL l'estimait satisfaisant eu égard « à la finalité du fichier et à l'importance de la population concernée »¹⁹⁸. Mais la loi du 18 mars 2003, dans ses dispositions relatives aux fichiers de police judiciaire, n'a pas inscrit de droit à l'information des personnes figurant dans les fichiers de police judiciaire, ni ménagé de garanties particulières d'informations. Elle est même allée dans le sens opposé à celui d'une plus grande transparence ou accessibilité des règles relatives aux fichiers de police judiciaire puisque que le parti pris a été celui de la non codification des règles afférentes aux fichiers de police dans le Code de procédure pénale. C'est ainsi, que le Code de procédure pénale est silencieux sur les fichiers de police. En effet, il ne comporte des dispositions que sur le casier judiciaire, et depuis les lois du 18 juin 1998 et du 9 mars 2004 sur le FNAEG et sur le fichier dit des délinquants sexuels.

Mais à défaut d'une telle information délivrée par le responsable du fichier, la diffusion et l'aide à l'accès au droit reposent sur d'autres acteurs. La CNIL assure une telle mission mais les informations qu'elle diffuse n'apparaissent accessibles qu'à une personne déjà sensibilisée au problème de la protection des données et qui entendrait exercer son droit d'accès. Dès lors, la diffusion de l'information repose sur des acteurs non institutionnels et sur une prise de

¹⁹⁷ Délibération n° 03-001 du 9 janvier 2003 portant avis conforme sur le projet de décret en Conseil d'Etat portant création du système d'information judiciaire « JUDEX » et faisant application à ce traitement des dispositions du troisième alinéa de l'article 31 de la loi du 6 janvier 1978, CNIL, 24^{ème} Rapport, 2003, p. 299

¹⁹⁸ Délibération n° 03-001 du 9 janvier 2003, précitée, *in* CNIL, 24^{ème} Rapport, 2003, p. 304

conscience citoyenne. C'est pourquoi, les initiatives associatives¹⁹⁹, qui tendent à se multiplier, doivent être saluées. Les rapports annuels de la CNIL témoignent d'ailleurs du rôle que ces associations sont susceptibles de jouer dans la régulation des fichiers de police, car elle relève depuis plusieurs années l'influence des sites Internet et de la presse sur un certain nombre de demandes de droit d'accès indirect²⁰⁰. Mais les rapports annuels de la CNIL révèlent que le droit d'accès ne souffre pas d'une déficience de conscience et de l'action démocratique, mais bien d'un manque d'information quant à son existence même.

B : Un droit d'accès insuffisamment exercé

Alors que le droit d'accès peut être utilisé comme un outil de défense des droits et des libertés pour modifier les rapports de force avec les pouvoirs publics, ce droit tourne à vide parce qu'il n'est pas exercé car méconnu. Il est vrai que le nombre de demandes d'exercice de droit d'accès indirect adressé à la CNIL est en augmentation constante et exponentielle. Cependant, ces chiffres, lorsqu'ils sont rapportés au nombre de personnes qui figurent dans les fichiers de police paraissent ridiculement bas. Ainsi, les personnes intéressées font un usage modéré pour ne pas dire assez faible de cet outil juridique.

Depuis la création de la CNIL, 8 686 demandes de droit d'accès indirect ont donné lieu à plus de 14 500 investigations. Alors que dans ses rapports annuels des années 1980, la CNIL faisait état d'une quarantaine de demandes de droit d'accès indirect, leur nombre est passé à 243 en 1995 pour atteindre celui de 1 163 en 2003. Cette « explosion » des demandes de droit d'accès indirect, comme le relevait la CNIL dans son rapport pour l'année 2002, fait suite à l'ouverture des fichiers de police à la consultation à des fins d'enquête administrative. Ainsi, la CNIL est le plus souvent saisie suite à l'opposition par l'administration d'une décision défavorable au requérant. Cette décision peut être un refus d'embauche, un non

¹⁹⁹ Un site internet est né : il s'agit de « RenseignementsGeneraux.net » dont les instigateurs définissent la mission en ces termes : « il vise à expliquer aux gens pourquoi et comment il convient de vérifier ses fichiers policiers (français et européens), et n'est pas l'émanation des Renseignements Généraux, du gouvernement ou de la CNIL : ce devrait pourtant être le cas, mais les autorités suscitées ne se vantent guère des "droits" accordés aux citoyens en la matière. »

²⁰⁰ CNIL, 24^{ème} rapport d'activité 2003, p. 50 : « Les autres demandes (...) résultent d'articles de presse ou d'émissions télévisées sur les fichiers des renseignements généraux, de police ou encore d'informations diffusées sur des sites internet décrivant les modalités de droit d'accès aux fichiers de police. » ; CNIL, 23^{ème} Rapport, 2002, p. 29 ; CNIL, 22^{ème} Rapport 2001, p. 9

renouvellement de port d'arme ou un refus de délivrance de visa. Pourtant, en 2003, le seul fichier STIC traitait 20,55 millions de procédures, concernait 4,55 millions de personnes mises en cause et 15,67 millions de victimes²⁰¹, soit près de 35 % de la population française.

§ 2 : Les prolongements nécessaires du droit d'accès : un droit de rectification des données

Le droit d'accès est un droit qui n'a de signification qu'à travers sa finalité : celle de contrôle des données personnelles qui ont été collectées et conservées dans le fichier. Ainsi, le droit d'accès n'a de sens que s'il est prolongé d'un droit de rectifications des données. C'est pourquoi, un droit de rectification des données est consacré (A), mais ce droit apparaît illusoire en matière de fichiers de police (B).

A : Le principe de rectification des données

Le droit de rectification des données inexactes est garanti par les textes internationaux et par le droit interne.

1. Le droit international

La Convention 108 du Conseil de l'Europe dispose en son article 8 c) que « *toute personne doit pouvoir obtenir, le cas échéant, la rectification ou l'effacement des données personnelles la concernant lorsqu'elles ont été traitées en violation des dispositions de droit interne donnant effet aux principes de base énoncés dans les articles 5 et 6 de la présente Convention* ». Ces articles sont relatifs à la qualité des données et prohibent le traitement des données sensibles. Ce principe de droit de rectification est réaffirmé quant aux fichiers de police. Ainsi, la recommandation du Conseil de l'Europe, visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police²⁰², dispose, dans son article 6.3, que « *la personne concernée devrait pouvoir obtenir, le cas échéant, la rectification des données la concernant contenue dans un fichier. Les données à caractère personnel que l'exercice du droit d'accès a révélé inexactes, ou qui sont apparues excessives, inexactes, non pertinentes*

²⁰¹ C. ESTROSI, Rapport sur le projet de loi pour la sécurité intérieure n° 0508

en application des autres principes contenus dans cette recommandation, devraient être effacées ou corrigées ».

2. Le droit national

En droit interne, le droit de rectification est également consacré. Il figure à l'article 40 de la loi du 6 janvier 1978 qui dispose que « *toute personne physique (...) peut exiger du responsable du traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite* ». Cependant, en matière de fichiers de police, si le principe du droit de rectification est conservé, il s'exerce de manière spécifique.

B : Un droit de rectification illusoire en matière de fichiers de police

La rectification ou l'effacement des données s'exerce en matière de fichiers de police, par principe, par l'intermédiaire de la CNIL et par exception auprès du procureur de la République.

1. L'exercice du droit de rectification par l'intermédiaire de la CNIL

Le droit interne a mis en place un mécanisme de rectification des données inexactes enregistrées dans le fichier de police qui apparaît comme le pendant du droit d'accès indirect de l'article 41. En effet, de même que les personnes concernées ne peuvent, par principe, exercer leur droit d'accès que par l'intermédiaire de la CNIL, elles ne pourront que s'en remettre à la CNIL pour procéder aux vérifications nécessaires. Ainsi, aux termes de l'article 41 de la loi du 6 janvier 1978 modifiée, il ressort de la compétence de cette dernière de « faire procéder aux vérifications nécessaires ». Suite à la saisine de la CNIL par la personne concernée, celle-ci a le devoir de procéder aux rectifications et suppression qui s'averrent nécessaires. Le droit de rectification des données se heurte alors aux restrictions de l'article 41 de la loi qui fait obstacle, par principe, à la communication des données du fichier à l'intéressé. En effet, les intéressés, n'ayant pas connaissance du détail des informations, ne

²⁰² Recommandation n° R (87) 15 du Comité des Ministres du Conseil de l'Europe

sont pas à même de les contester. Mais surtout dans un bon nombre de cas, le commissaire chargé de procéder aux rectifications ne saura pas si les informations contenues dans le fichier sont effectivement pertinentes²⁰³. Le Commissaire ne sera en mesure, le plus souvent, que d'opérer la suppression des informations dont la collecte est illégale, car non conforme à la finalité du fichier ou celle dont la conservation n'est plus autorisée, en raison de l'encadrement des durées de conservation. Ainsi, en 2002, la CNIL relevait quant à ses investigations dans les fichiers de police judiciaire et, en particulier dans le STIC, qu'elle avait fait procéder à une rectification voire à une suppression dans 37 % des cas²⁰⁴. En 2003, seules 23 % des investigations ont donné lieu à une rectification ou à une suppression.

2 . L'exercice du droit de rectification par l'intermédiaire du procureur de la République

De même que des modalités particulières d'accès aux fichiers de police sont aménagées, un droit de rectification au bénéfice de la personne concernée par l'intermédiaire du procureur de la République a été mis en place pour le STIC et le FNAEG.

a) Le STIC

Le décret du 5 juillet 2001 relatif au STIC a ménagé un droit de rectification auprès du procureur de la République au bénéfice de la personne fichée.

Ainsi, est prévu la possibilité pour la personne fichée de s'adresser directement au procureur de la République qui a en charge le contrôle du fichier. C'est ainsi que toute personne mise en cause peut demander directement au procureur de la République, en cas de décision de non lieu, relaxe ou acquittement, de mettre à jour le fichier²⁰⁵. Cependant, aucun recours n'avait été ménagé par le décret contre la décision du procureur de la République. Sa décision apparaissait alors déterminante en la matière, sauf à admettre que le juge administratif reconnaisse sa compétence en la matière.

Mais encore, toute personne peut exiger que la qualification des faits finalement retenue par l'autorité judiciaire soit substituée à la qualification initiale enregistrée dans le fichier²⁰⁶. Cette

²⁰³ S. PREUSS-LASSINOTTE, « Les fichiers et les étrangers au cour des nouvelles politiques de sécurité », coll. Bibliothèque de droit public, tome 209, LGDJ, 2000, p. 340

²⁰⁴ CNIL, 23^{ème} Rapport, 2002, p. 30

²⁰⁵ Art. 3 alinéa 4 du décret n° 2001-583 du 5 juillet 2001

²⁰⁶ Art. 3 alinéa 3 du décret n° 2001-583 du 5 juillet 2001

disposition est remarquable, car elle ne laisse aucun pouvoir d'appréciation au procureur de la République : la substitution de qualification est de droit pour la personne qui en fait la demande.

Ce dispositif d'exercice du droit de rectification par l'intermédiaire du procureur de la République n'a pas été repris par le législateur de 2003. Il devrait être vraisemblablement repris dans les actes réglementaires qui devraient être prochainement présentés à la CNIL.

b) Le FNAEG

La loi du 18 mars 2003²⁰⁷ a mis en place un droit de rectification auprès du procureur de la République au bénéfice des personnes dont les profils génétiques sont inscrits dans le fichier national automatisé des empreintes génétiques.

Il est prévu que la personne intéressée puisse saisir le procureur de la République afin que son profil soit effacé. Il sera fait droit à sa demande lorsque la conservation n'apparaîtra plus nécessaire au regard de la finalité du fichier. Cette disposition, par sa formulation vague renvoyant à la finalité du fichier, laisse un grand pouvoir d'appréciation du procureur quant à l'opportunité de faire droit à une telle demande. Mais la loi a ménagé une voie de recours à la personne qui se verrait opposer un refus à sa demande par le procureur de la République. Ainsi, lorsque le procureur de la République ne fait pas droit à la demande, il est possible de saisir le Juge des libertés et de la détention dont la décision pourra être contestée devant le Président de la Chambre d'Instruction²⁰⁸.

L'efficacité du contrôle opéré sur les fichiers de police par l'intermédiaire de l'exercice du droit d'accès indirect ne peut que pâtir de la non communication des informations au requérant, ce qui rend difficile de vérifier leur exactitude, que ce droit soit exercé auprès de la CNIL ou auprès du procureur de la République. Il est alors possible de conclure avec Sylvie PREUSS-LASSINOTTE que le droit d'accès indirect est un « droit sans contenu »²⁰⁹.

Si le droit d'accès aux fichiers de police n'apparaît pas être de nature à permettre une régulation exigeante des fichiers de police par les citoyens, en raison de la trop grande opacité

²⁰⁷ Art. loi du 18 mars 2003 et art. 706-54 C.P.P.

²⁰⁸ Sur les détails de cette procédure : art. R. 53-13-1 et R. 53-13-2, insérés par le décret du 25 mai 2004, *JO*, 2 juin 2004

²⁰⁹ S. PREUSS-LASSINOTTE, op. citée, p. 340

qui règne en matière de fichiers de sécurité publique, il convient d'autant plus de mettre en place un contrôle judiciaire sur les fichiers de police afin de permettre une régulation judiciaire de ces fichiers.

Chapitre 2 : Vers une régulation judiciaire des fichiers de police ?

Il convient dans un premier temps d'examiner les contraintes structurelles de nature à peser sur les choix opérés par le législateur en matière de politique criminelle suivie quant aux fichiers de police (Section 1) pour, dans un deuxième temps, apprécier l'effectivité de ces contraintes, c'est à dire leur capacité à orienter la politique criminelle suivie en la matière (Section 2).

Section 1 : Les contraintes structurelles en matière de judiciarité des fichiers de police

Il convient d'examiner, dans un premier temps, les exigences constitutionnelles en matière de judiciarité des fichiers de police (§1) et, dans un deuxième temps, les exigences européennes (§2).

§ 1 : Les contraintes constitutionnelles et les exigences de judiciarité

Pour déterminer les contraintes constitutionnelles en matière de contrôle des fichiers de police (B), il convient d'examiner au préalable les fondements de la protection constitutionnelle en la matière (A).

A : Le fondement de la protection constitutionnelle

La protection constitutionnelle à l'égard des données nominatives figurant dans des fichiers automatisés se fonde sur la liberté personnelle (1) et conduit le Conseil constitutionnel à reconnaître un statut particulier à la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et libertés (2)

1. Une protection au titre de la liberté personnelle et de la vie privée

Le Conseil constitutionnel a tout d'abord fondé la protection des données personnelles à l'égard des traitements automatisés sur celle de la liberté personnelle, puis sur celle de la vie privée.

Le Conseil constitutionnel a eu l'occasion de reconnaître la valeur constitutionnelle de la protection des données personnelles en la rattachant dans un premier temps au principe de la liberté personnelle. En effet, dans sa décision du 25 juillet 1991 portant sur la loi d'approbation à l'adhésion de la France à la Convention d'application Schengen²¹⁰, le Conseil constitutionnel, saisi de la constitutionnalité des dispositions relatives au fichier Schengen, va écarter les critiques en soulignant que la Convention comporte un dispositif très important de mesures à même d'assurer le respect de la liberté personnelle en cas d'exploitation ou d'utilisation des catégories de données collectées par le système d'information Schengen. Le concept de liberté personnelle apparaît dans la doctrine du Conseil constitutionnel pour la première fois dans sa décision du 1988. La liberté personnelle est un principe à valeur constitutionnel et a été consacrée plusieurs fois par le Conseil constitutionnel.

Le Conseil constitutionnel avait hésité à distinguer directement dans la protection de la vie privée un principe constitutionnel. Pour ce faire, il s'est fondé sur son concept prétorien de liberté personnelle, issu du principe général de liberté, posé par la Déclaration des droits de l'homme et du citoyen. Alors que dans sa décision du 18 janvier 1995, le Conseil constitutionnel affirmait que la méconnaissance du droit au respect de la vie privée pouvait être de nature à porter atteinte à la liberté individuelle, ce qui semblait indiquer que la méconnaissance du droit au respect de la vie privée n'était constitutionnellement protégée qu'à raison d'une atteinte suffisamment grave pour constituer une atteinte à la liberté individuelle. Dans sa décision du 23 juillet 1999, le Conseil constitutionnel va préciser le fondement constitutionnel du droit au respect de la vie privée. Il va fonder la protection de la vie privée sur « la liberté proclamée par l'article 2 de la Déclaration de 1789 qui implique le respect de la vie privée ». Le droit au respect de la vie privée bénéficie désormais d'une protection constitutionnelle et non plus seulement par le biais de certains de ses éléments.

Décision n° 91-294 DC du 25 juillet 1991 Loi autorisant l'approbation de la convention d'application de l'accord de Schengen du 14 juin 1985 entre les gouvernements des Etats de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes.

Cela semblerait signifier que lorsque l'atteinte au droit au respect de la vie privée est d'une certaine gravité, elle relèverait de la protection constitutionnelle au titre de la liberté individuelle et qu'en deçà le droit au respect de la vie privée serait protégé via la liberté personnelle. C'est ainsi que le Conseil constitutionnel, dans toutes les affaires qui lui ont été soumises par la suite et relatives à des traitements de données nominatives, s'est fondé sur le droit au respect de la vie privée qu'implique la Déclaration des droits de l'homme et du citoyen pour examiner la constitutionnalité des dispositifs qui lui étaient déférés. En effet, dans sa décision du 13 mars 2003, qui lui a donné à examiner la conformité du dispositif de traitement automatisé de l'information par la police judiciaire, le Conseil constitutionnel a considéré « qu'il appartenait au législateur d'assurer la conciliation entre d'une part, la sauvegarde de l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la protection de principes et de droits de valeur constitutionnelle et, d'autre part, le respect de la vie privée »²¹¹ et examiné le dispositif qui lui était soumis pour s'assurer que cette conciliation avait bien été opérée au regard du respect de la vie privée. De la même manière, dans sa décision du 2 mars 2004, le Conseil constitutionnel a examiné la constitutionnalité du fichier judiciaire national automatisé des auteurs d'infractions sexuelles notamment au regard du droit au respect de la vie privée, pour considérer que le législateur n'avait pas mis en place un dispositif propre à assurer une conciliation qui n'est pas manifestement déséquilibrée entre le respect de la vie privée et la sauvegarde de l'ordre public²¹².

2. Une protection au titre de la loi du 6 janvier 1978, loi protectrice de la liberté individuelle

Dans sa décision en date du 20 janvier 1993²¹³, le Conseil constitutionnel consacrait la valeur particulière de la loi du 6 janvier 1978 informatique et libertés. En effet, le Conseil constitutionnel la qualifiait de loi protectrice des libertés individuelles. C'est ainsi que la loi est devenue une référence dans la doctrine du Conseil lors de l'examen de la conformité de

²¹¹ Décision n° 2003-467 DC du 13 mars 2003, Loi pour la sécurité intérieure, Considérant 20

²¹² Décision n° 2004-492 DC du 2 mars 2004, Loi portant adaptation de la justice aux évolutions de la criminalité, Considérant 87

²¹³ Décision n° 92 316 DC, du 20 janvier 1993, Loi relative à la prévention de la corruption et à la transparence de la vie économique et des procédures publiques : « qu'en lui confiant cette mission, le législateur n'a pas entendu déroger aux dispositions protectrices de la liberté individuelle prévues par la législation relative à l'informatique, aux fichiers et aux libertés »

dispositions nouvelles se rapportant à des fichiers informatiques. Dans plusieurs décisions²¹⁴, le respect des dispositions de la loi du 6 janvier 1978 est apparu comme conditionner la constitutionnalité des dispositions soumises à son examen. Mais c'est surtout dans sa décision du 29 décembre 1998 que le Conseil confirmait la position de la loi du 6 janvier 1978. Ainsi, à propos de dispositions qui autorisaient la direction générale des impôts et d'autres administrations financières à collecter, conserver et échanger avec d'autres administrations de même nature le numéro d'identification au répertoire national²¹⁵, le Conseil constitutionnel subordonnait la constitutionnalité des dispositions en cause au fait que « le législateur n'ait pas entendu déroger aux dispositions protectrices de la liberté individuelle et de la vie privée établies par la législation relative à l'informatique, aux fichiers et aux libertés »²¹⁶. Dans sa décision en date du 13 mars 2003, le Conseil se penchant sur la conformité de dispositions relatives à des fichiers de police au regard de la Constitution, reconnaissait leur conformité à la Constitution, au prix de la réserve d'interprétation selon laquelle « il ressortait des travaux parlementaires que le législateur n'avait pas entendu écarter les dispositions de la loi du 6 janvier 1978 ». Ainsi, le Conseil constitutionnel subordonne la constitutionnalité de la loi au respect des dispositions législatives. Pour autant, la loi informatique et libertés n'a pas en soi valeur constitutionnelle et le législateur a tout loisir pour la compléter, la modifier, l'actualiser ou supprimer des dispositions, comme l'a expressément rappelé le Conseil constitutionnel dans sa décision en date du 29 juillet 2004 relative à la loi sur la protection des personnes physiques à l'égard des traitements de données à caractère personnel, modifiant la loi du 6 janvier 1978²¹⁷. Pour autant, la loi informatique et libertés comporte des dispositions qui fondent une protection constitutionnelle. Mais le Conseil constitutionnel s'est abstenu depuis 1998 de qualifier la loi informatique et liberté de protectrice de la liberté individuelle.

²¹⁴ Décision n° 93-325 du 13 août 1993, Loi relative à la maîtrise de l'immigration et aux conditions d'entrée, d'accueil et de séjour des étrangers en France ; Décision n° 97-389 DC, 22 avril 1997, Loi portant diverses dispositions relatives à l'immigration ; Décision n° 98-405 DC du 29 décembre 1998, Loi de finances pour 1999

²¹⁵ N.I.R ou numéro de sécurité sociale

²¹⁶ Décision n° 98-405 DC du 29 décembre 1998, Loi de finances pour 1999

²¹⁷ Décision n° 2004-499 DC du 29 juillet 2004, Loi relative la protection des personnes physiques à l'égard des traitements de données à caractère personnel, Considérant 3 : « il est à tout moment loisible au législateur, statuant dans le domaine de sa compétence, de modifier des textes antérieures ou d'abroger ceux ci en leur substituant, le cas échéant, d'autres dispositions, dès lors que, ce faisant, il ne prive pas de garanties légales des exigences constitutionnelles »

B : Les conséquences du fondement de la protection

Le Conseil constitutionnel a opté pour une protection des personnes à l'égard des traitements de données automatisées, fondée sur la liberté personnelle et le droit au respect de la vie privée qui en dérive plutôt que de la fonder sur la liberté individuelle de l'article 66 alinéa 2 de la Constitution. Cet article énonce en effet que l'autorité judiciaire est gardienne de la liberté individuelle et le Conseil constitutionnel s'était rangé à une conception large de la notion de liberté individuelle, dépassant la seule protection contre la détention arbitraire ou le droit à la sûreté et incluant la liberté d'aller et venir, l'inviolabilité du domicile, le secret des correspondances²¹⁸ ... Mais ce choix n'est pas paru anodin. En effet, en optant de fonder cette protection sur la liberté personnelle plutôt que sur la liberté individuelle, ce rattachement avait pour objet de laisser aux deux ordres de juridiction le soin de veiller au respect de ce principe. Certains auteurs y ont même vu une stratégie du Conseil constitutionnel pour soustraire à la compétence de l'ordre judiciaire la sauvegarde de la liberté personnelle. Mais il s'agirait plutôt d'accroître la protection constitutionnelle des libertés, sans pour autant en réserver la compétence exclusive à l'ordre judiciaire. Certains auteurs y ont vu plus précisément une volonté de la Haute Assemblée de ne pas remettre en cause la compétence de la CNIL et du juge administratif sur le contentieux juridictionnel de ses décisions²¹⁹. En effet, en matière de protection des données personnelles à l'égard de l'informatique, la loi a confié à une autorité administrative indépendante, non pas à l'autorité judiciaire mais à la CNIL sous le contrôle de la juridiction administrative et non pas sous le contrôle de l'autorité judiciaire le rôle prépondérant. Mais qu'importe ce rattachement si la garantie des libertés est effective ? Un commentateur de la décision du Conseil constitutionnel du 13 mars 2003, dans laquelle il examinait la constitutionnalité des fichiers de police judiciaire, n'a pas manqué de relever que cette décision témoignait de manière manifeste sa volonté d'éviter toute référence à la liberté individuelle et regrettait la référence au droit au respect de la vie privée, alors qu'étaient en cause des fichiers de police judiciaire en y voyant une « certaine privatisation du monde et des esprits et estompent cette différence fondamentale entre la privée, attribut de la personnalité mêlé de bien patrimonial, à laquelle on peut renoncer ou que l'on peut monnayer avec une liberté publique garantie par l'État de droit, « inaliénable et sacrée », elle, la liberté

²¹⁸ M. de VILLIERS, Th. S. RENOUX, Code constitutionnel, Litec, 2001, p. 568

²¹⁹ Le Conseil d'Etat est compétent en premier et dernier ressort des décisions de la CNIL

individuelle »²²⁰. Cependant, le Conseil constitutionnel assure sur ce fondement une protection des personnes à l'égard des traitements de données nominatives automatisés. Cette protection, qui se veut avant tout procédurale et non pas substantielle, passe en particulier par l'assurance du respect des dispositions protectrices de la loi de 1978 relatives à l'informatique, aux fichiers et libertés lors de la mise en œuvre de traitements automatisés par le législateur. Parmi ces garanties figure l'intervention de la CNIL *a priori* et *a posteriori*. De plus, si le Conseil constitutionnel n'impose pas en la matière l'intervention de l'autorité judiciaire, il considère la mise en place de l'intervention de cette autorité comme une garantie qui participe de la constitutionnalité du dispositif législatif. Ainsi, dans sa décision du 13 mars 2003, le Conseil constitutionnel relevait, au titre des garanties ménagées par le législateur quant aux fichiers de police judiciaire, que le traitement de l'information avait lieu sous le contrôle du procureur de la République²²¹, magistrat relevant de l'autorité judiciaire²²². Le Conseil constitutionnel insistait également sur le rôle prépondérant de ce magistrat dans la mise à jour des fichiers. De même, dans sa décision du 2 mars 2004, le Conseil constitutionnel relevait, à propos du fichier judiciaire des auteurs d'infractions sexuelles, que le législateur avait opéré une conciliation qui n'est pas manifestement déséquilibrée entre la sauvegarde de l'ordre public et le respect de la vie privée, en se fondant entre autre sur « l'attribution à l'autorité judiciaire du pouvoir d'inscription et de retrait des données nominatives »²²³. Un proche observateur²²⁴ remarquait que la constitutionnalité du dispositif avait été acquise parce que le contrôle du fichier est confié à un magistrat, le chef du service du casier judiciaire et que les informations qui y figurent résultent de décisions prises par un magistrat.

Ainsi, le Conseil constitutionnel assure une protection constitutionnelle qui le conduit à exiger la mise en place de garanties procédurales propres à garantir les personnes contre des atteintes excessives à leur droit au respect de la vie privée, mais il n'impose pas l'intervention de l'autorité judiciaire. Cette doctrine rejoint la jurisprudence européenne.

²²⁰ J. BOYER, « Fichiers de police judiciaire et normes constitutionnelles : quel ordre juridictionnel ? », *Les petites affiches*, 22 mai 2003, p. 14

²²¹ Décision n° 2003-467 DC du 13 mars 2003, Loi pour la sécurité intérieure, Considérant 22

²²² Décision n° 93-323 DC du 5 août 1993, Loi relative aux contrôles et vérifications d'identité

²²³ Décision n° 2004-492 DC du 2 mars 2004, Loi portant adaptation de la justice aux évolutions de la criminalité, Considérant 87

²²⁴ J.-E. SCHOETTL, « La constitutionnalité du fichier judiciaire national automatisé des auteurs d'infractions sexuelles », *Petites Affiches*, 26 juillet 2004, n° 248, p. 15

§ 2 : Les contraintes européennes et les exigences de judiciarité : incitation à la mise en place de garanties procédurales propres à prémunir contre les abus

La Cour incite également les États, soumis à sa juridiction, à la mise en place de garanties procédurales qui doivent être propres à prémunir contre les abus. Pour ce faire, la Cour va s'appuyer sur le contrôle qu'elle opère de la nécessité de la mesure de surveillance secrète dans une société démocratique à la poursuite d'un but légitime. Si les buts légitimes, poursuivis par les États, sont limitativement énumérés par le § 2 de la CEDH, ils laissent aux États une grande latitude quant aux buts leur permettant d'adopter des mesures de surveillance secrète. La poursuite d'un tel but légitime est d'ailleurs largement admise par la Cour. Ce sera, par exemple, la manifestation de la vérité dans le cadre d'une procédure pénale. A l'inverse, la nécessité de l'ingérence sera strictement appréciée par la Cour. En effet, le pouvoir de surveiller en secret les citoyens, qui est une caractéristique de l'État policier, n'est tolérable dans une démocratie que dans la mesure strictement nécessaire à la sauvegarde de l'intérêt public²²⁵. Dans le mécanisme protecteur contre l'arbitraire est en jeu la sauvegarde du modèle de référence, le modèle État-société libéral. Ainsi, dès l'affaire Klass, la Cour affirmait qu'elle devait se convaincre de l'existence de garanties adéquates et suffisantes contre les abus. Elle énonçait également le caractère relatif de cette appréciation, qui allait dépendre, entre autre, du type de recours offert dans l'ordre interne. Donc, la Cour va rechercher si les procédures destinées au contrôle de l'adoption et de l'application de la mesure attentatoire à la vie privée sont aptes à limiter ces mesures à ce qui est nécessaire dans une société démocratique. Les procédures de contrôle doivent respecter les valeurs d'une société démocratique, parmi lesquelles figurent la prééminence du droit qui implique un contrôle efficace de l'ingérence du pouvoir exécutif²²⁶. Il apparaît que trois types de contrôle s'avèrent nécessaires au regard de la jurisprudence de la Cour. En raison des risques que font courir le recours aux mesures de surveillance secrète pour le modèle État société démocratique, la Cour va opérer une appréciation stricte.

²²⁵ Cour EDH, KLASS c. RFA, 6 septembre 1978, requête n° 5029/71

²²⁶ Cour EDH, KLASS c. RFA, 6 septembre 1978 ; Cour EDH, LAMBERT c. France, 24 août 1998, obs. V. LEGRAND, JDI, 1999, p.230-232

A : Un contrôle en amont et lors de l'exécution de la mesure de surveillance

L'exigence de contrôle à ce stade est d'autant plus stricte que la mesure attentatoire au droit au respect de la vie privée s'exerce en secret et que ce caractère fait obstacle à ce que la personne intéressée puisse elle-même veiller au respect de ses droits. La procédure de contrôle devra respecter les valeurs des sociétés démocratiques, dont la prééminence du droit qui postule un contrôle efficace. La Cour marque sa préférence pour un contrôle de l'autorité judiciaire, le principe de judiciarité étant de nature à apporter les garanties nécessaires d'indépendance et d'impartialité. Ainsi, dans l'affaire *Kruslin*, la Cour va reconnaître que constitue une garantie le fait que les écoutes téléphoniques soient ordonnées par un juge d'Instruction, magistrat indépendant. Cette exigence de judiciarité se retrouve également dans le cadre de l'examen que fait la Cour des mesures de surveillance secrètes au regard des règles du procès équitable, ainsi des infiltrations qu'elle refuse de considérer, depuis l'affaire *Lüdi* en date du 15 juin 1992²²⁷, comme des ingérence dans la vie privée. C'est ainsi qu'elle va retenir, en matière de surveillance secrète, le caractère non équitable en se fondant, entre autre, sur le fait que la surveillance n'a pas été exercée sur autorisation et sous le contrôle de l'autorité judiciaire²²⁸.

Cependant, si la Cour marque sa préférence pour le contrôle de l'autorité judiciaire, elle admet que l'autorité de contrôle ne soit pas un juge, si elle répond à certaines exigences. Ainsi, on peut déduire du contrôle, opéré par la Cour de la commission G 10 dans l'affaire *Klass*, qu'elle exige que l'autorité de contrôle soit indépendante par rapport à l'autorité de surveillance, qu'elle soit dotée de pouvoirs et d'attributions suffisants pour exercer un contrôle efficace et permanent et qu'elle doit avoir une composition équilibrée.

B : Un contrôle *a posteriori*

La Cour européenne des droits de l'homme impose un contrôle *a posteriori* des mesures attentatoires au droit au respect de la vie privée au titre de l'article 8 de la Convention et de

²²⁷ Cour EDH, *LÜDI* c. Suisse, 15 juin 1992, n° de requête 12433/86

²²⁸ Cour EDH, *TEXEIRA DE CASTRO* c. Portugal, 9 Juin 1998, requête n° 25829/94

et plus récemment Cour EDH, *EDWARDS et LEWIS* c. RU 22 juillet 2003, n° de requête : 39647/98 et 40461/98 : la Cour relève au § 49 que l'intervention des policiers n'a pas été ordonnée et contrôlée par un magistrat

l'article 13. L'exigence de contrôle *a posteriori* de l'exécution de la mesure résulte de l'appréciation de la nécessité dans une société démocratique de la mesure, en vertu de l'article 8 mais également de l'article 13 (droit à un recours effectif en cas de violation d'un droit garanti par la convention). Dans le cadre de l'article 8 CESDH, le contrôle opéré après l'exécution de la mesure doit être un « contrôle efficace »²²⁹. Le problème qui peut apparaître est que la possibilité de contrôle *a posteriori* peut s'avérer liée à l'information ultérieure de l'intéressé de la surveillance dont il a fait l'objet. Mais la Cour, liant l'efficacité des mesures de surveillance à l'absence de leur notification ultérieure, considère que ni l'article 8, ni l'article 13 ne confèrent un droit à la notification postérieurement à l'exécution de la mesure. Dans le cadre de l'article 13, l'individu doit pouvoir contester la validité de la mesure et demander réparation devant une autorité qui n'est pas nécessairement l'autorité judiciaire, mais dont les pouvoirs et les garanties entrent en ligne de compte pour apprécier l'efficacité du contrôle. Ainsi, l'autorité de contrôle doit présenter des garanties d'indépendance²³⁰.

²²⁹ Cour EDH, LAMBERT c. France, 24 août 1998, obs. V. LEGRAND, *JDI*, 1999, p.230-232 ;

²³⁰ Cour EDH Khan c. RU 12 mai 2000 ; Amstrong c. RU, 16 juillet 2002 ; Hewiston c. RU 27 mai 2003 : dans ces affaires, la Cour examine l'indépendance de la direction de la police à laquelle une personne victime d'une surveillance policière peut se plaindre et constate qu'elle n'est pas indépendante du pouvoir exécutif car d'une part elle est tenue de prendre en considération les conseils du ministre quant à l'engagement ou l'abandon de poursuites et, d'autre part, le ministre joue un rôle important dans sa nomination, sa rémunération voire sa révocation

Section 2 : Les fichiers de police et judiciarisation

Il convient, dans un premier temps, d'examiner le rôle du Ministère public dans le contrôle des fichiers de police (Section 1), pour dans un second temps, d'observer les limites à l'efficacité de ce contrôle mais l'existence d'autres acteurs qui seraient susceptibles d'y remédier (Section 2).

§ 1 : Le rôle du Ministère public dans le contrôle des fichiers de police

Les magistrats du parquet se voient confier une responsabilité dans le contrôle des fichiers de police (A) qui tend à leur conférer le rôle central dans la mise à jour des fichiers de police, les magistrats jouant alors en quelque sorte le rôle d'une courroie de transmission entre les services de police et l'autorité judiciaire (B).

A : Une mission générale de contrôle des fichiers de police

Les fichiers de police sont soumis par principe au contrôle des magistrats du parquet (1) mais leur rôle dans l'alimentation des fichiers demeure limité (2).

1. Le principe du contrôle des fichiers de police par le parquet

Aux pouvoirs généraux conférés par le Code de procédure pénale aux magistrats du parquet sur la police judiciaire, fait écho la mission de contrôle confiée à ces mêmes magistrats sur le traitement de l'information par la police.

En effet, l'article 12 du Code de procédure pénale dispose que la police judiciaire est exercée sous la direction du procureur de la République, et l'article 13 du même code prévoit que la police judiciaire est placée dans le ressort de cour d'appel sous la surveillance du procureur général et sous le contrôle de la chambre de l'instruction. Ces dispositions ont reçu une application spécifique au traitement de l'information par la police puisque le Ministère public se voit confier une mission de contrôle générale sur le traitement de l'information par la police.

Les fichiers de police judiciaire ont été placés par l'article 21 de la loi du 18 mars 2003 « sous le contrôle du procureur de la République compétent qui peut demander qu'elles soient

effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire. ». Cet article a repris le principe du contrôle qui avait été d'ores et déjà ménagé pour le STIC par le décret du 21 juillet 2001. En effet, sous les pressions de la CNIL²³¹, à l'occasion de l'examen des projets de décret qui lui étaient soumis, afin d'obtenir son autorisation, avait été prévu que « le traitement des informations nominatives s'effectue sous le contrôle du procureur de la République territorialement compétent qui peut demander leur rectification ou leur effacement, ou que soient ajoutées certaines des informations de l'article 4 »²³², lequel article détermine les catégories d'informations nominatives enregistrées dans le fichier²³³.

Les garanties de contrôle par l'autorité judiciaire apparaissent renforcées pour le FNAEG car il est placé sous le contrôle d'un magistrat²³⁴ qui disposera d'un accès permanent au fichier et du droit de se déplacer sur le site. Ce magistrat est un magistrat du parquet hors hiérarchie, nommé pour trois ans, par arrêté du garde des sceaux²³⁵ et assisté par un comité composé de trois membres également nommés par arrêté du garde des sceaux²³⁶. Afin de mener à bien sa mission de contrôle, ce magistrat et à sa demande les membres du Comité disposeront d'un accès permanent au fichier et au lieu où il se trouve²³⁷. L'autorité gestionnaire du fichier est tenue d'adresser un rapport annuel d'activité à ce magistrat et doit lui communiquer toute information relative au fichier qu'il lui demanderait.

²³¹ V. CNIL 19^{ème} rapport d'activité 1998, p. 65

²³² Art. 3 alinéa 1 du Décret n° 2001-583 du 5 juillet 2001, *JO* du 6 juillet 2001

²³³ Art. 4 du Décret n° 2001-583 : il permet d'enregistrer des informations nominatives en opérant une distinction entre les informations susceptibles d'être mémorisées sur les personnes mises en cause et les victimes. Ainsi, concernant les personnes mises en cause figurent : l'identité ; le surnom, les alias ; la date et le lieu de naissance ; la situation familiale ; la filiation ; la nationalité ; l'adresse ; la profession ; l'état de la personne ; son signalement ; sa photographie alors que pour les victimes ne figurent ni leur signalement, ni leur photographie à moins qu'il ne s'agisse de personnes disparues et de corps non identifiés. Doivent également figurer dans le fichier les informations non nominatives qui concernent les faits objet de l'enquête, les lieux, dates de l'infraction et mode opératoires ainsi que les informations relatives aux objets, y compris celles qui sont indirectement nominatives.

²³⁴ Art. 706-54 alinéa 1 C.P.P.

²³⁵ Le premier magistrat fut désigné par arrêté du 2 avril 2001, il s'agissait de M. Denys Millet, avocat général à la cour d'appel de Paris, *J.O.* Numéro 83 du 7 Avril 2001 ; Par un arrêté du 20 juillet 2004, son successeur et les membres du comité d'experts étaient nommés, *J.O.* 178 du 3 août 2004

²³⁶ Art. R. 53-16 C.P.P

²³⁷ Art. R 53-17 C.P.P.

2. L'alimentation des fichiers : un rapport faible à l'autorité judiciaire

L'alimentation des fichiers de police repose sur une initiative policière. Cette alimentation caractérise les fichiers de police et constitue l'un des critères de distinction de ces fichiers avec les fichiers judiciaires. Cependant, cela ne signifie pas que la police bénéficie d'une totale autonomie dans cette alimentation. Se pose, dès lors, le problème du contrôle de cette initiative (a) et de la qualification des faits opérée par le policier lors de la saisie des informations (b).

a) Le contrôle de l'alimentation des fichiers de police

L'autorité judiciaire exerce un faible contrôle sur l'alimentation des fichiers, que ce soit le FNAEG ou les fichiers de police judiciaire.

A l'origine, le FNAEG s'apparentait, de par son alimentation, à un fichier judiciaire. Il est devenu, à la suite de la loi du 18 mars 2003, un fichier proprement policier. Initialement, l'autorité judiciaire avait la maîtrise de son alimentation. Depuis la loi du 18 mars 2003, si l'autorité judiciaire participe toujours à son alimentation, la police a une part de responsabilité. En effet, alors que sous l'empire de la loi du 17 juin 1998²³⁸ qui avait créé le fichier, seules les analyses des personnes définitivement condamnées pouvaient figurer dans le fichier avec une autorisation émanant de l'autorité judiciaire car était requise soit l'autorisation du procureur de la République soit celle du juge d'instruction²³⁹, peuvent désormais figurer les résultats d'analyse d'identification génétique des échantillons biologiques prélevés sur une personne à l'encontre de la quelle existe des indices graves ou concordants de commission d'une infraction visée à l'article 706-55 du Code de procédure pénale à l'initiative du seul officier de police judiciaire.

Les fichiers de police judiciaire sont alimentés en amont du procès pénal, sans aucune intervention préalable de l'autorité judiciaire. En effet, ils sont alimentés au cours des enquêtes préliminaires, de flagrance ou des investigations sur commission rogatoire²⁴⁰. La CNIL a considéré irréaliste une subordination de l'alimentation des fichiers de police à une vérification préalable des procureurs de la République. Le contrôle de l'alimentation est donc opéré par ces magistrats en aval de l'alimentation des fichiers, ce qui suppose que le magistrat

²³⁸ L. n° 98-468 du 17 juin 1998

²³⁹ Ancien Art. R. 53-10 C.P.P. dans sa rédaction issue du Décr. n° 2000-413 du 18 mai 2000

²⁴⁰ Art. 21 de la loi du 18 mars 2003

soit informé de l'enregistrement des informations nominatives. Ce système a pour inconvénient de laisser subsister des informations inexactes ou tout du moins non vérifiées, pendant une durée qui peut être longue, ce qui peut être gravement préjudiciable pour les personnes qui y sont signalées, notamment en ce qui concerne la qualification juridique des faits.

b) La qualification juridique des faits

Les fichiers de police sont alimentés dans la phase préalable du procès pénal, avant même que ne soit décidé de l'exercice de l'action publique, avant même que la certitude de l'existence de la commission d'une infraction ne soit acquise.

A ce stade, les qualifications juridiques des faits ne sont pas opérées par un magistrat mais par un policier. La qualification juridique des faits recèle pourtant une importance non négligeable. Cette importance est directement liée au fait que le fonctionnement du fichier de police est conditionné par la qualification des faits.

En effet, la qualification des faits peut, en premier lieu, conditionner l'inscription même dans le fichier des faits, puisque cette inscription n'est prévue que relativement à des infractions déterminées pour chaque fichier. C'est ainsi que pour le FNAEG, le problème de la qualification se pose avec peut-être encore plus d'importance puisque les infractions pouvant donner lieu à un enregistrement des résultats de l'analyse du matériel biologique sont déterminées de manière limitatives par l'article 706-55 du Code de procédure pénale. La compétence de l'officier de police judiciaire en la matière paraît, dès lors, problématique. Il conviendrait de soumettre cette qualification à l'examen préalable d'un magistrat.

Mais encore, la qualification juridique des faits conditionne la durée de conservation des informations nominatives et de la mise en œuvre du droit à l'oubli, puisque celle-ci doit être, par principe, modulée en fonction de la gravité de l'infraction.

Enfin, le problème de la qualification des faits est à mettre en relation avec l'ouverture de l'accès des fichiers de police à des consultations à des fins administratives. Il ne faut alors pas négliger l'aspect plus ou moins stigmatisant d'une mention dans le fichier, en fonction du degré de réprobation sociale dont jouissent les infractions. C'est ainsi que figurer dans un fichier de police comme auteur de telle infraction n'aura pas le même impact que le fait d'y figurer pour une autre. En ce sens la qualification peut avoir un impact sur l'issue d'une enquête de moralité et sur la décision qui sera finalement opposée à l'intéressé.

B : Un rôle primordial dans la mise à jour des fichiers de police

Si en principe la mise à jour du fichier relève du gestionnaire du fichier, la loi du 18 mars 2003 a conféré au procureur de la République la responsabilité d'assurer la mise à jour des informations. Les conditions de mise à jour des informations conservées dans les fichiers de police judiciaire ont été encadrées de manière suffisamment lâche pour laisser un pouvoir d'appréciation important au procureur de la République quant à son opportunité (1), mais le procureur de la République dispose d'un pouvoir d'appréciation encore plus important quant à l'opportunité d'une mise à jour du FNAEG (2).

1. Les fichiers de police judiciaire : des conditions de mise à jour peu encadrées

La loi du 18 mars 2003 a conféré au procureur de la République un rôle déterminant dans la mise à jour des informations consignées dans le fichier de police judiciaire. En effet, il lui appartient d'ordonner la mise à jour des informations. Cette mise à jour doit être opérée au regard des suites judiciaires de l'affaire. Ainsi, il appartient au procureur de la République de demander que « les données soient effacées, complétées, ou rectifiées »²⁴¹. La mise à jour des informations peut se faire selon deux modalités : elle peut consister en un ajout d'informations complémentaires ou en un effacement des informations.

a) Les conditions d'un ajout d'informations complémentaires

En cas de décision de relaxe ou d'acquiescement devenue définitive, le principe posé est l'effacement des données personnelles concernant les personnes mises en cause. Cependant, une exception est ménagée à ce principe d'effacement des données puisque le procureur de la République dispose de la faculté d'en prescrire le maintien pour des raisons liées à la finalité du fichier, auquel cas, devra tout de même figurer dans le fichier une mention des suites de la procédure. Ainsi, le dispositif retenu par le législateur s'avère moins favorable aux personnes mises en cause que celui initié par le Décret du 5 juillet 2001 relatif au STIC²⁴², obtenu suite aux pressions de la CNIL. A la différence du dispositif ménagé par la loi pour la sécurité intérieure, le décret relatif au STIC laissait moins de pouvoir d'appréciation au procureur de la

²⁴¹ Art. 21 de la loi du 18 mars 2003

²⁴² Art. 3 du décret n° 2001-583 du 5 juillet 2001

République quant à l'opportunité de la mise à jour du fichier. En effet, en cas de relaxe et d'acquiescement définitifs, l'effacement des informations était obligatoire²⁴³.

b) Les conditions d'effacement

En cas de décision de non lieu et de classement sans suite motivée par une insuffisance de charges, le principe est l'ajout de cette information complémentaire au fichier. Ce principe est applicable à toutes les décisions de non lieu, mais pas à toutes les décisions de classement sans suite. Seules les décisions de classement sans suite, motivées par une insuffisance de charges, doivent faire l'objet d'une mise à jour, c'est à dire qu'en sont exclues toutes les décisions de classement sans suite qui seraient motivées par une autre raison, comme le choix d'une alternative aux poursuites. Une exception au principe de mise à jour est ménagée dans un sens plus respectueux de la présomption d'innocence, puisque le procureur de la République peut ordonner l'effacement des données personnelles.

2. Le FNAEG : un effacement soumis au pouvoir souverain d'appréciation du procureur de la République

L'article 706-54 C.P.P. prévoit que peuvent faire l'objet d'un enregistrement dans le FNAEG les résultats des analyses effectuées au cours de l'enquête et de l'instruction sur les personnes à l'encontre desquelles sont réunis des indices graves ou concordants rendant vraisemblable qu'elles aient commis une infraction²⁴⁴. Est alors prévu l'effacement de ces empreintes lorsque leur conservation n'apparaît plus nécessaire, compte tenu de la finalité du fichier, sur instruction du procureur de la République qui peut agir d'office ou à la demande de l'intéressé²⁴⁵. La loi n'apporte pas plus de précision quant à ce qu'il faut entendre par « empreinte dont la conservation ne serait plus nécessaire compte tenu de la finalité du fichier ». Il est manifeste que la volonté du législateur était de laisser la plus grande latitude possible, le plus de pouvoir d'appréciation aux magistrats du parquet quant à l'opportunité d'un tel effacement, tout en donnant l'impression que l'effacement allait être le principe. On aurait pu s'attendre à ce que le législateur mette en place des garanties au moins similaires à celles organisées pour les fichiers de police judiciaire dans l'article 21 de cette même loi. L'absence de telles précisions dans la loi aurait peut être été de nature à fonder une censure du

²⁴³ Art. 3 alinéa 2 du décret n° 2001-583 du 5 juillet 2001

²⁴⁴ Art. 706-54 alinéa 2 C.P.P.

²⁴⁵ Art. 706-54 alinéa 2 C.P.P.

Conseil constitutionnel, mais le fichier des empreintes génétiques est resté inédit à ce niveau de la hiérarchie des normes, ce qui est assez regrettable. En effet, le Conseil constitutionnel, dans sa décision du 18 mars 2003, s'était appuyé, entre autre, sur le dispositif de mise à jour et d'effacement ménagé par la loi qui lui était déférée pour considérer que la conciliation entre le respect de la vie privée et la sauvegarde de l'ordre public, opérée par le législateur n'était pas manifestement déséquilibrée²⁴⁶. Il est vrai qu'au regard de l'examen que le Conseil constitutionnel a fait du dispositif de mise à jour, à la lumière du principe de la présomption d'innocence, on pourrait déduire que le dispositif mis en place pour le FNAEG ne porterait pas atteinte à ce principe. Toutefois, dans le cadre du FNAEG, il n'y a pas un principe d'effacement des données en cas de relaxe ou d'acquiescement à l'inverse de ce qui est prévu pour les fichiers de police judiciaire. Le législateur n'a apporté aucune précision sur les conditions d'effacement des empreintes. Il ne s'agit pas d'un principe d'effacement assorti d'une exception. On aurait pu penser que le décret d'application²⁴⁷ serait venu apporter de plus amples précisions en la matière. Or, cela n'a pas été le cas. En effet, le décret s'est borné à reprendre les dispositions de la loi²⁴⁸. Il s'agit de laisser toute latitude au magistrat du parquet quant à l'opportunité d'un tel effacement (et non pas du maintien). Le gouvernement a ainsi indiqué que les critères d'effacement des informations enregistrées au FNAEG « relèvent de l'appréciation souveraine des faits par les magistrats compétents » mais s'est engagé à donner des indications par voie de circulaire. La circulaire devrait indiquer qu'en cas de mise hors de cause d'une personne, l'effacement des informations devrait être ordonné. A l'inverse, l'effacement n'interviendrait pas « s'il apparaît dans la procédure que la personne a bien commis les faits reprochés » (n'est-ce pas à une juridiction de le décider ?) « et que la décision la concernant est fondée sur d'autres motifs que sa mise hors de cause ». Seraient visés les cas de classement en opportunité, de prescription ou de trouble mental. Mais afin de ménager le respect de la présomption d'innocence, le gouvernement a indiqué que dans les cas de relaxe, d'acquiescement, de classement sans suite ou de non lieu intervenus au bénéfice du doute, une analyse détaillée des faits devra être opérée pour apprécier si l'effacement des informations doit être opéré. A ceux qui s'interrogeraient sur les causes du silence du décret sur les modalités d'effacement des données du fichier, on serait tenter de répondre que le gouvernement n'entend pas exposer ce dispositif à la lumière qu'il mérite et préfère opérer

²⁴⁶ Considérant 22 et 27

²⁴⁷ Décret n° 2004-470 du 25 mai 2004, *JO* du 2 juin 2004

²⁴⁸ R 53-13-1 CPP

par voie de circulaire, alors même que les circulaires sont difficilement accessibles, dans l'ombre. Il est vrai que les déclarations du gouvernement sur les orientations d'une prochaine circulaire poussent le juriste à s'interroger sur la place que réserve le dispositif de mise à jour au respect des principes fondamentaux de notre procédure pénale et notamment au respect de la présomption d'innocence, présenté par l'article préliminaire du Code de procédure pénale, issu de la loi du 15 juin 2000, comme un principe directeur du procès pénal. Le dispositif qui serait ainsi mis en œuvre ne prévoit en effet nullement des mises à jour du fichier en distinguant entre mise à jour et effacement. Il semblerait pourtant, que la constitutionnalité du dispositif mis en place pour les fichiers de police judiciaire, au regard du respect dû à la présomption d'innocence, ait été acquise, notamment, au regard de la mention de la décision de relaxe et d'acquiescement dans le fichier et cela, quand bien même la conservation des informations s'averrait nécessaire au regard des finalités du fichier²⁴⁹.

§ 2 : Les limites du contrôle du Ministère public et ses relais

A : Les limites au contrôle du Ministère public sur les fichiers

Il y a deux limites au contrôle du Ministère public sur les fichiers de police. La première limite tient à des difficultés pratiques quant aux possibilités d'exercice effectif de cette mission de contrôle. La seconde limite est directement liée à la fonction même exercée par le titulaire du pouvoir de contrôle.

1. Des difficultés de mise en œuvre

Les difficultés de mise en œuvre tenant au contrôle des magistrats du parquet sur les fichiers de police sont directement liées à la surcharge de travail de ces magistrats et à des problèmes de circulation de l'information entre le monde judiciaire et le monde policier.

La surcharge de travail des magistrats est une limite pratique, mais non moins réelle, au contrôle que doivent opérer les magistrats du parquet sur les fichiers de police. Ce point n'avait pas manqué d'être soulevé par les parlementaires qui avaient conscience des risques à faire reposer la responsabilité de la mise à jour des informations sur ces magistrats alors

²⁴⁹ V., Ch. LAZERGES, D. ROUSSEAU, Commentaire de la décision du Conseil constitutionnel, *Revue du droit public*, n° 4, 2003, p. 1161

même qu'ils sont confrontés à une surcharge de travail. En effet, les parquets traitent en moyenne annuellement plus de cinq millions d'affaires, ce qui donne lieu à d'autant de mentions dans les fichiers de police et rend très difficile en pratique les possibilités d'un réel contrôle.

Mais encore, la mise à jour des fichiers de police n'est possible que si l'information circule entre les services de police et le monde judiciaire. La courroie de transmission est le procureur de la République, qui est chargé d'assurer cette liaison. Pour le fichier STIC, la circulaire d'application avait préconisé la mise en place d'un système de « fiches navettes » qui devaient servir de support à la circulation de l'information. En effet, ces fiches devaient circuler au cours de la procédure entre le parquet et les services de police. Ces fiches navettes devaient permettre d'assurer la transmission systématique des suites de la procédure au gestionnaire du fichier. La mise en œuvre de ces fiches navettes apparaît très difficilement réalisable. C'est ainsi, que le dispositif mis en place pour le STIC, après trois années de fonctionnement suite à sa légalisation, n'a pas reçu d'application concrète. Mais la circulation de l'information doit également se faire du côté des services de police vers les parquets, afin que les magistrats soient à même de pouvoir contrôler l'initiative de l'inscription et la qualification des faits. Lors des négociations relatives au STIC qui s'étaient tenues entre le gouvernement et la CNIL, cette dernière avait obtenu l'engagement qu'une copie des informations insérées dans le fichier soit adressée aux services du procureur de la République. On peut douter de la possibilité pratique, pour le procureur, de contrôler l'ensemble des faits insérés. De plus aucun dispositif de mise à jour des informations contenues dans les fichiers relatives à des procédures anciennes n'est prévu.

2. Le procureur de la République : juge et partie ?

Le contrôle du fichier est certes confié à un magistrat, mais ce magistrat ne bénéficie pas des mêmes garanties d'indépendance qu'un magistrat du siège et surtout sa position peut faire douter de l'opportunité de ce choix. En effet, il est en quelque sorte juge et partie puisqu'il est l'un des utilisateurs du fichier dans sa mission de direction de la police judiciaire²⁵⁰. Il est donc possible de craindre que le contrôle de ce magistrat du parquet soit plus guidé par un souci d'efficacité de l'action policière et de sécurité que par celui de la préservation des libertés des personnes figurant dans ces fichiers²⁵¹. En ce sens, il est douteux que le parquet puisse constituer une autorité indépendante au sens de la recommandation (R 87) et de la jurisprudence de la Cour européenne des droits de l'homme.²⁵²

B : Le rôle de la CNIL dans le contrôle de la mise en œuvre des fichiers de police

En sus du contrôle exercé par la CNIL, à l'initiative de la personne concernée, dans le cadre de l'exercice du droit d'accès indirect, la CNIL dispose de pouvoirs de contrôle *a posteriori* sur les fichiers (1) qui s'accompagnent de pouvoirs de sanctions limités quant aux fichiers de police (2).

1. Le contrôle de la mise en œuvre des fichiers de police par les investigations

La loi du 6 août 2004 a comporté d'importantes modifications touchant aux pouvoirs de la CNIL dans son contrôle du fonctionnement des fichiers. Les pouvoirs concernant le contrôle de la mise en œuvre des traitements par les investigations sont précisés et renforcés.

La CNIL disposait déjà, en vertu de la loi du 6 janvier 1978, d'un pouvoir de contrôle sur le traitement automatisé de l'information, afin de pouvoir assurer le respect des dispositions

²⁵⁰ Art. 12 C.P.P.

²⁵¹ En ce sens, J. DANET, « Le droit pénal et la procédure pénale sous le paradigme de l'insécurité », *Archives de politique criminelle* n° 24, Pédone, 2003, p. 51

²⁵² V. C. MOREL, « Droit des fichiers, droit des personnes ; Seconde partie : droit des personnes », *La Gazette du Palais*, n° 11, 11 janvier 2004, p. 6

législatives²⁵³. Ainsi, elle disposait déjà du pouvoir de charger un de ses membres ou de ses agents, assistés, le cas échéant d'experts, de procéder, à l'égard de tout traitement, à des vérifications et de se faire communiquer tous renseignements et documents utiles à sa mission. Elle pouvait également demander aux premiers présidents de Cours d'appel, s'il s'agit de traitements du secteur privé, et aux présidents de tribunaux administratifs, s'il s'agit de traitements du secteurs publics, de déléguer un magistrat de leur ressort, éventuellement assisté d'experts, pour effectuer sous sa direction des missions d'investigation et de contrôle²⁵⁴. Ces dispositions étaient applicables à tous les traitements automatisés d'informations nominatives, sans distinction, en fonction de la nature du fichier. Ainsi, elles étaient applicables aux fichiers dits de souveraineté, parmi lesquels figurent les fichiers de police. La loi du 6 août 2004 a précisé et innové dans la mise en œuvre de ces investigations. Ainsi, les membres de la Commission, s'ils disposaient déjà d'un pouvoir de se rendre sur place pour contrôler la régularité des fichiers, ont vu l'étendue de leurs pouvoirs précisée. Ainsi, ils pourront se rendre dans les lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre du traitement, à l'exclusion des parties affectées au domicile privé, entre 6 heures et 21 heures²⁵⁵ après information préalable du procureur de la République. Ces vérifications sur place pourront être opérées malgré l'opposition du responsable des lieux, sur autorisation du président du tribunal de grande instance ou du magistrat délégué par lui dans le ressort duquel sont situés les locaux à visiter. Le magistrat statue par une ordonnance motivée. La visite s'effectue sous l'autorité et le contrôle du juge qui l'a autorisée. Dans le cadre de ce contrôle sur place, les membres de la commission pourront demander la communication de tous les documents nécessaires, en prendre copie. Ils pourront également recueillir tout renseignement ou toute justification utiles. Mais encore, ils pourront accéder aux programmes informatiques et aux données et en demander la transcription. A ces fins, la loi prévoit la possibilité de se faire assister d'un expert pour les membres de la Commission sur demande de son Président²⁵⁶.

²⁵³ Ancien Art. 6 de la loi n° 78-17 du 6 janvier 1978 chargeait la CNIL de veiller au respect des dispositions de la loi du 6 janvier 1978 et l'ancien art. 21 détaillait les pouvoirs de la Commission pour l'exercice de sa mission de contrôle.

²⁵⁴ Ancien Art. 11 de la loi n° 78-17 du 6 janvier 1978

²⁵⁵ Cet encadrement des horaires des investigations sur place s'inspire des règles applicables aux perquisitions judiciaires des domiciles privés, prévues par l'article 59 du code de procédure pénale. Les mêmes règles s'imposent à d'autres autorités administratives indépendantes.

²⁵⁶ Art. 44 paragraphe 3 alinéa 2 de la loi du 6 janvier 1978 modifiée

2. Le contrôle-sanction

Sous l'empire de la loi ancienne, la CNIL était doté d'un pouvoir d'avertissement, de destruction des données et de dénonciation des infractions au parquet dont elle avait connaissance dans l'exercice de sa mission²⁵⁷. La loi nouvelle l'a dotée de réels pouvoirs de sanction de nature à donner une réelle portée à son contrôle *a posteriori* des fichiers (a) mais cette extension des pouvoirs de la CNIL dans le contrôle *a posteriori* des fichiers ne bénéficie pas aux fichiers de police (b).

a) Un pouvoir de sanction de nature à assurer une effectivité au contrôle *a posteriori*

La Commission peut désormais prononcer des sanctions à l'encontre des contrevenants à la loi de 1978. Il peut s'agir d'une sanction pécuniaire, d'une injonction de faire cesser le traitement qui peut devenir un retrait de l'autorisation en vertu de l'article 25 de la loi.

La CNIL dispose d'un pouvoir d'avertissement et de mise en demeure dans un délai qu'elle fixe à l'égard du responsable du traitement. Si le responsable du traitement ne se conforme pas à la mise en demeure, la Commission pourra mettre en œuvre une procédure contradictoire, pouvant aboutir au prononcé d'une sanction, à moins que le traitement ne soit mis en œuvre par l'État, ce qui exclut ce pouvoir à l'égard des fichiers de police ; ou au prononcé d'une injonction, mais ce pouvoir ne lui est pas conféré pour les fichiers autres que ceux relevant de l'article 22 de la loi ou au retrait de l'autorisation accordée en vertu de l'article 25, les fichiers de police sont donc exclus de ce pouvoir d'injonction et de retrait de l'autorisation. Ces pouvoirs peuvent être mis en œuvre, dès lors que le responsable du traitement ne remplit pas ses obligations, quelles qu'elles soient.

La Commission dispose en cas d'urgence et de violation des droits et liberté, mentionnés à l'article 1, d'un pouvoir d'interruption du traitement ou de verrouillage des données à caractère personnel, traitées pour une durée de trois mois. Ces pouvoirs sont exclus pour les fichiers mentionnés à l'article 26 de la loi informatique et libertés modifiée, à savoir les traitements dits de souveraineté.

Toutes ces possibilités sont exclues à l'égard des traitements mentionnés à l'article 26 de la loi, parmi lesquels figurent les fichiers de police. En fait le seul pouvoir dont dispose la CNIL

²⁵⁷ Ancien art. 21 de la loi du 6 janvier 1978

à l'égard des traitements d'informations par la police est un pouvoir d'avertissement du Premier ministre pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée.

b) Un pouvoir d'information du Premier ministre quant aux fichiers de police

Le législateur n'a semble-t-il pas souhaité faire bénéficier les traitements de souveraineté de l'extension des pouvoirs de sanction de la CNIL. Si le projet de loi initial²⁵⁸ avait prévu que le pouvoir de sanction pécuniaire de la CNIL pourrait s'exercer quelle que soit la nature du traitement, ce pouvoir lui a été retiré en vertu d'un critère organique à l'égard de tous les traitements mis en œuvre par l'État. La CNIL ne dispose, quant aux fichiers de police, que du seul pouvoir d'information du Premier ministre. Ce pouvoir est, par ailleurs, conditionné par la réunion de deux conditions cumulatives, à savoir une condition d'urgence et une condition de violation des droits et libertés mentionnés à l'article 1 de la loi de 1978²⁵⁹. *A contrario*, lorsque ces deux conditions ne sont pas réunies, la CNIL ne dispose pas de pouvoir d'information du Premier ministre. Cela semble signifier qu'en cas de simple violation de ses obligations par le responsable du traitement, la CNIL ne pourrait user de ce nouveau pouvoir. Encore faut-il s'interroger sur la portée d'un tel pouvoir. La loi précise la finalité d'une telle information : elle devrait conduire le Premier ministre « *à prendre le cas échéant les mesures permettant de faire cesser la violation constatée* ». La loi précise encore que le Premier ministre disposera d'un délai de quinze jours pour faire connaître à la commission les suites données à cette information. Dès lors, il apparaît difficile de saisir quelle garantie particulière ce dispositif d'information du Premier ministre est de nature à apporter pour les droits et libertés. A l'origine, le projet de loi initial²⁶⁰ avait prévu que la position du Premier ministre

²⁵⁸ Projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés n° 3250 (2000-2001) de Mme LEBRANCHU, garde des Sceaux, ministre de la justice, déposé à l'Assemblée Nationale le 18 juillet 2001

²⁵⁹ Art. 1 de la loi n° 78-17 du 6 janvier 1978 dont la rédaction est restée inchangée par la loi du 6 août 2004 : « *l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit ni porter atteinte à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.* »

²⁶⁰ Projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés n° 3250 (2000-2001) de Mme LEBRANCHU, garde des Sceaux, ministre de la justice, déposé à l'Assemblée Nationale le 18 juillet 2001

devrait bénéficier de publicité, serait rendue publique. Cette garantie de publicité a été supprimée à l'initiative de la commission des lois du sénat qui a jugé que cette exigence de publicité était « *inédite et mal adaptée à des fichiers dont certains affectent la défense nationale ou la sûreté de l'État, ou répondent à des finalités de lutte contre la délinquance ou le terrorisme* »²⁶¹, mais que la « *CNIL demeurait libre d'informer le public par le biais de son rapport annuel des signalements effectués à l'intention du Premier ministre et des suites que celui-ci y a apportées.* » Pourtant, toute l'efficacité du mécanisme reposait sur la publicité de cette procédure qui aurait été de nature dissuasive pour les pouvoirs publics²⁶². En effet, l'information qu'est susceptible d'assurer la publicité du rapport annuel de la CNIL est de nature différente, car elle ne vise pas le même public que celle qui pourrait être assurée par la publicité de la réponse du Premier ministre qui serait susceptible de recevoir un plus large impact médiatique²⁶³.

Les mouvements d'ouverture des fichiers de police à la société civile et de renforcement de la relation à l'autorité judiciaire, s'ils sont d'ores et déjà perceptibles, ne sont pas, en l'état du droit actuel, de nature à permettre un contrôle exigeant des conditions de fonctionnement des fichiers de police. Dans une société libérale, ces mouvements devraient être poursuivis.

²⁶¹ A. TURK, Rapport de la commission des lois du sénat n° 218, déposé le 19 mars 2003

²⁶² J. FRAYSSINET, « Le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel : constantes et nouveautés », *Communication-Commerce Electronique*, janvier 2002, p. 13

²⁶³ V., J. Le CLAINCHE, « Les nouveaux pouvoirs « a posteriori » de la CNIL », 21 juin 2004, disponible sur www.droit-ntic.com

CONCLUSION

En matière de fichiers de police, l'équilibre entre sécurité et libertés n'apparaît pouvoir être trouvé qu'au prix d'un strict encadrement des conditions de fonctionnement de ces fichiers et d'un contrôle du respect de leur mise en œuvre

Cet équilibre, difficile à trouver et à préserver, semblait avoir été atteint par le système mis en place par la loi du 6 janvier 1978, dite informatique et libertés. Cette loi, non content de faire sortir de l'ombre les fichiers de police, faisait reposer cet équilibre sur un contrôle *a priori* des caractéristiques des fichiers et sur un contrôle *a posteriori* du respect de leurs conditions de fonctionnement. La loi confiait à une autorité administrative indépendante, la CNIL l'exercice du contrôle *a priori*. Elle a effectué en la matière un travail remarquable en œuvrant pour la soumission des fichiers de police au droit commun des fichiers par une interprétation exigeante de la loi. Ce contrôle était alors considéré comme « *la pierre de touche de l'indépendance de la CNIL et la mesure de la soumission de l'État au droit commun* »²⁶⁴. Quant à l'exercice du contrôle *a posteriori*, la loi le faisait reposer sur une initiative citoyenne et sur l'intervention de la CNIL. Cet équilibre a été profondément modifié par le récent courant législatif.

Alors que dans les années soixante dix la France s'était dotée d'un système de protection des citoyens à l'égard des fichiers de police relativement performant, une trentaine d'années après, cette protection régresse sous l'effet du courant sécuritaire.

Les fichiers de police, placés au cœur de la lutte contre la délinquance ont vu leur encadrement profondément remanié, leurs conditions d'alimentation facilitées de sorte à accroître le plus possible leur efficacité. Mais peut-être plus encore, c'est la remise en cause de l'effectivité du contrôle de la CNIL sur les fichiers de police qui semble avoir fait passer de l'autre côté le balancier entre sécurité et libertés. En effet, depuis la récente refonte de la loi informatique et libertés par la loi du 6 août 2004, l'accent est mis non plus sur le contrôle *a priori* des fichiers mais sur un contrôle *a posteriori* des conditions de fonctionnement des fichiers. Si en lui-même, un contrôle *a posteriori* ne peut se révéler aussi efficace qu'un

²⁶⁴ M. GENTOT, ancien président de la CNIL, « La CNIL et les fichiers de sécurité publique », Conférence de printemps des commissaires à la protection des données, Séville, 3 et 4 avril 2003.

contrôle *a priori*, que dire lorsqu'il n'est pas donné aux acteurs de ce contrôle les moyens juridiques mais aussi pratiques d'en faire une réelle arme face aux fichiers ?

A l'équilibre difficilement trouvé a été substitué un nouveau rapport de force contre lequel les courants mis en évidence d'ouverture à la société civile et de judiciarisation ne paraissent pas encore à même d'apporter de réelles garanties.

Dès lors, le citoyen apparaît bien démuné face au fichage et, cela d'autant plus que l'opinion publique se trouve le plus souvent favorable au développement de ces fichiers, oubliant que nous avons tous vocation à faire un jour l'objet d'une signalisation dans ces fichiers : du fait, par exemple, d'une simple déclaration de vol au commissariat.

Et si nous avons tous vocation à faire un jour l'objet d'un signalement dans un fichier de police, tous les fichiers de données nominatives, publiques ou privées, ont vocation à devenir des outils policiers, depuis que les lois du 18 mars 2003 et du 9 mars 2004 ont autorisé les OPJ à requérir de toute personne la communication des traitements de données nominatives susceptibles d'intéresser l'enquête, sans que le secret professionnel puisse leur être opposé²⁶⁵.

²⁶⁵ Art. 60-1 CPP ; 77-1-1 CPP ; 151-1-1 CPP.

BIBLIOGRAPHIE

OUVRAGES

Ouvrages généraux

ALDERSON, *Les droits de l'homme et la police*, Direction des droits de l'homme, Strzbourg, 1984, 216 p.

B. MORIN (Dir.), « Les fichiers de personnes et le droit », coll. Memento-guide Alain Bensoussan, éd. Hermes, 1991, 112 p.

CNIL, *Dix ans d'informatique et libertés*, Economica, 1988, 228 p.

A. DECOCQ, J. MONTREUIL, J. BUISSON, *Le droit de la police*, 2^{ème} édition, 1998, Litec, 868 p.

M. DELMAS-MARTY, *Les grands systèmes de politique criminelle*, coll. Thémis, PUF, 1992

M. DELMAS-MARTY, *Modèles et mouvements de politique criminelle*, Economica, 1983

M. DELMAS-MARTY, *Le flou du droit*, coll. Les voies du droit, PUF, 1986

C. DIAZ, *La police technique et scientifique*, coll. Que sais-je ?, PUF, 2000

C. DOUTREMEPUICH (Dir.), *Les empreintes génétiques en pratique judiciaire*, La Documentation française, 2001

C. ELEK, *Le casier judiciaire*, coll. Que sais-je ?, PUF, 1988

J. FOMBONNE, *La criminalistique*, coll. Que sais-je ?, PUF, 125 p.

J. FRAYSSINET, « Informatique, fichiers et libertés », éd. Litec, 1992, 229 p.

J. GAYET, *ABC de police technique et scientifique*, Payot, 1973, 263 p.

J-J. GLEIZAL, J. GATTI-DOMENACH, C. JOURNES, *La police, Le cas des démocraties occidentales*, coll. Thémis, éd. PUF, 1993, 390 p.

P. KAYSER, *La protection de la vie privée par le droit, Protection du secret de la vie privée*, Economica, 3^{ème} éd., 1995, 605 p.

C. LAZERGES, *Introduction à la politique criminelle*, l'Harmattan 2000

R.M. LOZANO, *La protection européenne des droits de l'homme dans le domaine de la biomédecine*, coll. Monde européen et international, La Doc. Fr., 2001, 461 p.

A.LUCAS, J. DEVEZE, J. FRAYSSINET, *Droit de l'informatique et de l'Internet*, coll. Thémis, éd. PUF, 2001

B. MATTHIEU, M. VERPEAUX, *Contentieux constitutionnel des droits fondamentaux*, coll. Manuel, L.G.D.J., 2001, 790 p.

R. MERLE, A. VITU, *Traité de droit criminel. Procédure pénale*, éd. Cujas, 5^{ème} édition, 2001

E. MOLINA, *La liberté de la preuve des infractions en droit français contemporain*, Presses universitaires d'Aix- Marseille, 2001

G. STEFANI, G. LEVASSEUR B. BOULOC, *Droit pénal général*, coll. Précis Dalloz, Dalloz, 17^{ème} édition, 2000

D. THOMAS (Dir.), « Les transformations de l'administration de la preuve pénale : perspectives comparées », Recherche réalisée par l'Université de Montpellier I, Equipe de Recherche sur la Politique criminelle, avec le soutien de la Mission de recherche Droit et Justice, Juin 2004, non publié, synthèse disponible sur www.gip-recherche-justice.fr

Ouvrages spécialisés

D.MARTIN, « Les fichiers de police », coll. Que sais-je ?, PUF, 1999

S. PREUSS-LASSINOTTE, « Les fichiers et les étrangers au cour des nouvelles politiques de sécurité », coll. Bibliothèque de droit public, tome 209, LGDJ, 2000, 425 p.

ARTICLES

H. ANCEL, « La preuve biologique », in « Les transformations de l'administration de la preuve pénale : perspectives comparées », G. GIUDICELLI-DELAGÉ (dir.), à paraître.

M. AUTESSERRE, « A quoi sert le casier judiciaire des mineurs ? », *Rev. Sc. Crim.*, avril/juin 2003, pp. 309-324

M. AUBOUIN, « Les empreintes génétiques », *Revue Administrative*, n°304, pp. 527-529

P. BAUDOIN, « Sécurité et technologies. Constats et problématiques », *Revue de la gendarmerie nationale*, n° 208, 3^{ème} trimestre 2003, pp. 22-28

J. BEER-GABEL, « Le contrôle de l'administration par la commission nationale de l'informatique et des libertés », *Rev. Dr. Publ.*, 1980, p. 1043

BELLIVIER, chron. lég., *RTD civ.*, 2000, pp. 648-655

M. BONNIEU, « Le juge d'instruction et les empreintes génétiques à l'aube du troisième millénaire », *Revue pén. Dt. Pen.*, n° 2, juillet 2000, pp. 203-219

B. BOULOC, « Le fichier national automatisé des empreintes génétiques (article 56 de la loi du 15 nov. 2001) », in *Chronique législative*, *Rev. Sc. Crim.*, juillet/septembre 2003, p. 591

B. BOULOC, « Régime procédural propre aux infractions de nature sexuelle », in *Chronique législative*, *Rev. Sc. Crim.*, janv. Mars 1999

J. BOYER, « Interconnexions et fichiers policiers : deux débats de notre temps », *Les Cahiers de la sécurité intérieure* n° 34, 1998, p. 140

J. BOYER, « Fichiers de police judiciaire et normes constitutionnelles : quel ordre juridictionnel ? », *Les petites affiches*, 22 mai 2003, pp. 4-19

L. CADOUX, « L'adaptation du droit aux nouvelles technologies intéressant la sécurité » *in* Sécurité et technologies, actes du comité d'experts réuni les 2 et 3 décembre 1993 à l'IHESI, coll. Etudes et recherches, IHESI

C. CHARBONNEAU, F-J. PANSIER, « Le système de traitement des infractions constatées ou les faits infractionnels à l'épreuve de la « memory STIC » », *Les petites affiches*, 24 août 2001, p. 3

C. CHARBONNEAU, F-J. PANSIER, « Présentation de la loi du 18 mars 2003 pour la sécurité intérieure : de la LSQ à la LSI », *Gaz. Pal.*, n° 85, 26 mars 2003, pp. 2-16

J. Le CLAINCHE, « Les nouveaux pouvoirs « a posteriori » de la CNIL », 21 juin 2004, disponible sur www.droit-ntic.com

J. L. CROIZIER, « Le consentement aux analyses génétiques », *in Les empreintes génétiques en pratique judiciaire*, La Documentation française, Paris, 1998, p. 49-53

C. CUTAJAR, « La loi pour la Sécurité intérieure », *Dalloz*, 2003, p. 110

J. DANET, « Le droit pénal et la procédure pénale sous le paradigme de l'insécurité », *Archives de politique criminelle* n° 24, Pédone, 2003, p. 37

O. DE SCHUTTER, « Vie privée et protection de l'Individu vis-à-vis des traitements de données à caractère personnel », *Rev. Trim. Dr. H.*, 2001, pp. - 183

M. C. DESDEVISES, « L'effacement des condamnations », *A.P.C.*, n° 12, 1990, pp. 123-144

R. DENOIX de SAINT MARC, « La transparence : pertes et limites », *Revue de la gendarmerie nationale*, n° 210, mars 2004, pp. 29-31

E. DROUARD, « Projet de loi de modification de la loi « informatique et libertés »...ou comment s'en débarrasser ? », *Expertises*, octobre 2001, pp. 337-341

O. DUFOUR, « Une méfiance grandissante à l'égard des nouvelles technologies », *Les petites affiches*, 27 juillet 2000, p. 3

R. ERRERA, « Le STIC : histoire et contenu d'une réglementation négociée », XXIIIème conférence internationale des commissaires à la protection des données. », Paris 24-26 septembre 2001, disponible sur le site de la CNIL

F. FALLETI, « L'apport de la police scientifique dans l'enquête et le procès pénal », *Revue internationale de criminologie et de police technique et scientifique*, avril-juin 2001, pp. 145-151

J. FAUVET, « La commission nationale de l'informatique et des libertés vingt ans après ... », *Mélanges Jacques Robert, Libertés, Monchrétien*, 1998, p. 111-123

J. FERRY, « L'utilisation de l'informatique par la gendarmerie, Le respect des libertés individuelles », *Revue de la gendarmerie nationale*, 1999, pp. 108-113

F. FOURETS, « La protection des données : entre transparence et confidentialité », *Revue de la gendarmerie nationale*, n° 210, 1^{er} trimestre 2004, pp. 44-48

G. FRANCOIS, « Colloque de l'Institut des hautes études sur la sécurité intérieure « Les empreintes génétiques en pratique judiciaire » », *Rev. Sc. Crim.*, oct.-déc., 1998, p. 859

J. FRAYSSINET, « La légalité de la collecte et la gestion informatisée des photographies anthropométriques et des empreintes digitales à l'occasion d'une enquête préliminaire », *D.* 1996, Jurisprudence, p. 40

J. FRAYSSINET, « Le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel : constantes et nouveautés », *Communication-Commerce Electronique*, janvier 2002, pp. 11-15

J. C. GALLOUX, « L'empreinte génétique : la preuve parfaite ? », *J.C.P.*, 1991, I, n° 3497, pp. 104-110

M. GENTOT, « La CNIL et les fichiers de sécurité publique », Conférence de printemps des commissaires à la protection des données, Séville, 3 et 4 avril 2003.

GIROD, O. RIBAU, P. MARGOT, S. WALSH, « Base de données ADN : un potentiel peu exploité de mise en relations d'évènements criminels », *Revue internationale de criminologie et de police technique et scientifique*, avril-juin 2001, pp. 131-147

B. GRAVET, « Police technique et scientifique et pratiques professionnelles », *Les Cahiers de la sécurité intérieure*, n° 21, 1995, pp. 25-34

E. HEILMANN, « En quête de l'identité », in *Science ou justice ? Les savants, l'ordre et la loi*, Série Mutations/ Sciences en société, Ed. Autrement, 1994, pp. 30-42

M. KALUSZINSKI, « Le criminel sous le regard du savant », in *Science ou justice ? Les savants, l'ordre et la loi*, Série Mutations/ Sciences en société, Ed. Autrement, 1994, pp. 74-87

X. LAMEYRE, « Du régime spécial appliqué, en France, aux auteurs d'infractions sexuelles », *Rev. Sc. Crim.*, juillet/septembre 2002, p.

C. LAZERGES, « La dérive de la procédure pénale », *Rev. Sc. Crim.*, juillet/septembre 2003, p. 645

N. LENOIR, « Informatique et libertés », *Déviante et Société*, 1984, Vol. 8, n° 3, pp. 309-313

N. LENOIR, « La loi 78-17 du 6 janvier 1978 et la Commission nationale de l'informatique et des libertés, Eléments pour un premier bilan de cinq années d'activité », *Revue Administrative*, 1983, pp. 451-466

N. LENOIR, H. MAISL, « La C.N.I.L. et le contrôle de l'administration, Premières orientations (1978-1983) », *AJDA*, 20 décembre 1983, pp. 645-652

V. LESCLOUS, C. MARSAT, « Du procès pénal et du juge à propos des empreintes génétiques », *Chronique des parquets et de l'instruction, Droit pénal*, juin 1998, pp. 5-7

Vincent LESCLOUS, « Empreintes génétiques et procédure pénale », in *Les empreintes génétiques en pratique judiciaire*, La Documentation française, Paris, 1998, p. 111-121

C. LIENHARD, « La loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure », *JCP*, 4 juin 2003, p. 1029

M. LINGLET, « La Cnil légalise le mégafichier policier Stic. Information criminelle ou infractions constatées ? », *Expertises*, janvier 1999, p. 403-404

M. LINGLET, « Le fichier informatisé Stic. Réflexions et témoignages. Un « pré-jugement » policier », *Expertises*, juin 2000, p. 166

D.LOCHAK, « Secret, sécurité et liberté », in *Information et transparence administrative*, CURAPP, P.U.F, 1988, pp. 51-69

D. LOCHAK, « Informatique, police et libertés », *Après-demain*, n° 327, oct.-nov. 1990, pp. 13-21

G. LORHO, « Les impacts du nouveau code pénal et de la loi n° 92-1336 du 16 décembre 1992 relative à son entrée en vigueur sur la gestion du casier judiciaire national », *Rev. Sc. Crim.*, juill.-sept. 1993, pp. 511-521

D.MARTIN, « La Cnil et les renseignements généraux », *Expertises*, décembre 1994, p. 427

D.MARTIN, « La directive 95/46/CE (protection des données) et sa transposition en droit français », *Gaz. Pal.*, n° 135, 15 mai 1998, pp. 16-27

D.MARTIN, « La vérité sur le fichier de recherches criminelles », *Expertises*, juillet/août 1996, pp. 264-265

G. MARX, « Technologies de sécurité et société », *Les Cahiers de la sécurité intérieure*, n° 21, 1995, pp. 9-15

N.-J. MAZEN, « Tests et empreintes génétiques : du flou juridique au pouvoir scientifique », *Petites affiches*, 14 décembre 1994, n° 149

C. MOREL, « Droit des fichiers, droit des personnes ; Seconde partie : droit des personnes », *Gaz. Pal.*, n° 11, 11 janvier 2004, pp. 2-7

H. OBERDORFF, « La liberté individuelle face aux risques des technologies de sécurité », *Mélanges Jacques Robert, Libertés*, Monchrétien, 1998, p. 177-188

H. OBERDORFF, « Comment réglementer les nouvelles technologies de sécurité ? », *Les cahiers de la sécurité intérieure*, n° 21, 1995, p. 114-119

Y. PADOVA, « Droit des fichiers, droit des personnes ; Première partie : droit des fichiers », *Gaz. Pal.*, n° 9, 9 janvier 2004, pp. 2-13

R. PELLET, « Les conditions constitutionnelles d'une réforme de la loi « informatique et libertés », *Rev. Dr. Public*, 1995, pp. 361-382

E. PICARD, « La police et le secret des données d'ordre personnel en droit français », *Rev. Sc. Crim.*, avr-juin 1993, p. 275-310

J. PRADEL, J.-L. SENON, « De la prévention et de la répression des infractions sexuelles. Commentaire de la loi n° 98-468 du 17 juin 1998 », *Rev. Pén. Dr. Pén.*, p. 208-243

M. ROBERT, « Empreintes génétiques et base de données », in *Les empreintes génétiques en pratique judiciaire*, La Documentation française, Paris, 1998, p. 127-136

Ch. ROQUE, D. VIAULT, « Informatique et casier judiciaire », *in* Informatique et droit pénal, Travaux de l'Institut des sciences criminelles de Poitiers, 1981-4, Cujas, pp. 100-121

S. ROZENFELD, « La Cnil se saisit des questions émergentes », *Expertises*, août-septembre 2001, p.1

D. SAINT DIZIER, « Fichier national automatisé des empreintes génétiques », *Méd. et Droit*, 2001, n° 53, pp. 1-5

U. SCHALCHLI, « Le STIC, Un raid technique du ministère de l'intérieur sur la justice », *Justice* n° 161, juillet 1999, p. 15

J.-E. SCHOETTL, « « La loi pour la sécurité intérieure » devant le Conseil constitutionnel », *Petites affiches*, n° 63, 28 mars 2003, pp. 4-26

C. SCHOULER, « Les nouveaux sables mouvants de la procédure pénale », *Justice* n° 178, mai 2004, p. 13-16

M.SCHWENDENER, « Les principaux fichiers de la police », *AJ Pénal* n°1 octobre 2003, p. 21

J.-F. SEUVIC, Chronique législative, *Rev. Sc. Crim.*, Avril/juin 2004, pp. 401-403

N. SOULLIERE, « Police et innovations technologiques », *Les Cahiers de la sécurité intérieure*, 34, 1998, pp. 69-90

P. TABEL, « ADN et preuve pénale », *Revue de la gendarmerie nationale*, n° 208, 3^{ème} trimestre 2003, pp. 22-28

V. TCHEN, « La loi sur la sécurité intérieure : aspects de droit administratif », *Droit administratif*, n°6, 1/06/2003, pp. 10-19

J.-P. TAK, G. A. van EIKEMA HOMMES, « Le test ADN et la procédure pénale en Europe », *Rev. Sc. Crim.*, oct.-déc., 1993, pp. 679-693

R. VANDERMEEREN, « La procédure administrative contentieuse et les secrets de l'administration », *AJDA*, Chroniques, p. 61

G. VEDEL, « Droits de l'homme, sécurité intérieure et modernisation : l'expérience du juriste », in *Les Cahiers de la sécurité intérieure*, Actes du colloque des 2 et 3 novembre 1989, IHESI, Doc. Fr., 1990, p. 132

ENCYCLOPEDIE

J. BUISSON, Crimes et délits flagrants, Art. 53 à 73 : fasc. 20, décembre 2003

J. BUISSON, Contrôles et vérifications d'identité, Art. 78-1 à 78-6 : fasc. 20, sept. 2000

R. GASSIN, Informatique et libertés, Rép. Pén. Dalloz, 1987

M. GIACOPELLI, Casier judiciaire, Rép. Pén. Dalloz, février 2003

G. LORHO, Casier judiciaire, Art. 768 à 781 : fasc. 20, nov. 1999

M. SCHWENDENER, Signalement et identification, Rép. Pén. Dalloz, octobre 2003

THESE, MEMOIRE

W. BAFFARD, « Le Système de Traitement des Infractions Constatées (STIC) et la protection des données personnelles », Mémoire de DEA Informatique et Droit, Montpellier I, 2003

A.-S. BRANGER, « Le Fichier National Automatisé d'Empreintes Génétiques », Mémoire de DEA de Sociologie du droit, Dir. N. MOLFESSIS, Paris II, 2003

M. GIRARDON, *Les fichiers en procédure pénale*, Dir. Y. MAYAUD, Mémoire de DEA de Droit pénal et sciences pénales, Paris II, 2003

D. MARTIN, *Les fichiers de police en France : dérive sécuritaire ou sécurité à la dérive ?*, thèse de doctorat, Droit privé, Paris X, 1996

H. MATSOPOULO, *Les enquêtes de police*, thèse de doctorat, Droit privé, Dir. B. BOULOC, Paris I, 1994

V. VELASCO, « *Les libertés individuelles face aux nouveaux moyens de surveillance*, thèse de doctorat », Droit public, Dir. D. LOCHAK, Paris X, 1999

RAPPORTS OFFICIELS

CNIL, *Rapports d'activité, 1978- 2003*, La documentation française

G. BRAIBANT, *Données personnelles et société de l'information*, Rapport au Premier ministre, La documentation française, 1998

M. Le FUR, *Rapport d'information sur le fichier national automatisé des empreintes génétiques*, Enregistré à la Présidence de l'Assemblée nationale le 18 décembre 2002.

Ch. CABAL, *Rapport de l'Office parlementaire d'évaluation des choix scientifiques sur les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre*, n° 0938, Enregistré à la Présidence de l'Assemblée nationale le 16 juin 2003.

ARTICLES DE PRESSE

B.ALVERGNAT, L. CADOUX, S. CANEVET, R. FORNI, O. ITEANU, L. JOINET, « Il faut sauver la loi informatique et libertés », *Le Monde*, 14 juillet 2004, p. 14

P. CEAUX, « Le Conseil d'État émet des réserves sur le projet de grand fichier de police », *Le Monde*, 16 février 1999, p. 10

P. CEAUX, « La France se dote d'un fichier national d'empreintes génétiques », *Le Monde*, 21 mars 2000, p. 10

P. CEAUX, « Le fichier illimité de la Grande-Bretagne », *Le Monde*, 21 mars 2000, p. 10

P. CEAUX, « Le gouvernement encadre le contenu et l'usage du fichier controversé de la police », *Le Monde*, 7 juillet 2001, p. 7

S. FOUCART, « Les pouvoirs de la CNIL doivent être considérablement amoindris », *Le Monde*, 14 juillet 2004, p. 6

S. FOUCART, « A l'heure du passeport biométrique, le contrôle des fichiers internationaux est plus sensible que jamais », *Le Monde*, 14 juillet 2004, p. 6

A. GARCIA, N. GUIBERT, M. Sarkozy veut créer un fichier permanent des délinquants sexuels, *Le Monde*

P. ROBERT-DIARD, Le Conseil constitutionnel valide la création de fichiers d'internautes pirates, *Le Monde*, 1^{er}/ 2 août 2004, p. 7

P. SMOLAR, Policiers et gendarmes disposent de nombreuses bases informatisées de renseignement, *Le Monde*

P. SMOLAR, Liberté et sécurité : l'histoire d'une lutte inégale, *Le Monde*, 14 juillet 2004, p 6

Libertés rognées, Éditorial, *Le Monde*, 1^{er}/ 2 août 2004, p. 12

Les associations s'inquiètent d'un affaiblissement des pouvoirs de la CNIL, *Le Monde*, 1^{er}/ 2 août 2004, p. 12

INTERNET

www.cnil.fr

www.conseilconstitutionnel.fr

www.ladocumentationfrancaise.fr

www.renseignementsgeneraux.org

www.echr.coe.int

www.assemblee-nat.fr

www.senat.fr

ENTRETIENS

Entretien téléphonique du 5/08/2004 avec Bérengère MOUEGIER, juriste à la CNIL, responsable du droit d'accès indirect

Entretien du 20/08/2004 avec Clément SCHOULER, substitut du procureur de la République à Versailles, membre du Syndicat de la Magistrature

JURISPRUDENCE

Jurisprudence nationale

Jurisprudence administrative

- CE, 19 mai 1983, Bertin : Rec. CE, p. 173
- CE, 27 avril 1988, Mme Lochak : Rec. CE, p. 173
- CE, 29. 12.1997, Thorel : Rec. CE, tables, p. 650 et 824
- CE M. Ruwayha, obs. J. FRAYSSINET, *AJDA*, 1994, Jurisprudence, p. 145

- CE, 2 juin 2003, n° 1924296, 219588 et n° 1924295, 219587, M. et Mme Moon, conclusions de Mme MAUGUEE, *JCP*, n° 3, 14 janvier 2004, pp. 81-82 ; obs. V. TCHEN, *Dr. Adm.*, 2003, comm. n° 201 ; obs. C.M, *Dr. Adm.*, comm. n° 200, octobre 2003 ; obs. C.M., *Dr. Adm.*, comm. n° 43, février 2003, p. 36 ; obs..F. DONNAT, D. CASAS, *AJDA*, Jurisprudence, 2002, p. 1337
- CE 30 juillet 2003, M. Raoust, n° 242812, obs.C.M., *Dr. Adm.*, 2003, comm. n° 244, pp. 31-32
- CE, 28 avril 2004, 3 arrêts, requêtes n° 251396, n° 251397, n° 243417, inédits au Recueil Lebon

Jurisprudence judiciaire

- TGI, Marseille, 23 mars 1995, obs. J. FRAYSSINET, « Système expérimental « Canonge », *Expertises*, juillet/août, 1995, pp. 268-270
- Cour de cassation, Crim., 30 avril 1998, obs. A. GIUDICELLI, *Rev. Sc. Crim.*, juill.-sept. 2001, 607-610
- Cour de cassation, Crim. 13 juin 1989, Derrien, *JCP*, 1990, jurisprudence, n° 21418
- Cour d'appel de Grenoble, 7 mai 1999, *JCP*, 2000. IV. 1572
- Cour de cassation, 2^{ème} civ., 18.12.2003, n° de pourvoi : 02610237, obs. P. REMILLIEUX, *AJ Pénal*, mars 2004, p. 120

Jurisprudence constitutionnelle

- Décision n° 91-294 DC du 25 juillet 1991
- Décision n° 92 316 DC du 20 janvier 1993
- Décision n° 93-323 DC du 5 août 1993
- Décision n° 93-325 du 13 août 1993
- Décision n° 97-389 DC du 22 avril 1997
- Décision n° 98-405 DC du 29 décembre 1998
- Décision n° 2003-467 DC du 13 mars 2003, obs. Ch. LAZERGES et D. ROUSSEAU, « Commentaire de la décision du Conseil constitutionnel du 13 mars 2003 », *Revue du droit public*, 2003, pp. ; obs. M. Bertrand, M. VERPEAUX, in *Petites affiches*, 18 septembre 2003, n° 187, pp. 6-13 ; obs. J.-E SCHOETTL, « La « loi pour la sécurité

intérieure » devant le Conseil constitutionnel », *Petites Affiches*, 28 mars 2003, pp. 16-22

- Décision n° 2004-492 DC du 2 mars 2004, obs. J.-E. SCHOETTL, « La constitutionnalité du fichier judiciaire national automatisé des auteurs d'infractions sexuelles », *Petites Affiches*, 26 juillet 2004, n° 248, pp. 9-16
- Décision n° 2004-492 DC du 2 mars 2004
- Décision n° 2004-499 DC du 29 juillet 2004

Jurisprudence européenne

- Cour EDH, KLASS c. RFA, 6 septembre 1978, requête n° 5029/71
- Commission EDH, 18 mars 1981, Mc Veigh, O'Neill et Evans c. RU, requêtes n° 8022/77 ; 8025/77 et 8027/77
- Cour EDH, MALONE c. RU, 2 août 1984, requête n° 8691/79
- Cour EDH, LEANDER c. Suède, 26 mars 1987, requête n° 9248181, obs. L.-E. PETTITI et F. TEITGEN, *Chronique des droits de l'homme, Rev. Sc. Crim.*, juill-sept. 1987, pp. 749-750
- Cour EDH, SCHENK c. Suisse, 12 juillet 1988, requête n° 10862/84
- Cour EDH, KRUSLIN c. France, 24 avril 1990, obs. G. COHEN-JONATHAN, RUDH 1990, p. 185-191; obs. PRADEL, *Dalloz* 1990, jurisprudence, p. 353
- Cour EDH, HUVIG c. France, 24 avril 1990, obs. G. COHEN-JONATHAN, RUDH 1990, p. 185-191
- Cour EDH, MURRAY c. RU, 28 octobre 1994, obs. F. MASSIAS, *Rev. Sc. Crim.*, 1995, avril/juin, p. 392-393
- Cour EDH, HALFORD c. RU, 27 mai 1997, requête n° 20605/92
- Cour EDH, TEXEIRA DE CASTRO c. Portugal, 9 Juin 1998, requête n° 25829/94
- Cour EDH, VALENZUELA CONTRERAS c. Espagne, 30 juillet 1998, obs. V. LEGRAND, *JDI*, 1999, p. 230-232 ; L-E PETITI, *RSC*, 1998, p. 829
- Cour EDH, LAMBERT c. France, 24 août 1998, obs. V. LEGRAND, *JDI*, 1999, p.230-232 ; L-E PETITI, *RSC*, 1998, p. 829
- Cour EDH, KOPP c. Suisse, 25 mars 1998, obs. V. LEGRAND, *JDI*, 1999, p. 230-232
- Cour EDH, ROTARU c. Roumanie, 4 mai 2000, obs. O. De Schutter, *RTDH*, 2001, pp. 145-183

- Cour EDH, KHAN c. RU, 12 mai 2000, obs. O. BACHELET, *JDI*, 2001, p. 205
- Cour EDH, PG et JH c. RU, 25 septembre 2001, n° de requête : 44787/98
- Cour EDH, ARMSTRONG c. RU, 16 juillet 2002, n° de requête : 48521/99 (disponible en langue anglaise)
- Cour EDH, ALLAN c. RU 5 novembre 2002, requête n° 48539/99
- Cour EDH, PRADO BUGALLO c. Espagne, 18 février 2003, requête n° 58496/00
- Cour EDH, HEWITSON c. RU, 27 mai 2003, n° de requête : 50015/99 (disponible en langue anglaise)
- Cour EDH, PERRY c. RU, 17 juillet 2003, n° de requête : 63737/00
- Cour EDH, EDWARDS et LEWIS c. RU 22 juillet 2003, n° de requête : 39647/98 et 40461/98
- Cour EDH, DOERGA c. Pays-Bas, 27 avril 2004, requête n° 50210/99

Table des matières

PLAN GENERAL.....	2
INTRODUCTION.....	4
PARTIE 1 : LES FICHIERS DE POLICE : DES OUTILS TOUJOURS PLUS PERFORMANTS AU SERVICE DE LA SECURITE	9
Chapitre 1 : Autonomie policière et caractéristiques des fichiers de police	10
Section 1 : Soustraction des caractéristiques des fichiers de police au pouvoir d'influence de la CNIL	11
§ 1 : La CNIL, une autorité influente sur les caractéristiques des fichiers de police	12
A : Un pouvoir d'influence grâce au système d'autorisation préalable	12
B : Un pouvoir d'influence grâce à la procédure de codécision	13
§ 2 : La CNIL, une simple autorité morale	15
A : Un contrôle préalable des caractéristiques du fichier de police par la CNIL dénué de porté contraignante	15
1. La procédure de constitution des fichiers de police, une procédure dérogatoire au droit commun des fichiers dangereux pour les libertés	15
a) Un régime d'autorisation par la CNIL pour les traitements dangereux pour les libertés	15
b) Les fichiers de police soustraits au régime d'autorisation par la CNIL	16
2. La procédure de constitution des fichiers de police, une procédure problématique au regard du droit international	18
a) Constitution des fichiers de police et droit communautaire	18
b) Constitution des fichiers de police et le droit du Conseil de l'Europe	19
B : Le contrôle préalable des caractéristiques du fichier de police par la CNIL : entre publicité et secret	20
1. La publicité des avis de la CNIL en matière de fichiers de police	20
2. Un secret critiquable au regard des exigences européennes	21
Section 2 : Les caractéristiques des fichiers de police : efficacité au détriment des libertés	22

§ 1 : Un encadrement des finalités insuffisant à circonscrire l'étendue des fichiers de police	23
A : Les fichiers de police : des finalités insuffisamment circonscrites	23
1. Le principe de finalité	23
2. Les finalités des fichiers de police	24
B : Extension des fichiers de police : vers une surveillance généralisée ?	26
1. Extension du domaine des infractions concernées par les fichiers de police	26
a) Extension du domaine des infractions pouvant justifier une mention dans le FNAEG	26
b) Extension du domaine des infractions pouvant justifier une mention dans les fichiers de police judiciaire	28
2. Des critères d'inscription élargis	28
§ 2 : Le principe de finalité insuffisant à circonscrire la mémoire et l'usage des fichiers de police	29
A : Un droit à l'oubli menacé : quelle limite à la mémoire policière ?	30
B : Un accès aux fichiers de police élargi à des fins d'enquête administrative	33

Chapitre 2 : Autonomie policière dans la collecte de l'information destinée à alimenter les fichiers de police **35**

Section 1 : Élargissement des pouvoirs de police dans la collecte des données de signalisation 36

§ 1 : Encadrement du recours aux procédés de signalisation de nature à limiter les risques d'abus au stade de la recherche d'identité 36

 A : Subsidiarité du recours aux procédés de signalisation 36

 1. Distinction entre vérification d'identité sommaire et technique 36

 2. Le recours à la vérification technique et alimentation des fichiers de police 37

 B : Accroissement encadré des pouvoirs policiers 37

 1. Extension du domaine du recours aux procédés de signalisation 37

 2. Mise en place de garanties 38

 a) Le contrôle de l'autorité judiciaire 38

 b) L'interdiction du recours à la coercition 38

 c) Une alimentation encadrée des fichiers de police 39

§ 2 : Autonomie policière restreinte dans le cadre de la vérification d'imputabilité 39

 A : Les exigences européennes de prééminence du droit 40

1. Les procédés de signalisation : des procédés attentatoires au droit au respect de la vie privée	40
2. Incitation européenne à un mouvement de prééminence du droit	42
B : Confrontation du droit national aux exigences européennes	42
1. Le recours aux procédés de signalisation : absence de base légale avant la loi du 18 mars 2003	42
a) La recherche d'une base légale formelle avant la loi du 18 mars 2003	43
b) Appréciation de la légalité par la jurisprudence interne	43
2. Légalisation du recours aux procédés de signalisation par la loi du 18 mars 2003	45
Section 2 : Élargissement des pouvoirs de police dans la collecte du matériel biologique nécessaire à l'établissement de l'empreinte génétique	47
§1 : Accroissement des possibilités de prélèvement	48
A : L'absence de pouvoir policier autonome de collecte du matériel biologique antérieurement à la loi du 18 mars 2003	48
B : Des pouvoirs policiers de prélèvement insuffisamment encadrés	49
1. Un rapport à l'autorité judiciaire déterminé par le cadre de l'enquête	50
2. Un rapport faible à la loi	51
a) Absence d'encadrement des personnes pouvant faire l'objet d'un prélèvement	51
b) La notion de « prélèvement externe », une notion floue	51
§ 2 : La problématique du consentement au prélèvement : tension entre sécurité et respect de l'intégrité physique	52
A : Incertitudes face à un refus de prélèvement	53
1 Les différents systèmes concevables	53
2 Le système français avant la loi du 9 mars 2004	54
B : La loi du 9 mars 2004, un encadrement insuffisant et critiquable	57
1. Le recours à la contrainte sur les personnes définitivement condamnées	57
a) La constitutionnalité du recours à la contrainte	57
b) Un recours à la force problématique en terme de proportionnalité	58
c) Un cumul exécution forcée / peine inconstitutionnel ?	58
2. Le prélèvement sur les simples suspects	59
a) Consentement au prélèvement et recours à la ruse	59
b) Consentement au prélèvement et incrimination	60

PARTIE 2 : VERS DE NOUVEAUX ACTEURS DE LA REGULATION DES FICHIERS DE POLICE ? 62

Chapitre 1 : Une régulation citoyenne : ouverture des fichiers de police à la société civile 63

Section 1 : Les moyens de la régulation citoyenne : le droit d'accès aux fichiers de police 64

§ 1 : Le droit d'accès aux fichiers de police : entre transparence et secret 64

A : Le droit supranational en matière de droit d'accès : de faibles contraintes structurelles quant au droit d'accès aux fichiers de police 64

1. La Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales 65

2. La Convention 108 du Conseil de l'Europe 66

3. La Recommandation R (87) sur l'utilisation de données personnelles dans le secteur de la police 67

A : Un droit d'accès dérogatoire au droit commun 67

1. Le principe d'un droit d'accès indirect 68

2. L'interprétation de l'article 39 par la CNIL : une interprétation audacieuse et controversée 69

a) Des fichiers de police soumis au droit d'accès direct 69

b) Des fichiers de police soumis au « droit d'accès mixte » 70

§ 2 : Consécration d'un droit d'accès indirect aménagé au détriment d'un droit d'accès direct 72

A : Ouverture des fichiers de police à la société civile : l'impulsion du juge administratif 72

1. La jurisprudence Moon : droit d'accès direct et communicabilité des données du fichier de police 72

2. La juridictionnalisation de la procédure : exercice du droit d'accès sous le contrôle du juge administratif 75

Le droit d'accès s'exerce désormais sous le contrôle du juge administratif. 75

a) Le contrôle du juge sur l'exercice du droit d'accès 75

b) Les moyens de contrôle du juge 76

B : L'influence de la doctrine de la CNIL sur le droit d'accès aux fichiers de police 77

1. Influence sur le pouvoir exécutif 77

a) Les fichiers des renseignements généraux 77

b) Le STIC	78
2. Influence sur le pouvoir législatif	79
Section 2 : Les conditions d'une régulation citoyenne des fichiers de police par le droit d'accès	80
§ 1 : Limite au droit d'accès : sous utilisation et défaut d'information	81
A : Une information insuffisante des citoyens	81
B : Un droit d'accès insuffisamment exercé	83
§ 2 : Les prolongements nécessaires du droit d'accès : un droit de rectification des données	84
A : Le principe de rectification des données	84
1. Le droit international	84
2. Le droit national	85
B : Un droit de rectification illusoire en matière de fichiers de police	85
1. L'exercice du droit de rectification par l'intermédiaire de la CNIL	85
2. L'exercice du droit de rectification par l'intermédiaire du procureur de la République	86
a) Le STIC	86
b) Le FNAEG	87
Chapitre 2 : Vers une régulation judiciaire des fichiers de police ?	88
Section 1 : Les contraintes structurelles en matière de judiciarité des fichiers de police	88
§ 1 : Les contraintes constitutionnelles et les exigences de judiciarité	88
A : Le fondement de la protection constitutionnelle	88
1. Une protection au titre de la liberté personnelle et de la vie privée	89
2. Une protection au titre de la loi du 6 janvier 1978, loi protectrice de la liberté individuelle	90
B : Les conséquences du fondement de la protection	92
§ 2 : Les contraintes européennes et les exigences de judiciarité : incitation à la mise en place de garanties procédurales propres à prémunir contre les abus	94
A : Un contrôle en amont et lors de l'exécution de la mesure de surveillance	95
B : Un contrôle <i>a posteriori</i>	95
Section 2 : Les fichiers de police et judiciarisation	97
§ 1 : Le rôle du Ministère public dans le contrôle des fichiers de police	97
A : Une mission générale de contrôle des fichiers de police	97

1. Le principe du contrôle des fichiers de police par le parquet	97
2. L'alimentation des fichiers : un rapport faible à l'autorité judiciaire	99
a) Le contrôle de l'alimentation des fichiers de police	99
b) La qualification juridique des faits	100
B : Un rôle primordial dans la mise à jour des fichiers de police	101
1. Les fichiers de police judiciaire : des conditions de mise à jour peu encadrées	101
a) Les conditions d'un ajout d'informations complémentaires	101
b) Les conditions d'effacement	102
2. Le FNAEG : un effacement soumis au pouvoir souverain d'appréciation du procureur de la République	102
§ 2 : Les limites du contrôle du Ministère public et ses relais	104
A : Les limites au contrôle du Ministère public sur les fichiers	104
1. Des difficultés de mise en œuvre	104
2. Le procureur de la République : juge et partie ?	106
B : Le rôle de la CNIL dans le contrôle de la mise en œuvre des fichiers de police	106
1. Le contrôle de la mise en œuvre des fichiers de police par les investigations	106
2. Le contrôle-sanction	108
a) Un pouvoir de sanction de nature à assurer une effectivité au contrôle <i>a posteriori</i>	108
b) Un pouvoir d'information du Premier ministre quant aux fichiers de police	109
CONCLUSION	111
BIBLIOGRAPHIE	113