Les fichiers de police : une catégorie juridique incertaine ?

LARBRE David
Doctorant, ATER en Droit public, Université Paris Ouest Nanterre La Défense (UPOND)
Centre de recherche CREDOF

0612659982
davidlarbre@aol.com
12 rue Roger Salengro
94270 Kremlin Bicêtre

Résumé :

Le droit français ignore la notion de fichier de police qui recouvre les instruments de recherches utilisés à des fins de prévention et répression d'infraction. Les travaux préparatoires de la loi modifiant la loi 'informatique et libertés » se sont appuyés sur le concept de traitement de souveraineté. Ce glissement sémantique n'est pas anodin. Il traduit un nouveau paradigme de la sécurité comprenant la lutte contre la criminalité, le terrorisme, l'immigration clandestine et pouvant s'étendre à la sécurisation des titres d'identité. Épousant les missions des services de police, les fichiers de police se caractérisent par leur diversité. Le remise en cause de l'existence d'une catégorie juridique propre à ces fichiers sensibles et la difficulté de saisir les contours de cette notion est en partie liée à la multiplication des finalités des fichiers dits « administratifs ». Ce partage de l'information doit favoriser une mutualisation des données au profit de la police mais également de l'administration. Ainsi, on peut donc s'interroger pour savoir si la valeur juridique du principe de finalité, pierre angulaire de la protection des données personnelles, ne conduit pas à favoriser à une dilution de la notion de fichier de police et à un affaiblissement des droits qui doivent être garanties.

French law bypasses law enforcement data basing, a concept which includes all research tools used when one's goal is to prevent and sanction infringements. Preliminary efforts made towards establishing the law which is to amend the existing data processing and freedoms law ("loi informatique et libertés") have been based on the concept of sovereignty treatment("traitement de souveraineté"). Such a semantic slip is not to be taken for granted. It translates a safety paradigm move in the direction of the fight against criminality, terrorism and illegal immigration. This shift may be extended to involve the securization of one's identification papers. By combining different police services' missions, law enforcement files are unique in their diversity. Questioning a specific legal category dedicated to these files' existence, as well as grasping what such a concept should entail, is partly related to defining the aim of "administrative" databases and supervising these files' proliferation. Sharing data in such a manner must be helpful for both the police force and administrative workers. Questions regarding such mutual benefits lead us to consider the principle of aim/finality ("finalité") and its legal authenticity. This principle should be central in any undertaking where the protection of personal data is concerned; it may cause the dilution of the ideas behind law enforcement data basing and thus weaken some rights which have to be guaranteed.

Rattacher une expression courante, telle que les fichiers de police, à une catégorie juridique n'est pas chose aisée. Les fichiers de police[1] sont définis de manière générique comme des instruments de « recherche » utilisés à des fins de prévention et répression d'infraction[2], alors qu'une catégorie juridique renvoie à un ensemble de règles qui s'applique à un objet juridique donné[3]. L'intérêt pour le juriste est d'en déterminer le régime et, en matière de libertés publiques, d'en apprécier le degré de protection. En la matière, quelque soit les incidences sur la vie privée et la protection des données personnelles, la difficulté est d'établir une classification à partir de leur finalité et des données collectées. En épousant les missions des services de police, ces fichiers se caractérisent par leur diversité tant du point de vue de leurs objets que des informations qu'ils contiennent. A cela s'ajoute le fait qu'il existe différentes règles désignant les autorités compétentes pour les créer. Aussi, ils forment une catégorie juridique hétérogène qui remet en cause la notion même de fichier de police. Dans la doctrine, on lui préfère celle de fichier de sécurité ou de traitement de souveraineté. Ce glissement sémantique n'est d'ailleurs pas anodin. *Primo*, il traduit un nouveau paradigme de la sécurité, globalisant, intégrant le concept de sécurité intérieure et comprenant notamment les questions migratoires et celles des titres d'identité. *Secundo*, il reflète la tendance actuelle à faciliter la mutualisation des données entre autorité de sécurité et administrative. Dès lors, il nous semble que la finalité et le partage de l'information contribuent à perturber l'appréhension d'une catégorie juridique propre aux fichiers de police. Plus encore, elle ne correspond pas à la doctrine traditionnelle de l'autorité de protection des données, la Commission nationale de l'informatique et des libertés qui apprécie strictement le principe de finalité en adoptant une lecture orthodoxe des textes. Mais paradoxalement, c'est peut-être de ce même principe, pierre angulaire de la protection des données personnelles, que peut émerger, par la voie prétorienne, un statut de ces traitements sensibles pouvant aboutir à une une catégorie singulière. Cette dernière devrait toutefois tenir compte du nécessaire compris qui doit exister entre sécurité et liberté.

Ainsi, cela nous conduit à considérer que l'absence d'une catégorie juridique propre aux fichiers de police (1) nécessite d'appréhender la valeur juridique du principe de finalité pour déterminer les droits garanties (2)

1. L'absence d'une catégorie juridique propre aux fichiers de police

Elle se révèle à travers les matières qu'ils recouvrent caractérisant une certaine diversité (1.1), que l'on retrouve dans le partage des compétences pour les créer (1.2).

1.1. La dimension matérielle des fichiers de police : une tendance à la diversité

La dimension matérielle des fichiers de police pourrait s'analyser à l'aune de la distinction des missions de police établie par la doctrine, mettant en lumière les notions de police judiciaire et de police administrative. La première s'exerce toujours en relation avec une infraction et se veut donc répressive, alors que la deuxième a pour objet d'éviter que l'ordre public ne soit troublé ; elle est donc préventive[4]. La finalité et les données de certains fichiers

1 Notre étude porte sur les principaux fichiers mis en œuvre par la police nationale, la gendarmerie nationale et les douanes. Corrélativement et pour des raisons de commodité, nous emploierons le terme « police » pour la police nationale, la gendarmerie nationale et les douanes.

2 Terme employé pour caractériser les fichiers de police, in, DECOCQ (A.), MONTREUIL (J.), BUISSON (J.), *Le droit de la police*, Paris, Litec, 1998 p. 731.

3 Voir BERGEL (J.-L.), *Méthodologie juridique*, PUF Thémis, Droit privé.

4 CHAPUS (R.), *Droit administratif général Tome 1*, Paris, Montchrestien, 2001, p. 737-745.

semblent révéler l'existence d'une catégorie à part entière, que l'on pourrait qualifier de « fichiers de police judiciaire », et de fichiers permettant l'accomplissement de missions de police administrative. Cependant, certains d'entre eux recouvrent ces deux dimensions ou s'inscrivent dans le cadre des missions imparties aux services de renseignements. Ainsi, la distinction entre « fichiers de police judiciaire » et « fichiers de police administrative » n'est pas toujours opérante. Au final, il s'agit de voir qu'il existe une diversité des règles relatives aux fichiers de police (1.1.1.) et que la notion peut-être envisagée de manière extensible (1.1.2.).

1.1.1. La diversité des règles relatives aux fichiers de police

L'appréhension des fichiers de police par le droit induit que l'on s'interroge sur l'existence d'un statut spécifique. Dans l'affirmative cela se traduirait par des règles propres[5] à leur création ou aux données qu'ils collectent. Or, dans la loi « informatique et libertés » originelle, les fichiers de police sont soumis à un régime juridique relevant du droit commun[6]. Ce n'est qu'à l'occasion de la transposition de la directive sur la protection des données personnelles, qu'un régime semble leur être consacré, affaiblissant notamment le contrôle relatif à leur création. Le rapport Braibant avait envisagé qu'une loi spécifique aux fichiers de police soit adopté, ce qui aurait eu pour conséquence d'éclater le *corpus juridique* ayant trait aux données personnelles. Cette option n'était pas souhaitable et c'est donc un régime oscillant entre droit commun et dérogatoire (avis simplifiée de la CNIL, droit d'accès restreint) qui a été retenue[7]. Ainsi, l'article 26 de la loi du 6 janvier 1978 modifiée [8]prévoit que sont autorisés par arrêté « les traitements (…) mis en œuvre pour le compte de l'État qui intéressent la sûreté de l'État, la défense ou la sécurité publique ou qui ont pour objet, la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ». Par ailleurs, la loi pour la sécurité intérieure de 2003 (LSI) a dans son article 21 autorisé les services de police nationale et de gendarmerie nationale à collecter des informations « afin de faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs ». La doctrine et la CNIL y voient la consécration juridique des fichiers de police judiciaire sur le modèle du Système de Traitement des Infractions Constatées (STIC)[9]. Reste que, ces règles ne s'appliquent pas lorsque l'autorité administrative met en œuvre des traitements qui sont utilisés par la police.

1.1.2. L'extension de la notion de fichier de police

Le nouveau paradigme sécuritaire nous incite à dépasser une approche « organique » et " finaliste " pour appréhender les fichiers de police à partir des finalités, des données ou des autorités pouvant y accéder. Cette perspective permet de mieux comprendre les raisons qui confèrent une nature policière au fichier AGDREF[10]. On peut également s'interroger sur le

---

5 Voir une définition de la catégorie juridique, in, LOCHAK (D.), " La *race* : une catégorie juridique ? ", *Mots*, n° 33, décembre 1992, p. 292

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

7 BRAIBANT (G.), *Rapport au premier ministre : Données personnelles et société de l'information*, La documentation française, p.69 et 70. Des pays comme l'Allemagne, l'Espagne ou les Pays-Bas ont adopter une législation spécifique aux fichiers de police judiciaire.

8 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 relative à l'informatique à l'informatique, aux fichiers et aux libertés, *Journal Officiel,* 7 août 2004, p. 14063.

9 Voir en ce sens le *Rapport d'activité de la CNIL pour l'année 2002*, Paris, La documentation française, 2003. CHARBONNEAU (C.), PANSIER (F.-J.), " Présentation de la loi du 18 mars 2003 pour la sécurité intérieure : de la LSQ à la LSI ", *Gazette du Palais*, mars 2003, p. 15. BOYER (J.), " Fichiers de police judiciaire et normes constitutionnelles : quel ordre juridictionnel ? ", *Petites Affiches*, mai 2003, n° 102, p. 3.

10 PREUSS- LAUSSINOTTE (S.), *Les fichiers et les étrangers au cœur des nouvelles politiques de sécurité,* thèse de droit public,

traitement de gestion de titres tels que la carte nationale d'identité. Mis en œuvre par un service administratif, il a pour finalité principale le suivi et la sécurisation des titres. Accessoirement, il doit « faciliter pour les services de la police nationale et de la gendarmerie nationale, l'exercice de leurs missions de recherche et de contrôle de l'identité des personnes »11. Aussi le projet Identité Nationale Électronique Sécurisée (INES), qui incorpore des éléments biométriques dans la nouvelle carte d'identité pour mieux lutter contre l'usurpation d'identité, ne peut laisser indifférent12. Le « politiste » Pierre Piazza n'hésite pas à le considérer comme un fichier de police[13].La teinture policière des traitements mis en œuvre par l'administration, résultant de la multiplication de leur finalité atteste de la plasticité de la notion. Et s'il en était besoin, elle confirme l'incertitude d'une catégorie juridique propre aux fichiers de police. Celle-ci se retrouve s'agissant des autorités compétentes pour les créer.

1.2. La compétence partagée pour la création des fichiers de police

La compétence pour créer les fichiers de police se partage entre le pouvoir réglementaire (1.2.1) que lui a délégué le pouvoir législatif (1.2.2.)

1.2.1. La compétence déléguée au pouvoir réglementaire

La création des fichiers de police n'obéit pas à des règles juridiques clairement définies. Si l'on se réfère à la loi relative à l'informatique et aux libertés, une disposition est susceptible de concerner ce type de traitement. L'article 26 de la loi précitée dispose : « Sont autorisés par arrêté les traitements (…) qui intéressent la sûreté de l'État, la défense ou la sécurité publique ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ». Moins que l'étendue couvert par les traitements de souveraineté, c'est la valeur du texte autorisant leur création qui nous renseigne ici sur l'autorité compétente. En l'occurrence, il s'agit du pouvoir réglementaire qui peut prendre soit des décrets, soit des arrêtés. En principe, seul le Premier ministre dispose du pouvoir réglementaire mais dans certains cas les ministres peuvent en disposer[14]. Il s'agit notamment de la situation où le législateur l'a prévu dans la loi, ce qui est le cas en l'espèce. En effet, l'emploi du mot « arrêté » qui est pris par le ministre et non de « décret » ne laisse pas de place au doute. Enfin, si les ministres disposent d'une telle compétence, elle ne saurait empêcher le Premier ministre d'intervenir dans ce domaine, dès lors qu'il est titulaire d'un pouvoir réglementaire en matière de police qui lui a été reconnue par le juge administratif[15]. Le législateur a « délégué » au pouvoir réglementaire la possibilité de créer des fichiers de police mais pour le Premier ministre, celui-ci dispose d'un pouvoir autonome résultant de la Constitution.

1.2.2- La compétence retrouvée du législateur

Au regard de ce qui précède on peut se demander si le législateur s'est dessaisi définitivement de sa compétence. Cela ne paraît pas être le cas. Tout d'abord, en théorie, le fait que législateur puisse accorder à une autorité certaines compétences ne saurait lui interdire de les exercer lui-même. En outre, l'article 21 de la loi relative à la sécurité

Université de Paris X- Nanterre, janvier 1998, p.117. Le fichier AGDREF doit faciliter la gestion informatique des ressortissants étrangers.

11 Voir en ce sens l'article 6-2° du décret n° 55-1397 du 22 octobre 1955 précité instituant la carte nationale d'identité.

12 FOUCART (S.), " Le fichage de tous les Français est envisagé ", *Le Monde*, 18 décembre 2003, p.25.

13 PIAZZA (P.), « Les résistances au projet INES », *Culture et conflits*, n° 64, 2006.

14 CE Section, 7 février 1936, Jamart, *Recueil Lebon,* p. 172.

15 CE 8 août 1919, Labonne, *Recueil Lebon*, p. 737.

intérieure précité a bien autorisé la création de fichiers dits de « police judiciaire » tout en précisant leur encadrement; ce qui atteste de ce que le Parlement dispose bien d'une telle compétence. Enfin, il ne faut pas oublier l'article 34 de notre Loi fondamentales aux termes duquel : « La loi fixe les garanties pour l'exercice des Libertés publiques et les règles concernant la procédure pénale ». Il recouvre la protection de la vie privée et fixe le cadre des investigations pénales ; il s'applique donc bien aux fichiers de police. A cet égard, dans le contexte sécuritaire, on peut observer que le législateur s'est appuyé sur la loi pour créer de nouveaux fichiers de police (ex : Fichier National des Empreintes Génétiques) et pour en déterminer les règles de fonctionnement. Lors de l'adoption du la LSI, son rapporteur justifiait ainsi le recours à la loi : « En raison de la nature même des informations figurant dans les fichiers de police et de gendarmerie, propice à de nombreux fantasmes, comme chacun sait, l'intervention de la loi est donc hautement souhaitable et fondée »[16]. Il est évident que cela permet, comme nous le verrons, de justifier une gestion particulière de ces traitements sensibles. Mais ce qu'il faut déjà retenir, c'est la nécessité de prendre en compte la compétence intrinsèque du législateur dans ce domaine. Celle-ci aurait pu d'ailleurs être consacrée il y a quelques mois à la faveur d'un amendement de la loi « informatique et libertés ». Des députés ont déposé une proposition de loi visant à soumettre les traitements mentionnés à l'article 26 – en clair les fichiers de police – à l'autorisation de la loi[17]. Mais cette proposition a été rejetée. La compétence exclusive du législateur serait pourtant souhaitable ; moins pour les garanties juridiques, que pour la possibilité d'avoir un débat national sur des traitements sensibles qui concernent le renseignement (fichier « Edvige » remplacée par deux traitements distincts[18]) ou l'ensemble de la population (projet INES)[19].En effet, la loi constitue à n'en pas douter l'un des symboles le plus fort de l'expression de la volonté générale et, partant, la norme pouvant légitimer la création ou la modification des fichiers de police en contournant, au besoin, le principe de finalité.

2. **Le principe de finalité comme garantie face aux fichiers de police**

La finalité d'un traitement de données peut se définir comme étant « l'objet, le but assigné à sa création et qui détermine ses fonctionnalités ainsi que les différentes opérations pouvant être effectuées dans le cadre de celui-ci ». En déterminer la portée et sa valeur permet d'en apprécier son effectivité. Toutefois, les textes juridiques ne donnent pas une définition de la finalité. Ils ne font simplement que la mentionner en exigeant qu'elle soit déterminée, nécessaire et légitime. La loi du 6 janvier 1978 modifiée synthétise les formules des textes européens de protection des données personnelles20 et énonce au 2° de son article 6 que « les données sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités ». Autant dire que l'absence de définition de la finalité ne peut conduire *de facto* à la consécration d'un principe. Surtout son absence de reconnaissance dans l'ordre juridique peut-elle garantir le respect des droits et libertés ? Reste qu'en toute hypothèse, le principe de finalité constitue la pierre angulaire de la protection des données personnelles (2.1) qui implique l'existence de certaines garanties (2.2.)

---

16 ESTROSI (C.), Rapport sur le projet de loi pour la sécurité intérieure, Assemblée nationale, n° 508, décembre 2002.

17 Proposition de loi n° 1659 relative aux fichiers de police.

18 Le fichier Edvige a été remplacée par un fichier de prévention des atteintes à la sécurité publique et un fichier relatif aux enquêtes administratives liées à la sécurité publique.

19 Elle n'est pas évidente puisque la loi « informatique et libertés » permet de fonder sur un décret les traitements qui portent sur les données biométriques nécessaires à l'authentification ou contrôle des personnes.

20 Voir en ce sens l'article 5-B de la Convention 108 du Conseil de l'Europe sur la protection des données personnelles et l'article 6-B de la directive 95/ 46 CE du Conseil et du Parlement européen.

2.1. Le principe de finalité : pierre angulaire de la protection des données personnelles

En droit, le texte est généralement le fondement d'une solution à un litige. En son absence, le juge saisi d'un contentieux peut révéler l'existence d'un principe lui permettant de le résoudre. Dans le domaine de la protection des données personnelles, l'environnement institutionnel s'est renforcé avec l'apparition de la première autorité administrative indépendante, la CNIL, permettant de promouvoir le respect du principe de finalité (2.1.1.) qui, en matière de sécurité, est difficile à circonscrire (2.1.2.)

2.1. Le respect du principe de finalité assurée par la CNIL .

Face au carence de la loi informatique et libertés, elle a su jouer, non sans difficultés, le rôle de régulateur de l'activité administrative et des services de police. Aussi, sa doctrine a mis en lumière les principes essentiels de cette loi qui s'attachent à protéger notamment la vie privée. S'agissant de la finalité, la CNIL la considère comme " un principe cardinal de toutes les législations de protection des données (…) »21. Ce faisant, l'autorité de contrôle a toujours veillé à ce que la finalité des fichiers de police soit la plus précise possible en tenant compte de la spécificité de leur travail de renseignement et en s'inspirant des textes européens. Exercice périlleux et délicat, car les missions de la police sont diverses (Ordre public, Police judiciaire, renseignement etc.). De fait, l'inexistence d'une catégorie juridique propre aux fichiers de police rend plus qu'incertain la détermination de leur finalité. La commission a donc opéré une conciliation entre le type de missions confiées aux services de police et la (ou les) finalité(s) qu'ils souhaitent assignées à leur traitement.

2.2. La difficulté de circonscrire la finalité en matière de sécurité

Lorsque l'on confronte l'objet de traitement tels que le STIC, le FNAEG ou plus récemment celui de la Prévention des Atteinte à la Sécurité Publique (PASP), et les missions des services de police qui les gèrent, on observe que la finalité de ces traitements est extrêmement vaste. Autrement dit, la conciliation opérée n'est pas toujours satisfaisante pour la protection des données personnelles, aboutissant à une formulation très large dans les actes réglementaires portant création des traitements de données. Mais ces dispositions correspondent aux missions des services de police telles qui existent dans les lois vigueurs. Aussi, il nous semble que c'est davantage le respect du principe de finalité, et sa promotion dans l'ordre juridique qui doit conduire à apporter des garanties pour les personnes.

2.2-Les garanties rattachées au principe de finalité

Le respect du principe de finalité devraient permettre une meilleure protection des données personnelles. Si la sécurité peut justifier un détournement de la finalité (2.2.1) il doit comporter certaines garanties (2.2.2.).

2.2.1. *Le détournement de finalité lié à des motifs de sécurité*

.

La CNIL s'est toujours efforcé de confiner l'utilisation d'un fichier de police judiciaire à sa finalité première, à savoir l'exercice des missions de police judiciaire. A ce titre, elle a rappelé « qu'en aucun cas le STIC ne pourra être consulté dans le cadre des enquêtes

21 CNIL, *19ème Rapport d'activité 1998*, La documentation française, 1999, p. 39.

administratives dites « de moralité », là encore, seul le casier judiciaire devant faire foi ». Pourtant, sur ce même traitement, la CNIL reconnaît que si « la consultation [du STIC à des fins de police administrative est] étrangère aux finalités de police judiciaire elle peut être admise dès lors que la sécurité des fonctionnaires de la police nationale ou la sécurité des tiers est susceptible d'être mise en danger dans des circonstances particulières » 22. La loi est apparue comme la seule pouvant permettre et justifier l'élargissement de la finalité de fichiers de police judiciaire. La loi pour la sécurité quotidienne de 2001 et la LSI ont élargi les finalités du STIC et du FNAEG et généralisé la pratique des enquêtes administratives. De même la création du Fichier Judiciaire des Auteurs d'Infractions Sexuelles (FJAIS) par la loi Perben II est assez topique. Tenu par le service du casier judiciaire – service administratif déconcentré du ministère de la justice, ce traitement doit permettre de rechercher les auteurs d'infractions sexuelles et de les prévenir, en communiquant les informations aux autorités administratives pour l'examen de demandes d'agrément relatives aux activités impliquant un contact avec les mineurs. Cette instrumentalisation de la loi peut laisser dubitative quant à la portée du principe de finalité. Autrement dit, si le législateur, qui n'est pas soumis à l'autorité de la CNIL, s'autorise à élargir la finalité de certains traitements, on peut se demander quelle est l'appréciation du Conseil constitutionnel sur une telle pratique.

2.2.2- Les garanties face au détournement du principe de finalité

Le Conseil constitutionnel s'est prononcé à différentes reprises sur la pratique consistant à assigner différentes finalités à un fichier. Celle-ci peut s'opérer par la voie de l'interconnexion ou de la communication à des tiers. Dans une décision du 29 décembre 1998, le Conseil constitutionnel a admis l'interconnexion des fichiers fiscaux et sociaux, sur la base du NIR alors qu'ils ont une finalité distincte. Il rappelle que ces échanges de données « doivent être strictement nécessaires et exclusivement destinés à l'appréciation des conditions d'ouverture et de maintien des droits aux prestations, au calcul de celles-ci (…) [et que l'utilisation du NIR] a pour finalité d'éviter les erreurs d'identité, (…), et ne conduit pas à la constitution de fichiers nominatifs sans rapport direct avec les opérations incombant aux administrations fiscales et sociales »[23]. Le secrétaire général de la Haute juridiction précise que c'est dans un souci de « bonne administration et de contrôle » que l'interconnexion n'a pas été censurée[24]. S'agissant la communication à des autorités tiers, le Conseil a été saisi en 2003 de la loi pour la sécurité intérieure de la légalisation des enquêtes administratives fondées sur la consultation d'un fichier de police. Il y estime « qu'aucune norme constitutionnelle ne s'oppose par principe à l'utilisation à des fins administratives de données recueillies dans le cadre d'activités de police judiciaire » tout en admettant qu'elle « 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 »[25]. Cette énonciation quelque peu impressionniste ne laisse pas de place au doute sur un point : le principe de finalité, qui n'est pas mentionné, n'a pas de valeur constitutionnelle. Cette ignorance serait-elle susceptible de permettre au législateur d'autoriser la consultation de fichiers de sécurité à des fins indéterminées et incompatibles ? Cette hypothèse n'est pas envisageable comme nous le montre les décisions précitées. Dès lors, on pourrait considérer que l'absence de reconnaissance par la Haute juridiction du principe de finalité n'autorise pas l'utilisation de fichiers de police à des fins administratives sans l'existence de garanties. C'est

---

22 Voir en ce sens " le STIC suite… ", in CNIL, *21ème rapport d'activité pour l'année 2000, op. cit.*, 2001, p.73-99.

23 Conseil constitutionnel, décision n° 98-405 DC du 29 décembre 1998, loi de finances pour 1999, *JORF* du 31 décembre 1998, p. 20 138. Considérant 60 et 61.

24 SCHOETTL (J.-E.), « La loi pour la sécurité intérieure devant le Conseil constitutionnel », *Les Petites Affiches*, mars 2003, n° 63, p. 13.

25 Conseil constitutionnel, décision n° 003-467 DC 13 mars 2003, *loi relative à la sécurité intérieure,*JORF du 19 mars 2003, p. 4789. Considérant 32.

cette voie médiane que les juges de la rue Montpensier ont emprunté et qui ne vise pas à interdire mais à autoriser sous réserves un fichier servant plusieurs objectifs. Du point de vue des libertés, il apparaît difficile de se satisfaire de l'absence de reconnaissance du juge suprême du principe cardinal de protection des données personnelles. Cela est d'autant plus vrai que son contrôle en matière de sécurité est minimum et formel. Plus précisément, même s'il vérifie que des garanties existent, il censure rarement voire jamais les dispositions relatives aux fichiers de police. Toutefois, la protection de l'ordre public – de la sécurité – , objectif à valeur constitutionnelle permettant l'exercice des libertés doit se concilier avec d'autres droits à valeur constitutionnelle. Par ailleurs, le Conseil constitutionnel dispose des instruments juridiques tels les principes généraux du droit, à valeur constitutionnelle ou la technique de l'effet cliquet permettant d'assurer le respect de la protection des données personnelles. Enfin, il faut souligner le mouvement d'autonomie de ce droit, au niveau européen, et souhaiter qu'il inspire la jurisprudence du Conseil constitutionnel voire du Conseil d'État. Cette activisme « judiciaire » permettrait de préciser les garanties qui s'attachent aux fichiers de police, et ce faisant, façonner par la voie prétorienne les contours d'une catégorie juridique spécifique en devenir.

BIBLIOGRAPHIE :

Manuels, thèses et ouvrages

FRAYSSINET (J.), *Droit de l'informatique*, Paris, LGDJ, 2001.

DECOCQ (A.), MONTREUIL (J.), BUISSON (J.), *Le droit de la police*, Paris, Litec, 1998.

CHAPUS (R.), *Droit administratif général Tome 1*, Paris, Montchrestien, 2001.

BERGEL (J.-L.),*Méthodologie juridique*, PUF, Thémis Droit privé, 2001.

PREUSS- LAUSSINOTTE (S.), *Les fichiers et les étrangers au cœur des nouvelles politiques de sécurité,* thèse de droit public, Université de Paris X- Nanterre, janvier 1998.

PIAZZA (P.), *Histoire de la carte nationale d'identité*, Paris, Odile Jacob 2004.

Rapports

Rapports d'activité de la CNIL, Paris, La documentation française, 1980 -2010.

BRAIBANT (G.), *Données personnelles et société de l'information*, rapport au Premier ministre, La documentation française, coll. des « Rapports officiels », 1998.

ESTROSI (C.), *Rapport sur le projet de loi pour la sécurité intérieure*, Assemblée nationale, n° 508, décembre 2002.

BAUER (A.), *Fichiers de police et de gendarmerie: comment améliorer leur contrôle et leur gestion ?*, La documentation française, coll. des « Rapports officiels » 2006.

BATHO (D.), BENISTI (A.), *Rapport sur la proposition de loi relative aux fichiers de police*, Assemblée nationale, n° 1659, décembre 2009.

Articles

CHARBONNEAU (C.), PANSIER (F.-J.), " Présentation de la loi du 18 mars 2003 pour la sécurité intérieure : de la LSQ à la LSI ", *Gazette du Palais*, mars 2003.

BOYER (J.), « Fichiers de police judiciaire et normes constitutionnelles : quel ordre juridictionnel ? », *Petites Affiches*, mai 2003, n° 102.

FOUCART (S.), « Le fichage de tous les Français est envisagé », *Le Monde*, 18 décembre 2003, .

PIAZZA (P.), « Les résistances au projet INES », *Culture et conflits*, n° 64, 2006.