INTERCONNEXIONS, RAPPROCHEMENTS, CROISEMENTS : LES DANGERS DES NOUVEAUX OUTILS DE LA SURVEILLANCE D'ETAT

Ines BRANCO-LOPEZ, Anne KERAVEC,
Clara MERIENNE et Dimitri PERREAU-SAUSSINE

Sous la supervision de Charlotte Girard

Rapport remis le 29 juin 2021

REMERCIEMENTS

Nous tenons à remercier en premier lieu le Syndicat de la Magistrature, pour la confiance qui nous a été accordée dans la rédaction de ce rapport sur le sujet aussi passionnant qu'alarmant des fichiers de police. En particulier, nous remercions Sarah Massoud pour sa compréhension et sa disponibilité.

Nous remercions Charlotte Girard, pour sa réactivité, sa disponibilité et ses réflexions qui nous ont permis de mener à bien un travail approfondi.

Nous souhaitons également remercier Christophe Daadouch, Fouad Eddazi, Virginie Gautron, Paul Mathonnet, Mathieu Rigouste, ainsi que l'équipe de la Quadrature du Net d'avoir pris le temps de répondre à nos questions et de nous avoir guidé·e·s dans nos recherches par leur connaissance du sujet.

Nous remercions tous les collectifs, associations et syndicats qui mènent la bataille juridique contre les dangers pour nos libertés individuelles que représentent les fichiers de police.

SOMMAIRE

ANNEXE : LISTE DES ABREVIATIONS ET ACRONYMES UTILISES

ANSSI	Agence nationale de la sécurité des systèmes d'informations.
BCEF	Bureau du contrôle et de l'évaluation des fichiers.
CC	Conseil constitutionnel.
CE	Conseil d'État.
CNCTR	Commission nationale de contrôle des techniques de renseignement.
CNIL	Commission nationale de l'Informatique et des Libertés.
Convention EDH	Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.
Cour EDH	Cour européenne des droits de l'Homme.
DDHC	Déclaration des droits de l'Homme et du citoyen.
DGGN	Direction générale de la gendarmerie nationale.
DGPN	Direction générale de la police nationale.
DGSE	Direction générale de la sécurité extérieure.
DGSI	Direction générale de la sécurité intérieure.
DSIC	Direction des systèmes d'information et de la communication.
JLD	Juge des libertés et de la détention.
NEO	Nouvel équipement opérationnel.
ONDRP	Observatoire national de la délinquance et des réponses pénales.
OPJ	Officier de police judiciaire.
PPN	Procédure pénale numérique.
SNEAS	Service national des enquêtes administratives de sécurité.
UE	Union européenne.
RGPD	Règlement général sur la protection des données

Ce rapport sur les fichiers de police a été rédigé dans le cadre de la clinique EUCLID de l'Université Paris-Nanterre, en partenariat avec le Syndicat de la Magistrature. C'est en tant qu'étudiant·e·s de Master 2 qu'il nous a été proposé de réaliser ce travail, mais c'est surtout en tant que militant·e·s que nous nous sommes investi·e·s dans ces recherches.

La surveillance d'État devient d'autant plus problématique lorsque les outils technologiques permettent de la généraliser à l'entière population, lorsque qu'il est possible d'identifier, centraliser, archiver des données de toutes sortes concernant une personne, pour après pouvoir les interpréter de façon accusatrice. Le devoir de transparence est ainsi inversé dans un panoptisme de genre nouveau : ce n'est plus au politique d'être transparent face à ces citoyen·ne·s, mais aux citoyen·ne·s de l'être face aux institutions politiques.

Enfin, nous souhaitons nous situer face à cette problématique : s'il est vrai que chaque citoyen·ne est concerné.e par la surveillance de masse, et donc potentiellement victime, toutes les populations n'en subissent pas les mêmes conséquences. Notre investigation part d'un regard extérieur, en tant que personnes généralement non visées par une surveillance et un fichage spécifiques, tel·le·s que ceux qui seront examinés dans ce rapport.

Nous appelons **fichiers de police** tous les **traitements de données à caractère personnel pouvant être utilisés dans le cadre d'enquêtes judiciaires mais également administratives et à des fins de renseignements mis à la disposition de services aussi divers que la police et la gendarmerie nationales, les services du Parquet ou encore les services du renseignement territorial**. Ainsi, il existe des fichiers judiciaires, tel que le casier judiciaire, des fichiers de police administratifs, tel que l'accès aux dossiers de contravention, des fichiers de police d'antécédents, notamment le traitement des antécédents judiciaires, des fichiers de police d'identifications, tels que le FAED ou le FNAEG mais également des fichiers de renseignement, notamment ceux utilisés par la DGSI et la DGSE.

Ces fichiers posent de nombreuses questions d'ordre philosophique, éthique, politique, mais aussi sur le plan légal, notamment en matière de libertés individuelles et publiques.

De nombreux fichiers en tant que tels, ou leur utilisation, ont fait l'objet de polémiques récentes quant à leur caractère extra-légal voire illégal. Ainsi, très récemment, la finalité du fichier Accès aux dossiers de contravention (ADOC) a été détournée afin d'y inscrire les contraventions liées au non-respect du confinement. Un arrêté publié le 16 avril 2020 a alors modifié la finalité du fichier ADOC afin de permettre l'inscription des

contraventions liées au non-respect des restrictions prévues par l'état d'urgence sanitaire, venant légaliser une pratique policière.

La légalisation des pratiques policières *a posteriori* en matière de fichiers de police n'est pas une nouveauté. Ainsi, les trois décrets très récents du 2 décembre 2020 permettant le recueil non seulement des données concernant les « activités » mais également des « *opinions* politiques, des *convictions* philosophiques, religieuses ou une *appartenance* syndicale » dans les fichiers PASP, GIPASP et EASP - validés par le Conseil d'État - sont venus légaliser une pratique policière préexistante.

Par ailleurs, la possibilité de plus en plus large de récolter des données personnelles pour des raisons aussi diverses que la commission d'une infraction ou une suspicion d'idéologie radicale, mais également le fait d'avoir été victime d'une infraction, nous paraît inquiétant sur le plan des libertés individuelles. Elle invite à souligner l'aspect particulièrement mouvant et évolutif du fichage : il est probable que ce rapport lui-même devienne vite obsolète, tant la forme fichier prolifère à grande vitesse.

S'ajoute, au-delà du développement des traitements de données à caractère personnel en tant que tel, le phénomène grandissant des interconnexions entre ces différents fichiers, permettant la consultation voire l'alimentation automatisées et simultanées de plusieurs fichiers. Ainsi, non seulement les fichiers deviennent plus nombreux, mais la tendance est également à l'élargissement des possibilités d'accès et de croisement des informations enregistrées dans les différents fichiers.

Dans ce rapport, nous nous proposons donc tout d'abord de dresser un état des lieux général sur la problématique des fichiers de police (**Partie 1**) dans lequel nous aborderons, après quelques généralités, l'encadrement de l'usage des fichiers. Puis nous nous concentrerons dans la seconde partie sur la problématique de l'interconnexion (**Partie 2**). Pour cela, nous proposons une étude de cas précise sur le fichier Automatisation de la consultation centralisée de renseignements et de données (ACCReD).

PARTIE 1 :
GENERALITES SUR LES FICHIERS

Détailler le cadre conceptuel dans lequel notre étude sur l'interconnexion s'inscrit suppose de s'attacher à deux aspects : tout d'abord aux caractéristiques principales entourant les fichiers de données, bien que mettre en exergue une forme-type s'avère difficile (Titre 1) ; puis à l'encadrement pratique apporté à l'usage parfois nébuleux des fichiers (Titre 2).

Titre 1 :
Les caractéristiques générales des fichiers

Chacun des aspects entourant les fichiers se caractérise par une certaine opacité : la définition légale du fichier semble impropre à saisir la plasticité de la forme-fichier (chapitre 1), le mode de création d'un fichier est pour sa part caractérisé par la mainmise d'un pouvoir réglementaire aux contours imprécis (chapitre 2), l'usage empirique est quant à lui difficilement maîtrisable en pratique (chapitre 3).

CHAPITRE 1 :
DÉFINITION ET RÉGIME JURIDIQUE DU FICHIER :
QUAND LE DROIT S'EFFACE DEVANT À LA PRATIQUE

Le cadre légal posé par la loi « Informatique et Liberté » est marqué par l'incertain : la définition légale du fichier, trop vague, ne rend suffisamment pas compte des formes multiples du fichier (I), le régime juridique est par ailleurs trop flou pour incarner un réel carcan autour de la pratique du fichier (II).

I. Une définition légale impropre à saisir la réalité du fichier

Si la définition du fichier proposée par la loi de 1975 est suffisamment large pour couvrir l'ensemble des formes de fichiers possibles (A), elle ne permet pas en revanche de

rendre compte de la forme plurale et multidimensionnelle que peut observer le fichier de données (B).

A) La définition légale des fichiers au regard de la loi « Informatique et Liberté »

L'ambition de ficher la population n'est pas nouvelle. Dès le XIIIème siècle, des registres de criminels, de proscrits ou de vagabonds étaient utilisés par les cours de justice et les armées[1]. En 1904, la population découvrait qu'il existait des enregistrements des opinions politiques et religieuses dans l'armée française[2], provoquant une crainte générale dans la population. **En matière de fichiers, la pratique précède souvent la règle de droit.**

C'est cependant dans les années 1960 que les fichiers de police connaissent un essor sans précédent, dû notamment à l'émergence de l'informatique. La collecte de données personnelles n'étant à cette époque prévue par aucun texte législatif, l'opacité autour de la constitution de pareils fichiers entraîne alors une contestation de la part de la population[3].

Il faudra cependant attendre la loi du 6 janvier 1978 dite « Informatique et Libertés »[4] pour qu'un régime juridique du fichier de collecte de données soit prévu par la loi. Ainsi, ce texte – retoqué à de multiples reprises depuis lors – propose une définition du fichier :

Loi « Informatique et Libertés », Article 2

« *Constitue un fichier de données à caractère personnel tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.* »

En ce qui concerne des fichiers à portée européenne ou transfrontalière, la disposition précitée renvoie au règlement européen 2016/679, qui propose une définition de nature similaire mais fournit une liste davantage exhaustive[5].

[1] Virginie Gautron, Surveiller, sanctionner et prédire les risques : les secrets impénétrables du fichage policier, *Champ pénal*, 2019, vol. n°17, (DOI : https://doi.org/10.4000/champpenal.10843), §1.
[2] Surveiller, sanctionner et prédire les risques : les secrets impénétrables du fichage policier, *op. cit.*, §3.
[3] Virginie Gautron, *Fichiers de police*, Dalloz, Rép. Pénal, avr. 2015, p. 5.
[4] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[5] Règlement (UE) 2016/679 du 27 avril 2016, art. 4 : "«*traitement*», *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de*

La définition fournie par la loi de 1978 couvre donc un ensemble assez large de pratiques. Si en ce sens elle permet l'application du régime juridique à de nombreuses objets de collecte portant sur le traitement de données, elle ne fournit que peu d'informations afin de caractériser ce que représente réellement un fichier. Ceci est notamment dû à une **forme extrêmement plastique du fichier de collecte de données**.

B) Une difficile caractérisation au regard de la nature variable du fichier

Les fichiers sont certes définis par la loi de 1978, mais cette définition apparaît pour le moins lacunaire. **Il est en effet difficile de tirer de la législation actuelle une catégorie juridique propre aux fichiers de collecte de données**, soit un ensemble de règles s'appliquant à un objet juridique donné[6]. D'un point de vue d'accessibilité de la norme, tant à l'égard des agents opérateurs que des usagers, la définition légale laisse de nombreuses zones d'ombres. Néanmoins, l'étude des fichiers de collecte, et plus particulièrement des fichiers de police, laisse entrevoir la possibilité de procéder à une première classification.

Certaines caractéristiques semblent ainsi pouvoir se dégager de ces différents fichiers de police. Ainsi, il est concevable d'imaginer une classification entre les **fichiers de police judiciaire à dimension répressive et les fichiers de police administrative, visant à prévenir une atteinte à l'ordre public**. Cependant, certains fichiers semblent troubler cette distinction, notamment les fichiers de renseignement, dont l'opacité en matière de publicité[7] ne permet pas à cette catégorisation d'être parfaitement opérante[8]. Le régime juridique régissant les fichiers de police oscille ainsi entre droit commun et régime dérogatoire et ne permet pas de tirer une catégorie juridique claire des fichiers de police[9].

---

données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction".

[6] V. notamment : Jean-Louis Bergel, *Méthodologie juridique*, PUF, coll "Thémis" [cité par David Larbre, Les fichiers de police, une catégorie juridique incertaine?, *Technologie de l'information, culture & société*, 2011, vol. 108-109, p. 141-151, p. 142].

[7] Voir en *infra* p. 6.

[8] David Larbre, *Les fichiers de police : une catégorie juridique incertaine ?*, *Terminal*, 108-109 | 2011, 141-151, https://journals.openedition.org/terminal/1364 §8.

[9] *Les fichiers de police : une catégorie juridique incertaine ?, op. cit.,* §10.

Sur un autre volet, la loi « Informatique et Libertés » impose que soient définies des finalités « déterminées, explicites et légitimes » pour autoriser la collecte de données personnelles au 2° de l'article 4. Ainsi, serait admissible une catégorisation des fichiers en fonction de leur finalité. Cependant, la définition peu claire et très large de la notion de finalité dans la loi de 1978 laisse une grande marge de manœuvre à la collecte des données personnelles pour des finalités extrêmement diverses[10].

Enfin, il serait possible de classifier les différents fichiers selon leur échelle et rayon d'action. Si l'actualité juridique traite régulièrement de fichiers centralisés et de portée nationale, souvent destinés à prévenir et rechercher les auteur·ice·s d'infractions - par exemple le TAJ ou le FPR, pour n'en citer que deux - de nombreux autres types de fichiers existent[11]. Les fichiers de police prolifèrent également au niveau local, souvent en marge de la légalité[12]. Il s'agit de collectes informelles pour un but opérationnel précis : document en libre accès pour un service, inscription collective de données etc. Pourtant, ces pratiques emportent la qualification de « collecte de données » au sens de la loi de 1978. Une fois encore, ce critère de classification présente potentiellement certaines limites : informels par essence, il est difficile de savoir si ces fichiers locaux ne viendraient pas dans un second temps alimenter des fichiers « nationaux ».

La pluralité des formes de fichiers et leur plasticité ne nous permet donc pas de dégager des catégories opérantes et définitives. La loi « Informatique et Liberté » pour sa part ne permet que d'ériger une catégorie universelle des fichiers, qui lisse l'ensemble des différences entre eux : de police ou destinés à un autre usage, selon leur finalité, selon leur taille et centralisation etc. **Nul doute qu'un affinement de cette définition produirait à son tour un impact sur les pratiques** : forcée de s'identifier à une catégorie, la création d'un fichier devrait ainsi prévoir un encadrement plus précis de son usage.

Au-delà d'un cadre définitionnel large, la loi de 1978 « Informatique et Liberté » fixe un ensemble de règles relatives à la collecte de données, permettant - à défaut de se représenter ce qu'est un fichier de police - de connaître les règles légales de collecte de données.

[10] *Les fichiers de police : une catégorie juridique incertaine ?*, *op. cit.*, §26.
[11] Cet aspect, bien que peu présent dans la littérature juridique, se concentrant souvent sur les "grands" fichiers nationaux, a pourtant été souligné par la plupart des intervenant.e.s que nous avons interrogé.
[12] Rapport parlementaire Paris-Morel-à-L'huissier, n°1335, 17 oct. 2018, p. 27.

II. Le régime juridique du fichier dans la Loi "Informatique et Liberté" : un carcan général et imprécis

La loi « Informatique et Libertés » précise les conditions dans lesquelles peuvent être collectées des données à caractère personnel et permet d'édicter des règles protectrices dans un domaine qui n'avait jusqu'alors jamais été réglementé. Cette partie les résume brièvement.

Loi « Informatique et Libertés », Article 4

« Les données à caractère personnel doivent être :

1°: **Traitées de manière licite, loyale** et, pour les traitements relevant du titre II, transparente au regard de la personne concernée.

2°: **Collectées pour des finalités déterminées, explicites et légitimes**, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités.

3°: **Adéquates, pertinentes** et, au regard des finalités pour lesquelles elles sont traitées, limitées à ce qui est nécessaire ou, pour les traitements relevant des titres III et IV, non excessives.

4° **: Exactes** et, si nécessaire, **tenues à jour**. Toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder.

6°: **Traitées de façon à garantir une sécurité appropriée des données à caractère personnel**, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, ou l'accès par des personnes non autorisées, à l'aide de mesures techniques ou organisationnelles appropriées. »

Cependant, on ne peut que relever **l'aspect générique et abstrait de ces textes**. Nulle définition n'est donnée de ce qu'est une "finalité légitime", ou encore une collecte traitée de manière "licite et loyale". Au regard des faibles garde-fous entourant l'usage des fichiers de police[13], ou de la mainmise du pouvoir réglementaire sur leur création[14], cette imprécision

[13] Voir en *infra* p. 26.
[14] Voir en *infra* p. 7.

des termes mobilisés est problématique, mais surtout dommageable tant l'exercice de collecte est porteur de potentielles atteintes aux libertés individuelles[15].

Outre l'article 4, l'article 5 de la loi de 1978 précise au-delà de la forme que doit revêtir un fichier la manière dont doivent être assurées les collectes de données. Afin d'être licite, la collecte et le traitement de données doivent remplir l'une de ces conditions alternatives : le traitement doit avoir reçu le consentement du·de la concerné·e[16], être nécessaire à l'exécution d'un contrat qui lie le·la concerné·e[17], au respect d'une obligation légale[18], à la sauvegarde des intérêts vitaux du·de la concerné·e[19], d'une mission d'intérêt public[20], ou encore si la finalité du traitement du fichier est en elle-même légitime[21]. Là encore, les termes imprécis desdites dispositions ne semblent pas aptes à créer un régime juridique suffisamment clair et circonscrit.

L'adoption de la loi « Informatique et Libertés » est ainsi venue encadrer et formaliser une pratique existante. Toutefois, cet encadrement s'est fait au prix d'une **imprécision** des textes, tant au regard de la définition du fichier que de la déclinaison de son régime. À ce caractère occulte de la loi de 1978 doit s'ajouter la relative **complexité** du régime de création d'un fichier de police, qui **concourent tous deux à renforcer l'aspect clandestin et informel des fichiers de police**.

---

[15] Virginie Gautron, *Usages et mésusages des fichiers de police : la sécurité contre la sûreté* ?, *AJ Pénal*, 2010, p. 266.

[16] 1° : "Le traitement, lorsqu'il relève du titre II, a reçu le consentement de la personne concernée, dans les conditions mentionnées au 11 de l'article 4 et à l'article 7 du règlement (UE) 2016/679 du 27 avril 2016 précédemment mentionné".

[17] 2°: "Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci".

[18] 3°: "Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis".

[19] 4°:"Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique".

[20] 5°: "Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement".

[21] 6°: "*Sauf pour les traitements effectués par les autorités publiques dans l'exécution de leurs missions, le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant"*

CHAPITRE 2 :
LE MODE DE CRÉATION D'UN FICHIER :
LA MAINMISE DU POUVOIR RÉGLEMENTAIRE
DANS UN CADRE PEU CONTRAIGNANT

Le mode de création d'un fichier se caractérise par un cadre souple et peu contraint, notamment à l'égard du pouvoir réglementaire (I). Afin d'y parer, un monopole de création par le·a législateur·rice a été envisagé, sans toutefois que cette proposition ait pu aboutir (II).

I. Des obligations de publication peu consistantes et peu respectées

Le mode de création d'un fichier est marqué par des obligations de publication très diffuses (A), ce qui n'empêche toutefois pas l'émergence de nombreux fichiers en marge de la légalité (B).

A) Le mode de création d'un fichier de collecte de données

Le régime déclaratif de droit commun s'illustre par une faible coercition et une certaine complexité juridique (1), auxquelles s'ajoutent de nombreuses dérogations (2).

1. Le régime de droit commun

Il n'est pas aisé de résumer succinctement le mode de création de droit commun d'un fichier de collecte de données, au sens de la loi du 6 janvier 1978[22]. Ceux-ci font en effet l'objet d'un « d'un encadrement juridique particulièrement complexe »[23], mêlant des normes juridiques de degré et nature variés.

En effet, l'article 31 de la loi précitée dispose que les fichiers les plus communs[24] sont créés par arrêté ou, si ils portent sur des données sensibles, par décret en Conseil d'État. Il

[22] Pour une définition d'un fichier de police, v. en *supra*.
[23] Rapport parlementaire Paris-Morel-A-L'huissier, n°1335, 17 oct. 2018, p. 21.
[24] Il s'agit ici des fichiers ne nécessitant pas un mode de publication particulier. Voir en *infra* les exceptions au régime de droit commun.

semble à première vue que le pouvoir réglementaire ait la mainmise sur la création d'un fichier. Si le législateur lui octroie en effet cette discrétion, il ne se départit cependant pas de sa compétence pour autant[25]. Fort de cette « diversité de bases normatives »[26], une forme d'opacité règne autour de la création de fichiers, et nécessite d'en expliquer avec plus de précision les modalités. Dans le cadre d'une compétence double, exercée alternativement par les pouvoirs réglementaire et législatif[27], il convient d'observer les modalités de chacun de ces régimes tout en prenant en considération l'autre pan du mode de création des fichiers de police.

La création d'un fichier par le pouvoir réglementaire tout d'abord. Alors que le texte antérieur à l'ordonnance du 12 décembre 2018[28] laissait planer le doute sur le fait de savoir si seul le Premier ministre était titulaire du pouvoir de création d'un fichier de police ou si les autres ministres pouvaient en disposer par extension[29], tel n'est plus le cas avec la loi de 1978 dans sa forme actuelle, puisque l'article 31 mentionne que **l'arrêté emportant création d'un fichier est pris par « un ou des ministres compétents ».** Par ailleurs, ce mode de création constitue la voie régalienne du pouvoir réglementaire pour mettre sur pied un nouveau fichier[30] et incarne la voie la plus fréquemment utilisée. L'article 35 de la loi de 1978 précise l'ensemble des informations qui doivent intégrer la publication du décret : la finalité du traitement, les catégories de données visées etc. Parmi beaucoup d'autres, c'est par exemple par cette voie qu'ont été créés les fichiers PASP ou EASP : par un décret signé par le Premier ministre sur rapport du ministre de l'Intérieur.

Au surplus, le pouvoir réglementaire ne se limite pas à la création de fichiers, il vient également régir le droit applicable aux fichiers. Un certain nombre de décrets prolongent le travail du législateur en venant préciser le droit applicable aux fichiers[31]. C'est notamment le cas des fichiers mis à disposition des forces de sécurité. Par exemple le décret du 15 mai 2007[32] qui vient préciser les fichiers « intéressant la sûreté de l'Etat, la défense ou la sécurité publique » visés par l'article 30 de la loi de 1978.

[25] Les fichiers de police : une catégorie juridique incertaine ?, *op. cit.* , §20.
[26] Rapport parlementaire Batho-Bénisti, n°4113, 21 déc. 2011, p. 17.
[27] *Les fichiers de police : une catégorie juridique incertaine ?*, *op. cit.*, §15.
[28] Ordonnance n°2018-1125 du 12 décembre 2018.
[29] *Les fichiers de police : une catégorie juridique incertaine ?*, *op. cit.*, §18.
[30] Rapport parlementaire Batho-Bénisti, *op. cit.*, p. 18.
[31] Rapport parlementaire Paris-Morel-à -L'huissier, *op. cit.*, p. 25.
[32] Décret n°2007-914 du 15 mai 2007.

Pour autant, les délégations de compétence par le pouvoir législatif n'emportent pas son dessaisissement[33]. **L'intervention du législateur dans le processus de création des fichiers est double**. Tout d'abord, il fixe le cadre général de création des fichiers et définit le droit qui lui y applicable[34]. La loi « Informatique et Liberté » de 1978 a donc été modifiée à plusieurs reprises pour adapter ce droit. Il reste qu'une large partie de ces changements a été opéré par la voie d'ordonnances laissant la main au pouvoir exécutif[35]. Selon une autre modalité, le pouvoir législatif a pu lui-même créer directement des fichiers concomitamment à des créations réglementaires. C'est notamment le cas de fichiers d'importance majeure, tels que le FNAEG[36], le FIJAISV[37] ou encore plus récemment du FIJAIT[38].

Une exception doit néanmoins être apportée à ce cadre juridique dual et complexe. **Les fichiers portant sur des données dites « sensibles », visées à l'article 6 de la loi de 1978[39] doivent être créées par décret en Conseil d'État**. Il ne s'agit du reste pas d'un avis conforme du Conseil. Si bien que seule la demande est nécessaire à la création dudit fichier[40]. Ces données, dont la collecte est en soi litigieuse, n'exigent ainsi qu'une simple déclaration – et non une autorisation – supplémentaire.

À cette double compétence, il convient d'ajouter **l'intervention de la CNIL**. Cette dernière dispose d'un champ de compétence étendu, puisque selon l'article 8 de la loi de 1978, elle « doit être consultée sur tout projet de loi ou de décret relatif à la protection des personnes à l'égard des traitements automatisés ». Cependant, depuis la réforme de son statut en 2004[41], ce rôle a été amoindri : un simple avis de cet organe, motivé et publié en même temps que le décret, suffit pour créer un fichier. Le contenu de la demande de création d'un fichier est détaillé à l'article 33 de la loi de 1978. Priver la CNIL d'un avis contraignant à l'égard du pouvoir réglementaire accentue ainsi la discrétion de ce dernier[42].

---

[33] *Les fichiers de police : une catégorie juridique incertaine ?, op. cit.,* §20.
[34] Rapport parlementaire Paris-Morel-à -L'huissier, *op. cit.,* p. 23.
[35] V. l'historique des modifications sur https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/
[36] Loi n° 98-468 du 17 juin 1998.
[37] Loi n° 2004-204 du 9 mars 2004.
[38] Loi n° 2015-912 du 24 juillet 2015.
[39] « Données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique».
[40] Virginie Gautron, *Fichiers de police*, Dalloz, Rép. Pénal, avr. 2015, p. 11.
[41] *Ibid*.
[42] *Fichiers de police*, *op. cit.*, p. 14.

Ce cadre allégé d'intervention doit par ailleurs être nuancé selon le type de fichier. Si le cas le plus fréquent reste la publication d'un avis au sens de l'article 31, certains types de fichiers font l'objet d'exigences amoindries au vu d'exceptions introduites par la même disposition.

2. Les exceptions en termes de publicité

L'article 31 de la loi de 1978 énonce des exceptions au régime de création de fichiers. Il mentionne en effet que « certains traitements […] peuvent être dispensés, par décret en Conseil d'État, de la publication de l'acte réglementaire qui les autorise ». Plus encore, seul le sens de l'avis émis par la CNIL est publié en même temps que le décret. Cet avis de la CNIL se prononce d'ailleurs sur une base d'informations tronquée en comparaison avec le régime de droit commun. En effet, l'article 33 I 10° de la loi de 1978 précise que le même décret en Conseil d'État portant création du fichier concerné précise également « la liste de ces traitements et des informations que les demandes d'avis portant sur ces traitements doivent comporter au minimum ». Ce régime, portant le plus souvent sur des fichiers intéressant la sûreté de l'État, la défense ou la sécurité publique, ainsi que la disposition précitée le suggère, **offre une marge discrétionnaire supplémentaire au pouvoir réglementaire**. Sous couvert d'un énoncé large, les pouvoirs publics ont souvent mobilisé cette exception pour pouvoir se soustraire à l'obligation de publicité en matière de création de fichier[43].

Tel est le cas pour les fichiers relatifs au terrorisme. Le décret du 2 août 2017[44] venant modifier le décret du 5 mars 2015 portant sur la création du FSPRT n'est ainsi qu'une coquille vide qui se borne à rappeler la possibilité de non-publication de la création du fichier. N'y seront ainsi indiquées aucune des informations visées à l'article 35 de la loi de 1978. Cette exception concerne par ailleurs de nombreux fichiers entourés du secret militaire. Ainsi, le décret du 4 août 2017[45] portant création du Biopex, fichier propre au renseignement militaire, n'est pas publié, et ne renvoie qu'à la modification de décrets également non-publiés.

[43] Virginie Gautron, *Surveiller, sanctionner et prédire les risques : les secrets impénétrables du fichage policier*, *Champ pénal*, 2019, vol. n°17, (DOI : https://doi.org/10.4000/champpenal.10843), §12.
[44] Décret n° 2017-1227 du 2 août 2017.
[45] Décret n° 2017-1231 du 4 août 2017.

Il est par essence difficile de connaître la bonne utilisation de cette prérogative, et la nécessité d'un tel secret peut apparaître cohérente avec la fonction même de l'activité militaire ou des services de renseignement.

L'absence totale de contrôle ou de garde-fou consacre cependant la possibilité d'un détournement des fonctions de ce régime dérogatoire. La pratique révèle en effet de nombreux écarts avec le cadre légal des fichiers, notamment au vu de l'essor d'un nombre marqué de fichiers clandestins.

B) La prolifération de fichiers en marge du régime déclaratif

Malgré un cadre juridique peu contraignant, de nombreux rapports font état de l'émergence de fichiers en marge du régime déclaratif. **L'essaimage de fichiers clandestins est ainsi marqué par l'absence de publication dans le journal officiel**, bien qu'existant en pratique. Ainsi, de nombreux fichiers sont dépourvus de base textuelle propre[46].

La clandestinité des fichiers s'observe souvent au niveau local, où les enquêtes parlementaires relèvent que « le développement spontané de fichiers de police demeure une pratique courante »[47]. Il est nécessaire ici de faire un lien avec la forme plastique des fichiers[48]. La définition d'un fichier ne couvre en effet pas uniquement la collecte de données au niveau national, mais également de nombreux logiciels de taille restreinte en interne, qui sont en ce sens plus difficiles à surveiller que les fichiers nationaux. Par exemple, la commission parlementaire Batho-Bénisti de 2011 relève ainsi que 28 fichiers effectivement utilisés sur un total de 62 dénombrés n'ont fait l'objet d'aucune déclaration à la CNIL ni de publication par un décret, ce qui représente une hausse de 27% à 47% entre 2009 et 2011[49] ; au point que le rapport préconise une régularisation *a posteriori* de ces nombreux fichiers clandestins[50], notamment à l'aide d'accords-cadres régularisant plusieurs fichiers en un seul texte[51] - malgré le risque d'une analyse plus succincte de chacun de ces fichiers. Il est par définition difficile d'évaluer le nombre actuel de fichiers clandestins.

[46] *Fichiers de police*, *op. cit.*, p. 11.
[47] Rapport parlementaire Batho-Bénisti, *op. cit.*, p. 27.
[48] Voir en *supra* p. 2.
[49] Rapport parlementaire Batho-Bénisti, *op. cit.*, p. 27.
[50] Rapport parlementaire Batho-Bénisti, *op. cit.*, p. 29.
[51] Rapport parlementaire Batho-Bénisti, *op. cit,* p. 30.

Plusieurs explications sont avancées pour expliquer ce phénomène. Le rapport parlementaire précité y voit pour sa part une absence de « culture Informatique et Libertés » ainsi qu'un manque de prise de conscience de la part des directions de la police et de la gendarmerie[52]. Le rapport Paris-Morel insistant pour sa part sur l'essor d'un régime juridique devenu trop complexe pour connaître le droit applicable[53], il est probable qu'un cadre déclaratif unique pour les fichiers de données permettrait d'éviter la prolifération de fichiers clandestins. Enfin, il reste à souligner que **les fichiers s'inscrivent souvent dans le cadre d'une culture des forces de police, pensant connaître à elle seule les réalités du terrain et leur permettant ainsi de s'exonérer de tout cadre réglementaire ou légal**[54]. La célérité des besoins empiriques pourrait ainsi pousser à s'abstraire de toute déclaration à la CNIL ou de base légale, ce d'autant plus que l'essor de fichiers locaux est très difficile à repérer.

À ces fichiers clandestins, il faut ajouter le fait que la CNIL n'est pas nécessairement consultée lors de la publication d'un décret portant création d'un fichier[55]. Cela a par exemple été le cas du fichier CRISTINA en juin 2009. Au surplus, la CNIL est investie d'un délai de deux mois pour rendre un avis lorsqu'elle est consultée *a priori* de la publication d'un décret. Alors que l'institution manque parfois de moyens pour se prononcer dans les temps[56], l'article 33 de la loi de 1978 énonce que l'absence de réponse dans le délai imparti vaut avis favorable. L'absence de consultation de la CNIL est d'autant plus étonnante que l'institution n'est pas réputée pour une grande fermeté en matière de fichiers : « en pratique, elle adopte une stratégie pragmatique et cherche un compromis sur les aspects les plus contestables des banques de données[57] ». Son absence de consultation est ainsi **révélatrice d'une culture de la création de fichiers parfois en marge du cadre légal**.

L'essor de fichiers clandestins pose par ailleurs la question d'une éventuelle réforme du régime de création des fichiers, en faveur d'un monopole législatif. Si plusieurs tentatives ont été opérées, aucune n'a jusqu'ici abouti, dans un domaine lourd d'enjeux en matière de libertés fondamentales.

[52] Rapport parlementaire Batho-Bénisti, *op. cit.*, p. 29.
[53] Rapport parlementaire Paris-Morel-à-L'huissier, *op. cit.*, p. 22.
[54] Rapport parlementaire Batho-Bénisti, *op. cit.*, p. 24.
[55] *Fichiers de police*, *op. cit.*, p. 16.
[56] *Fichiers de police*, *op. cit.*, p. 14.
[57] *Ibid*.

II. L'échec d'un transfert de compétences vers le législateur

Les deux rapports parlementaires Batho-Bénisti de 2009 et 2011 plaident pour une refonte du cadre juridique des fichiers de police, jugé trop complexe et porteur en son sein d'atteintes aux droits individuels. Cette proposition ne sera pas cependant reprise par le plus récent rapport Paris-Morel, preuve d'une attention davantage portée sur les succès opérants du fichage que sur les potentiels dysfonctionnements structurels du cadre juridique.

Pourtant, une refonte du texte de 1978 en faveur d'une compétence exclusive du législateur en matière de création de fichier semble plus que pertinente[58]. Le contenu de ce projet de réforme tout d'abord. Le monopole législatif porterait sur l'ensemble des fichiers visés par l'article 31 de la loi « Informatique et Libertés », et induirait des garanties supplémentaires.

Par exemple, chaque loi autorisant la création de fichiers devrait obligatoirement contenir certains **éléments essentiels pour décrire le fichier**[59] – et davantage que l'actuel article 35 de la loi de 1978. Le dispositif devrait également prévoir des **garanties supplémentaires en matière de données sensibles**, et remplacer l'actuel décret en Conseil d'État par une autorisation expresse du législateur[60]. Enfin, chaque projet de loi devrait prévoir une **clause de rendez-vous** dans le temps afin de juger de l'utilité de chaque fichier, et **supprimer d'éventuels fichiers obsolètes ou inutiles**[61].

Si une telle refonte est jugée nécessaire, c'est parce que le cadre juridique de création actuel est perçu comme « susceptible de porter atteinte aux droits et libertés de chacun »[62]. Parce que ne comportant aucune réelle autorisation pour la création d'un fichier par le pouvoir réglementaire, parce qu'étant porteur d'une certaine complexité juridique dans le cadre d'une double compétence, le régime actuel de création d'un fichier doit être réformé. **L'absence de suite à ces propositions de loi et recommandations des rapports parlementaires[63] peut donc être comprise comme une volonté politique du pouvoir exécutif de conserver sa mainmise sur la création de fichiers.**

[58] Rapport parlementaire Batho-Bénisti, *op. cit.*, p. 16.
[59] Rapport parlementaire Batho-Bénisti, *op. cit*,.p. 18.
[60] Rapport parlementaire Batho-Bénisti, *op. cit.*, p. 21.
[61] Rapport parlementaire Batho-Bénisti, *op. cit.*, p. 22.
[62] Rapport parlementaire Batho-Bénisti, *op. cit.*, p. 23
[63] Rapport parlementaire Batho-Bénisti, *op. cit.*, p. 23.

CHAPITRE 3 :
LA RÉALITÉ EMPIRIQUE DU FICHIER :
LA DIFFICULTÉ DE L'ENCADREMENT DE LA TECHNIQUE PAR LE DROIT

Le régime juridique des fichiers laisse dans son ombre une pratique non prise en compte par le droit. Certains logiciels d'exploitation permettent des ponts entre des fichiers isolés par les textes (I), que le traçage des consultations ne permet pas de combattre efficacement (II). Il existe par ailleurs de nombreuses anomalies et erreurs d'inscriptions dans de nombreux fichiers, qui rendent une refonte particulièrement nécessaire (III).

I. La variété de logiciels d'exploitation rendant un encadrement des fichiers davantage complexe

Dans l'utilisation interne des fichiers par les forces de l'ordre, il semble important de **différencier les fichiers des logiciels d'exploitation qui les hébergent**. Ces derniers permettent d'alimenter, de rapprocher, de saisir les signalements, de créer une gestion automatique des données récoltées dans les fichiers.

La majorité des fichiers se fondent sur un support informatique, donc un logiciel qui répond à **des finalités et des logiques propres et distinctes du fichier de police**. Certains de ces logiciels, tels que le LRPPN et son jumeau de la gendarmerie LRPGN, se constituent juridiquement comme un fichier, tout en étant utilisé comme outil pour nourrir et rapprocher différentes données d'autres fichiers. D'autres logiciels sont considérés uniquement comme des outils d'exploitation, étant mis au service de plusieurs fichiers.

Afin de mieux illustrer ces distinctions, nous allons prendre comme exemple les logiciels les plus communs et importants, en détaillant leur finalité, usage et leur connexion avec les fichiers.

A) Le LRPGN et le LRPPN : la centralisation de nombreux fichiers pourtant isolés dans leurs statuts

Le LRPGN est un programme informatique destiné à faciliter la rédaction des procès-verbaux et autres actes de procédure de la police pour de la gendarmerie.

Décret n° 2011-110 du 27 janvier 2011, Article 1

« Le ministre de l'Intérieur (direction générale de la police nationale) est autorisé à mettre en œuvre un traitement automatisé de données à caractère personnel ayant pour finalités :

1° De permettre aux services de police d'assurer la clarté et l'homogénéité de la rédaction des procédures judiciaires et administratives qu'ils ont compétence pour mettre en œuvre en vertu des lois et règlements ;

2° D'en réaliser l'archivage ;

3° De permettre la collecte des informations issues de ces procédures, en vue de leur diffusion et de leur exploitation ;

4° De permettre, en vue de leur alimentation, la mise en relation avec des traitements de données relatives aux procédures judiciaires. »

Plus concrètement, le logiciel propose aux fonctionnaires des champs à remplir sur la nature et le lieu de l'infraction, la catégorie socioprofessionnelle de la victime, la manière d'opérer du suspect, son mobile apparent etc. **Ainsi, il n'offre que peu d'espace pour inscrire des commentaires, permettant de ce fait de limiter le nombre d'approximations, comme cela avait pu être révélé par la CNIL en 2008 à l'égard de l'ancien fichier STIC au taux d'erreurs pouvant aller jusqu'à 83%**[64].

Ainsi, l'enjeu est double : d'une part la coordination avec le système judiciaire, pour une information encore plus fiable et facile à exploiter, d'autre part l'exploitation statistique des données, pour une réponse policière mieux ciblée[65].

[64] BugBrother (le blog de Jean-Marc Manach), *En 2008, la CNIL a constaté 83% d'erreurs dans les fichiers policiers*, Le Monde, 21 janvier 2009.

[65] Rapport de l'école Nationale Supérieure de la Police, *Former au LRPPN, une étape cruciale du dispositif*, 21 novembre 2013, (URL : https://www.ensp.interieur.gouv.fr/Actualites/Former-au-LRPPN-une-etape-cruciale-du-dispositif).

Le logiciel LRPGN faciliterait ainsi les rapprochements de données dans les enquêtes judiciaires tout en alimentant automatiquement une base de données du service concerné pour réaliser des bases statistiques et une cartographie de la délinquance, grâce aux données géographiques récoltées. D'ailleurs, l'ONDRP qui travaille avec un algorithme prédictif utilise une extraction du logiciel LRPPN, « pour identifier des variables environnementales communes par types de faits de délinquance. L'objectif étant de créer des associations entre facteurs contextuels et événements délictuels, afin de mieux anticiper leur commission mais aussi d'allouer les ressources (humaines et matérielles) adéquates. L'algorithme, en fonction des types de délits, permet d'attribuer une valeur de vulnérabilité aux lieux, en fonction de ses caractéristiques contextuelles répertoriées »[66].

Ce logiciel alimente automatiquement les fichiers TAJ, FOVeS, CASSIOPEE et échange des informations avec le logiciel GASPARD NG[67]. Mais il existe également un lien entre le LRPGN et Gendnotes, application mobile mise à disposition des gendarmes qui facilite la collecte de photographies et d'informations sensibles (religion, politique, sexualité, prétendue origine raciale). Cette application a été **utilisée pendant des années sans cadre juridique**, mais un décret l'a officialisée en février 2020.

Néanmoins, ce décret est problématique en ce que, comme l'explique La Quadrature du Net[68], les photos et informations sont au moins transmises au LRPGN, qui les transmet à son tour au TAJ si les gendarmes décident d'ouvrir une procédure. Néanmoins, le TAJ n'est du reste **pas autorisé à recenser des informations sensibles comme certaines données collectées par Gendnotes**. Il n'en demeure pas moins qu'en plus d'intégrer des informations qui ne devrait pas l'être, celles-ci seront **conservées dans le TAJ pendant 20 ans**, accessibles par toute la police et la gendarmerie, de même que les photos pourront être utilisées ultérieurement par un système de reconnaissance faciale pour identifier des personnes[69].

[66] Camille Gosselin, *La police prédictive. Enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique*, IAU Ile-de-France, avr. 2019, p. 39.
[67] Décrets n°2011-110 et 2011-111 du 27 janvier 2011.
[68] La Quadrature du Net, *Gendnotes, faciliter le fichage policier et la reconnaissance faciale*, 25 février 2020, (Url : https://www.laquadrature.net/2020/02/25/gendnotes-faciliter-le-fichage-policier-et-la-reconnaissance-faciale) .
[69] *Ibid.*

Cet exemple révèle de manière flagrante que des **fichiers qui entre eux ne sont pas interconnectés mais échangent tout de même des informations par le biais de logiciels**, rendant le contrôle de la circulation des informations plus difficile.

Le LRPPN a quant à lui été mis à disposition en 2015 pour combler les lacunes de la saisie des données du STIC avec les logiciels ODYSSEE et OMEGA. Pourtant, il est déjà perçu comme obsolète depuis 2017 avec de nombreuses insatisfactions qui ont conduit la DGPN à mettre en place un projet de complet remplacement en le subsituant par le logiciel SCRIBE. Les évolutions majeures concernent « les échanges avec les autres applications du système d'information et d'investigation de la police nationale, pour une fiabilisation accrue des données, une ouverture vers les télé-services offerts à la population (projet Thésée de plainte en ligne pour les cyber escroqueries) et un module de pilotage et de management des portefeuilles d'enquête, intégré, moderne et adapté »[70]. Cette initiative s'inscrit dans le projet de la PPN, qui serait un vaste programme d'interconnexions de différentes applications des ministères de l'intérieur et de la justice, avec pour objectif d'aboutir en 2022 à la dématérialisation complète de la procédure pénale[71].

B) Le cas des logiciels de rapprochement judiciaire ou la centralisation de données de gendarmerie

Ces outils sont essentiellement les fichiers exploités par la Gendarmerie et dénommés ANACRIM.

ANACRIM comporte quatre logiciels :

- ANACRIM-ATRT, qui a pour objectif l'exploitation de relevés bancaires et de documents téléphoniques,
- ANACRIM-ANB (bientôt remplacé par ANACRIM-NG), qui a pour objectif l'analyse et la représentation visuelle des données,

[70] Assemblée Nationale, Question N° 24092 de Momain Grau, *Logiciel rédaction de procédure de la police*, déc. 2019, p. 10765.
[71] UNSA Police, *Dématérialisation de la procédure pénale / Logiciel Scribe*, févr. 2019, (Url : http://police.unsa.org/dossiers/procedure-penale/article/dematerialisation-de-la-procedure-penale-logiciel-scribe).

- ANACRIM-IVC qui se focalise sur la gestion des données afin d'identifier les victimes de catastrophes,
- Et enfin MERCURE, qui analyse et traite des données téléphoniques obtenues sur réquisition. MERCURE est le seul logiciel d'ANACRIM à être issu des services de la police.

Ainsi, avec ces quatre logiciels, ANACRIM peut rapprocher automatiquement un nombre élevé d'informations sur une enquête particulière, et assure en ce sens une représentation graphique des éléments de cette enquête (relation entre les personnes, numéros de téléphone et bornes utilisées, véhicules...)[72]. Il s'agirait donc d'un outil de visualisation de données[73]. L'objectif, selon le décret n° 2012-687 du 7 mai 2012 relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle est "l'exploitation et le rapprochement d'informations sur les modes opératoires réunis au cours d'une même enquête par les unités de gendarmerie et les services de police chargés d'une mission de police judiciaire.".

Ce texte autorise le ministre de l'Intérieur à utiliser les traitements de données à caractère personnel uniquement dans un cadre déterminé. Il s'agit, selon l'Article 1er, « des enquêtes de flagrance ou des enquêtes préliminaires et des investigations exécutées sur commission rogatoire relatives à des crimes et délits punis d'une peine d'emprisonnement, ou des procédures de recherche des causes de la mort ou d'une disparition ».

Ce logiciel est utilisé depuis 1994 mais n'a bénéficié d'un cadre légal qu'en 2012.

D'après le rapport Batho-Bénisti, ANACRIM est un outil de travail à vocation temporaire, ce qui signifie que les informations et données collectées ne sont utiles que pendant sa durée d'exécution et ne peuvent donc pas résider en mémoire. Néanmoins, la

[72] *Rapport parlementaire Batho-Bénisti*, n°4113, 21 déc. 2011.
[73] « ANACRIM-ANB est un logiciel d'analyse et de représentation visuelle de données. Il permet de représenter des données sous forme de graphes relationnels ou événementiels, afin de représenter par exemple des réseaux de relations entre individus ou des enchaînements chronologiques d'événements. Les informations contenues dans les pièces et documents de procédures (procès-verbal, compte rendu, etc.) sont ainsi représentées sous différentes formes, qui peuvent être enrichies par les enquêteurs, afin de mettre en évidence des contradictions entre certaines données ou de confirmer certains faits ».

CNIL considère ce fichier comme un traitement de données à caractère personnel, malgré sa nature temporaire[74].

Dans le même rapport il est indiqué que le nouveau logiciel ANACRIM Nouvelle Génération (ANACRIM-NG) est un « logiciel temporaire [qui] a vocation à remplacer l'outil Analyst's Notebook soumis à des frais de licences annuels. Il devrait être déployé à l'été 2012 et faire bientôt l'objet d'une déclaration à la CNIL ».[75] De ce que nous savons, **aucune déclaration de la CNIL n'a été encore réalisée**.

C) GASPARD : une base concomitante au TAJ et au FAED

Il s'agit d'un **logiciel de saisie de signalement** (photographie, état civil, marques particulière) qui alimente le fichier CANONGE.

GASPARD NG transmet des références communes au TAJ et au FAED, ce qui est un facteur de fiabilisation des données contenues dans ces deux applications. L'outil GASPARD NG permet aussi d'alimenter le TAJ des photographies des mis en cause. Il est ainsi désormais possible de lancer dans le TAJ des recherches à partir d'une photographie. Les résultats de la recherche font apparaître les photographies déjà présentes susceptibles d'y correspondre en fonction d'un certain nombre de paramètres (écartement des yeux, etc.). La recherche peut ailleurs être affinée par certains critères, tels que le sexe, la couleur des yeux ou des cheveux, etc. Le TAJ constitue déjà, de ce point de vue, un outil de reconnaissance faciale[76].

La CNIL a constaté que le logiciel GASPARD allait permettre l'alimentation, *via* le logiciel LRPPN, du traitement d'antécédent judiciaires TAJ et du Fichier automatisé des empreintes digitales FAEG, néanmoins la commission a relevé que la photographie des victimes ne fera pas l'objet d'un traitement[77].

[74] Rapport Batho-Bénisti, *op. cit.*, p. 66.
[75] Rapport Batho-Bénisti, *op. cit.*, p. 169.
[76] Rapport d'information Paris-Morel-à-L'huissier , nº1335, 17 oct. 2018.
[77] CNIL, Délibération 2012-365 du 11 octobre 2012.

D) Le logiciel Métamorpho ou l'amélioration de relevés des empreintes

Métamorpho est un logiciel de nouvelle génération de **traitement des empreintes digitales**, créé par l'entreprise Morpho, anciennement dénommée Sagem sécurité[78]. Avec pour objectif d'alimenter le FAED, il présente la nouveauté d'intégrer les empreintes de la paume de la main, en plus de celle des dix doigts déjà existants, tout en offrant des algorithmes de calcul plus performants[79]. Néanmoins, il semblerait que ce logiciel ne compte pas de cadre législatif.

E) La passerelle CHEOPS : la centralisation d'un nombre problématique de fichiers

La passerelle CHEOPS est un portail sécurisé qui permet l'accès limité aux :

- Fichier des brigades spécialisées (FBS) ;
- Fichier informatisé du terrorisme (FIT) ;
- Fichier national automatisé des empreintes génétiques (FNAEG) ;
- Fichier national du faux monnayage (FNFM) ;
- Fichier national transfrontières (FNT) ;
- Fichier des personnes recherchées (FPR) ;
- Fichier des renseignements généraux (FRG) ;
- Fichier des Objets et Véhicules Signalés (FOVeS), anciennement appelé Fichier des véhicules volés (FVV) ;
- Système de traitement des infractions constatées (STIC);
- Système National des Permis de Conduire (SNPC)
- Système d'Immatriculation des Véhicules (SIV).

Ce logiciel permet de limiter les accès, maîtriser et connaître précisément les personnes autorisées à le consulter. Néanmoins, beaucoup d'anomalies ont été détectées et dénoncées par les fonctionnaires de police, notamment des pannes de leur parc informatique

[78] Cette même entreprise collabore avec le ministère de l'intérieur afin de développer de nouveaux systèmes biométriques de contrôle aux frontières (CCAF). Ce projet s'inscrit dans le Entry-Exit System (EES), qui a pour objectif de sécuriser l'espace Schengen au-delà de ces frontières, en se focalisant plus particulièrement au étranger ayant dépassé leur limite de visa. Cf. https://www.idemia.com/press-release/french-ministry-interior-selects-idemia-and-sopra-steria-develop-new-standard-border-control-system-2021-01-29

[79] V. Gautron, Fichiers de police, *Répertoire de droit pénal et de procédure pénale*, mars 2019, p. 52.

« bien souvent inadapté et vétuste »[80]. En 2011, le rapport Batho-Bénisti a pointé l'obsolescence technique du FPR, qui repose sur une technologie dépassée que la DSIC du ministère de l'Intérieur ne parviendrait plus à gérer. Si l'interface de consultation a été modernisée, l'alimentation proprement dite se fait toujours par le biais de l'ergonomie d'origine. Accessible uniquement par le biais de la passerelle CHEOPS, sa consultation serait parfois rendue impossible pendant plusieurs heures[81]. Depuis 2005, un nouveau système amélioré dénommée CHEOPS-NG est utilisé par la gendarmerie, depuis 2017 pour le fichier des personnes recherchées et 2019 pour le LRPPN.

F) Le logiciel Néogend – Néopol

Le projet NEO a été lancé en 2015 dans le cadre d'un plan de modernisation de la sécurité intérieur qui « vise à doter les agents de solutions numériques sécurisées de mobilités (smartphone et tablette) »[82].

Les terminaux Néogend sont utilisés pour la gendarmerie et Néopol pour la police. Cet ensemble est le premier outil partagé entre les forces de police et de gendarmerie et qui permet de **faciliter les contrôles au cours de leur mission grâce à des tablettes et smartphones**, permettant aux agents de transporter leur « bureau » facilement. Les outils sont connectés en 4G au réseau du ministère de l'Intérieur, permettant une interrogation des fichiers lors de contrôles routiers ou d'identité en toute autonomie.

« Parmi les applications disponibles, on peut distinguer l'application permettant l'interrogation simultanée des fichiers de police, la messagerie interpersonnelle et l'agenda, une application de navigation permettant notamment d'afficher les habitations du programme Opération Tranquillité Vacances, la messagerie instantanée de l'État TCHAP, les applications GendNotes pour la gendarmerie et CRIM'IN pour la police permettant des notes ou relevés judiciaires, les applications Inter'Ferroviaire ou Inter'Electrique réalisées respectivement par

[80] Sénat, Question écrite N° 13314 de M. Jean-Pierre Grand, *Dysfonctionnements des fichiers de police*, oct. 2014, p. 2330.
[81] *Fichiers de police*, *op. cit.*, p. 54.
[82] Avis sur le projet de mobilité des forces de sécurité intérieure NEOPOL-NEOGEND, Direction Interministériel du Numérique et du Système d'Information et de Communication de l'Etat, Paris, 20 avril 2016.

la SNCF et ENEDIS, l'application APPUI pour la gendarmerie et l'application PSQ pour la police permettant d'enrichir le contact citoyen ».[83]

Ainsi, un des objectifs de ces logiciels est de **renforcer la coopération au sein du ministère**, en connectant les équipements et permettant aux agents d'obtenir un accès direct aux informations de divers fichiers de police, comme par exemple fichier national du permis de conduire, fichier de personnes recherchées… Alors qu'auparavant, la consultation devait se faire par demande via le terminal de radio, nécessitant donc un autre fonctionnaire ayant lui accès aux fichiers.

Néanmoins, il ne semble pas avoir de détails sur les modes d'accès à la consultation simultanée des fichiers de police : la connexion se fait-elle par le biais d'un identifiant et mot de passe ? Chaque fonctionnaire aurait son propre terminal avec le numéro de série associé à l'identité de l'agent ? Ces informations sont pourtant indispensables pour permettre une meilleure traçabilité de connexion afin de limiter les consultations abusives.

II. Le traçage des consultations de fichiers

« Parler de traçabilité implique que soient réunis trois éléments: il faut qu'il y ait des traces et donc un support qui permettra de les repérer; il faut qu'il y ait un mécanisme de recueil des traces; il faut enfin une structure qui permette de les traiter, de les analyser pour en tirer des conclusions »[84]. La traçabilité est un concept créé au début des années 1960 dans les manuels militaires américains de définition des bonnes pratiques de mesure. Dans les années qui ont suivi, le terme a connu une généralisation et un élargissement. Selon la norme NF X 50-120, « la traçabilité est l'aptitude à retrouver l'historique, l'utilisation ou la localisation d'un article ou d'une activité, ou des activités semblables, au moyen d'une identification enregistrée »[85].

Afin de permettre un contrôle sur l'accès aux fichiers, l'utilisation de logiciels comme ceux que nous avons présentés permet une traçabilité informatique plus facile et directe, par

[83] Assemblée Nationale, Avis Mazars, nº3404, Tome VII, Sécurité, oct. 2020.
[84] Phillipe Pédrot, Traçabilité et responsabilité, *Economica*, 2003.
[85] Jean-Luc Viruéga, *Traçabilité: outils, méthodes et pratiques*, Éditions d'Organisations, 2005, p. 1.

l'intermédiaire de l'identifiant du consultant, date et nature de l'interrogation[86]. Ce type de contrôle est présenté comme garde-fou contre l'arbitraire et l'inexactitude (A).

Néanmoins, toute application informatique ne possède pas de capacité de traçabilité et celles qui en possèdent présentent de nombreuses lacunes. D'autant plus que beaucoup de consultations et échanges de données extra-officielles des fichiers ne sont pas traçables informatiquement (B).

A) Les précautions de contrôles existantes

La CNIL a plusieurs fois demandé au ministère de la Justice de prendre des mesures nécessaires pour remédier à cette situation en rappelant **que « la traçabilité des fichiers contenant des données sensibles est une mesure de sécurité qui garantit de pouvoir connaître tout usage d'un fichier, y compris lorsque la consultation vise à faire un usage détourné des informations enregistrées »**. Pour y remédier, la CNIL a proposé comme précaution élémentaire la mise en place d'un « système de journalisation, (c'est-à-dire un enregistrement dans des « fichiers journaux » ou « logs ») des activités des utilisateurs, des anomalies et des événements liés à la sécurité »[87].

Une note technique rédigée par l'ANSSI, référencée dans le site de la CNIL[88], présente les « Recommandations de sécurité pour la mise en œuvre d'un système de journalisation » et détaille leur usage et leur utilité. Ils peuvent servir *a priori* à détecter des incidents de sécurité mais également *a posteriori* pour retrouver les traces d'un incident de sécurité. **Il est donc entendu que l'objectif premier de ces journaux serait d'anticiper et comprendre des incidents techniques plutôt que des abus volontaires de consultation des fichiers.**

Parmi les recommandations techniques et bonnes pratiques figure l'importance d'une centralisation des données. Leur centralisation a pour but de faciliter leur exploitation. Ce mode de fonctionnement comporte plusieurs avantages : « le recoupement d'informations provenant de journaux d'équipements différents est plus aisé lorsque ceux-ci sont stockés au

[86] *Fichiers de police, op. cit.,* point 30.
[87] CNIL, *Sécurité : Tracer les accès et gérer les incidents*, (url : https://www.cnil.fr/fr/securite-tracer-les-acces-et-gerer-les-incidents).
[88] *Ibid.*

même endroit ». Le transfert des informations en temps réel sur les serveurs centraux serait, selon eux, préférable à un mode différé[89].

Selon les recommandations, « les utilisateurs peuvent ne pas être autorisés à consulter les journaux résultant de leur propre activité ». Il semble pourtant indispensable pour anticiper les consultations abusives, que les utilisateur·ice·s des fichiers n'aient aucun accès aux journaux. Il s'agit là d'un exemple parlant pour démontrer les dangers de posséder des journaux avec pour double objectif de prévenir les incidents techniques ainsi que de contrôler des usages abusifs. En effet, face à un incident technique, il semble approprié que les usager·e·s puissent accéder aux journaux afin d'analyser le contexte. Mais dans un cas de consultations abusives, il peut être très problématique que cette consultation ne se fasse pas par un organe ou une institution indépendant, pour empêcher une manipulation des données. Comme c'est le cas pour la CNIL qui, en tant qu'autorité indépendante, a le pouvoir de se déplacer dans les lieux de stockage et de consultation des données. Malheureusement, les contrôles nécessitent des moyens humains importants « alors que la CNIL est l'une des autorités de régulation des données les moins dotées de l'UE »[90].

Selon la CNIL[91], la journalisation doit concerner « au minimum, les accès des utilisateurs en incluant leur identifiant, la date et l'heure de leur connexion, et la date et l'heure de leur déconnexion ». La durée de conservation ne devrait, selon eux, pas être excessive et donc ne pas dépasser six mois. Mais certains fichiers demanderaient une traçabilité « haute », comme c'était le cas avec le STIC, signifiant que « les données de connexion, qui comptent l'identifiant de l'utilisateur, la date, l'heure et la nature de la consultation, sont conservées pendant cinq ans et centralisées auprès de l'inspection générale de la gendarmerie nationale »[92]. Un autre danger est que la CNIL n'a aucun pouvoir de sanction face à l'État, comme elle en a pourtant en matière commerciale. Au surplus, ses rapports, simples avertissements, ne sont pas rendus publics[93].

[89] Secrétariat général de la défense et de la sécurité nationale, Note technique, No DAT-NT-012/ANSSI/SDE/NP, le 2 décembre 2013.
[90] Yoann Nabat, *Cnil, Conseil d'Etat, Conseil constitutionnel : comment est contrôlé le fichage policier en France*, Journal du Dimanche, 18 décembre 2020.
[91] CNIL, *Sécurité : Tracer les accès et gérer les incidents, op. cit.*
[92] Rapport parlementaire Batho-Bénisti, n°4113, déc. 2011.
[93] *Conseil d'Etat, Conseil constitutionnel : comment est contrôlé le fichage policier en France, op.cit.*

Dans un rapport élaboré en 2013, la CNIL rappelle qu'effectivement, les fichiers faisant usage de logiciels informatiques permettent une traçabilité quant à la connexion des fonctionnaires, comme par exemple la passerelle CHEOPS ou les logiciels NEO qui, de par la facilité d'accès aux fichiers permettent une augmentation significative de leurs consultations et donc augmentent également les traces de connexions. Par ailleurs, grâce à la généralisation de nouvelles cartes à puces professionnelles avec un code PIN qui doit être saisi pour la plupart des accès au sein des unités de la gendarmerie, la traçabilité serait de plus en plus normalisée et efficace. Néanmoins, ce même processus rencontre des lacunes, notamment parce que le retrait de la carte professionnelle ne met pas automatiquement fin à la connexion, « ce qui nuit à l'intérêt apporté par le procédé d'authentification retenu ». Effectivement, cette lacune pourrait favoriser l'usurpation de compte et par conséquent limiter le rôle premier de contrôle[94].

D'autres mesures plus éparses existent, comme par exemple des contrôles ponctuels et aléatoires sur les connexions aux fichiers et portail, ainsi qu'à des relevés mensuels du volume de connexions et des audits ponctuels et aléatoires sur les connexions réalisées par la gendarmerie, la police nationale ainsi que l'IGPN.

L'inspection générale de la gendarmerie nationale a créé en 2009 un bureau du contrôle et de l'évaluation des fichiers (BCEF) utilisant un fichier spécifique qui trace les connexions et repère les consultations anormales[95].

Il y a également la perspective d'intégrer la biométrie comme une norme de sécurisation de l'accès aux fichiers afin d'éviter certains écarts lorsque la sécurisation n'est qu'un simple mot de passe ou identifiant, qui peut être partagé entre divers OPJ ou affiché à proximité de certains postes de travail[96].

Le rapport de la CNIL rappelle que malgré ces dispositions, beaucoup d'écarts sur la consultation des fichiers se font par échanges d'informations par voie téléphonique, postale ou face à face, des pratiques qui ne sont pas protégées par les mesures de traçabilité. Effectivement, beaucoup des échanges d'informations abusives ne se font pas via les logiciels

[94] CNIL, *Conclusions du contrôle des fichiers d'antécédents du ministère de l'intérieur*, 13 juin 2013.
[95] Rapport parlementaire Batho-Bénisti, *op. cit.*, p. 79.
[96] Rapport parlementaire Batho-Bénisti, *op. cit.* , p. 80.

automatisés mais bien par le biais du fonctionnaire lui-même. Il est effectivement plus difficile de contrôler ces pratiques, et jusqu'à nos jours, aucun moyen satisfaisant et efficace n'a su être mis en place, mettant en exergue la dangerosité potentielle d'un fichage massif *per se.*

B) Les dangers d'une opacité législative

Le risque de consultations non-officielles et abusives n'est pas uniquement favorisé par une absence de contrôle des échanges entre agents, mais peut exister du fait de l'absence ou l'opacité du cadre législatif.

Les fichiers couverts par le secret de la défense nationale en général sont peu encadrés, du fait que les décrets ne sont pas publiés, et le socle d'information transmis à la CNIL tronqué, ce qui engendre une absence de contrôle de traçabilité, comme par exemple avec le fichier CRISTINA. Une des seules informations sur la traçabilité de l'interrogation indirecte de CRISTINA est mentionnée dans la délibération n° 2017-152 du 18 mai 2017 concernant le fichier ACCReD. Effectivement il est énoncé que « concernant l'interrogation indirecte de CRISTINA et GESTEREX, les réponses sont envoyées à ACCReD en pièce jointe chiffrée de courrier électronique. La confidentialité des transferts de données est ainsi systématiquement sécurisée par la mise en œuvre d'un chiffrement, soit au niveau de la donnée, soit par l'utilisation de tunnels chiffrés ».

Plus particulièrement, les fiches S des personnes recherchées ont un système de traçabilité limité, d'après une note parlementaire : « Les services inscripteurs des fiches S n'ont pas accès à l'identité de l'ensemble des agents ayant consulté telle fiche. Seule une enquête disciplinaire ou judiciaire sur des divulgations graves d'informations contenues dans des fiches S peut conduire la direction centrale de la police judiciaire à communiquer, sur réquisition, l'identité des personnes ayant consulté telle ou telle fiche »[97].

Le rapport Batho-Bénisti dénonce également un danger dans la traçabilité des consultations du fait qu'il est effectivement « possible de connaître l'identité de la personne

[97] Rapport du Sénat Pillet, nº219, déc. 2018, p. 51.

qui s'est connectée, ainsi que la date et l'heure de la connexion, mais pas les données relatives à la recherche qu'elle a effectuée »[98].

L'absence de cadre législatif, connu ou inconnu, ne concerne pas uniquement des fichiers protégés par un secret militaire. En effet, selon le même rapport, **de nombreux fichiers de police locaux existent et n'ont pas fait l'objet d'une déclaration auprès de la CNIL**, chaque unité de police ou de gendarmerie ayant donc pu développer au niveau local ses propres outils de travail. Ils seraient, selon le rapport, une centaine. Ce serait par « la création, par des unités locales, de traitements de données personnelles non perçus comme tels. En effet, la définition extensive qu'en donne la loi est à l'origine de l'illégalité d'un très grand nombre de fichiers ». Cet état des lieux est pour le moins inquiétant en ce qu'il rend compte d'une opacité tant liée à l'absence d'information publique tenant à l'existence d'un fichier qu'à l'absence subséquente de contrôle interne et externe de ce fichier.

III. Les erreurs d'inscriptions et de non-effacement : des fichiers remplis d'anomalies

Aux dangers de consultations abusives doivent s'ajouter les er**reurs, volontaires ou non, techniques ou humaines, telles que les erreurs d'inscriptions et de non effacement, en plus de nombreuses anomalies dues à un dysfonctionnement des logiciels utilisés pour les fichiers**. Pour mieux comprendre cet aspect nous prendrons comme exemple certains fichiers en définissant leur objectif principal, présentant leurs anomalies et en expliquant quelles ont été les conséquences (A et B). Les solutions envisagées pour parer à ces déficiences restent néanmoins largement insuffisantes (C).

A) Le cas des fichiers STIC, JUDEX, TAJ et CASSIOPÉE : la transmission à travers les fichiers de nombreuse inexactitudes.

Selon les conclusions du contrôle du STIC effectué par la CNIL en 2009, le STIC et JUDEX avaient un taux d'erreur assez élevé, comme par exemple de mauvaises qualifications pénales, les victimes qui figurent en tant que délinquant·e·s, inscriptions de données sensibles

[98] Rapport parlementaire Batho-Bénisti, *op. cit.*, p. 80.

dans le fichier JUDEX alors que ce n'est pas prévu par la loi[99], information sur le suivi de l'affaire tel un classement sans suite non transmis… En somme, **72% des fiches du STIC et 62% des fiches JUDEX étaient inexactes selon la CNIL**.

En 2012, suite aux diverses anomalies affectant les fichiers STIC et JUDEX, le gouvernement de Nicolas Sarkozy décida de créer le TAJ, fusionnant les deux-dits fichiers et recensant près de 9 millions de personnes. Les grandes différences ont été l'intégration des données sensibles comme les origines raciales ou ethniques, les opinions politiques philosophiques ou religieuses, l'appartenance syndicale, l'usage de technologies biométriques pour reconnaissance faciale. Parer à l'inexactitude de fichiers a donc permis d'étendre le rayon de fichage. Le TAJ peut par ailleurs être consulté à de multiples reprises, dans le cadre d'enquêtes administratives pour certains recrutements - qui concernent un million d'emplois, les naturalisations, la délivrance de titre de séjour et les enquêtes de moralité.

Dans la délibération nº2011-204 du 7 juillet 2011, la CNIL a indiqué que la reprise des données du STIC et JUDEX ne devrait se faire qu'après une importante mise à jour pour ne pas transmettre des informations erronées, ce qui n'a pas été fait. Effectivement, aucune correction ou vérification n'a été réalisée lors de la fusion, et de nouvelles erreurs sont apparues, comme par exemple la création de plusieurs fiches pour une même personne lorsque celle-ci avait plusieurs antécédents[100].

Pour anticiper ou corriger ces erreurs, un accès direct du procureur de la République aux fichiers pourrait permettre une vérification et un contrôle des données abusives ou la non-transmission des décisions de relaxe, de non-lieu et de classement sans suite qui ne sont pas automatiquement transmises aux officier·e·s de police et de la gendarmerie gestionnaire du TAJ. Cependant, bien que cet accès soit prévu par les textes depuis 2003, aucun terminal n'est mis à disposition pour le rendre effectif.

Afin de permettre une actualisation des données du TAJ, meilleure et plus fiable, un **rapprochement avec CASSIOPÉE** s'est généralisé en 2015. CASSIOPÉE est un fichier qui concerne les procédures pénales, procédures d'assistance éducative, procédures devant le juge des libertés et de la détention et certaines procédures civiles enregistrés par le parquet. Ce

[99] Rapport parlementaire Batho-Bénisti, *op. cit.*, p. 78.
[100] *Fichiers de police*, *op. cit.*, p. 49.

fichier s'alimente grâce aux applications LRPPN et LRPGN déjà présentées. Une interconnexion entre les deux fichiers serait une avancée majeure en permettant une actualisation immédiate au TAJ des suites judiciaires. Néanmoins, ces avancées ne concernent que les affaires pénales à venir et ne permettent pas une actualisation *a posteriori,* mettant de côté plus d'un million de fiches. Une actualisation progressive de ces données inscrites, comme le proposait le ministre de l'Intérieur en 2014, nécessiterait plusieurs décennies avant d'être complétée[101].

En plus de nombreuses erreurs d'inscription, qui peuvent avoir des conséquences directe sur l'intéressé·e comme un refus de naturalisation, de titre de séjour, ou d'embaiche, ainsi que des conséquences judiciaires en termes de comptabilisation d'antécédents, le droit à l'effacement n'est pas respecté, pas même pour les victimes des informations erronées[102]. En 2010, 33% des 1589 affaires examinées dans le cadre du droit d'accès indirect au fichier STIC ont fait l'objet d'une carence de réponse des parquets.

B) Le cas du FIJAISV ou le défaut d'obligations de suivi

Le FIJAISV a pour objectif de prévenir la récidive des auteur·ice·s d'infractions sexuelles ou violentes déjà condamné·e·s et faciliter l'identification des auteur·ice·s de ces mêmes infractions, ainsi que leur localisation plus rapide. Une des obligations des personnes inscrites dans ce fichier est de justifier de leur adresse une fois par an et de déclarer tout changement d'adresse dans les quinze jours. Toutefois, ces obligations ne sont pas toujours contrôlées faute de moyen pour en assurer le suivi des obligations, ou bien faute de mentions spécifiques par les services judiciaires, outre que le prononcé de telles mesures a pu se faire rare. En 2011, près de 9 000 personnes étaient inscrites au FIJAISV sans pour autant être suivies, faute de notification[103].

[101] *Fichiers de police, op. cit.,* p. 49 : « en 2007, seuls 21,5 % des classements pour insuffisance de charges ou infraction mal caractérisée ont été transmis aux services de police pour rectification, 0,47 % des décisions de non-lieu, 6,88 % des acquittements et 31,17 % des relaxes ».
[102] *Fichiers de police, op. cit.,* p. 50.
[103] *Fichiers de police, op. cit.,* p. 60.

C) Des solutions inadaptées au problème à de l'inexactitude des fichiers

Ainsi nous avons voulu démontrer que les fichiers ne sont pas protégés d'anomalies ou de taux d'erreurs importants, soit comme conséquence d'incidents techniques soit d'erreurs de traitements et de transmission.

Comme réponse à ces inexactitudes, des interconnexions entre fichiers sont alors mises en place, comme CASSIOPEE et TAJ afin de réduire les doublons et imperfections[104]. Néanmoins, ces interconnexions ne sont pas suffisantes, surtout lorsqu'il s'agit de modifier toutes les données déjà existantes, travail qui nécessite des moyens humains importants.
D'autres solutions pour empêcher les erreurs de traitement de fichiers et de suivi de données sont trouvées dans la mise en place de formation parcellaire en interne à destination les forces de police[105]. Malheureusement, ces formations ne sont pas encore accessibles pour le personnel administratif[106] alors que le nombre de contributeur·ice·s direct·e·s des fichiers ne fait qu'augmenter.

À ce jour, **aucune solution potentielle n'apparaît suffisante pour parer aux inexactitudes d'un fichage de plus en plus étendu, et aux conséquences personnelles importantes**.

[104] *Fichiers de police*, *op. cit.*, p. 60.
[105] Rapport parlementaire Batho-Bénisti, *op. cit.*, p. 71
[106] Rapport parlementaire Batho-Bénisti, *op. cit.*., p. 73.

Titre 2 :
L'encadrement de l'usage des fichiers :
un contrôle diffus et inopérant

Le contrôle de l'usage des fichiers de police est tout autant diffus que de nature variée. La CNIL exerce un contrôle *ante* et *poste* de nature conciliante (I). Le contrôle interne aux services de police ne semble pour sa part que peu utilisé (II). Le contrôle juridictionnel reste pour sa part éparse et peu qualifié (III).

I. La CNIL, une autorité de contrôle conciliante avec l'exercice du pouvoir réglementaire

Le contrôle opéré par la CNIL ne peut s'analyser sans s'intéresser à son architecture interne (A). Cela se traduit notamment par un rôle consultatif peut efficient (B) et un contrôle *a posteriori* sans moyens réels (C).

A) Le fonctionnement général de la CNIL ou la doctrine du non-coercitif

La CNIL est composée d'un Collège de 18 membres et d'une équipe d'agent·e·s contractuel·le·s de l'État. Les 18 membres du Collège sont des représentant·e·s des hautes juridictions (deux pour le Conseil d'Etat, deux pour la Cour de cassation et deux pour la Cour des comptes), des personnalités qualifiées (5 membres) qui sont désignées par le·la président·e de l'Assemblée Nationale, le·la président·e du Sénat, des parlementaires (4 membres), des membres du Conseil économique, social et environnemental (2 membres) et des membres de la Commission d'accès aux documents administratifs (2 membres). Leur mandat est de cinq ans ou d'une durée égale au mandat électif pour les parlementaires. La CNIL est divisée en cinq directions : direction de la conformité, direction de la protection des droits et des sanctions, direction des technologies et de l'innovation, direction des relations avec les publics et de la recherche, direction administrative et financière. Elle bénéficie d'un budget de 18,5 millions d'euros par an.

Elle se réunit en assemblée plénière une fois par semaine : dans ce cadre, elle examine les projets de lois et les décrets soumis pour avis par le Gouvernement, et « analyse les conséquences des nouveautés technologiques sur la vie privée »[107]. Une formation restreinte, composée de cinq membres et d'un·e président·e distinct·e du·de la président·e de la CNIL, est chargée de prononcer les sanctions, qui peuvent être rendues publiques, à l'égard des responsables de traitement qui ne respectent pas la loi. Les sanctions sont pour la plupart des injonctions, des rappels à l'ordre, ou des retraits de certifications, et les sanctions pécuniaires ne concernent pas les fichiers mis en œuvre par l'Etat[108].

C'est son approche collaborative basée sur la pédagogie qui lui a permis d'asseoir son autorité, plutôt que l'exercice de son pouvoir de sanction, qu'elle exerce assez peu en pratique[109]. Elle développe en effet une « doctrine » composée de décisions réglementaires, avis, autorisations, recommandations, conseils, rapports annuels d'activité, rapports thématiques, contributions, rencontres internationales, guides pratiques et site internet. Selon certains auteurs, cette doctrine est devenue « indispensable » à la compréhension des dispositions juridiques encadrant les fichiers[110]. Elle prétend d'ailleurs être « un véritable régulateur, du secteur privé avant tout »[111] : s'il existe en effet un consensus sur le fort niveau de protection en matière d'informatique et libertés pour les individus auquel elle contribue, on peut émettre des doutes sur sa capacité à représenter un véritable contre-pouvoir en matière de fichage. En particulier, elle n'a pas une approche « normative » de la règle de droit, puisqu'elle considère que les arguments juridiques ne sont que des arguments parmi d'autres, une source d'inspiration pour construire ses opinions[112]. Dès lors, elle ne peut être considérée comme exerçant un véritable contrôle de l'usage des fichiers, comme le ferait une juridiction.

[107] CNIL, *Statut et organisation de la CNIL*, (url : https://www.cnil.fr/fr/statut-et-organisation-de-la-cnil).
[108] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Section III.
[109] Céline Bloud-Rey, *Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles ? Analyse et perspectives*, *Recueil Dalloz*, 2013, p. 2795, point 12.
[110] Jean Frayssinet, Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques, *J.-Cl. Pénal*, fasc. 20, n° 3 et 10.
[111] *Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles ? Analyse et perspectives*, *op. cit.*, point 26.
[112] *Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles ? Analyse et perspectives*, *op. cit.*., point 13.

B) Le rôle consultatif de la CNIL : un contrôle fragile

Jusqu'en 2004, pour tout nouveau traitement, un avis conforme de la CNIL devait intervenir. Désormais, la demande d'avis est obligatoire pour tout nouveau traitement mais un avis simple, publié et motivé suffit. Concrètement, le gouvernement dispose sur ce point d'un pouvoir discrétionnaire[113], puisque seule la demande d'avis est obligatoire. Il existe en outre plusieurs types d'exceptions à cette procédure, qui peuvent rendre l'avis de la CNIL sans intérêt : pour les fichiers dont la base réglementaire est dispensée de l'obligation de publication, seul le sens de l'avis de la CNIL est publié. D'autres fois, concernant les traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique, elle doit donner un avis sans que le gouvernement ne soit contraint de lui fournir toutes les informations normalement exigées à l'article 33 de la loi Informatique et Libertés. **Plus encore, lorsqu'elle ne rend pas l'avis qui lui est demandé dans un délai de deux mois, son avis est réputé favorable**.

Sur les tendances de son contrôle *a priori*, lorsqu'elle contrôle les finalités des fichiers, elle laisse généralement un large pouvoir d'appréciation au pouvoir réglementaire. Elle s'inquiète toutefois de la large définition de la finalité de prévention du terrorisme, et considère que ces dispositions comportent des risques graves d'atteinte aux libertés individuelles. S'agissant de la durée de conservation et la nature des données collectées, elle alerte généralement lorsque la gamme des données collectées lui semble excessive ou insuffisamment définie. **Le pouvoir réglementaire, qui ne se contente pas de saisir la CNIL tardivement, partiellement, voire pas du tout[114], ignore fréquemment ses recommandations**. Ce fut le cas pour le FIJAISV, le TAJ, les fichiers STIC et JUDEX. Pourtant, son approche est réputée pragmatique et conciliante, « *au point que l'on peut se demander aujourd'hui si le « réalisme » de la commission n'a pas contribué à banaliser l'existence de ces fichiers* »[115].

[113] *Fichiers de police*, *op. cit*., point 34.
[114] *Fichiers de police*, *op. cit*., point 35.
[115] Éric Heilmann, Le désordre assisté par ordinateur. L'informatisation des fichiers de police en France (1968-1988), *Les Cahiers de la sécurité*, 2005, n°56, p. 145.

C) *Un contrôle* a posteriori *qui pâtit d'un manque de moyens*

La CNIL bénéficie également d'un pouvoir de contrôle au quotidien de l'usage des fichiers. En effet, au titre de l'article 19 de la loi Informatique et Libertés, elle dispose d'un accès aux lieux, locaux, enceintes, installations, établissement servant à la mise en œuvre d'un traitement de données à caractère personnel de 6 heures à 21 heures. Elle ne peut toutefois pas effectuer des contrôles par surprise : elle doit prévenir le procureur par écrit au moins vingt-quatre heures avant son déplacement et précise la date, l'heure, le lieu et l'objet de son contrôle. Par ailleurs, les décrets en Conseil d'État qui dispensent de publication certains décrets peuvent aussi prévoir que soient écartées les dispositions instaurant le contrôle de la CNIL, ce qui prive cette dernière d'un droit de regard *a posteriori* sur les usages de ces fichiers[116].

De surcroît, le **manque de moyens** affectant la CNIL l'empêche d'effectuer son travail correctement. En effet, si son budget a constamment augmenté depuis sa création, il n'a pas été à la hauteur de l'augmentation des sollicitations : elle est bien souvent dans l'incapacité de remplir ses missions à temps. En réalité, elle n'effectue que de rares contrôles sur place : seulement 20 en 2013, 29 entre 2015 et 2019 pour les traitements mis en œuvre par les directions générales de la police, de la gendarmerie et la préfecture de police de Paris[117].

Autant l'avis consultatif que le contrôle de l'usage des fichiers par la CNIL ne peuvent être regardés comme représentant une garantie sérieuse de respect des droits et libertés. Certes, il faut reconnaître à la CNIL un rôle dans la diffusion d'une doctrine de protection des données personnelles, mais elle est loin de pouvoir constituer un garde-fou à elle seule.

[116] *Fichiers de police*, *op. cit*., préc., point 30.
[117] Virginie Gautron, *Surveiller, sanctionner et prédire les risques : les secrets impénétrables du fichage policier*", *Champ pénal*, vol. 17, 2019, p. 36.

II. Le contrôle de l'usage des fichiers au sein des services de police : un contrôle *in loco* insuffisant

L'encadrement interne aux services de police prend la forme d'un tryptique : l'usage des fichiers est encadré par la technique (A), par une faible immiscion du Parquet dans l'exercice de police (B) et par des sanctions disciplinaires internes (C).

A) L'encadrement par la technique

Pour certains auteurs, la technicité même du domaine des fichiers est une garantie contre les mésusages : les bases de données sont segmentées, les interconnexions sont expressément interdites dans la plupart des textes créant des fichiers, les consultations sont tracées[118]. **Pour la CNIL, la traçabilité est techniquement possible mais en pratique, presque jamais utilisée pour contrôler les usages des agent·e·s**[119]. On aura l'occasion de démontrer, en particulier, que l'interdiction des interconnexions n'est pas sérieusement appliquée dans nombre de cas.

B) Le contrôle normal opéré par le Parquet

Le contrôle de l'usage des fichiers de police est normalement effectué par le.a procureur.e de la République. Alors que la Cour EDH conteste l'appartenance du parquet à l'autorité judiciaire qui, selon elle, doit être la gardienne du droit au respect de la vie privée, le procureur de la République est chargé de surveiller et de diriger la police judiciaire au titre des articles 12 et 13 du code de procédure pénale. Puisque le Conseil constitutionnel considère que les magistrat·e·s du parquet appartiennent à l'autorité judiciaire, il a évidemment validé cette organisation en considérant que le contrôle exercé par le procureur de la République sur les fichiers d'antécédents était l'une des garanties de nature à assurer une conciliation *a priori* équilibrée entre le respect de la vie privée et la sauvegarde de l'ordre public[120].

[118] Alain Bauer, Christophe Soullez, Les fichiers de police et de gendarmerie, éd. Presses Universitaires de France, coll. « Que sais-je ? », 2011, p. 73.
[119] *Les fichiers de police et de gendarmerie, op. cit.,* , p. 77.
[120] *Fichiers de police, op. cit*, point 74.

Le·la procureur·e de la République territorialement compétent autorise les actes d'enquête, la collecte de données par des techniques de renseignement, a accès aux fichiers d'antécédents et dispose d'un pouvoir de rectification et d'effacement, et peut utiliser les logiciels de rapprochement judiciaire[121]. Le·la procureur·e de la République est assisté dans son contrôle par un·e magistrat·e du parquet hors hiérarchie, nommé· pour trois ans par le garde des Sceaux et assisté·e d'un comité de trois membres nommé·e·s dans les mêmes conditions. Le FAED est contrôlé par le procureur général près la Cour d'appel dans le ressort de laquelle est situé le service gestionnaire du fichier ; le FNAEG est contrôlé par un·e autre magistrat·e du parquet hors hiérarchie, le FIJAISV est contrôlé par le·la magistrat·e qui est directeur·ice du service du casier judiciaire.

En pratique, comme il a été évoqué plus haut, les parquets n'ont pas les moyens ou bien pas la culture du contrôle des fichiers. Bien trop souvent, cette prérogative est considérée comme annexe et en marge du traitement judiciaire d'une procédure.

C) Les sanctions de mésusage

L'article R. 434-21 du code de la sécurité intérieure, dans la section codifiant la déontologie de la police et de la gendarmerie nationales, rappelle que le·la policier·e ou le·la gendarme, dans l'accomplissement de sa mission, « se conforme aux dispositions législatives et réglementaires qui régissent la création et l'utilisation des traitements de données à caractère personnel », et « respecte et préserve la vie privée des personnes ». Bien que le respect de la loi par les agent·e·s des services de police et de gendarmerie ne devrait peut-être pas nécessiter une disposition spécifique du code de déontologie, on en comprend l'utilité au regard de l'importance des fichiers dans l'action policière[122].

Le supérieur hiérarchique, c'est-à-dire le ministre de l'Intérieur et ses relais (les commissaires pour la police et les officier·e·s pour la gendarmerie), veille au respect des obligations inscrites dans le code de déontologie[123]. La violation du code de déontologie

[121] Gildas Roussel, Police judiciaire, *Répertoire de droit pénal et de procédure pénale*, oct. 2020, point 420.
[122] Gildas Roussel, *Police judiciaire*, op. cit., point 462
[123] Jean Buisson, Force publique, *Répertoire de droit pénal et de procédure pénale*, oct. 2019, points 81 et 83.

policière emporte sanctions disciplinaires (administratives) ou pénales (article R. 434-27 du code de la sécurité intérieure). Les sanctions disciplinaires sont celles de la fonction publique dans la police[124] et celles des militaires dans la gendarmerie[125].

III. Un contrôle juridictionnel éparse et peu qualifié

Le contentieux relatif aux fichiers de police est tiraillé entre plusieurs juridictions. Le juge judiciaire, bien que compétent, ne se démarque pas par un contrôle ferme (A). Le juge administratif, bien que plus spécialisé, reste dans une démarche conciliante à l'égard du pouvoir réglementaire (B). Le juge constitutionnel enfin exerce un contrôle superficiel en matière de création de fichiers (C).

A) Le contrôle opéré par le juge judiciaire : un juge manifestant peu d'intérêt

En droit français, **plusieurs arguments de nature juridique plaident pour un contrôle judiciaire des usages des fichiers de police**. Premièrement, l'autorité judiciaire est la gardienne de la liberté individuelle au sens de l'article 66 de la Constitution. Bien que le respect de la vie privée n'entre pas dans le champ de cet article, l'indépendance de l'autorité judiciaire est une garantie constitutionnelle. Ensuite, la police judiciaire est sous la direction du procureur de la République et la surveillance du procureur général près la cour d'appel (articles 12 et 13 du code de procédure pénale)[126]. Le droit européen souligne l'importance d'un contrôle juridictionnel judiciaire en matière de respect de la vie privée, la Cour EDH considère même que c'est l'une des garanties permettant aux juges strasbourgeois de regarder comme proportionnée une atteinte au droit au respect à la vie privée[127]. Le juge judiciaire est le juge « naturel » des litiges relatifs à la vie privée de la personne[128].

En matière de recours contre les refus du procureur d'effacement ou de rectification, le contentieux est dual : le juge des libertés et de la détention est compétent pour examiner la

[124] Décret n°95-654 du 9 mai 1995.
[125] Code de la défense, Article L. 4137-2.
[126] Gérald Bégranger, *Le contrôle des fichiers de police par les juges*, AJ Pénal, 2014, p. 176.
[127] "Fichiers de police", op. cit., point 74.
[128] *Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles ? Analyse et perspectives*, *op. cit* point 26.

requête d'une personne qui se serait vu opposer le refus du·de la magistrat·e du parquet responsable pour l'effacement ou la rectification des données la concernant, lorsque les textes prévoient cette voie de droit. Mais lorsque ce n'est pas le cas, le Conseil d'État a considéré que ces actes sont détachables d'une procédure judiciaire et constituent des actes de gestion administrative du fichier qui sont susceptibles de recours pour excès de pouvoir devant la juridiction administrative[129]. Cette dualité est une source évidente de complexité inutile[130].

Le juge pénal est compétent pour la répression des pratiques illégales. Il juge des délits concernant « des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques » (Section V du titre II du Code pénal) : les manquements à la loi « Informatique et Liberté », le délit d'entrave à l'action de la CNIL, la mise en œuvre d'un traitement automatisé de donnes personnelles clandestin, la collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite, le non-respect des délais de conservation ou le traitement illégal des données conservées, le détournement de finalité des informations personnelles traitées, etc. Toutefois, les poursuites, et d'autant plus les condamnations sur ces fondements, visent surtout des personnes privées et sont rares à l'égard d'agent·e·s public·que·s[131].

La doctrine conclut au manque d'intérêt du juge pour ce contentieux, dû à une méconnaissance des enjeux individuels et sociaux de la matière ainsi que de l'état du droit chez les professionnels du droit en général[132]. Pour Céline Bloud-Rey, les autorités administratives indépendantes comme la CNIL occupent la place vidée par le juge judiciaire, alors qu'elles ne sont pas un véritable substitut à la recherche de solutions juridiques effectives par le juge[133]. En outre, la CNIL se montre incapable d'assumer cette charge croissante[134].

Ainsi, **l'essentiel du contentieux est donc administratif**.

[129] Conseil d'État, 17 juillet 2013, req. n°359417, à propos du fichier STIC.
[130] *Le contrôle des fichiers de police par les juges, op. cit.*
[131] *Fichiers de police,* op. cit., point 79.
[132] *Ibid.*
[133] *Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles ? Analyse et perspectives, op. cit.*, point 25.
[134] *Fichiers de police,* op. cit., point 79.

B) Le contrôle opéré par le juge administratif : un juge chargé et en voie de spécialisation

Le contentieux administratif se subdivise entre les actes à l'origine de création de fichiers (1), une kyrielle de contentieux de nature variée (2) et les requêtes soumises à la formation spécialisée du Conseil d'État (3). Aucun de ces pans ne permet cependant un contrôle juridictionnel suffisant pour incarner un garde-fou à l'exercice des fichiers de police.

1. Le contrôle des actes créant les fichiers : un contrôle conciliant à l'égard du pouvoir réglementaire

En premier lieu, le Conseil d'État examine la légalité des actes réglementaires instaurant des fichiers. Il vérifie notamment que la CNIL a bien été saisie d'une demande d'avis et qu'il a été publié, mais également, en matière de traitement de données sensibles ou biométriques, que le texte adopté par le pouvoir réglementaire est similaire à celui qui a été soumis au Conseil d'Etat pour consultation[135].

En particulier, il examine la dispense de publication des actes réglementaires instituant des fichiers. Alors que la Cour EDH a censuré plusieurs fichiers de renseignement pour non-publication des textes les instituant, pour le Conseil d'État, « aucun texte ni aucun principe ne fait obligation à un décret dispensant de publication [...] d'indiquer, même sommairement, les motifs de fait et de droit qui déterminent la décision de dispense de publication prise par l'autorité administrative »[136]. La marge d'appréciation est absolue et, selon le Conseil d'État, ne viole pas le principe de sécurité juridique, selon lequel la règle de droit est accessible et prévisible[137].

Le contrôle effectué par le juge administratif est un **contrôle de la proportionnalité**. Le considérant de principe est le suivant : « *l'ingérence dans l'exercice du droit de toute personne au respect de sa vie privée que constituent la collecte, la conservation et le traitement, par une autorité publique, d'informations personnelles nominatives, ne peut être légalement autorisée que si elle répond à des finalités légitimes et que le choix, la collecte et*

[135] *Ibid.*, point 55.
[136] Conseil d'État, 16 avril 2010, req. n°320196.
[137] Fichiers de police, *op. cit.*, point 56.

le traitement des données sont effectués de manière adéquate et proportionnée au regard de ces finalités »[138]. Le contrôle du juge administratif est donc un contrôle normal de l'acte créant le traitement. Ce contrôle reste un contrôle de la légalité uniquement : **le contrôle de l'opportunité relève du pouvoir discrétionnaire de l'exécutif**.

En cas d'échec au test de proportionnalité, le juge administratif peut annuler totalement l'acte réglementaire instituant un fichier, ce qui est très rare[139]. Il peut également annuler partiellement l'acte en question : ce fut le cas en 2009 pour le fichier ELOI et en 2011 pour le fichier des passeports électroniques.

2. Les contentieux variés concernant les fichiers soumis au juge administratif ordinaire

Le juge administratif est également compétent pour les recours contre les décisions de la CNIL[140], ou contre les refus d'effacement ou de rectification du procureur lorsque la possibilité de saisir le JLD n'est pas prévue par les textes. Il n'hésite pas à sanctionner l'absence de motivation des refus de communiquer certaines informations[141], et considèrent que le refus de communiquer des données ne relève pas d'un pouvoir discrétionnaire absolu des responsables de traitement et de la CNIL[142].

Il est aussi le juge des décisions administratives fondées sur la consultation des fichiers de police : principalement des décisions de refus d'agrément, mais aussi des refus d'autorisations à se présenter au concours d'admission à l'école des officiers de la gendarmerie nationale, d'habilitations permettant l'accès à certaines zones des aéroports, d'autorisations d'acquisition et détention d'armes, de demandes de naturalisation, de délivrance d'un titre de séjour, etc.[143].

Il connaît aussi des recours contre des sanctions disciplinaires infligées par le ministère de l'Intérieur à l'encontre de policier·e·s ou gendarmes reconnu·e·s coupables de consultation illégale de fichiers.

[138] Conseil d'État, 26 octobre 2011, req. nº 317827.
[139] Gérald Béranger, *op. cit.*
[140] Conseil d'État, 12 mars 1982, Recueil Lebon, p. 107.
[141] Fichiers de police, *op. cit.*, point 64.
[142] *Ibid.*, point 67.
[143] *Ibid.*, points 69 et 70.

3. La formation spécialisée du Conseil d'Etat : un contrôle restreint par les impératifs du secret d'État

La loi 2015-912 du 24 juillet 2015 créé au sein du Conseil d'État une formation spécialisée, compétente pour contrôler les services de renseignements, et notamment les fichiers qu'ils utilisent ainsi que les techniques de renseignement qu'ils mettent en œuvre. L'objectif est de remédier au caractère ineffectif du contrôle par le juge administratif, limité par l'impossibilité d'accéder à certains contenus protégés par le secret de la défense nationale[144]. Pour la première fois en 2015, un organe juridictionnel est autorisé à accéder aux données classifiées au titre du secret de la défense nationale sans que l'administration puisse s'y opposer. L'article R. 841-2 du code de la sécurité intérieure liste les traitements automatisés de données à caractère personnel intéressant la sûreté de l'Etat qui sont concernés par le contrôle de la formation spécialisée : CRISTINA, SIREX, DOREMI, FSPRT, FPR, STARTRAC, BCR-DNRED, GESTEREX, BIOPEX, LEGATO, ACCReD. De leur fonctionnement on ne connaît que leur nom, car les décrets les instituant ne sont pas publiés. La grande majorité du contentieux (90%) devant cette formation concerne les fichiers[145].

L'existence d'une juridiction unique pour connaître de ce contentieux permet de limiter les agent·e·s habilité·e·s au secret de la défense nationale et de spécialiser cette formation dans ce contentieux. La formation est composée de trois membres et un·e rapporteur·ice public·que, comme une formation de base du Conseil d'État. Ses membres reçoivent une habilitation ès qualité de membre de la formation et non pas personnelle[146].

Cette formation peut être saisie par la CNCTR ou par « *toute personne* ». Pour la CNCTR, la saisine est facultative en principe et intervient soit lorsque le gouvernement est passé outre un avis défavorable ou n'a pas mis fin aux irrégularités dénoncées, soit à titre initial dans un délai d'un mois suivant la connaissance de la mise en œuvre d'une technique de renseignement. La saisine est obligatoire pour la CNCTR dans le cas où le gouvernement autorise l'utilisation de dispositifs de surveillance dans un lieu privé à usage d'habitation malgré un avis défavorable de la CNCTR. La saisine par « *toute personne* », vraisemblablement, renvoie à une saisine par toute personne juridique et non uniquement par

144 Olivier Le Bot, *Le contentieux du renseignement devant la formation spécialisée du Conseil d'État,* RFDA, 2017, p. 721.
145 *Ibid.*
146 *Ibid.*

des personnes physiques : il serait en effet peu probable, au regard de la finalité de la loi, que le CE restreigne l'accès à son prétoire aux seules personnes physiques, bien qu'elles soient les seules à saisir cette formation jusqu'alors[147]. La demande est recevable lorsque l'auteur a un intérêt à agir, apprécié largement, c'est-à-dire que la demande doit concerner sa situation personnelle ; le ministère de l'avocat n'est pas obligatoire ; le requérant doit avoir préalablement saisi la CNIL ou la CNCTR.

Le contentieux devant cette formation est tout à fait spécifique et répond à des règles d'instruction et de jugement dérogatoires : les pièces du dossier qui comportent des informations classées secret de la défense nationale – dont les fameuses « notes blanches » - ne sont pas communiqués au·à la requérant·e, les parties sont entendues séparément, les conclusions du·de la rapporteur·ice public·que sont la plupart du temps lues en l'absence des parties et du public. Ce fonctionnement est fortement critiqué en ce qu'il porte atteinte à l'égalité des armes et au principe du contradictoire : l'administration, défenderesse, a accès aux informations qui sont gardées secrètes à l'égard du·de la requérant·e.

Il convient toutefois de souligner que l'efficacité du contrôle juridictionnel est garantie par deux éléments capitaux. Premièrement, **le juge a accès à tous les documents qu'il juge nécessaires à sa décision, sans que l'on puisse lui opposer le secret de la défense nationale**. C'est tout l'intérêt de cette formation spécialisée. En outre, « *la formation de jugement peut soulever d'office tout moyen* » (article L. 773-5 du code de justice administrative), dérogeant ainsi au principe selon lequel le juge ne peut relever d'office que les moyens d'ordre public. Cette possibilité permet de combler les lacunes éventuelles dans l'argumentation du requérant, dues au secret des pièces du dossier. **Le juge a donc le pouvoir de sanctionner d'office toute illégalité**[148]. On pourrait, pour augmenter le niveau d'information du requérant en préservant le secret de la défense nationale, autoriser sa représentation par un·e avocat·e spécialement habilité·e au secret de la défense nationale, comme c'est le cas au Royaume-Uni[149].

Le contrôle effectué par le juge est celui de la légalité, et non pas de l'opportunité. Il contrôle uniquement la légalité interne. La motivation de la décision est souvent réduite : le

[147] *Ibid.*
[148] *Ibid.*
[149] *Ibid.*

requérant doit faire confiance au juge sur la façon dont ses vérifications ont été menées. Le juge peut seulement enjoindre à l'autorité gestionnaire du fichier de rétablir la légalité en effaçant ou rectifiant les données. Les censures dans le cadre de cette procédure sont rares, mais il est difficile de savoir si cette rareté doit être analysée comme le fruit de la retenue du juge ou de l'inefficacité de son jugement, ou bien comme étant la preuve d'une réelle absence d'illégalité[150].

Il s'agit désormais de généraliser le recours à cette formation, dont les spécificités règlent un certain nombre de problèmes qui se posent pour les autres juges du contentieux relatif aux fichiers. Pour être à la hauteur des enjeux individuels et sociaux, la formation devrait être élargie, et « il serait souhaitable que tout refus de levée du secret puisse lui être soumis, tant à l'initiative d'un juge qu'à celle d'un particulier »[151].

C) Le contrôle opéré par le Conseil constitutionnel : un juge peu regardant à l'égard de la création de fichiers

Le Conseil constitutionnel, quant à lui, est susceptible d'examiner la constitutionnalité des fichiers créés par voie législative. Il les examine au regard de l'article 8 de la Convention EDH, mais également au regard de l'article 66 de la Constitution[152] et de l'article 2 de la DDHC[153]. Pour lui, comme pour le Conseil d'État, le droit au respect de la vie privée implique que « la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiées par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif ». Le contrôle de la proportionnalité effectué par le juge constitutionnel est de même porté que celui effectué par le juge administratif.

En pratique, le juge constitutionnel a validé la quasi-totalité des fichiers qui ont été soumis à son examen. En cas d'atteinte excessive au droit au respect de la vie privée, il peut valider des systèmes qu'il estime suffisamment protecteurs en les complétant par des

[150] *Ibid.*
[151] *Ibid.*
[152] CC, 18 janvier 1995, déc. n°94-352DC.
[153] CC, 23 juillet 1999, déc. n°99-416DC ; CC, 13 mars 2014, déc. n°2014-690DC.

réserves d'interprétation, comme ce fut le cas pour le FNAEG[154]. Au contraire, il n'a pas validé la création du fichier d'identité biométrique car le fichier avait vocation à s'appliquer à une part importante de la population, les données concernées étaient très sensibles et les précautions insuffisantes[155].

IV. Le contrôle opéré par les personnes concernées par le fichier : un recours individuel restreint et indirect

Le contrôle exercé par les personnes concernées par le fichier est un enjeu majeur, tant il permet l'accès de chacun·e à ses données collectées, et représente ainsi une prérogative importante en matière de libertés individuelles (A). Ce droit reste cependant peu accessible, au vu d'une procédure lente, indirecte et juridiquement complexe (B).

A) Un enjeu de taille : les conséquences personnelles du fichage

Par définition, le traitement de données personnelles constitue une atteinte à la vie privée. Par opposition au casier judiciaire, les fichiers contiennent des informations sur des personnes qui n'ont pas nécessairement été condamnées : **la ligne rouge de l'atteinte à la présomption d'innocence est proche, si ce n'est franchie dans certaines situations, d'autant plus que le nombre d'agent·e·s public·que·s bénéficiant d'un accès direct ou indirect ne cesse de croître**[156]. La CNIL dénonce ainsi un détournement de la finalité première des fichiers, qui est de faciliter l'investigation policière, et leur utilisation comme une « mémoire policière supplantant totalement la mémoire du casier judiciaire »[157].

Le risque principal réside du point de vue de la personne dans les enquêtes préalables au recrutement et à l'agrément de certaines professions. Ces enquêtes peuvent mener à des licenciements et des refus d'embauche injustifiés[158] pour les professions d'agent·e de sécurité privée, dans les sociétés de transports parisiens, de médiateur·ice et délégué·e du procureur,

[154] *Le contentieux du renseignement devant la formation spécialisée du Conseil d'État, op. cit.*
[155] CC, 22 mars 2012, déc. n°2012-652DC.
[156] Virginie Gautron, *La prolifération incontrôlée des fichiers de police*, *AJ Pénal*, 2007, p. 57.
[157] Jean Danet, *Le droit pénal et la procédure pénale sous le paradigme de l'insécurité,* Arch. po. crim., n° 25, 2003, p. 37-69.
[158] CNIL, 26e rapport d'activité 2005 de la CNIL, 2006, p. 93 et s.

de contrôleur·ice judiciaire, de magistrat·e, préfet·e, ambassadeur·ice, policier·e, personnels de l'administration pénitentiaire, agent·e des services publics urbains de transports en commun, agent·e des concessionnaires d'autoroute, etc. Dans une circulaire du 15 avril 2005, le ministre de l'Intérieur a toutefois précisé aux préfets qu'une simple mention sur un fichier de police ou au casier judiciaire ne saurait conduire à un avis défavorable : ces fonctionnaires doivent apprécier les éléments mentionnés aux fichiers et « leur gravité, leur ancienneté, les suites judiciaires qui, le cas échéant, leur ont été données, et leur éventuelle répétition »[159]. Il existe également un risque d'atteinte à la liberté d'aller et venir car l'inscription à certains fichiers peut justifier l'interdiction de certains lieux, un refus de délivrance de visa ou d'un titre de séjour, ou le refus d'entrée sur le territoire de la République.

Ces enjeux sont compensés juridiquement par des droits au profit des citoyen·ne·s : le droit d'information, le droit d'opposition, le droit d'accès, et le droit de rectification. En matière de fichiers d'Etat, **ces droits subissent tellement d'exceptions qu'ils sont parfois presque vidés de leur substance**.

- Le **droit d'information** (article 116 de la loi « informatique et libertés ») correspond au droit de connaître l'identité du·de la responsable de traitement, la finalité du fichier, etc. Mais puisque dans certains cas, le droit à l'information est considéré comme pouvant compromettre les enquêtes, il y est fait exception notamment lorsque les données sont collectées pour la prévention, la recherche ou la poursuite d'infractions pénales, ou pour les traitements intéressant la sûreté, la défense, la sécurité publique, ou ayant pour objet l'exécution de condamnations pénales ou de mesures de sûretés. C'est le cas du fichier CRISTINA et du TAJ.

- Le **droit d'opposition** (article 110 de la loi « informatique et libertés ») à ce que des données à caractère personnel concernant une personne fassent l'objet d'un traitement est quasi inopérant en matière de fichiers de police et de gendarmerie[160], puisqu'il ne s'applique pas « lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte instaurant le traitement »[161].

[159] *La prolifération incontrôlée des fichiers de police*, *op. cit.*.
[160] Alain Bauer, Christophe Soullez, *Les fichiers de police et de gendarmerie*, *op. cit.*, p. 56.
[161] Loi n°78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, Article 110, alinéa 2.

- Le **droit d'accès** (article 119 de la loi « informatique et libertés ») est le plus important : en principe, toute personne a le droit d'obtenir « la confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet » d'un traitement, ainsi que « la communication, sous une forme accessible » de ces données[162]. Ce droit est la condition de la rectification ou de l'effacement des données inexactes ou conservées de façon illégale. Nous y reviendrons.

B) Un droit à l'accès malmené par une procédure complexe

Le droit d'accès est direct ou indirect : lorsqu'il est direct, la personne qui souhaite connaître les informations la concernant enregistrées dans un fichier peut solliciter directement le service gestionnaire du fichier pour obtenir confirmation ou infirmation de son enregistrement dans un fichier et une copie des données la concernant. Ainsi, pour le FAED et le FNAEG, l'accès est direct car le fichier contient des informations strictement objectives[163] que sont les empreintes digitales ou d'autres informations génétiques.

Mais pour les fichiers intéressant la sûreté de l'État, la défense et la sécurité publique, c'est-à-dire la majeure partie du temps, l'accès est indirect. Dans ce cas, c'est via la CNIL qu'il existe : le·la commissaire de la CNIL chargé des vérifications exerce en lieu et place du·de la demandeur·se le droit d'accès, de rectification ou d'effacement des données inexactes ou conservées en contradiction avec la loi.

Le droit à l'accès conditionne en partie le droit à la rectification ou à l'effacement des données : lorsque les personnes concernées n'ont pas connaissance du détail des informations enregistrées, il n'est pas toujours possible de les contester pour les faire rectifier. Dans ces cas, la CNIL peut uniquement demander la suppression des informations dont la collecte ou la conservation est illégale. Si les informations étaient transmises à la personne concernée, elles pourraient être corrigées : cela permettrait la conservation de données rectifiées au lieu de les supprimer, alors qu'elles pourraient être utiles pour la sécurité publique, ainsi que la rectification d'informations qui ne correspondraient pas aux critères pour être supprimées.

[162] *Ibid.*, Article 119, II., 1° et 4°.
[163] Alain Bauer et Christophe Soullez, *Les fichiers de police et de gendarmerie, op. cit.*, p. 60.

La procédure est généralement très complexe et longue : il faut s'adresser à plusieurs services différents, qui ne sont pas toujours aisément identifiés, que ce soit la CNIL, des services de police, des parquets. C'est d'autant plus le cas si le·la requérant·e fait l'objet de multiples inscriptions, dans des ressorts juridictionnels différents. Il faut noter toutefois que l'exercice du droit d'accès a été assoupli par le juge administratif à partir de 2002, lorsqu'il s'est reconnu compétent pour apprécier le caractère communicable ou non communicable des informations contenues dans un fichier.

Pour remédier à ces lourdeurs administratives, certains défenseurs des libertés proposent la **mise en place d'un système où chacun·e pourrait constater en ligne la consultation de données la·le concernant**. Sans nécessairement impliquer d'atteintes au secret inhérent à certains fichiers, ce système pourrait servir de garde-fou car les agent·e·s ayant accès aux fichiers se garderaient de les consulter lorsque cela n'est pas nécessaire ou pour des motifs étrangers aux finalités et à la consultation régulière des fichiers. Par ailleurs, un tel dispositif pourrait désengorger la CNIL en satisfaisant certain·e·s citoyen·ne·s désireux de consulter la « mémoire policière ».

A l'issue de l'examen de l'encadrement national des fichiers, force est de constater deux problèmes majeurs. Premièrement, **les modalités de l'encadrement des fichiers de police sont, comme nous l'avons vu, totalement éclatées**. Le contrôle est réparti entre autorités administratives indépendantes (CNIL, CNCTR), juridictions administrative, judiciaire et constitutionnelle, juge ordinaire et juge spécial, procureurs, hiérarchie des services de police et de gendarmerie, ministères. L'attribution de la compétence pour les contentieux concernant les fichiers répond à une logique, certes, mais elle est extrêmement complexe et difficile d'accès pour le justiciable. Cet éclatement peut en partie être expliqué par la multiplicité des usages des fichiers de police, en matière de police administrative et de police judiciaire. Il conviendrait d'unifier cette répartition des compétences, et la formation spécialisée du Conseil d'Etat offre pour cela des perspectives intéressantes.

Enfin, **la chaîne de l'encadrement des fichiers, à partir de leur création et pendant leur durée d'usage, ne paraît pas satisfaisante du point de vue des droits et libertés**. Les fragilités des procédures de création des fichiers, et notamment le caractère superflu de la consultation de la CNIL, ne sont pas réellement compensées par les autres étapes de la vie du

fichier, puisque les juges sont difficiles d'accès et leurs contrôles souvent permissifs. **Une juridiction véritablement spécialisée et investie dans ce champ juridique, ainsi qu'un avis conforme de la CNIL, au moins pour certains types de fichiers, permettraient de pallier quelque peu ce manque d'encadrement sérieux**.

PARTIE 2 :
LES CROISEMENTS ENTRE FICHIERS :
L'EXEMPLE DU TRAITEMENT « ACCRED »

Plus précisément, dans ce rapport, nous souhaiterions nous concentrer sur la question de l'interconnexion, dont nous tenterons de donner une définition, à la fois légale mais également critique afin de tenter de déceler la dangerosité de cette pratique et plus largement des croisements entre fichiers (Chapitre 1, I). Afin de rendre compte de ce danger, il nous paraissait pertinent de nous pencher sur un fichier qui interconnecte et relie lui-même différents fichiers. Nous avons ainsi décidé de prendre l'exemple du fichier « automatisation de la consultation centralisée de renseignements et de données » (ACCReD) (Chapitre 1, II).

Pour cela, nous verrons les croisements de fichiers sensibles permis par ACCReD en détaillant les fichiers auxquels l'ACCReD donne accès (Chapitre 2). Finalement, une approche critique nous paraît nécessaire pour voir comment l'ACCReD met en péril et menace avec acuité nos libertés individuelles (Chapitre 3).

CHAPITRE 1 :
INTERCONNEXIONS ET CROISEMENTS ENTRE FICHIERS DE POLICE :
ACCRED, UN ARCHETYPE

Avant d'analyser l'ACCReD précisément, il convient de revenir sur des éléments de définition en nous interrogeant sur la définition légale de l'interconnexion. Celle-ci paraît largement critiquable, nous lui substituerons donc par la suite le terme de croisement de fichier (I). Nous expliquerons ensuite pourquoi notre choix s'est porté précisément sur l'ACCReD comme symptômatique de l'intensification des croisements entre fichiers (II).

I. De la définition légale insatisfaisante des « interconnexions » à l'élaboration de nouveaux critères des « croisements »

L'interconnexion entre fichiers a intéressé le législateur dès l'adoption de la loi Informatique et Libertés. En effet, la loi du 6 janvier 1978 a été adoptée après que le journal Le Monde a révélé l'intention de l'INSEE de fusionner l'ensemble des fichiers détenus par l'administration via un identifiant unique afin de créer un système automatisé pour les fichiers administratifs et le répertoire des individus[164].

L'émoi populaire provoqué par cette découverte a conduit à la mise en place de la commission d'enquête dirigée par Bernard Tricot, qui a abouti au vote de la loi n°78-17 du 6 janvier 1978. Dès l'adoption de cette loi, la méfiance envers les interconnexions entre fichiers a pu être consacrée par les textes.

Ainsi, la loi initiale prévoyait en son article 25 que « *sont mis en œuvre après autorisation de la CNIL : 5e) les traitements automatisés ayant pour objet : [...] (ii) l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes* ».

Plus encore, depuis l'application du RGPD, l'interconnexion reste mentionnée par l'article 30 de la loi parmi les éléments devant être précisés dans les demandes d'autorisation et les demandes d'avis adressées à la CNIL.

Il n'existe cependant **aucune définition légale de l'interconnexion**[165], bien que la notion soit présente dans la loi de 1978, et même dans le code de procédure pénale[166]. Le Conseil d'État a cependant précisé la notion d'interconnexion : « *l'interconnexion doit être regardée comme l'objet même d'un traitement qui permet d'accéder à, d'exploiter et de traiter automatiquement les données collectées pour un autre traitement et enregistrées dans le fichier qui en est issu* »[167].

[164] *Fichiers de police, op. cit.,* p. 10.

[165] Rapport parlementaire Batho-Bénisti, n°4113, 21 déc. 2011, p. 96, (URL : https://www.assemblee-nationale.fr/13/rap-info/i4113.asp#P896_262530).

[166] Article 777-3 du code de procédure pénale : Aucune interconnexion au sens du 3° du I de l'article 33 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ne peut être effectuée entre le casier judiciaire national automatisé et tout autre fichier ou traitement de données à caractère personnel détenus par une personne quelconque ou par un service de l'Etat ne dépendant pas du ministère de la justice. Le casier judiciaire national peut toutefois recevoir les données d'un fichier ou traitement de données à caractère personnel détenu par un service de l'Etat pour l'exercice des diligences prévues au présent titre.

[167] Conseil d'Etat, 19 juillet 2010, Décision N°317182, 323441.

De cette définition dégagée par le Conseil d'État, la CNIL a développé un faisceau d'indices permettant de reconnaître un traitement d'interconnexion. Ainsi, les trois critères sont les suivants : **l'objet du traitement porte sur la mise en relation entre fichiers, il concerne au moins deux fichiers distincts ayant des finalités différentes, et enfin il intervient dans le cadre d'un processus automatisé**. Si ce processus n'est pas automatisé, la CNIL considère qu'il s'agit d'un simple rapprochement de fichiers[168].

Les **objectifs de ces interconnexions sont clairement affichés par les pouvoirs publics : l'échange d'informations automatique entre différents services, la mutualisation de l'alimentation entre différents fichiers, la mise à jour automatique des données, la consultation simultanée de plusieurs fichiers, le recoupement des informations sur une même personne**[169]. D'ailleurs, le décret du 2 août 2017 « *modifiant les traitements automatisés de données à caractère personnel prévus aux articles R. 236-1, R. 236-11 et R. 236-21 du code de la sécurité intérieure* » a abrogé les anciens articles R. 236-8, R. 236-18 et R. 236-28, qui disposaient respectivement que le traitement des enquêtes administratives liées à la sécurité publique (EASP), le traitement « Prévention des atteintes à la sécurité publique » (PASP) et le traitement « Gestion de l'information et prévention des atteintes à la sécurité publique » ne pouvait faire « *l'objet d'aucune interconnexion, aucun rapprochement ni aucune forme de mise en relation avec d'autres traitements ou fichiers* ». Dès lors, **les derniers verrous ayant sauté, tout semble possible en matière d'interconnexion entre fichiers de police**[170].

De nombreux fichiers sont d'ores et déjà interconnectés selon la définition de la CNIL. Ainsi, par un décret n°2019-412 du 6 mai 2019, le gouvernement a autorisé le croisement du fichier Hopsyweb, relatif au suivi des personnes en soins psychiatriques sans consentement, avec celui des signalements pour la prévention et la radicalisation à caractère terroriste. Par une décision du 27 mars 2020, le Conseil d'État a validé cette interconnexion en rejetant l'ensemble des recours contre ce décret. Pourtant, la CNIL avait, dans son avis,

[168] Rapport parlementaire Batho-Bénisti, *op. cit*.
[169] Rapport parlementaire Paris-Morel-à-L'huissier, *op.cit,* p.43,
[170] Marc Rees, Dans la torpeur de l'été, la grande foire aux fichiers de sécurité, 16 août 2017, NextInpact, (URL : https://www.nextinpact.com/article/27019/104933-dans-torpeur-lete-grande-foire-aux-fichiers-securite?fbclid=IwAR2iaCsyjcrHGn9jVyVpxju7KlQXeSQ0roN4eFW2F_Rsqcof2WHxzNtW4j4).

largement critiqué la possibilité d'interconnecter ces deux fichiers au regard de la « *différence profonde entre les deux fichiers* » et appelait à une grande vigilance[171].

L'interconnexion entre les fichiers semble être une question intéressant particulièrement les pouvoirs publics. Ainsi, dans leur rapport du 17 octobre 2018, les députés Paris et Morel soulignait « *l'intérêt du développement des interconnexions* »[172]. Pourtant, la CNIL reconnaît elle-même des risques majeurs de l'interconnexion de fichiers distincts. Ainsi, **le nouveau traitement formé à partir d'une interconnexion pourra avoir d'autres finalités que celles initialement prévues**. L'interconnexion peut révéler une "*extension occulte du champ du fichier*". Elle fait peser un risque sur le respect des secrets professionnels et peut avoir un effet néfaste sur la durée de conservation des données[173].

Cependant, en contraste avec toutes les potentialités nouvelles posées par les interconnexions entre fichiers, celles-ci restent obscures, du fait notamment qu'**il n'existe aucune définition légale précise de la notion d'interconnexion**. De plus, le développement certain des interconnexions interroge à plus d'un titre, surtout au regard du respect des libertés individuelles. Pourtant, cette problématique de l'interconnexion entre fichiers n'est que très peu traitée, tant par la littérature scientifique que par le champ médiatique. `
Pour toutes ces raisons, nous avons choisi de nous saisir de la problématique de l'interconnexion dans ce rapport.

Pour autant, la définition dégagée par le Conseil d'Etat ainsi que les critères retenus par la CNIL nous paraissent **trop restrictifs** pour envisager le phénomène de rapprochement, comparaison, interconnexion des données contenues dans les fichiers. Par exemple, le critère de l'automatisation du traitement rapprochant deux fichiers distincts exclut de nombreux croisements déjà constitués et non nécessairement automatisés et passés sous silence ; ces derniers ne portent d'ailleurs pas le nom d'interconnexion. Ces différents croisements, échappant à la notion d'interconnexion selon la CNIL, interrogent sur leur légalité, permettent

[171] Lisa Carayon, "Quelle folie !", La Revue des droits de l'homme [Online], Actualités Droits-Libertés, Online since 11 June 2020, connection on 14 June 2021. (URL: http://journals.openedition.org/revdh/9746; DOI: https://doi.org/10.4000/revdh.9746).
[172] Rapport parlement Paris-Morel-à-L'huissier, op. cit., p. 44.
[173] Rapport parlementaire Batho-Bénisti, op. cit., p. 96.

des rapprochements entre des fichiers pour lesquels le législateur ou le gouvernement avait pourtant exclu la possibilité d'interconnexion.

C'est pourquoi **nous proposons de distinguer les interconnexions selon le faisceau d'indices développé par la CNIL, des rapprochements de fichiers et de la notion de *croisement* que nous leur préférons**. Plus large, elle permet de mieux rendre compte de la fluidité de ces types d'usages des fichiers, et donc des menaces que ces derniers représentent pour les droits et libertés fondamentaux. Nous évoquerons ainsi les interconnexions prévues par les textes juridiques, telles que le croisement entre HOPSYWEB et le FSPRT mais également les croisements effectifs mais non prévus par un fondement juridique. Pour cela, nous avons élaboré une liste de critères qui constitue à son tour **un faisceau d'indices alternatif à celui de la CNIL**. Ils permettent d'identifier des croisements réels ou potentiels entre fichiers, que ces critères se cumulent ou non.

- Tout d'abord, **le critère des finalités** prévues par les textes au sens de la loi n°78-17 du 6 janvier 1978 nous permet d'observer les finalités communes entre les fichiers permettant certains rapprochements. Par exemple, les fichiers FIJAIT (Fichier judiciaire national automatisé des auteurs d'infractions terroristes), PASP (Fichiers de prévention des atteintes à la sécurité publique de la police), GIPASP (Gestion de l'information et prévention des atteintes à la sécurité publique) et FSPRT (Fichier de traitement des signalés pour la prévention et la radicalisation à caractère terroriste) ont tous pour finalité de prévenir ou lutter contre les activités terroristes.

- Ensuite, nous envisageons le **critère des usages thématiques**, plus large que celui des finalités, afin de regrouper les fichiers par thématiques communes pour identifier les domaines régis via ce fichier. Ainsi, de nombreux fichiers semblent concerner les personnes étrangères. Des fichiers aussi variés que l'AGDREF (Application de gestion des dossiers des ressortissants étrangers en France), le FPR (Fichier des personnes recherchée) mais également SETRADER ou l'ACCRED (Automatisation de la consultation centralisée de renseignements et de données) sont utilisés dans ce domaine (lutte contre l'immigration irrégulière, fichier répertoriant les personnes bénéficiant d'un titre de séjour, fichiers consultables lors de la délivrance d'un titre de séjour…).

- En outre, il nous paraît important de nous pencher sur les **autorités ayant accès aux fichiers**. A travers ce critère organique, le but serait d'observer un éventuel éloignement empirique par rapport à la lettre des textes, et de voir comment la pratique cache des croisements possibles et non prévus par la loi. Ce critère permettrait notamment d'observer les croisements réels. En effet, si les fichiers ne s'autoalimentent pas automatiquement, le fait qu'une même personne ait accès à plusieurs fichiers a nécessairement un impact, extrêmement difficile à analyser, sur le croisement entre les différents fichiers. Ainsi, si un OPJ habilité veut observer les opinions politiques d'un militant venant de se faire arrêter, il pourra tout d'abord consulter le TAJ mais également le PASP.

- Le **critère des logiciels utilisés** paraît de plus en plus important. Il s'agit ici d'étudier quel logiciel de gestion est propre à quel groupe de fichiers, et d'observer ainsi si la même plateforme ne permet pas des ponts plus aisés entre fichiers n'ayant *a priori* pas de liens entre eux. Ainsi, les logiciels LRPPN (Logiciel de rédaction des procédures de la police nationale) et LRPGN alimentent automatiquement le TAJ, le Fichier des Objets et Véhicules signalés (FOVe) et CASSIOPEE et échangent des informations avec GASPARD NG, logiciel permettant de remplir simultanément le TAJ et le FAED. Par ailleurs, le dispositif de la reconnaissance faciale, de plus en plus utilisé, interroge sur les possibles croisements qu'il pourra effectuer. La reconnaissance faciale est déjà prévue pour le TAJ[174] mais semble également être développée pour les fichiers PASP et GIPASP[175]. L'ambition affichée de développer cette technologie a d'ailleurs déjà eu des effets sur les rapprochements entre fichiers. Ainsi, le décret n° 2020-151 du 20 février 2020 portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « application mobile de prise de notes » autorisait les gendarmes à prendre en photo n'importe quelle personne suspectée d'avoir commis une infraction, transmise au LRPGN qui les transmettait à son tour au TAJ. Les informations pouvaient alors être utilisées par un système de reconnaissance faciale pour identifier les personnes[176].

[174] Article R. 40-26 1° et 3° du code de procédure pénale.
[175] Décrets PASP: fichage massif des militants politiques, La Quadrature du net, 8 décembre 2020, (URL https://www.laquadrature.net/2020/12/08/decrets-pasp-fichage-massif-des-militants-politiques/?fbclid=IwAR1CQfXlw9s2sFfq2ldrhUt4ZC1cVL12MnqZAHg6sdLV2bSscYxn7Nqjb_4).
[176] Gendnotes, faciliter le fichage policier et la reconnaissance faciale, La Quadrature du net, 25 février 2020, https://www.laquadrature.net/2020/02/25/gendnotes-faciliter-le-fichage-policier-et-la-reconnaissance-faciale/

Si le Conseil d'Etat a annulé la possibilité d'alimenter le TAJ puis de récolter des données de reconnaissance faciale simplement à travers le transfert des notes de gendarmes et des photos, il appelle le gouvernement à encadrer le transfert de données et préciser les fichiers vers lesquels un tel transfert est possible[177]. **Ainsi, l'interconnexion des fichiers à travers la reconnaissance faciale apparaît comme inévitable dans le futur**.

Les croisements entre fichiers appellent différentes questions : ce croisement est-il automatisé, auquel cas peut-il répondre à la définition donnée par la CNIL ? Quel est l'encadrement législatif ou réglementaire des différents croisements ? Les croisements peuvent-ils être indirects et si oui, comment les détecter ? Quand les croisements entre fichiers correspondent-ils finalement à une légalisation d'une pratique clandestine préexistante ? Ces pratiques policières et gouvernementales illégales nous permettent-elles d'annoncer certains croisements à venir ?

Nous tenterons de répondre à ces questions en reprenant les critères nous permettant d'établir l'existence d'un croisement entre différents fichiers. Afin d'illustrer notre propos, nous nous proposons de réaliser une étude de cas sur ACCReD.

II. ACCReD comme symptôme de l'intensification des croisements entre fichiers

Le fichier « Automatisation de la consultation centralisée de renseignements et de données » (ACCReD) a été créée par le décret n°2017-1224 du 3 août 2017.

Décret n°2017-1224 du 3 août 2017

Article 1 :

Finalité : « *faciliter la réalisation d'enquêtes administratives en application des articles L. 114-1, L. 114-2 et L. 211-11-1 du code de la sécurité intérieure et de l'article 17-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité et d'exploiter les informations recueillies dans ce cadre* »

[177] *Ibid.*

Article 7

Le « *traitement mentionné à l'article 1er peut procéder à la consultation automatique et, le cas échéant, simultanée des traitements de données à caractère personnel suivants aux seules fins de vérifier si l'identité de la personne concernée y est enregistrée* ».

ACCReD permet donc un accès automatisé et simultané au TAJ, à l'EASP, au PASP, GIPASP, FPR, N-SIS II, FSPRT, FoVES, CRISTINA, GESTEREXT, SIREX et le fichier de la DGSE. Il était en effet possible pour l'administration, auparavant, d'accéder à ces fichiers dans le cadre de certaines enquêtes administratives. Cependant, le caractère automatisé de l'ACCReD permet, à travers la simple identité de la personne, de recueillir un nombre très important d'informations sur la personne de manière simultanée.

ACCReD n'est **pas un fichier d'interconnexions selon la définition de la CNIL**. En effet, il n'alimente pas automatiquement les fichiers auxquels ce traitement de données peut donner accès. C'est un **« logiciel de rapprochement »**, c'est-à-dire « *un logiciel qui permet, à travers une base de données aux entrées multiples, de créer des relations entre toutes les informations contenues dans différents fichiers : faciliter l'interconnexion de fichiers jusqu'alors séparés* »[178]. Cependant, la possibilité de conduire une consultation automatique et simultanée conduit à affirmer que l'ACCReD permet un croisement entre ces différents fichiers. En effet, il correspond à une base de données unique permettant de savoir, en ayant uniquement l'identité de la personne, si elle figure à l'un ou plusieurs de ces douze fichiers.

Ce fichier est consulté pour un nombre très conséquent d'enquêtes administratives. Ainsi, les décisions administratives de recrutement d'affectation, d'autorisation, d'agrément ou d'habilitation dans des secteurs très larges[179], tels que les emplois publics participant à l'exercice des missions de souveraineté de l'Etat peuvent faire l'objet d'une enquête administrative facilitée par l'ACCReD. Les enquêtes administratives permettent également de contrôler l'accès des personnes aux installations où se déroulent de grands évènements.

[178] Claire Bruggiamosca et Christophe Daadouch, *Le fichage des mineurs : entre ordre public et libertés individuelles*, 20 juin 2019, Berger-Levrault, p. 184libertés individuelles, 20 juin 2019, Berger-Levrault, p. 184p. 245.

[179] Patrick Canin, Le décret ACCRED ou comment automatiser le traitement de données à caractère personnel, Lettre d'information de la Ligue des droits de l'Homme, 20 septembre 2017, https://www.ldh-france.org/decret-3-aout-2017/

Cette possibilité très large de consulter l'ACCReD a fait l'objet de critiques de la part de la CNIL. Elle affirmait ainsi dans sa délibération qu'« *en l'absence de précisions fournies par le ministère sur les enquêtes précisément concernées par le dispositif projeté et en l'absence de justification sur la nécessité, pour chacune d'entre elles, de consulter ces traitements sensibles, la commission estime que la proportionnalité du dispositif n'est pas démontrée* »[180].

Ne prenant pas en compte les recommandations de la CNIL, le pouvoir réglementaire a même de nouveau élargi le périmètre de l'accès à l'ACCReD en permettant la consultation du fichier dès qu'une personne fait une demande de premier titre de séjour, de renouvellement ou de naturalisation[181]. Un tel positionnement et de tels choix ne peuvent que questionner sur la finalité réelle du dispositif.

En outre, les différents fichiers auxquels l'ACCReD donne accès contiennent des données dites sensibles. L'article 3 du décret du 3 août 2017 prévoit dès lors que sont « *autorisés, pour les seules fins et dans le strict respect des conditions définies par le présent décret, la collecte, la conservation, et le traitement de données mentionnées au I du même article 8, à la condition que leur collecte soit indispensable à la réalisation des enquêtes administratives et dans les seuls cas où ces données se rapportent à des opinions politiques, philosophiques ou religieuses* ». **Il paraît inquiétant que l'autorité administrative puisse se fonder sur des opinions personnelles pour prendre des décisions**[182].

Si l'administration avait préalablement accès à ces différents fichiers contenant des données dites sensibles dans le cadre d'enquêtes administratives, elle ne semblait pas pouvoir consulter ces données et être seulement dans la capacité de voir si une personne figurait dans un fichier particulier ou non. Cependant, il nous est difficile d'affirmer avec certitude **que le fichier ACCReD n'est pas venu légaliser une pratique préexistante**, qui consistait déjà en la consultation de ces données grâce à un cadre légal extrêmement flou.

[180] Délibération n° 2017-152 du 18 mai 2017 portant avis sur un projet de décret portant création d'un traitement automatisé de données à caractère personnel dénommé « ACCRED » (demande d'avis n° 17006644), CNIL, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000035467065/

[181] Décret n° 2019-1074 du 21 octobre 2019 modifiant le décret n° 2017-1224 du 3 août 2017 portant création d'un traitement automatisé de données à caractère personnel dénommé « Automatisation de la consultation centralisée de renseignements et de données »

[182] Le décret ACCRED ou comment automatiser le traitement de données à caractère personnel, Patrick Canin, Lettre d'information de la Ligue des droits de l'Homme, 20 septembre 2017, https://www.ldh-france.org/decret-3-aout-2017/

Nous nous proposons donc d'analyser le fichier ACCReD en tant qu'il nous paraît **symptomatique de l'intensification des croisements entre fichiers**, permettant l'établissement d'immenses bases de données personnelles automatisées auxquelles de nombreuses autorités administratives peuvent avoir accès. Nous étudierons en premier lieu les fichiers auxquels l'accès est permis par l'ACCReD. Puis plus précisément comment s'articulent les croisements entre les fichiers au sein de l'ACCReD, changeant potentiellement la nature des fichiers et les rendant d'autant plus dangereux pour les libertés individuelles.

CHAPITRE 2 :
LE DANGER DES CROISEMENTS EN CASCADE DE FICHIERS SENSIBLES PERMIS PAR ACCRED

Avant d'analyser le cas symptomatique d'ACCReD en tant que géante base de données et les dangers que cela pose pour nos libertés individuelles, nous allons analyser les fichiers auxquels cette méta-base de données donne accès. En effet, l'ACCReD permet d'accéder à douze fichiers contenant chacun des informations différentes sur les personnes et surtout dont de nombreux contiennent des données dites sensibles. Par ailleurs, ces fichiers mêmes font l'objet de croisements ou d'interconnexions avec d'autres fichiers non nécessairement compris dans l'ACCReD, permettant encore d'élargir les potentialités de croisement. Ainsi, pour mieux rendre compte de la problématique des croisements entre fichiers, nous décrirons chaque fichier en prenant en compte ses finalités, les données qui y figurent, les autorités y ayant accès et surtout les croisements dont il fait déjà l'objet.

I. Le TAJ

Le fichier de traitement des antécédents judiciaires est né de la fusion entre les fichiers JUDEX (Système d'information judiciaire de la gendarmerie nationale) et du STIC (système de traitement des infractions constatées) par l'article 11 de la loi LOPPSI du 14 mars 2011.

Il est intéressant de relever que ces deux fichiers aujourd'hui fusionnés dans le TAJ sont nés de pratiques policières légalisées *a posteriori*. Ainsi, le STIC est un fichier policier créé en 1985 mais soumis à la CNIL très tardivement. Il ne devient un fichier national que par

le décret n°2001-583 du 5 juillet 2001[183]. De la même manière, le JUDEX a été développé en 1986 mais n'a été institué formellement que par le décret n°2006-1411 du 20 novembre 2006[184]. Le TAJ est aujourd'hui codifié aux articles 230-6 et 230-11 du code de procédure pénale. Les modalités réglementaires le régissant découlent du décret n°2012-652 du 4 mai 2012 et ont été codifiées aux articles R. 40-23 et R. 40-34 du code de procédure pénale. D'après la CNIL, au 15 novembre 2018, plus de 18,9 millions de personnes mises en cause avaient une fiche au TAJ[185].

La finalité définie pour le TAJ paraît extrêmement large[186]. En vertu de l'article 230-6 du code de procédure pénale, le **TAJ a pour fonction de « *faciliter la constatation des infractions à la loi pénale* »**. D'après l'article R. 40-23 du code de procédure pénale, le TAJ vise « *à fournir aux enquêteurs de la police et de la gendarmerie nationales ainsi que la douane judiciaire une aide à l'enquête judiciaire, afin de faciliter la constatation des infractions, le rassemblement des preuves de ces infractions et la recherche de leur auteur* ».
La récolte des informations peut avoir lieu pour « tout crime ou délit ainsi que les contraventions de cinquième classe » qui sanctionnent soit un trouble à la sécurité ou à la tranquillité publiques, soit une atteinte aux personnes, aux biens ou à l'autorité de l'État.
Une des particularités très contestées de ce fichier est qu'il comprend également des informations sur les victimes de ces infractions bien qu'elles puissent s'opposer à ce que leurs données soient conservées lorsque l'auteur des fait a été définitivement condamné[187].

Les informations collectées sont extrêmement larges. Il s'agit de l'identité, du surnom ou alias, de la date et du lieu de naissance, de la profession, de la situation familiale, de la nationalité, de la filiation, de l'adresse, du téléphone, de l'adresse mail, des faits reprochés, des caractéristiques physiques, des dates des infractions reprochées etc… et peut contenir des données sensibles, si celles-ci « *résultent de la nature ou des circonstances de l'infraction ou se rapportent à des signes physiques particuliers, objectifs permanents, en tant qu'éléments de signalements des personnes, dès lors que ces éléments sont nécessaires* »[188].

[183] *Le fichage des mineurs : entre ordre public et libertés individuelles*, op. cit., p. 184
[184] Fichiers de police, op.cit, p. 48
[185] TAJ: Traitement d'Antécédents Judiciaires, 15 novembre 2018, CNIL, https://www.cnil.fr/fr/taj-traitement-dantecedents-judiciaires
[186] *Le fichage des mineurs: entre ordre public et libertés individuelles*, op. cit.,, *op. cit*., p. 185.
[187] *Le fichage des mineurs: entre ordre public et libertés individuelles*, op. cit.,, *op. cit*., p. 186.
[188] Article R. 40-24 du Code de procédure pénale.

Par ailleurs, le TAJ contient un dispositif de reconnaissance faciale, permettant de détecter de fausses identités. L'application offre la possibilité de faire ressortir automatiquement les liens et similitudes entre différentes fiches, notamment quant au mode opératoire. Il n'est d'ailleurs pas interdit de sélectionner une catégorie particulière de personnes à partir de données sensibles[189].

Les personnes habilitées à consulter le TAJ ne semblent plus correspondre aux finalités judiciaires initiales pour « *se rapprocher du rôle du casier judiciaire* »[190]. Ainsi, les agents spécialement habilités de la police et de la gendarmerie nationales, ainsi que ceux investis par la loi d'attributions de police judiciaire peuvent accéder aux informations nominatives figurant dans le fichier. Par ailleurs, les magistrats du Parquet et les juges d'instruction ont également accès à ce dossier.

En outre, et c'est ici que l'on peut s'interroger sur les finalités réelles du TAJ, les enquêtes administratives permettant l'accès au TAJ sont diverses[191]. Ainsi, l'accès est possible dans le cadre des demandes d'acquisition de la nationalité française et de délivrance ou renouvellement des titres de séjour[192] mais également dans le cadre d'enquêtes liées à l'accès à de nombreux emplois (missions de souveraineté de l'État, sécurité ou défense, paris et courses, sécurité des personnes et des biens au sein d'une entreprise…)[193]. Si la l'article 10 de la loi de 1978 interdit de prendre une décision produisant des effets juridiques sur le seul fondement d'un fichier, on peut tout de même s'interroger sur le respect de la finalité de ce fichier visant à fournir une aide à l'enquête judiciaire lorsqu'il est utilisé pour un grand nombres d'enquêtes administratives. **C'est d'ailleurs à ce titre que nous nous intéresserons au TAJ**. Déjà, le décret n°2015-648 du 10 juin 2015[194] avait élargi les informations auxquelles les agents de préfecture avaient accès leur permettant non seulement de consulter le TAJ afin de voir si une personne y figurait ou non mais également d'accéder aux faits pour lesquels une personne est inscrite au TAJ. Le TAJ est aujourd'hui consultable à travers l'automatisation de la consultation centralisée de renseignements et de données (ACCReD) autorisée par le décret n°2017-1224 du 3 août 2017. Par ailleurs, la loi n°2013-1168 du 18 décembre 2013 a ouvert l'accès au TAJ aux services de renseignement relevant du ministère

[189] *Fichiers de police op. cit.,* p. 48.
[190] Rapport parlementaire Paris-Morel-à-L'huissier, *op.cit.*
[191] *Le fichage des mineurs: entre ordre public et libertés individuelles*, op. cit.,, *op. cit.,* p. 190
[192] R. 40-29 du Code de procédure pénale
[193] Article L. 114-1 du Code de sécurité intérieur
[194] Circulaire NOT INTD1518940C

de la Défense à des fins de recrutement, de délivrance d'une autorisation « secret défense » et d'accès à des zones protégées.
Enfin, ce fichier est également accessible à des agents de renseignement (militaire, sécurité intérieur, renseignement territorial etc…) à des fins de prévention du terrorisme[195].

Les personnes inscrites au TAJ n'en sont pas avisées. La loi prévoit cependant un droit d'accès et de rectification. L'article 230-8 du code de procédure pénale permet aux personnes inscrites au TAJ de demander une rectification en cas d'erreurs factuelles ou, sous conditions, l'effacement des données la concernant. Le Conseil d'État a considéré dans un avis du 30 mars 2016 que l'article 230-8 du code de procédure pénale ne prévoit pas de règles particulières relatives au maintien ou à l'effacement des données au TAJ sauf en cas de relaxe ou acquittement, auquel cas le « principe est l'effacement des données et l'exception, le maintien pour des raisons tenant à la finalité du fichier ». Il est intéressant de noter que le principe, dans le cas d'une décision de non-lieu ou de classement sans suite, n'est pas l'effacement mais la prescription du maintien des données personnelles dans le TAJ avec inscription d'une mention en interdisant la consultation des informations à des fins administratives[196].

Ainsi, ce fichier collecte des informations considérables – dont des données sensibles, lorsque cela est permis – sur plusieurs dizaines de millions de personnes et est consultable par des autorités aussi diverses que celles remplissant des missions de police judiciaire, mais également des entreprises privées aux fins de recrutement concernant la sécurité des personnes et des biens.

Particulièrement nébuleux, **le TAJ fait en outre déjà l'objet d'interconnexions qui devraient devenir plus nombreuses encore**. Le TAJ est ainsi alimenté via l'application GASPARD NG, qui permet d'alimenter simultanément le TAJ et le FAED. La réflexion envisageant une base centrale commune reliant FAED, FNAEG et TAJ est engagée depuis 2011. Dans leur rapport de 2018, les députés Paris et Morel-A-L'Huisser préconisent une nouvelle fois cette interconnexion[197].

[195] Article 40-29-1 du Code de procédure pénale
[196] *Le fichage des mineurs: entre ordre public et libertés individuelles*, *op. cit.*, p. 201
[197] Rapport parlementaire Paris-Morel-à-L'huissier, *op.cit*, proposition n°10,

Par ailleurs, le TAJ est alimenté directement par les logiciels LRPPN et LRGPN qui alimentent également le fichier des objets et véhicules signalés et CASSIOPEE. D'ailleurs, une expérimentation de mise en relation entre le TAJ et CASSIOPEE a débuté, afin de permettre l'inscription dans le TAJ des condamnations pénales[198]. LRPPN alimente automatiquement les fichiers TAJ, FOVeS, CASSIOPEE et échange des informations avec le logiciel GASPARD NG. Mais il existe également un lien entre le LRPGN et Gendnotes, application mobile mise à disposition des gendarmes qui facilite la collecte de photos et d'informations sensibles (religion, politique, sexualité, prétendue origine raciale). Cette application a été utilisée pendant des années sans cadre juridique, mais en février 2020 un décret l'a officialisée. Il n'en demeure pas moins que ce décret est problématique dans la mesure où, comme l'explique La Quadrature du Net, les photos et informations sont systématiquement transmises au LRPGN qui les transmet à son tour au TAJ, si les gendarmes décident d'ouvrir une procédure. Néanmoins, le TAJ n'est pas autorisé à recenser des informations sensibles comme certaines données collectées par Gendnotes. De ce fait, en plus d'intégrer des informations qui ne devrait pas l'être, celles-ci seront conservées dans le TAJ pendant 20 ans, accessibles par toute la police et la gendarmerie et les photos pourront être utilisées ultérieurement par un système de reconnaissance faciale pour identifier des personnes *(cf. Partie 1 - Chapitre 3*)[199].

Surtout, les rapporteurs envisagent une interface permettant l'interrogation simultanée de différents fichiers en utilisant l'exemple de l'ACCReD, moteur de recherche à partir de la saisie d'une identité pour les enquêtes administratives. Le TAJ fait déjà partie des fichiers consultables à partir de l'ACCReD[200].

Concernant le TAJ, on peut également s'interroger sur le dispositif de reconnaissance faciale permettant des rapprochements avec les millions de photographies inscrites dans le fichier. Ce dispositif devrait sans doute s'étendre et permettre de nouvelles interconnexions à partir de la reconnaissance faciale, notamment avec le FPR, pour lequel il est techniquement envisageable de permettre une consultation à partir d'une photo[201].

---

[198] Rapport parlementaire Paris-Morel-à-L'huissier, *op. cit.*, proposition n°9

[199] Gendnotes, faciliter le fichage policier et la reconnaissance faciale, La Quadrature du Net, 25 février 2020, (URL : https://www.laquadrature.net/2020/02/25/gendnotes-faciliter-le-fichage-policier-et-la-reconnaissance-faciale/).

[200] Warren Azoulay, « *Du panoptique au technoptique : renforcement de l'arsenal de collecte de données* », 19 septembre 2017, Dalloz Actualité.

[201] Pierre Januel, « Fichiers de police partout », 19 octobre 2018, Dalloz Actualité.

En résumé, **ci-dessous un tableau recensant les croisements avec le TAJ** :

Nom du fichier	Finalité du fichier	Informations collectés	Type de croisement
FOVeS	Retrouver les objets et les véhicules volés, et surveiller les objets et les véhicules signalés.	Celles relatives à des vols, aux déclarations de perte, aux invalidations de documents et à toutes les mesures de surveillances mises en œuvre par la police, la gendarmerie et les douanes (article 2 de l'arrêté du 7 juillet 2017). Il est bien sûr en lien avec les polices étrangères.	FOVeS transmettra au TAJ les informations relatives à la découverte d'un objet déclaré ou volé. [202]
FAED	Facilite l'identification des auteurs de crimes et de délits, facilite la poursuite, instruction et jugement. Mémorise les traces et les empreintes digitales et palmaires transmises par des organismes de coopération internationale en matière de police judiciaire ou des services de police étrangers en application d'engagements internationaux.	Empreintes digitales, Sexe, Nom, prénom, Date et lieu de naissance, éléments de filiation, nature de l'affaire et référence de la procédure, clichés anthropométriques.	Le TAJ est alimenté via l'application GASPARD NG, qui permet d'alimenter Simultanément le TAJ et le FAED. En 2011, l'interconnexion des fichiers d'identification et d'antécédents (FAED, FNAEG et TAJ) était à l'étude, avec pour objectif de fiabiliser les données intégrées dans le fichier TAJ et de repérer plus aisément l'utilisation d'alias ou les problèmes d'homonymie. A chaque inscription d'une personne dans le fichier TAJ, il serait procédé automatiquement à une recherche dans le FNAEG et le FAED. Le cadre légal étant le même, c'est-à-dire l'enquête judiciaire, la CNIL ne semblerait pas opposée à une telle interconnexion[203] Actuellement nous ne savons pas où en est cette interconnexion
FNAEG	Outil d'identification généralisé. Initialement relatif à la	ADN	Comme le FAED

[202] Délibération n° 2017-158 du 18 mai 2017, *op.cit.*
[203] *Fichiers de police*, *op,cit*., p.47

	prévention et à la répression des infractions sexuelles.		
LRPN	Alimentent automatiquement TAJ, FOVeS, CASSIOPEE et échangent des informations avec GASPARD NG.	Etat civil des pers. mises en causes - victimes et témoins des infractions - surnom - date et lieu de naissance - filiation - nationalité - partenaire - diplômes, permis de conduire - contact info. relative aux GAV	La collecte des données s'opère automatiquement par la mise en relation du TAJ avec les traitements de rédaction des procédures LRPPN et LRPGN de la gendarmerie, créés par les décrets no 2011-110 et no 2011-111 du 27 janvier 2011 (JO 29 janv.)
CASSIOPEE	Suivi des procédures judiciaires au sein des tribunaux judiciaires et des cours d'appel. CASSIOPÉE concerne les procédures pénales, les procédures d'assistance éducative, les procédures devant le juge des libertés et de la détention et les procédures civiles et commerciales enregistrées par les parquets.	Concernant les personnes mises en cause, condamnées, victimes ou témoins, leur nom, prénom, nom d'usage, sexe, dates de naissance, lieu de naissance, nationalité, numéro de pièce d'identité, nom et prénom des parents, nombre de frères, de sœurs, d'enfants, rang dans la fratrie, niveau d'études, adresse, téléphone, professions, situation d'emploi, nom de l'employeur, langue parlée, données bancaires (sauf pour les témoins) sont renseignés. En ce qui concerne la procédure, CASSIOPÉE rassemble les antécédents de la personne, sa situation judiciaire, la nature du jugement, les infractions relatives à l'infraction (modalités de participation, alcoolémie, récidive, lieu et date de la commission de l'infraction), peine prononcée, ...	Futur interconnexion avec CASSIOPEE qui permettrait une mise à jour automatique des suites judiciaires dans le TAJ mais ne concerneront que les affaires pénales à venir

II. Le FPR

Il est possible de définir comme ancêtre du fichier des personnes recherchées le "carnet B", mis en place par une instruction ministérielle du 9 décembre 1886 par le général Boulanger, alors ministre de la guerre[204]. L'objectif était de recenser et de surveiller, sous l'autorité du préfet, les étrangers et les individus suspects par le biais de deux "carnets": le A et le B. Le premier était centré sur les étrangers en âge d'être mobilisés, et le deuxième un élément de contre-espionnage et un instrument de police politique, consacré aux individus représentant un risque en cas de trouble ou de conflit. Les étrangers pouvaient y être inscrits sans être suspect mais simplement parce qu'ils résidaient à proximité d'un « *ouvrage ou d'une voie ferrée stratégique*[205] ». Les anarchistes, communistes et syndicalistes y étaient également recensés.

Mais plus qu'un outil de surveillance passif, ce fichier permet l'arrestation et l'internement des personnes fichées, sur simple décision du préfet[206].

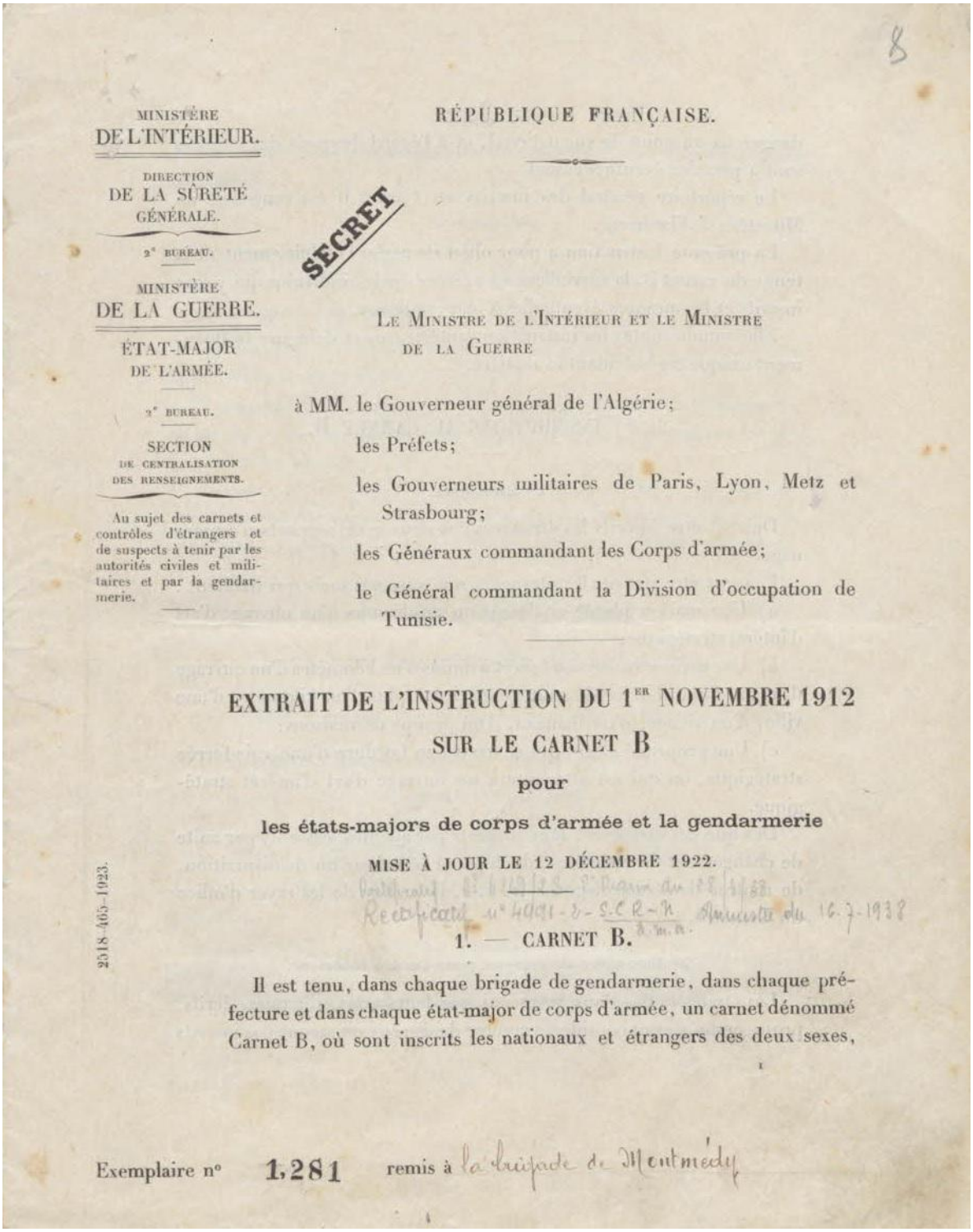
L'instruction secrète du 1er novembre 1912[207] en définit le mode opératoire : il s'agit d'instruire un fichier où seront inscrites **les personnes jugées dangereuses par l'ordre intérieur en cas de troubles, de conflit ou de tension politique**.

[204] Jean Mafart, « Carnet B », Hugues Moutouh éd., *Dictionnaire du renseignement,* Perrin, 2018, pp. 134-136. Disponible en ligne : https://www-cairn-info.faraway.parisnanterre.fr/dictionnaire-du-renseignement--9782262070564-page-134.htm

[205] *Ibid.*

[206] En 1922, l'article 10 du code d'instruction criminelle permet l'arrestation sur simple décision du préfet via un formulaire blanc, mandats préparés à l'avance et annexés à chaque dossier. En 1932 au nom des libertés individuelles l'article 10 est supprimé. Mais en 1935 la loi du 25 mars réintègre un nouvel article 10 qui permet aux préfets départementaux et le préfet de Police de Paris de requérir à la police judiciaire de faire "tout le nécessaire pour la sûreté de l'Etat". Cf. Deschodt, J-P., « La preuve par le carnet B », *Les Cahiers du Centre de Recherches Historiques*, 45 | 2010, 181-193.

[207] Instruction du 1er novembre 1912, mise à jour le 12 décembre 1922, Archives Nationales (AN), CAC, vers. 19940 500/1328.



8

MINISTÈRE
DE L'INTÉRIEUR.

DIRECTION
DE LA SÛRETÉ
GÉNÉRALE.

2e BUREAU.

MINISTÈRE
DE LA GUERRE.

ÉTAT-MAJOR
DE L'ARMÉE.

2e BUREAU.

SECTION
DE CENTRALISATION
DES RENSEIGNEMENTS.

Au sujet des carnets et contrôles d'étrangers et de suspects à tenir par les autorités civiles et militaires et par la gendarmerie.

RÉPUBLIQUE FRANÇAISE.

SECRET

LE MINISTRE DE L'INTÉRIEUR ET LE MINISTRE DE LA GUERRE

à MM. le Gouverneur général de l'Algérie;

les Préfets;

les Gouverneurs militaires de Paris, Lyon, Metz et Strasbourg;

les Généraux commandant les Corps d'armée;

le Général commandant la Division d'occupation de Tunisie.

EXTRAIT DE L'INSTRUCTION DU 1ER NOVEMBRE 1912
SUR LE CARNET B
pour
les états-majors de corps d'armée et la gendarmerie

MISE À JOUR LE 12 DÉCEMBRE 1922.

2518-465-1923.

Rectificatif n° 4091-2-S.C.R.-N. Ministre du 16.7.1938

1. — CARNET B.

Il est tenu, dans chaque brigade de gendarmerie, dans chaque préfecture et dans chaque état-major de corps d'armée, un carnet dénommé Carnet B, où sont inscrits les nationaux et étrangers des deux sexes,

Exemplaire n° 1,281 remis à la brigade de Montmédy

Au déclenchement de la Première Guerre Mondiale, le 1er Août 1914, le ministre de l'Intérieur Louis Malvy décide de ne pas mettre en œuvre ce fichier, « *constant que les partis de gauche et la CGT observaient une attitude patriotique, Louis Malvy, ministre de*

l'Intérieur, jugea préférable de ne pas les décapiter ni de les provoquer par des arrestations[208] ».

Néanmoins, en 1922 le carnet fut modifié et réactivé. L'objectif est toujours lié à la Défense Nationale et par conséquent au contre-espionnage, ainsi qu'à la sécurité politique. En effet, le ministre de l'Intérieur de l'époque, Maurice Maunoury, considère que le carnet n'est pas adapté aux nouveaux dangers car il ne comporte pas « *les noms de certains individus notoirement acquis aux idées extrémistes* ».

Le fichier se divise donc en trois groupes. Les deux premiers sont consacrés aux étrangers et aux Français suspectés d'espionnage, comme dans l'organisation de 1912. Les étrangers peuvent se voir inscrire au fichier simplement par leur localisation géographique. Enfin, pour les Français qui « *représentent réellement un danger pour l'ordre intérieur* »[209], c'est-à-dire les « extrémistes », intégrant les anarchistes, syndicalistes, communistes, autonomistes et fascistes[210].

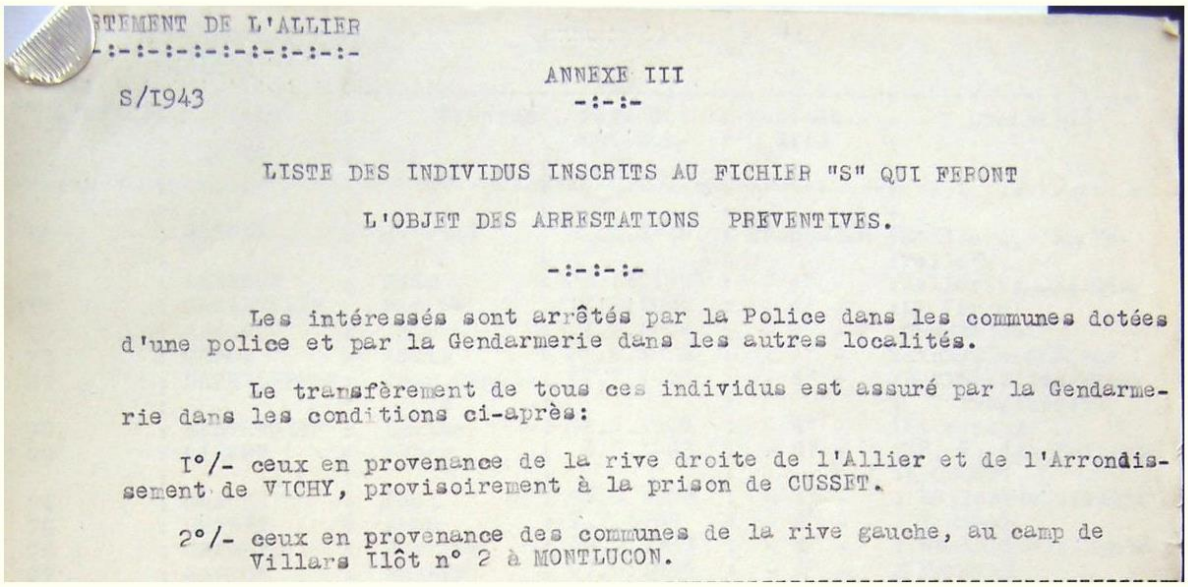
Une fois inscrit, il était possible d'être radié après être décédé, disparu ou parti de la France depuis deux ans, pour raisons médicales, c'est-à-dire atteint par une défaillance physique ou victime d'une pathologie évolutive, ou pour raisons politiques, c'est-à-dire ne plus manifester la même passion pour les idées révolutionnaires et marquer un désintérêt pour le militantisme, en se retirant de la vie politique ou syndicale.

En 1938 le fichier intègre un quatrième groupe qui regroupe tous les étrangers dangereux pour l'ordre intérieur qui « *par leurs actes, discours, écrits, propagandes, seront considérés comme dangereux ou ceux qui seront estimés susceptibles de se transformer en agitateurs à la faveur d'un incident sérieux* »[211].

Avant d'être abrogé officiellement et définitivement en 1947, René Bousquet – secrétaire Général de la Police – et Pierre Laval – Chef du gouvernement, décident de réformer les procédures encadrant les fichiers de police. Le carnet B serait trop confus et ne

[208] « Carnet B », Hugues Moutouh éd., *Dictionnaire du renseignement, op. cit.*
[209] Jean Pierre Deschodt, « La preuve par le carnet B », *Les Cahiers du Centre de Recherches Historiques*, 45 | 2010, 181-193.
[210] *Ibid.*
[211] *Ibid.*

« *permettrait matériellement pas aux services de police d'effectuer avec la promptitude désirable les arrestations prévues*[212] ». Ainsi la « Liste S » ou « Fichier S » est créé, pour « *des individus considérés comme* ***dangereux pour l'ordre public en évitant les individus simplement suspects***[213] » qui pourra intégrer des individus déjà dans le carnet B. L'objectif de ce nouveau fichier serait de réduire le nombre d'individus pour faciliter et optimiser les arrestations et internements dans des délais plus courts: « *Les opérations d'arrestation ne s'effectueront rapidement si la liste S est courte* »[214].



STEMENT DE L'ALLIER
-:-:-:-:-:-:-:-:-:-

S/1943

ANNEXE III
-:-:-

LISTE DES INDIVIDUS INSCRITS AU FICHIER "S" QUI FERONT L'OBJET DES ARRESTATIONS PREVENTIVES.

-:-:-:-

Les intéressés sont arrêtés par la Police dans les communes dotées d'une police et par la Gendarmerie dans les autres localités.

Le transfèrement de tous ces individus est assuré par la Gendarmerie dans les conditions ci-après:

1°/- ceux en provenance de la rive droite de l'Allier et de l'Arrondissement de VICHY, provisoirement à la prison de CUSSET.

2°/- ceux en provenance des communes de la rive gauche, au camp de Villars Ilôt n° 2 à MONTLUCON.

En tête du fichier S

215

A) Origines du fichier des personnes recherchées

Le fichier automatisé comme nous le connaissons existe depuis 1969, afin de remplacer les « bulletins périodiques » ou « fiches signalétiques » qui étaient diffusés aux

[212] Antoine Lafébure, "Fiches S, carte d'identité et ancêtre du numéro de Sécu, quand Vichy inventait les moyens de surveiller la population", *Slate*, 3 juin 2018
[213] *Ibid.*
[214] Antoine Lefébure, *Conversations secrètes sous l'occupation*, Broché, 2018,
[215] Document découvert dans les archives de l'Allier par l'historien Henri Billy. Ce document contient une liste de 46 noms, prénoms, dates de naissance et domice. Entre eux, vingt-deux communistes, parmi lesquels treize on fait l'objet d'arrêté d'internement. 3 mourront en déportation. Cf Billy,H-F., Le fichier S de l'Allier de 1943, Histoire et généalogie, 2016, disponible en ligne: http://histoire-et-genealogie.over-blog.com/2015/11/fichier-s-allier-1943.html

services locaux de police et de gendarmerie, regroupés dans plus de 300 fichiers manuels locaux[216].

Le cadre juridique de ce fichier a été, depuis sa création, flou et controversé. En effet, déjà en 1988 la CNIL, dans sa délibération nº 88-120 du 8 novembre 1988, demandait au ministère de l'intérieur de publier un décret pour encadrer ce fichier, au vu des informations sensibles qu'il contenait et pour permettre un accès indirect à ce fichier ainsi qu'une actualisation mensuelle et non pas tous les trois ans. Néanmoins, malgré cette délibération, ce n'est qu'en 2010 que l'arrêté du 15 mai 1996 modifié par l'arrêté du 2 septembre 2005 a été abrogé au profit du décret nº2010-569 du 28 mai 2010 relatif au fichiers des personnes recherchées.

Depuis sa création, ce fichier a fait l'objet de beaucoup de critiques notamment sur **la constante évolution de l'étendue des informations collectées**, des individus visés et le champ d'application du fichier. Il contient 21 sous-fichiers regroupant les personnes concernées en fonction du fondement juridique de la recherche avec au total près de 120 motifs de recherches associés à une conduite à tenir.

En plus des données collectées qui vont des plus banales aux plus sensibles - religieux, politique, philosophique-, **ce fichier est consulté plus de 100 000 fois par jour**[217] par les autorités judiciaires, les services de police, la gendarmerie, les douanes, les autorités administratives et quand le motif est lié, les services de police des autorités des pays frontaliers.

Tableau des 21 catégories de mesures de recherche en 1988 et 2018 :

Depuis 1988, les catégories n'ont pas beaucoup évolué. Pour en rendre compte, en vert les catégories nouvelles en 2018 recensé dans le rapport d'information par M. François Pillet le 19 décembre 2018 et en rouge les catégories qui ne figurent plus en 2018.

[216] *Fichiers de police, op cit.*, p,52
[217] Rapport parlementaire Pillet, nº219, 19 déc. 2019, p.7

Lettre attribuée	Catégories	Information délibération 1988 CNIL	Informations actuelles[218]
AF	Police de l'air et des frontières.	Concerne les personnes de nationalités françaises ou étrangères qui, en raison de leurs activités, doivent faire l'objet de mesures de surveillance ou de vérifications des situations particulières	
AL	Aliénées	Relative aux personnes qui ont fait l'objet d'une décision préfectorale de placement d'office dans un établissement psychiatrique sans que cette décision ait pu être exécutée, et aux personnes qui se sont évadées d'un établissement psychiatrique ; qu'un contrôle de validité de l'inscription n'étant effectué que trois années après la date de l'inscription	Voir l'article 706-136 du Code de procédure pénale. Personne recherchée en vue du placement d'office (et pas à la demande d'un tiers) dans un hôpital psychiatrique
CC	Contraintes par corps	Concerne les personnes qui ont fait l'objet d'une décision de justice prévoyant une contrainte par corps	
CJ	Contrôle judiciaire	Relative aux personnes qui font l'objet d'un contrôle judiciaire	
D	Déserteur	Concerne les déserteurs, insoumis, et auteurs de crimes et de délits en matière militaire et de sûreté de l'Etat	
E	Police générale des étrangers	Concerne les étrangers dont la présence sur le territoire national constitue une menace pour l'ordre public et qui ont fait l'objet d'un arrêté ministériel ou d'un arrêté préfectoral d'expulsion	
F	Recherche dans l'intérêt des familles	Concerne les personnes physiques disparues pour lesquelles une demande de recherches a été effectuée	

[218] Du fait d'un manque d'exhaustivité légale sur les motifs de mesures de recherche et de répartition dans les différentes catégories, ces informations ne sont pas exhaustives et il est possible que certains motifs ne correspondent pas au sous-fichier dans lequel il est inscrit. Néanmoins tous les motifs inscrits sont vérifiés et exacts. Des erreurs pourraient toutefois subsister indépendamment de notre volonté, sachant que nous nous appuyons sur une bibliographie très restreinte.

G	Mesures administratives relatives aux permis de conduire	Concerne des personnes qui ont fait l'objet d'un arrêté préfectoral pour un permis de conduire	Personne recherchée pour lui notifier une décision relative à leur permis de conduire. Personne dont le permis de conduire obtenu indûment a été retiré. Mesure de suspension du permis de conduire, d'interdiction de conduire certains véhicules, d'annulation du permis décidée par un juge Personne qui a perdu tous ses points et n'a pas remis son permis de conduire à la préfecture.[219]
I	Interdiction de séjour Interdictions judiciaires (à l'exception des interdictions judiciaires du territoire) Interdictions administratives de stade Interdictions administratives de sortie du territoire	Concerne les personnes qui font l'objet d'un arrêté d'interdiction de séjour	Interdiction d'exercer une profession, une fonction publique, une activité professionnelle ou sociale. Interdiction de paraître dans certains lieux, interdiction de séjour dans certains lieux, interdiction de fréquenter certaines personnes. Interdiction de manifestation. Interdiction de porter ou de détenir une arme soumise à autorisation.[220]
IT	Interdiction judiciaire du territoire	Concerne les étrangers frappés d'une mesure d'interdiction du territoire, que cette mesure est applicable notamment aux usagers et trafiquants de stupéfiants	Prononcée en application de l'article 131-30 du code pénal
J	Recherches de justice Mesure judiciaires	Concerne des personnes recherchées par les autorités judiciaires	Mandat, ordre ou note de recherche émis par un procureur, juge, juge d'instruction, juge de la liberté et de la détention, juge des enfants. Les obligations ou interdictions prononcées dans le cadre d'un sursis

[219] *Ibid.*
[220] *La folle volonté de tout contrôler*, Caisse de solidarité de Lyon, Juin 2020, p. 67

			probatoire, d'un suivi socio-judiciaire, d'une libération conditionnelle, d'une semi-liberté, d'un placement à l'extérieur, d'une détention à domicile sous surveillance électronique, d'une suspension ou d'un fractionnement de peine privative de liberté, d'un suivi post-libération[221]…. L'article 203-19 du code de procédure pénale énumère les décisions judiciaires inscrites au FPR
M	Mineurs fugueurs	recense des informations sur les personnes de moins de 18 ans et certains étrangers mineurs en application des lois de leur pays	
PJ	Recherche de police judiciaire	A trait aux personnes recherchées à titre de témoin ou d'auteur présumé d'un crime ou d'un délit	Les personnes recherchées dans le cadre d'une enquête préliminaire, d'une enquête de flagrance ou d'une instruction N'importe quelle recherche criminelle (donc crime, et non délit ni contravention…) Voir le II de l'article 2 du décret n°2010-569 du 28 mai 2010[222]
R	Opposition à résidence en France	Concerne des étrangers qui ne sont pas autorisés à établir leur résidence en France	
S	Sûreté de l'État	Recense des informations inscrites par la direction de la surveillance du territoire et la direction des renseignements généraux dans le cadre de leurs attributions	
T	Débiteur envers le trésor	Concerne les personnes de nationalité française ou étrangère recherchées comme redevables envers le trésor	Personne qui n'a pas payé sa dette à l'État, aux collectivités territoriales ou aux établissements publics[223].

[221] « Avant la réforme du 15 août 2014, on estimait à près de 11 % la part des peines nécessitant une inscription au FPR (RAIMBOURG, Rapport no 1974 relatif à la prévention de la récidive et à l'individualisation des peines, Assemblée nationale, 2014) », Virginie Gautron, *Fichiers de police*, *op.cit*, p.53
[222] *La folle volonté de tout contrôler*, *op.cit.*, p.67
[223] *La folle volonté de tout contrôler*, *op.cit.*, p.69

TE	Opposition à l'entrée en France	Concerne les étrangers dont la venue sur le territoire constituerait une menace pour l'ordre public	
TM	Sorti du territoire de mineurs	Concerne les mineurs français ainsi que les mineurs de nationalité étrangère dont les parents résident régulièrement en France	L'interdiction de sortie du territoire de l'enfant sans l'autorisation des deux parents prononcée par le JAF lors de la procédure de divorce (articles 373-2-6, 375-5 du Code civil), ou lors de la prise de mesures d'assistance éducative (article 375-7 du Code civil)[224]
TP	Opposition à délivrance de documents d'identité	Concerne des personnes pour lesquelles la délivrance d'un titre d'identité ou le renouvellement de ce titre est refusée	Personne qui a obtenu ou tenté d'obtenir indûment une carte d'identité ou un passeport.[225]
V	Évadés	Concerne les personnes mineures ou majeures qui se sont évadées d'un établissement où elles étaient gardées	
X	Personnes non-identifiées		En cas de découverte de personne décédée ou vivante non identifiée[226].
….[227]	Interdiction de séjour dans un département		
…[228]	Assignation à résidence		non-respect des mesures d'assignation : celles-ci ne font en effet l'objet d'aucune inscription informatique centralisée, contrairement par exemple aux mesures d'assignation de l'état d'urgence, qui étaient enregistrées au fichier des personnes recherchées[229]

[224] *Ibid.*
[225] *Ibid.*
[226] *Ibid.*
[227] « Ces nouvelles catégories, créées par le décret n° 2017-1219 du 2 août 2017, n'ont pas encore de lettres attribuées : elles ne sont pas encore effectives », Rapport Parlementaire Pillet, *op. cit.*, p. 10
[228] *Ibid.*
[229] *Ibid.*

…[230]	Personnes soumises au contrôle administratifs des retours sur le territoire national (CART)	

On peut noter que comme l'ancêtre du FPR, que ce soit le carnet B ou la liste S, les catégories majoritaires se focalisent sur le contrôle des étrangèr·e·s et le contrôle des individus représentant un risque pour le bon fonctionnement de l'État. La focalisation sur les étrangers est néanmoins très parlante de la politique française, en particulier depuis la Seconde guerre mondiale.

Ne figurant pas dans le tableau, voici une liste, non-exhaustives, des étrangèr·e·s qui peuvent figurer dans le FPR : étrangèr·e·s dont l'entrée en France peut être refusée car elle constituerait une menace pour l'ordre public, étrangèr·e·s qui n'a pas exécuté une OQTF, une interdiction de circuler sur le territoire français, un arrêté d'expulsion ou une assignation à résidence, et étranger expulsé car sa présence en France constitue une menace grave pour l'ordre public (article L521-1 du CESEDA), étrangèr·e·s également de nationalité suisse, islandaise, norvégienne ou d'un État membre de l'Union européenne ne résidant pas habituellement en France et qui fait l'objet d'une interdiction administrative du territoire français car il constituerait une menace réelle pour un intérêt fondamental de la société (articles L214-1 du CESEDA), personne de nationalité autre qui ne réside pas habituellement en France et qui ne se trouve pas sur le territoire national dans la même situation (article L214-2 du CESEDA).

B) Les informations contenues dans une fiche du FPR

Les informations contenues dans une fiche FPR sont :

[230] *Ibid*.

- Le numéro d'inscription au fichier des personnes recherchées.
- L'état civil (nom, prénoms, date et lieu de naissance, filiation), l'alias, le sexe et la nationalité.
- Le signalement.
- Les photographies.
- Les motifs de la recherche (éventuellement les actes administratifs ou judiciaires afférents).
- La conduite à tenir en cas de découverte.
- Le service ou autorité à l'origine de l'inscription.
- Les renseignements éventuels (dernière adresse connue, par exemple).
- Des données sensibles (l'origine ethnique, par exemple) peuvent être mentionnées si elles sont liées au motif de l'inscription ou si elles se rapportent à des signes physiques particuliers, objectifs et permanents qui participent au signalement de la personne.
- Un document peut éventuellement être joint.

Il est important de noter que les connaissances parmi l'entourage des personnes recherchées peuvent également être inscrites dans les fichiers.

Données à caractère personnel sensibles

L'article 8 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et du règlement général sur la protection des données (RGPD) du 27 avril 2016, il est interdit de traiter dans un fichier des **données à caractère personnel « *qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique* »**.

Par dérogation, cette interdiction **ne s'applique pas aux traitements mis en œuvre par l'État qui sont dûment autorisés et justifiés par l'intérêt public**[231].

[231] *La folle volonté de tout contrôler, op.cit.,* p.9.

L'enregistrement de données sensibles est autorisé « *dans les seuls cas où ces informations sont nécessairement liées au motif même de l'inscription ou se rapportent à des signes physiques particuliers, objectifs et permanents, en tant qu'éléments de signalement des personnes* »[232].

Cette dérogation est problématique notamment lors des croisements entre fichiers. Certains fichiers qui n'ont pas comme finalité l'intérêt public, peuvent avoir accès à des données sensibles par un croisement.

Tableau des différents croisements du fichier FPR :

Nom du fichier	Finalité du fichier	Informations collectés	Type de croisement[233]
SIS Système d'information Schengen	Commun à l'ensemble des États membres de l'espace Schengen, a pour objet de centraliser et de faciliter l'échange d'informations détenues par les services chargés de missions de police. Il est composé d'un système central installé à Strasbourg (C-SIS) et de systèmes nationaux (N-SIS) implantés dans chaque pays. Chaque État partie est responsable de la partie nationale du fichier, à laquelle les autres États accèdent à travers le système central[234].		Le FPR alimente automatiquement le SIS et il est systématiquement consulté lors des demandes de délivrance des titres de séjour simultanément avec l'ADGREF[235] La CNIL a alerté le ministère de l'Intérieur des risques d'une diffusion internationale, sans garanties, des données transmises par l'État français (Délib. no 2009-587 du 12 nov. 2009)[236].

[232] Décret n° 2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées.
[233] Information recensée dans le rapport parlementaire Pillet, *op.cit.*
[234] Danièle Lochak, "Des fichiers pour gérer, contrôler, surveiller les étrangers", *Plein droit*, nº71, 2006
[235] *Ibid.,*
[236] *Fichiers de police, op.cit,* p.54

API-PNR Advanced Passenger Information			Le « système API-PNR France » interroge indirectement le FPR2 (une copie de la base) à partir des données communiquées par les compagnies aériennes (données de réservations - PNR- et d'enregistrement et d'embarquement – API -) afin de prévenir, détecter et poursuivre les actes de terrorisme et les formes graves de criminalité, dans des conditions et limites fixées par la réglementation française, en application de la directive européenne 2016/681 du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.[237]
LRPN et LRPGN[238]	Alimentent automatiquement TAJ, FOVeS, CASSIOPEE et échangent des informations avec GASPARD NG décrets n°2011-110 et 2011-111 du 27 janvier 2011	- état civil des pers. mises en causes - victimes et témoins des infractions - surnom - date et lieu de naissance - filiation - nationalité - partenaire - diplômes, permis de conduire - contact info. relative aux GAV	Il peut être consulté et alimenté depuis ces fichiers, mais qu'il peut également alimenter ces derniers
FIJAISV	Personnes ayant fait l'objet d'une	Nom, prénom, sexe, date et	Une liaison informatique

[237] Rapport Parlementaire Pillet, *op.cit*, p.11
[238] Pour plus d'information sur ces fichiers se référer à la partie I de ce dossier

Fichier judiciaire national des auteurs d'infractions sexuelles ou violentes	condamnation même non définitive, d'une composition pénale, d'une décision d'irresponsabilité pénale pour trouble mental, d'une instruction lorsque le juge d'instruction le demande, par des tribunaux français ou étrangers, pour des faits constitutifs d'une infraction sexuelle (liste à l'article 706-47 du Code de procédure pénale).	lieu de naissance, nationalité... + nature et date de la décision, juridiction ayant prononcé, nature de l'infraction, date et lieu des faits Dates de justification d'adresse	permet également des consultations réciproques et une alimentation automatique
FIJAIT **Fichier judiciaire automatisé des auteurs d'infractions terroristes**	Il a pour finalité légale la prévention du renouvellement des infractions terroristes et vise à faciliter l'identification de leurs auteurs, Recense pers. ayant fait objet d'une condamnation pour des faits de terrorisme, interdiction de sortie du territoire, les personnes ayant fait l'objet d'une décision d'irresponsabilité pénale pour trouble mental, et même au stade de l'instruction si le juge d'instruction le demande. Il ne concerne pas les personnes condamnées pour apologie d'actes de terrorisme, ni pour transmission d'apologie d'actes de terrorisme	- Identité - adresses - déplacements transfrontaliers - informations relatives à la décision ayant donné lieu à l'enregistrement - info relatives aux obligations faites à la personne inscrite	Prochainement
ACCRED **Automatisation de la consultation centralisée de renseignement de données**			Les données stockées dans le FPR peuvent être consultées depuis ce traitement
SETRADER **Système européen de traitement des données d'enregistrement et de réservation**			Les données stockées dans le FPR peuvent être consultées depuis ce traitement

PARAFE3 **Passage automatisé rapide aux frontières extérieures**			Les données stockées dans le FPR peuvent être consultées depuis ce traitement
COVADIS **Système de contrôle et vérification automatique des documents sécurisés**			Des travaux sont en cours pour permettre le « criblage » du FPR par ce traitement
RMV **Réseau mondial visas**			Des travaux sont en cours pour permettre le « criblage » du FPR par ce traitement
SI-AEF **Système d'information d'administration des étrangers en France**			Des travaux sont en cours pour permettre le « criblage » du FPR par ce traitement
AGDREF **Application de gestion des dossiers des ressortissants étrangers en France**	Prenant la suite d'un fichier créé en 1982 et qui centralisent toutes les données nécessaires à la fabrication des titres de séjour, il a été créé en 1993 pour répondre à des finalités plus larges : améliorer la gestion administrative des dossiers des étrangers, lutter contre la fraude en fiabilisant la fabrication des titres de séjour, lutter contre l'immigration clandestine en vérifiant la régularité du séjour en France, établir des statistiques[239]	l'ensemble des informations administratives concernant les étrangers : état civil, numéro d'identification, adresse, filiation, situation familiale, conditions d'entrée en France (entrée régulière ou irrégulière, regroupement familial…), situation professionnelle, nature et durée de l'autorisation de séjour, refus de séjour éventuel, mesures d'éloignement, contentieux en cours[240]	Le FPR est systématiquement consulté lors des demandes de délivrance des titres de séjour, simultanément avec le SIS.[241]
TES **Titres électroniques sécurisés**			Des travaux sont en cours pour permettre le « criblage » du FPR par ce traitement

[239] Danièle Lochak, "Des fichiers pour gérer, contrôler, surveiller les étrangers", *op.cit*.
[240] *Ibid.*
[241] *Ibid.*

FSPRT
Fichier des signalements pour la prévention de la radicalisation à caractère terroriste

les « fiches S » du FPR et le FSPRT ont fait l'objet, au printemps 2018, d'un rapprochement.
Il est désormais procédé plus systématiquement à la création, par les services de renseignement, d'une fiche S au sein du FPR pour toute personne signalée pour radicalisation et inscrite au FSPRT

C) Enquêtes administratives

Le décret n° 2010-569 du 28 mai 2010 relatif au fichier des personnes recherchées permet sa consultation « *lors de la réalisation des enquêtes administratives prévues aux articles L. 114-1, L. 114-2 et L. 211-11-1 du code de la sécurité intérieure ou lors de l'instruction des demandes relatives à l'application de la réglementation relative aux étrangers, aux titres d'identité et de voyage, aux visas, aux armes et munitions et aux permis de conduire* ». Ainsi, sa consultation est légale avant la mise en place du fichier ACCReD.

D) Catégorie S

Le « fichier S » est la catégorie du FPR la plus médiatisée, notamment depuis le contexte de l'état d'urgence après les attentats de 2015. Pourtant, ses finalités, les critères d'inscription au fichier, ses conséquences ainsi que son accessibilité sont extrêmement flous et opaques. Nous allons tenter de déceler le fonctionnement de cette fiche.

Il existe 11 catégories (de S2 à S16), qui ne correspondent pas à des niveaux de dangerosité mais renvoient à des profils et des conduites à tenir. Toute personne qui présente sur territoire national ou non, qui directement ou indirectement, individuellement ou collectivement, est susceptible de porter atteinte à la sûreté de l'État ou à la sécurité publique

« *par le recours ou le soutien actif apporté à la violence, ainsi que toute personne entretenant ou ayant des relations directes et non fortuites avec ces personnes* » peut y être inscrite.

Nous insistons sur le mot *susceptible* car cette inscription ne résulte donc pas d'une action précise ou objective, mais uniquement d'une suspicion qui laisse beaucoup de place à **l'aléa, à la subjectivité des agents responsables de ce fichier** : les agents de la direction générale de la sécurité intérieure (DGSI)[242], du service central du renseignement de la préfecture de police de Paris (DRPP) et de la direction générale de la gendarmerie nationale (DGGN).

La finalité des fiches de signalement est d'alerter les agents et services qui entrent en relation avec cette personne, par exemple lors d'un contrôle routier, afin qu'ils collectent des informations à son égard. La fiche S précise les modalités de transmission, généralement par un appel téléphonique vers un numéro identifié sur la fiche, puis l'envoi d'un procès-verbal d'observation[243].

Si son apparence la rapproche d'un simple fichier de centralisation d'informations, cette catégorie représente néanmoins un danger *supplémentaire* pour les libertés individuelles : **aucune information recensée ne fait l'objet d'un quelconque contrôle**, le contenu de la fiche n'étant accessible que par les autorités responsables déjà nommées.

Pourtant, les informations transmises par des agents de plusieurs services dépendent de leur libre arbitre, souvent sous la forme d'un procès-verbal. Les procès-verbaux constituent d'ailleurs plus une représentation que l'agent s'est fait de la rencontre, révélant ainsi davantage une appréciation subjective que des éléments d'informations objectivés.

Il s'agit finalement d'une reconstitution ou recomposition, un résumé qui ne peut retranscrire les détails et les ambiguïtés. Il peut être d'autant plus dangereux s'il fait référence à une interaction dont la retranscription ne peut rendre compte des différences de niveaux de langage entre les deux interlocuteurs ce qui amène à une interprétation divergente puisque les niveaux de langage transforment le sens des mots.

[242] Au 13 Juin 2018, 80% des fiches S auraient été inscrites par la DGSI : Rapport Parlementaire Pillet, *op.cit*., p. 13.
[243] Rapport Parlementaire Pillet, *op.cit*., p.18.

Il s'agirait, selon un rapport parlementaire déjà cité, d'un « *mécanisme passif ne permettant qu'une collecte ponctuelle d'informations, la fiche ne « s'activant » qu'en cas de consultation ou de contrôle* »[244].

Ainsi, les personnes fichées peuvent faire l'objet d'une surveillance dite *active,* avec des écoutes téléphoniques, interception administrative de leurs correspondances, surveillance de l'entourage etc.

Les individus fichés peuvent également faire l'objet d'une surveillance « passive » et ponctuelle, à savoir être contrôlés, être interrogés sur la provenance et la direction de leur véhicule ou sur les personnes les accompagnant, outre la collecte d'un grand nombre d'autres informations les concernant. Cette surveillance passive semble donc être une surveillance déjà très poussée et très intrusive, surtout si elle n'est fondée que sur la base de soupçons, et peut permettre de construire le profil d'une personne, une cartographie de ses mouvements etc.

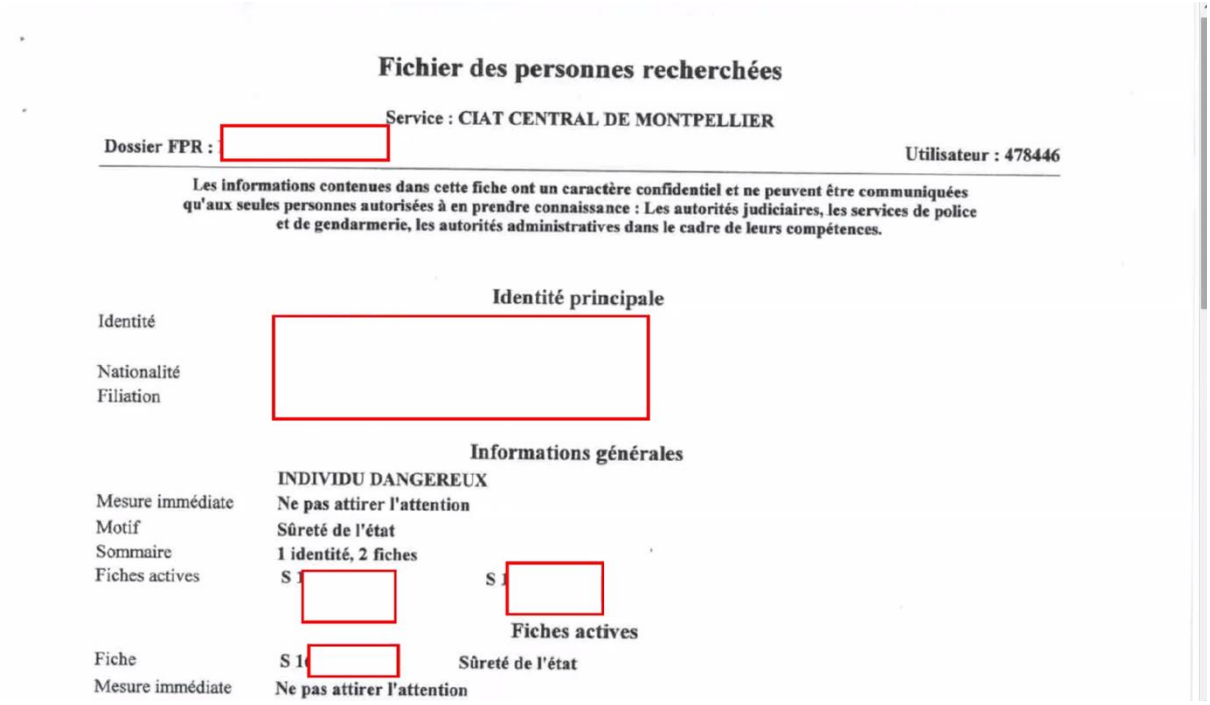
La fiche S ne contient pas les informations relatives à un éventuel suivi opérationnel de la personne. Ce fichier ne contient pas non plus les informations précises à l'origine de l'inscription « S » au FPR. Ces informations sont contenues dans d'autres fichiers, notamment le fichier Cristina de la DGSI et le fichier PASP.

Ce même rapport affirme également que l'inscription au fichier ne devrait pas pouvoir être un motif de décision administrative défavorable à son égard, ou de suivi « *dès lors que cette fiche n'est ni motivée ni notifiée à la personne, elle ne peut fonder une décision défavorable à son égard* »[245]. Pourtant, le FPR est consulté lors d'enquête administrative, pouvant fermer la porte à beaucoup d'emplois, notamment de la fonction publique et de la sécurité et peut complexifier l'obtention d'un passeport, d'une carte d'identité, d'un visa ou d'un titre de séjour.

Ainsi, une personne simplement soupçonnée de représenter une menace sur la base de critères inconnus peut faire l'objet d'une surveillance continuelle qui recense des informations diverses et variées notamment personnelles, sans aucun contrôle ou possibilité de

[244] Rapport Parlementaire Pillet, *op.cit*., p.15.
[245] Rapport Parlementaire Pillet, *op.cit*., p.14.

rectification. Cela peut affecter sa vie professionnelle et administrative. **L'expectative produit donc des conséquences dans le réel**.



Fichier des personnes recherchées

Service : CIAT CENTRAL DE MONTPELLIER

Dossier FPR : [redacted] Utilisateur : 478446

Les informations contenues dans cette fiche ont un caractère confidentiel et ne peuvent être communiquées qu'aux seules personnes autorisées à en prendre connaissance : Les autorités judiciaires, les services de police et de gendarmerie, les autorités administratives dans le cadre de leurs compétences.

Identité principale

Identité [redacted]

Nationalité

Filiation

Informations générales

INDIVIDU DANGEREUX

Mesure immédiate : Ne pas attirer l'attention

Motif : Sûreté de l'état

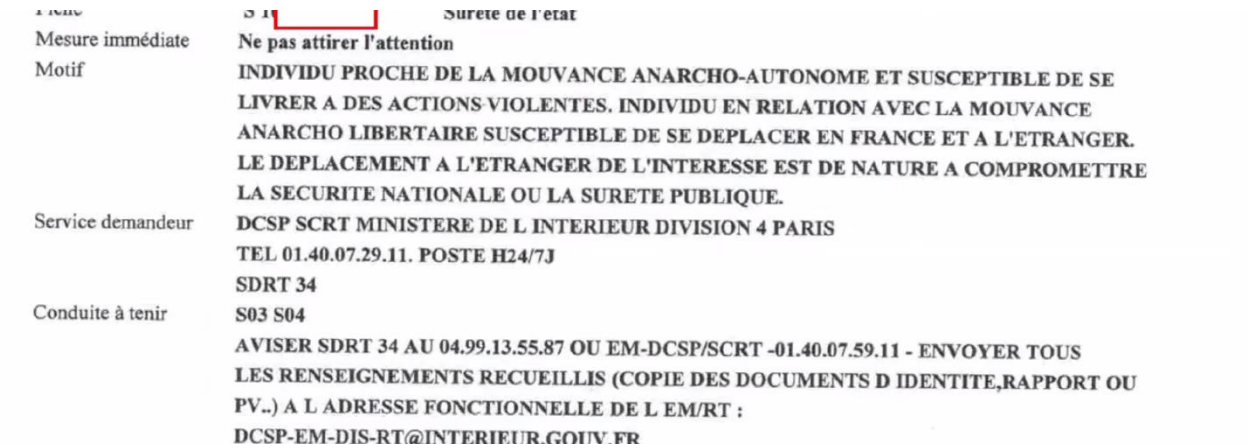
Sommaire : 1 identité, 2 fiches

Fiches actives : S 1[redacted] S 1[redacted]

Fiches actives

Fiche : S 1[redacted] Sûreté de l'état

Mesure immédiate : Ne pas attirer l'attention



Sûreté de l'état

Mesure immédiate : Ne pas attirer l'attention

Motif : INDIVIDU PROCHE DE LA MOUVANCE ANARCHO-AUTONOME ET SUSCEPTIBLE DE SE LIVRER A DES ACTIONS VIOLENTES. INDIVIDU EN RELATION AVEC LA MOUVANCE ANARCHO LIBERTAIRE SUSCEPTIBLE DE SE DEPLACER EN FRANCE ET A L'ETRANGER. LE DEPLACEMENT A L'ETRANGER DE L'INTERESSE EST DE NATURE A COMPROMETTRE LA SECURITE NATIONALE OU LA SURETE PUBLIQUE.

Service demandeur : DCSP SCRT MINISTERE DE L INTERIEUR DIVISION 4 PARIS
TEL 01.40.07.29.11. POSTE H24/7J
SDRT 34

Conduite à tenir : S03 S04
AVISER SDRT 34 AU 04.99.13.55.87 OU EM-DCSP/SCRT -01.40.07.59.11 - ENVOYER TOUS LES RENSEIGNEMENTS RECUEILLIS (COPIE DES DOCUMENTS D IDENTITE,RAPPORT OU PV..) A L ADRESSE FONCTIONNELLE DE L EM/RT :
DCSP-EM-DIS-RT@INTERIEUR.GOUV.FR

Exemple d'une fiche S de personne recherchée.

Pour conclure ce développement, indiquons sur quelles bases les soupçons sont construits dans le cadre d'un signalement. Sur la fiche reproduite ci-dessus en exemple, nous voyons que la personne est fichée parce que « *proche de la mouvance anarcho-autonome* ». **Un parallèle peut en ce sens être fait avec les « carnets B » utilisés à l'aube de la**

première guerre mondiale et surtout lors de la deuxième guerre mondiale, marquée par – outre un génocide – la persécution des ennemis politiques.

A la différence du carnet B, il n'est aujourd'hui effectivement pas possible d'interner ou d'arrêter les personnes fichées. Précisons tout de même que cette question est apparue dans le débat public et politique, notamment par une annonce du ministère de l'Intérieur visant à expulser du territoire français des personnes sans papier ni titre de séjour fichées pour radicalisation.

Les individus soupçonnés de radicalisation représentent plus de la moitié des inscrits dans ces fichiers sous la catégorie S, malgré la création en 2017 du fichier de traitement des signalements pour la prévention et la radicalisation à caractère terroriste (FSPRT) – **preuve que les fichiers ne se remplaçent pas mais s'additionnent**. En effet, *« en avril 2018 environ 17 000 fiches S, sur un total de 26 000, concernaient des personnes fichées pour radicalisation ou en raison de leurs relations avec des personnes radicalisées*[246]. »

Afin d'illustrer l'arbitraire qui entoure le FPR, il faut ici faire référence à deux listes de signes de radicalisation qui ont été distribuées et annoncées, soit par le ministre de l'Intérieur soit par d'autres membres du gouvernement ces dernières années. **Ces exemples servent à rendre compte de la facilité avec laquelle il est possible d'être considérée comme une personne radicalisée avec toutes les conséquences que cela implique, notamment l'inscription dans le FPR**.

Signes de radicalisation, donnés lors d'un discours de Christophe Castaner, alors ministre de l'Intérieur, le 8 octobre 2019[247] :

- Port de la barbe
- Refus de serrer la main à une femme
- Accepter de faire équipe ou non avec des femmes
- Fréquentation de personnes radicalisées
- Port du voile intégral en dehors du travail

[246] Rapport Parlementaire Pillet, *op.cit.*, p. 23.
[247] Quels sont les signaux qui permettent d'identifier un cas de radicalisation islamiste, Ambre Lepoivre, 9 novembre 2019, BFM TV, https://www.bfmtv.com/police-justice/quels-sont-les-signaux-qui-permettent-d-identifier-un-cas-de-radicalisation-islamiste_AV-201910090084.html.

- Pratique régulière et ostentatoire de la prière, particulièrement exacerbée en matière de ramadan
- Présence d'une hyperkératose au milieu du front
- Pratique religieuse rigoriste, particulièrement exacerbée en période de ramadan

Signes de radicalisation selon le gouvernement, février 2018[248] :

- Changements physiques, vestimentaires et alimentaires
- Propos asociaux
- Passage soudain à une pratique religieuse hyper ritualisée
- Rejet de l'autorité et de la vie en collectivité
- Rejet brutal des habitudes quotidiennes
- Repli sur soi
- Haine de soi, rejet de sa propre personne, déplacement de la haine de soi sur autrui
- Rejet de la société et de ses institutions
- Éloignement de la famille et des proches
- Modification soudaine des centres d'intérêt
- Appréhension complotiste, antisémite, apocalyptique de la société

III. Le FSPRT - Fichier des signalements pour la prévention de la radication à caractère terroriste

Le fichier FSPRT (Fichier des signalements pour la prévention de la radicalisation à caractère terroriste) est une base de données spécialisée dans le domaine de la lutte antiterroriste, créé par décret non-publié le 5 mars 2015, en réaction aux attentats de Charlie Hebdo et de l'Hyper Cacher.

Le rapport parlementaire sur l'amélioration de l'efficacité des fiches S du 19 décembre 2018 indique que ce fichier a été créé en parallèle au FPR, **spécifiquement pour intégrer les personnes engagées dans un processus de radicalisation, permettant d'assurer un suivi**

[248] Fiche Vigipirate, *Prévention et signalement des cas de radicalisation*, https://www.gouvernement.fr/sites/default/files/risques/pdf/fiche-prevention-et-signalement-des-cas-de-radicalisation-djihadiste.pdf.

individualisé et permanent, par le biais d'une prise en charge par le service qui lui a été désigné en fonction de son degré de dangerosité[249]. Pratiquement, les personnes présentant un caractère actuel et élevé de dangerosité sont suivies par la DGSI, et au contraire ceux représentant un danger relativement bas sont suivies par les agents territoriaux. Le service correspondant est indiqué dans la catégorie « chef de file » du fichier. Au total, six catégories correspondant à la fois au niveau de radicalisation (du « haut spectre » au « bas spectre ») et au degré de surveillance appliqué (en cours d'évaluation, en veille/en sommeil pour les personnes moins prioritaire mais toujours observées, fiche active) [250].

Le fichier serait donc structuré pour faciliter le suivi des personnes signalés pour radicalisation mais également pour faciliter l'échange des données et partage d'information entre services afin « d'appréhender le phénomène de la radicalisation sur le territoire français dans sa globalité »[251]. Des études statistiques sont réalisées à travers de l'UCLAT, contribuant à l'élaboration des politiques publiques de lutte contre la radicalisation.[252]

« Y sont recensées les informations relatives à l'ensemble des personnes résidant sur le territoire national et signalées pour radicalisation. Le FSPRT est, à cet égard, alimenté par plusieurs vecteurs :

- **les signalements émis par des particuliers** via le centre national d'assistance et de prévention de la radicalisation, soit par la plateforme téléphonique nationale de signalement, soit par un site internet dédié (30 % des personnes fichées). Les signalements reçus dans ce cadre font l'objet d'un processus de validation par l'UCLAT avant d'être enregistrés dans le fichier ;
- les **signalements effectués par les services territoriaux** (services de l'Éducation nationale, élus locaux, services municipaux, associations sportives, etc.), via les états-majors de sécurité de chaque préfecture (37 à 38 % des personnes fichées). Les signalements sont alors inscrits par l'UCLAT ;
- **les signalements effectués par les services de renseignement** (30 à 32 % des personnes fichées).

[249] Rapport parlementaire Pillet, op.cit, p.25
[250] *Ibid.*
[251] Rapport parlementaire Paris-Morel-à-L'huissier, *op.cit.*
[252] *Ibid.*

Le FSPRT répond à un besoin de décloisonnement et de partage de l'information entre services aux fins de suivi des personnes radicalisées. Conçu comme un **outil de travail collaboratif**, il comprend des informations précises sur les profils des personnes concernées (lieux de résidence, profession exercée, signes de radicalisation, velléités de départ à l'étranger, pratiques sportives à risque, etc.) et sur les mesures de suivi mises en place, enrichies au fil du temps. »[253]

A) Croisements

Depuis 2018 le fichier est en croisement avec le FPR dans le sens où une fiche S est systématiquement constituée en parallèle de la fiche FSPRT pour toute personne signalée pour radicalisation. **L'objectif de ce rapprochement est d'enrichir le FSPRT de donnée en provenance du FPR**, notamment pour les fichés qui sont du « bas du spectre » pour lesquels les moyens mis à disposition pour collecter des informations sont moindres[254]. Si ce rapprochement n'est pas à même de changer la finalité de la fiche S selon le rapport parlementaire Pillet[255], il a néanmoins une conséquence directe sur le nombre de personnes fichés pour cause de potentielle radicalisation au sein du FPR, plus particulièrement sous la catégorie S, comme nous le démontre les chiffres déjà cités (en avril 2018 environ 17 000 fiches S, sur un total de 26 000).

Le décret n° 2019-412 du 6 mai 2019 a rendu possible l'interconnexion entre le fichier HOPSYWEB et le FSPRT. HOPSYWEB est l'ancêtre du fichier HOPSY qui offrait la possibilité aux Agences Régionales de Santé (ARS) de mettre en place une gestion automatisée des données personnes des patients internés sous contrainte. En 2018, HOPSY est remplacé par HOPSYWEB, qui permet une interconnexion nationale des fichiers régionaux avec une durée de conservation de 3 ans, au lieu d'une année pour HOPSY. Selon l'analyse de Lisa Carayon dans un article pour la *Revue des droits de l'homme*, **il est très probable, mais indémontrable, que HOPSYWEB ait remplacé HOPSY uniquement pour faciliter l'interconnexion avec le fichier FSPRT**. Ainsi, d'un point de vue chronologique, il n'est pas

[253] Rapport parlementaire Pillet, *op. cit.*.
[254] Rapport parlementaire Pillet, *op.cit*, p. 25.
[255] « Il n'a toutefois conduit à modifier ni la finalité, ni la nature des « fiches S », dont la création demeure, en définitive, de la responsabilité des services de renseignement, auxquels il revient d'évaluer l'opportunité d'émettre ou non une fiche. » Rapport parlementaire Pillet, *op.cit*, p.26.

anecdotique de constater que HOPSYWEB a été créé en réaction au *Plan national de prévention de la radicalisation*, publié par le Gouvernement en février 2018 et intitulé « Prévenir pour protéger ».

Plan national de prévention de la radicalistion, Mesure n° 39 :

Actualiser les dispositions existantes relatives à l'accès et à la conservation des données sensibles contenues dans l'application de gestion des personnes faisant l'objet d'une mesure de soins psychiatriques sans consentement (HOPSY)[256].

« *Par « actualiser » il faut comprendre autoriser l'accès à ce fichier à des personnels à même de les intégrer ensuite à un plan de repérage de la radicalisation. En effet, la recommandation précédente suggère un renforcement de la coopération entre les préfectures et les ARS – en charge de la gestion des fichiers HOPSY* »[257].

HOPSYWEB est créé 3 mois après ce texte de recommandation du gouvernement. Et cinq mois plus tard, dans le rapport Paris-Morel-À-L'Huissier, il est indiqué une nécessité de prendre plus en compte des « perturbés mentalement » ou des « déséquilibrées », en faisant référence à la recommandation du Plan de lutte contre la radicalisation déjà mentionnée[258]. Sans réaliser une analyse des termes stéréotypant utilisés pour faire références aux personnes ayant des troubles psychiatriques, ils sont tout du moins significatifs du manque de scientificité et d'objectivité des propos assumés. Les seules données mises en avant pour justifier la relation entre attentats terroriste et troubles psychiatrique est qu'« *on évalue à 30 % la part de la population carcérale souffrant de troubles mentaux*[259] ». En plus du fait que la source de ce chiffre n'est pas indiquée, il ne semble pas être en cohérence avec le propos qu'il devrait justifier et selon lequel **il serait possible de prévenir les attentats terroristes grâce à un suivi des personnes ayant vécu des internements psychiatriques contraints**.

[256] « Prévenir pour protéger », *Plan national de prévention de la radicalisation*, publié par le Gouvernement en février 2018.

[257] Lisa Carayon, « Quelle folie ! », *La Revue des droits de l'homme*, 11 juin 2020, (URL : http://journals.openedition.org/revdh/9746 ; DOI : https://doi.org/10.4000/revdh.9746).

[258] « Rappelant les fameuses recommandations du Plan de lutte contre la radicalisation, le rapport affirme « Un pas [dans le sens de l'interconnexion] semble avoir été accompli en ce sens avec la publication du décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement », V. Lisa Carayon, *op.cit*.

[259] Rapport parlementaire Paris-Morel-à-L'huissier, *op.cit.*

Par ailleurs, l'absence de fondements, sources et scientificité de ces propos amène à réfléchir sur la pertinence pénale de ce lien. Effectivement, selon l'article 122-1 du code pénal, « *n'est pas pénalement responsable la personne qui était atteinte, au moment des faits, d'un trouble psychique ou neuropsychique ayant aboli son discernement ou le contrôle de ses actes*. ». Les actes commis par une personne souffrant de troubles psychiatriques doivent-ils être considéré comme des actes terroristes ? Une personne pénalement irresponsable peut-elle être jugé en tant que terroriste ? Un terroriste est-il de fait une personne ayant des troubles psychiatriques ? Toutes ces questions méritent d'être discutés, argumentés avant de supposer une quelconque corrélation, surtout si celle-ci a comme conséquence une violation des droits individuelles et du secret médical.

Car la publication du décret permettant l'interconnexion entre les deux fichiers a suscité de vives critiques des professionnels de santé. Cette interconnexion « constitue une étape supplémentaire inacceptable et scandaleuse au fichage des personnes les plus vulnérables touchées par la maladie mentale dans notre pays, dans un amalgame indigne entre le champ sanitaire et celui de prévention de la radicalisation »[260].

Le rapport parlementaire sur les services publics face à la radicalisation du 27 juin 2019 fait référence aux réticences des personnels de santé tout en cherchant à justifier l'interconnexion par les exceptions faites en droit pénal et code de l'action sociale et des familles prévus pour déroger au secret médical[261]. Néanmoins, ces exceptions sont liées à des situations où une **mise en danger immédiate existe, et non pas dans un désir de préserver la laïcité**, comme est affirmé à la fin du rapport : « *le développement de la formation des personnels soignants dans le cadre de la formation continue mais également dans le cadre des instituts de formations paramédicales devrait permettre une évolution des mentalités et des comportements. Cette formation doit donner une place essentielle aux cas pratiques pour aider les personnels à gérer les atteintes à la laïcité et à signaler les comportements préoccupants* »[262].

[260] Citation reprise de l'article Marc Rees, « Psychiatrie et radicalisation : un croisement de fichiers qui ne passe pas », NextInpact, 14 mai 2019.
[261] « Pourtant, le code pénal et le code de l'action sociale et des familles prévoient des dérogations au secret médical qui sont tout à fait applicables face à un individu radicalisé. », cf. Rapport parlementaire Diard-Poulliat, *op.cit.*
[262] *Ibid.,*

La CNIL dans sa délibération 2018-354 du 13 décembre 2018 déclare que cette interconnexion ne changeait pas la nature du fichier HOPSYWEB mais en rajoutait une secondaire. Une des lectures possibles de cette déclaration est que la CNIL a volontairement insisté sur ce point pour que le fichier réponde au droit commun et par conséquent à la législation du RGPD, notamment en regard de la durée de conservation des données et de son accès, ce qui ne pourrait pas être le cas si le fichier était considéré comme relevant de la sécurité de l'Etat[263]. Néanmoins, suite à une requête en annulation du décret du 6 mai 2019 sur l'interconnexion HOPSYWEB/FSPRT, le Conseil d'État considère lui que « la qualification à appliquer à leur interconnexion dépend de la raison pour laquelle on souhaite y procéder », et par conséquent ici « prévention de la radicalisation à caractère terroriste », démarche qui relève de la sûreté de l'État[264].

D'ailleurs, **il n'est pas tant question de prévention que de surveillance et répression**. « *L'interconnexion ne vise pas à éviter que les personnes se radicalisent ; elle se base sur l'idée selon laquelle une personne radicalisée atteinte de troubles psychiatriques est plus dangereuse qu'une personne radicalisée ne souffrant pas de tels troubles et qu'il convient dès lors de lui appliquer une surveillance plus adaptée.* »[265].

Concrètement, l'interconnexion se réalise par une actualisation toutes les 24 heures, et lorsque le nom, prénom et date de naissance coïncident, une alerte est automatiquement envoyée aux agents spécialement désignés de la préfecture du lieu d'hospitalisation. Après cela, il est possible de chercher plus d'informations pour vérifier l'identité de la personne. Pourtant, les informations qui peuvent être de ce fait accessibles ne semblent pas aider l'identification, puisque s'analysant simplement en : « *les dates de début et de fin de mesure, les types de mesures prononcées et le cas échéant le lieu d'hospitalisation* »[266]. L'intérêt de ce croisement doit donc se chercher ailleurs.

Les amalgames qui sont ainsi actés via ces processus d'interconnexion de fichiers, entre radicalités violentes et maladie mentale, ne sont pas près d'être corrigés, preuve en est le projet de loi relatif à la prévention d'actes de terrorisme et au renseignement dont l'actuel

[263] Lisa Carayon, *op.cit.*
[264] *Ibid.*
[265] *Ibid.*
[266] Délibération n° 2018-354 du 13 décembre 2018 portant avis sur un projet de décret modifiant le décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement (demande d'avis n° 18020552).

article 6 prévoit le renforcement de ces échanges de données personnelles entre HOPSYWEB et FSPRT.

IV. N-SIS II

Le système d'information Schengen résulte des articles 92 et suivants de la Convention d'application de l'Accord de Schengen du 14 juin 1985. Il a ensuite évolué vers le SIS II, institué en décembre 2006 mis en service le 9 avril 2013. En remplaçant le système d'information Schengen de première génération, il a permis d'y intégrer de nouvelles fonctions, notamment la possibilité d'interroger le système central et pas seulement la copie nationale des données ou encore la mise en relation de signalements concernant des personnes et des objets[267]. La finalité de cette base de données est de **permettre aux autorités nationales de consulter et saisir des signalements concernant des personnes ou des objets afin de renforcer la sécurité malgré l'absence de contrôle aux frontières intérieures à l'Union européenne**. Selon la CNIL, en 2019, les États membres ont procédé à 91 millions de signalements dans la base de signalements SIS II[268].

Au niveau national, ce fichier est placé sous le contrôle du ministre de l'Intérieur. Sa finalité exclusive est la « ***centralisation d'informations*** *concernant les personnes et objets signalés par les autorités administratives et judiciaires des Etats parties au règlement du Parlement européen et du Conseil (CE) n° 1986/2006 du 20 décembre 2006 sur l'accès des services des Etats membres chargés de l'immatriculation des véhicules au système d'information Schengen de deuxième génération (SIS II) ainsi qu'au règlement et à la décision mentionnés au 1° de l'article R. 231-3 afin de permettre aux autorités désignées par ces Etats de mettre en œuvre des conduites à tenir relatives aux personnes et objets recherchés* »[269].

Les informations contenues dans ce fichier concernent les personnes recherchées ou disparues, des personnes sous surveillance policière et des personnes non ressortissantes d'un

[267] Rapport n° 484 (2016-2017) de M. François-Noël BUFFET, fait au nom de la commission d'enquête, déposé le 29 mars 2017, Circuler en sécurité en Europe : renforcer Schengen, https://www.senat.fr/rap/r16-484/r16-484.html.
[268] CNIL, SIS II, 16 septembre 2020, https://www.cnil.fr/fr/sis-ii-systeme-dinformation-schengen-ii.
[269] Article R. 231-5 du Code de sécurité intérieure.

Etat membre de l'espace Schengen auxquelles l'entrée sur le territoire est interdite mais également des informations sur des véhicules ou objets volés ou disparus[270].

En France, **le N-SIS II découle d'une interconnexion**. En effet les signalements effectués dans le FPR, le FOVeS, le fichier des titres électroniques sécurisés (TES) et DOCVERIF (ayant pour objectif de faciliter le contrôle de la validité des documents émis par les autorités françaises et de lutter contre l'utilisation indue de faux documents) alimentent automatiquement le N-SIS II. D'autres fichiers sont interconnectés directement avec le fichier N-SIS II. Ainsi, le fichier LAPI (lecture automatisée des plaques d'immatriculation) est alimenté par les signalements des véhicules enregistrés dans le FoVES ou dans le N-SIS II.

Par ailleurs, d'autres fichiers peuvent permettre l'accès aux informations contenues dans le N-SIS II. Ainsi, le PASP contient une indication de l'enregistrement de la personne dans le N-SIS II[271]. Enfin, l'ACCReD permet d'avoir accès à toutes les informations contenues dans le N-SIS II.

En outre, certains nouveaux croisements pourraient voir le jour. En effet, la Commission européenne a présenté une communication en avril 2016 en vue d'aboutir à l'interopérabilité - définie par la Commission comme « *la capacité des systèmes d'information à échanger des données et à permettre le partage d'information* »[272] - des systèmes d'informations. En France, une application COVADIS permet déjà d'interroger simultanément le SIS II, le VIS, le fichier Interpol SLTD, le FPR et VISABIO[273].

Il pourrait s'agir dans le futur de la création d'une interface de recherche unique permettant d'interroger tous les systèmes d'informations européens. Une autre option présentée par la Commission européenne est l'interconnexion des systèmes d'informations[274]. Ainsi, de nombreux croisements sont d'ores et déjà possibles avec le N-SIS II et les autorités européennes semblent aller dans le sens d'un renforcement de ces croisements.

[270] Article R. 231-6 du Code de sécurité intérieure.
[271] Article R. 236-12 du Code de sécurité intérieure.
[272] Communication de la Commission au Parlement européen et au Conseil sur des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité, COM(2016) 205 final.
[273] Rapport n° 484 (2016-2017) de M. François-Noël BUFFET, *op. cit*.
[274] Rapport n° 484 (2016-2017) de M. François-Noël BUFFET, *op. cit.*

Tableau récapitulant les croisements existant entre le N-SIS II et d'autres fichiers :

Nom du fichier	Finalité du fichier	Informations collectés	Type de croisement
FPR	Inscrire toute personne faisant objet d'une requête ou mandat, contôle judiciaire ou aménagement de peine.	Voir partie II.	Alimente directement N-SIS II
FOVeS	retrouver les objets et les véhicules volés, et surveiller les objets et les véhicules signalés.	celles relatives à des vols, aux déclarations de perte, aux invalidations de documents et à toutes les mesures de surveillances mises en œuvre par la police, la gendarmerie et les douanes (article 2 de l'arrêté du 7 juillet 2017). Il est bien sûr en lien avec les polices étrangères.	Alimente directement N-SIS II
TES **Fichier des titres électroniques sécurisés**	Base de données gérée par ministère de l'intérieur qui rassemble les données personnelles et biométriques des français pour la gestion des cartes nationales d'identité et des passeport français	les nom et prénoms ; la date et le lieu de naissance ; le sexe ; la couleur des yeux ; la taille ; l'adresse postale ; les noms et prénoms des parents, leur date de naissance ainsi que leur nationalité ; le nom du responsable légal ; l'image numérisée du visage ; les empreintes digitales ; l'image numérisée de la signature ; l'adresse de messagerie électronique et les coordonnées téléphoniques ; l'image numérisée des pièces du dossier de demande de titre ; informations relatives à la carte d'identité ou au passeport, comme le numéro du titre, son type, ainsi que sa date et son lieu de délivrance.	Alimente directement N-SIS II
DOCVERIF	faciliter le contrôle de la validité des documents émis par les autorités françaises et de lutter contre l'utilisation indue de tels documents, leur falsification ou	Le type et le numéro du document ; la mention du caractère valide ou non valide du document ; pour les documents invalides, le motif avec la date de l'invalidité du document, les	Alimente directement N-SIS II

	leur contrefaçon	noms, prénoms, date et lieu de naissance mentionnés sur le document, sa date de délivrance.	
LAPI Lecture automatisée des plaques d'immatriculation	Répression du terrorisme, de la criminalité organisée, du vol et du recel de véhicules	photos des plaques d'immatriculation, le numéro d'immatriculation, la photo du véhicule et de ses occupants, la date et l'heure de la photo et sa géolocalisation.	alimenté par les signalements des véhicules enregistrés dans le FoVES ou dans le N-SIS II
PASP	Collecter des informations sur les persones qui "peuvent" porter atteinte à la sécurité publique, « notamment » celles « susceptibles » d'être impliquées dans des actions de violences collectives et, depuis 2017, des activités terroristes.	Critères d'enregistrements flous, et interdiction des données sensibles, mais si: - fréquentations - "activités publique" – politique - philosophiques - religieuses – syndicale - "comportements" - Déplacement - "origine géograhique" - signes physiques particuliers et objectifs, photographies, titres d'identité, immatriculation des véhicules, informations patrimoniales, activités publiques, comportement et déplacements, agissements susceptibles de recevoir une qualification pénale - Infos au sujet des personnes « entretenant ou ayant entretenu des relations directes et non fortuites avec l'intéressé ».	contient une indication de l'enregistrement de la personne dans le N-SIS II
ACCReD			accès à toutes les informations contenues dans le N-SIS II.
COVADIS			permet déjà d'interroger simultanément le SIS II, le VIS, le fichier Interpol SLTD, le FPR et VISABIO.

V. Le FoVES

Le FOVeS a été créé en 2014 à titre expérimental pour une durée de 2 ans et est définitif depuis 2017. Sa création s'intègre dans le cadre de la modernisation et de la rationalisation des fichiers de la police et de la gendarmerie nationale. Il a pour objectif de constituer une base unique et homogène de signalements pour les véhicules ou objets volés, placés sous surveillance ou perdus lors d'un signalement par une autorité française ou d'un État partie aux accords de Schengen.

Le FOVeS remplace la catégorie objet dans l'ancien fichier STIC, ainsi que l'ancien fichier des objets signalés FOS et le FVV, fichier des véhicules volés. Ainsi, les données de ce fichier sont celles reprises desdits fichiers ainsi que du LRPPN et LRPGN et des signalements directement saisis dans l'application.

A) Informations collectées

Les informations collectées concernent majoritairement l'objet perdu, volé ou surveillé ainsi que « l'identité de la personne susceptible d'utiliser le véhicule ou l'objet ». Dans la première délibération faite par la CNIL en 2013, celle-ci ne se préoccupe pas de ce recensement d'informations étant donné que le FOVeS n'a pas pour finalité « la recherche et la surveillance des personnes susceptibles d'utiliser un véhicule volé ou signalé »[275]. Ces recherches sont réalisées par le FPR. A cet égard, le FOVeS ne permettra d'ailleurs pas de faire une recherche à partir du nom ou d'un identifiant d'une personne[276].

D'autres informations collectées sont celles relatives aux mesures de surveillance mise en œuvre par la police, la gendarmerie et les douanes. Dans la première délibération, la CNIL déplore qu'il n'y ait pas plus d'informations sur la question des types de surveillance dont il était question, outre : « Mesures de surveillance exécutées dans le cadre des missions répressives ou préventives »[277].

[275] Délibération n° 2013-357 du 14 novembre 2013 portant avis sur un projet d'arrêté portant autorisation à titre expérimental d'un traitement automatisé de données à caractère personnel dénommé « Fichier des objets et des véhicules signalés » (FOVeS) (demande d'avis n° 1301197).
[276] *Ibid.*
[277] *Ibid.*

B) Interconnexions

L'une des particularités de ce fichier est qu'il comporte de nombreux croisements avec d'autres fichiers ; alors même que le décret qui l'encadre ne fait référence à aucune interconnexion ou rapprochement[278], limitant ainsi le contrôle. Faute d'interdiction expresse, toute interconnexion serait possible.

En plus d'être consulté par divers traitements du ministère de l'Intérieur comme LAPI, FAETON, AGRIPPA (cf. tableau ci-dessous), ce fichier transmet également directement les données relatives à différents fichiers comme le TAJ ou le N-SIS, de manière automatique et instantanée.

C) Conservation des données

Il s'agit également d'un des fichiers avec une durée de conservations des plus longues. En effet, pour les armes, munitions, explosifs, bijoux, montres et objets d'art volés les données sont conservées pendant 50 ans, 20 pour les billets de banque, 10 ans pour les véhicules containers, documents, plaques d'immatriculation, moteurs de bateau et 5 ans pour le reste. Pour les véhicules et armes perdus les données sont conservées 50 ans, et 10 pour les documents.

A partir du moment de la découverte du véhicule ou de l'objet perdu/volé, les données sont conservées pendant 4 mois et 5 ans pour les véhicules et bateaux. Mais même lorsque les données sont effacées, celles-ci sont archivées et par conséquent consultables pour une durée de 10 ans.

D) Enquêtes administratives

L'arrêté du 7 juillet 2017 qui encadre le fichier est encore en vigueur, à la différence de celui de 2014, et permet sa consultation « *lors de la réalisation des enquêtes administratives prévues aux articles L.114-1, L.114-2 et L.211-11-1 du code de la sécurité*

[278] *Ibid.*

intérieur » (art.1). Un mois plus tard est instauré le traitement de données ACCReD, qui facilitera d'autant plus l'accès à ces informations lors d'enquêtes administratives.

ACCReD est considéré comme un traitement de données de biens et non d'individus. C'est pourquoi la CNIL, dans sa dernière délibération, estime que la consultation automatique par ACCReD « *ne devrait intervenir qu'à partir du numéro du document ou de la plaque d'immatriculation du véhicule de la personne concernée* » [279].

Tableau des différents croisements du fichier FoVES[280] :

Nom du fichier	Finalité du fichier	Informations collectés	Type de croisement
TAJ			FOVeS transmettra au TAJ les informations relatives à la découverte d'un objet déclaré ou volé. [281]
LAPI Lecture automatisée des plaques d'immatriculations	Répression du terrorisme, de la criminalité organisée, du vol et du recel de véhicules	photos des plaques d'immatriculation, le numéro d'immatriculation, la photo du véhicule et de ses occupants, la date et l'heure de la photo et sa géolocalisation.	Chaque dispositif LAPI compare les données lues avec le FOVeS et le système d'information Schengen (SIS)
SIV Système d'immatriculation des véhicules	Gestion des certificats d'immatriculation (cartes grises) et des autres documents administratifs liés aux véhicules en circulation.	Identité du titulaire du certificat d'immatriculation du véhicule (carte grise) ; Informations concernant le véhicule et l'autorisation de circuler ; Identité des professionnels habilités à transmettre des données au SIV : vendeurs de véhicules, huissiers de justice, experts, assureurs, démolisseurs/broyeurs, sociétés de crédit..	

[279] Délibération n° 2017-158 du 18 mai 2017 portant avis sur un projet d'arrêté portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « Fichier des objets et des véhicules signalés » (FOVeS) (demande d'avis n° 2050106).
[280] Malgré notre volonté d'être le plus exhaustif·e·s possible, par un problème d'opacité et absence d'informations sur les interconnexions et rapprochement de ce fichier dans l'arrêté l'encadrant, nous ne pouvons pas être sûr de l'exhaustivité de ce tableau.
[281] Délibération n° 2017-158 du 18 mai 2017, *op. cit.*

Système de contrôle automatisé	relevé de l'infraction par un « radar », l'envoi de l'amende au domicile et les possibilités de paiement ou de contestation.	numéro d'identification unique de l'infraction; clichés concernant le véhicule et ses passagers relatifs aux infractions; données relatives à l'infraction; identification du véhicule; identification du titulaire du certificat d'immatriculation du véhicule ayant servi à commettre l'infraction; état civil ; identification du conducteur du véhicule ayant servi à commettre l'infraction; catégorie et numéro de permis de conduire du conducteur du véhicule ayant servi à commettre l'infraction ; informations sur l'amende	
BSVV **Base satellite des véhicules volés**	pour finalités d'accéder aux informations relatives à l'état de vol et de mise sous surveillance d'un véhicule	toutes "les caractéristiques permettant l'identification du véhicule" (numéro d'immatriculation, numéro diplomatique, marque...), l'état et les dates du vol ou de la mise sous surveillance.	
ACCReD			Consultation automatique du FOVeS en mode hit/no hit. Si le document de la personne qui fait l'objet de l'enquête administrative ou son véhicule est connu du traitement FOVes, les agents des deux services précités seront alors tenus de procéder à une consultation du FOVeS en vue d'obtenir les informations nécessaires complémentaires pour procéder à l'analyse.[282]
N-SIS			FOVeS transmettra en temps réel les données concernant

[282] *Ibid.*

			les objets et véhicules éligibles au système d'information Schengen : Arme à feu, billets de banque, documents vierges ou délivrés et des véhicules terrestre immatriculés.
TES Titres électroniques sécurisés	Base de données gérée par ministère de l'intérieur qui rassemble les données personnelles et biométriques des français pour la gestion des cartes nationales d'identité et des passeport français	les nom et prénoms ;la date et le lieu de naissance ; le sexe ;la couleur des yeux ;la taille ;l'adresse postale ;les noms et prénoms des parents, leur date de naissance ainsi que leur nationalité ;le nom du responsable légal; l'image numérisée du visage ; les empreintes digitales ;l'image numérisée de la signature ;l'adresse de messagerie électronique et les coordonnées téléphoniques ;l'image numérisée des pièces du dossier de demande de titre; informations relatives à la carte d'identité ou au passeport, comme le numéro du titre, son type, ainsi que sa date et son lieu de délivrance.	Proposition
LRPN - LRPGN			Les deux logiciels de rédaction permettent d'alimenter automatiquement par des informations issues de ces traitements, relatives à des objets identifiés dans le cadre d'une procédure de vol ou de découverte. [283]
ASF (automatic Search Facility) – SMV (Stolen Mobile Vehicles)	Base de données gérée par Interpol		Transmettre à cette base les signalements concernant les véhicules volés inscrits dans le FOVeS

[283] Délibération n° 2013-357 du 14 novembre 2013, *op. cit.*

ASF – SL TD (Stolen and Lost travel documents)	Base de données gérée par Interpol		transmettre les signalements concernant les documents de voyages volés, voire perdus
FAETON	Nouveau permis de conduire européen		interrogation transparente du système FAETON, afin d'obtenir le numéro de série du document, indispensable à la cession des informations relatives aux documents volés dans le N-SIS ou les bases de données d'Interpol. Le FOVeS transmettra quant à lui ses signalements de vol à FAETON.
AGRIPPA Application de gestion du répertoire informatisé des propriétaires et possesseurs d'armes	Recense tous les détenteurs d'armes	Caractéristiques de l'arme, date de la délivrance de l'autorisation ou du récépissé de déclaration, date d'expiration de l'autorisation, le cas échéant, date de refus et date de notification d'un refus d'autorisation, dates de recours déposés.	Depuis l'application FOVeS, de rapatrier directement des identifiants de l'arme ou du document d'autorisation
Système API/PNR France	Traitement qui procède de manière automatique et systématique à un rapprochement des données qu'il contient avec d'autres fichiers de police judiciaire ou administrative relatifs à des personnes ou des objets recherchés ou surveillés. Pour les besoins de la prévention et de la constatation des actes de terrorisme, des infractions mentionnées à l'article 695-23 du code de procédure pénale et des atteintes	les données dites de réservation (données PNR) ; les données dites d'enregistrement et d'embarquement (données API) présentes dans les systèmes d'information d'enregistrement et d'embarquement des compagnies aériennes ou des plateformes aéroportuaire ; copie partielle du FPR ; réponses aux requêtes formulées par les unités et services demandeurs[285]	Déterminer si le document d'identité ou de voyage présenté par le voyageur est inscrit dans FOVeS[286].

[285] Pour une liste plus exhaustive, voir le site officiel CNIL, à l'adresse suivante : https://www.cnil.fr/fr/le-systeme-api-pnr-france.
[286] Délibération n° 2017-158 du 18 mai 2017, *op.cit.*

	aux intérêts fondamentaux de la Nation, du rassemblement des preuves de ces infractions et de ces atteintes ainsi que de la recherche de leurs auteurs, les ministres de l'Intérieur, de la défense et chargés des transports et des douanes sont autorisés à mettre en œuvre ce fichier[284]	
DOCVERIF	faciliter le contrôle de la validité des documents émis par les autorités françaises et de lutter contre l'utilisation indue de tels documents, leur falsification ou leur contrefaçon	Le type et le numéro du document ; la mention du caractère valide ou non valide du document ; pour les documents invalides, le motif avec la date de l'invalidité du document, les noms, prénoms, date et lieu de naissance mentionnés sur le document, sa date de délivrance.

VI. EASP

Les trois fichiers EASP, PASP et GIPASP partagent des finalités communes, et ont d'ailleurs fait l'objet de modifications parallèles de leur régime juridique en 2017 et 2020. Le fichier EASP étant spécifiquement destiné à la conservation des résultats des enquêtes administratives, il sera présenté à part, puis les fichiers jumeaux PASP et GIPASP seront présentés ensemble.

Le régime juridique du traitement automatisé de données à caractère personnel dénommé « Enquêtes administratives liées à la sécurité publique » (EASP) relève des articles R. 236-1 à R. 236-10 du code de la sécurité intérieure (CSI), qui codifient le décret n°2009-1250 du 16 octobre 2009. Il vise principalement à « *faciliter la réalisation d'enquêtes administratives* » prévues en application des articles L. 114-1, L. 114-2 et L. 211-11-1 du CSI et de l'article 17-1 de la loi de 1995 d'orientation et de programmation relative à la sécurité (Art. R. 236-1 CSI). Pour ce faire, il regroupe les données issues de précédentes enquêtes administratives. Les enquêtes administratives reposant elles-mêmes sur la consultation des

[284] *Fichiers de police, op. cit,* p. 72.

fichiers de police, de gendarmerie et de renseignement, **le fichier EASP est la matérialisation du croisement d'informations contenues dans les fichiers consultés par l'agent responsable de l'enquête administrative**. Un peu moins de 222 000 personnes sont fichées dans EASP.

Parmi les types de données pouvant être enregistrées dans ce traitement, on trouve les photographies, l'origine géographique, les identifiants, la situation familiale, les comportements et habitudes de vie, les pratiques religieuses, les signes de radicalisation, les données relatives aux troubles psychologiques ou psychiatriques, les antécédents judiciaires, les addictions, l'indication de l'enregistrement ou non de la personne dans les traitements de données TAJ, N-SIS II, PASP, GIPASP, FPR, FSPRT, et le traitement des données relatives aux objets et véhicules volés ou signalés, etc.

L'article R. 236-3 organise une exception à l'article 6 de la loi Informatique et Libertés (interdiction de traiter les données sensibles) en autorisant le traitement dans le fichier EASP des données concernant les motivations politiques, religieuses, philosophiques ou syndicales, et les troubles psychologiques ou psychiatriques.

Notons que le terme « motivations » s'avère extrêmement problématique puisqu'il exclut toute possibilité d'appréciation objective. « *Détournements et dysfonctionnements du système de fichage sont alors à prévoir* »[287]. Ces données peuvent être conservées pendant un délai de 5 ans, qui court à compter de leur enregistrement. L'article R. 236-2 précise que « le traitement ne comporte pas de dispositif de reconnaissance faciale à partir de la photographie ». Le droit d'accès est indirect, c'est-à-dire qu'il se fait par l'intermédiaire de la CNIL.

Sont autorisé·e·s à accéder aux données les agent·e·s individuellement désigné·e·s et spécialement habilité·e·s du service central du renseignement territorial de la Direction générale de la sécurité publique, des services du renseignement territorial des Directions départementales de la sécurité publique ou des Directions territoriales de la police nationale, ou des services de la préfecture de police chargés du renseignement. En outre, peuvent être

287 G. Koubi, « Les données à caractère personnel, outil des services de renseignements », *JCP Adm.*, 2009, p. 2264 [cité par V. Gautron, « Fichiers de police », *Répertoire de droit pénal et de procédure pénale*, avril 2015, point 193].

destinataires des données « dans la limite du besoin d'en connaître » les agent·e·s individuellement désigné·e·s et spécialement habilité·e·s du Service national des enquêtes administratives de sécurité, du Commandement spécialisé pour la sécurité nucléaire, ainsi que tout autre agent d'une unité de la gendarmerie ou d'un service de la police nationale sur demande expresse mentionnant l'identité du demandeur et les motifs de la consultation. La collecte, la modification, la communication, le transfert, le rapprochement, la suppression de données dans le cadre de la mise en œuvre du fichier EASP donne lieu à enregistrement de l'identifiant de l'auteur, la date, l'heure et le motif de l'opération ainsi que les destinataires des données (Art. R. 236-7 CSI). Cet enregistrement sera conservé 3 ans, alors que les données fichées sont conservées 5 ans. Alors que, nous l'avons déjà vu[288], **l'enregistrement des connexions ne permet pas un véritable contrôle des usages des fichiers**, s'ajoute à cela l'impossibilité de vérifier des connexions au-delà de 3 ans alors que les données ayant fait l'objet de la connexion sont toujours enregistrées.

En 2017, le décret n° 2017-1216 du 2 août 2017 abroge l'article R. 236-8 du CSI, qui disposait que le traitement EASP « *ne fait l'objet d'aucune interconnexion, aucun rapprochement ni aucune forme de mise en relation avec d'autres traitements ou fichiers* ». Ce changement ouvre des possibilités de croisements avec le fichier EASP : le 3 août paraît le décret n°2017-1224, instaurant le fichier ACCReD.

On peut légitimement douter que la CNIL se soit prononcée sur l'ouverture aux croisements du fichier EASP, puisque celle-ci a eu lieu non pas à la création du fichier, mais par abrogation d'une partie de son régime juridique au cours de sa vie. Un autre sujet d'inquiétude est le décret n°2020-1510 du 2 décembre 2020 : s'agissant des accès aux données, réglementés à l'article R. 236-6, alors qu'auparavant le terme « *fonctionnaires* » désignait les agents avec accès autorisé, aujourd'hui de simples « *agents* » peuvent y accéder.

VII. PASP et GIPASP

Le fichier « Prévention des atteintes à la sécurité publique » (PASP) et son « *clone gendarmique* »[289] le fichier « Gestion de l'information et prévention des atteintes à la sécurité

[288] V. *infra*, p. 43.
[289] Fichiers de police, *op. cit*., point 164.

publique » (GIPASP) ont été créés suite à l'échec de la mise en place du fichier EDVIGE (« Exploitation documentaire et valorisation de l'information générale »). Celui-ci, introduit par le décret n°2008-632 du 27 juin 2008, avait pour finalités d'« informer le gouvernement et les représentants de l'Etat dans les départements et collectivités », de « *centraliser et analyser les informations relatives aux personnes physiques ou morales ayant sollicité, exercé ou exerçant un mandat politique, syndical ou économique ou qui jouent un rôle institutionnel, économique, social ou religieux significatif, sous condition que ces informations soient nécessaires au gouvernement ou à ses représentants dans l'exercice de leurs responsabilités* », ainsi que les « *informations relatives aux individus, groupes, organisations et personnes morales qui, en raison de leur activité individuelle ou collective, sont susceptibles de porter atteinte à l'ordre public* ».

A cela s'ajoute l'objectif plus général de faciliter la réalisation d'enquêtes administratives par les services de police. Le fichier EDVIGE tentait d'étendre considérablement le fichage en multipliant les catégories de personnes fichées et la gamme des données référencées. Il fait face à une intense polémique sociale et à une pétition populaire avant d'être supprimé par le décret 2008-1199 du 19 novembre 2009[290]. Les traitements PASP et GIPASP, créés respectivement par le décret 2009-1249 du 16 octobre 2009 et le décret 2011-340 du 29 mars 2011, et dont les régimes sont codifiés respectivement aux articles R. 236-11 à R. 236-20, et R.236-21 à R. 236-30 du CSI, remplacent le fichier EDVIGE.

Les finalités des traitements PASP et GIPASP sont de « *recueillir, conserver et analyser les informations qui concernent des personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique* » et « *les informations qui concernent les personnes susceptibles d'être impliquées dans des actions de violence collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives* » (Art. R. 236-11 et R. 236-21 CSI). Ces finalités, jugées plus restrictives que celles d'EDVIGE, emportent l'adhésion de la CNIL, qui précise dans sa délibération 2009-355 du 11 juin 2009 que la « *sécurité publique* » renvoie à « *l'élément de l'ordre public caractérisé par l'absence de périls pour la vie, la liberté ou le droit de propriété des individus* ».

S'agissant des types de données collectées, le principe est l'interdiction d'enregistrer des données sensibles (relevant de l'article 6 de la loi Informatique et

[290] *Fichiers de police, op. cit.*., point 162.

Libertés), sauf, par dérogation, pour les données relatives à des « *signes physiques particuliers et objectifs* » et à des « *activités politiques, philosophiques, religieuses ou syndicales* ». Certains auteurs relevaient déjà que ces informations permettaient dans les faits de déduire des opinions dépassant les faits objectifs[291], mais le décret 2020-1511 du 2 décembre 2020 va plus loin en **remplaçant le terme « *activités* » par « *opinions* »**, faisant **ainsi disparaître tout semblant d'objectivité dans la collecte de ces données**. Pourtant, le Conseil d'État a jugé que ce changement n'avait « *ni pour objet, ni pour effet de permettre d'enregistrer d'autres catégories de données que celles* » auparavant prévues. **Nous sommes plus inquiet·e·s que lui**. L'enregistrement de données relatives à la santé ou l'orientation sexuelle est également interdit en principe, mais depuis le décret précité du 2 décembre 2020, le traitement de « *données de santé révélant une dangerosité particulière* » est possible (Art. R. 236-13 et R. 236-23 CSI). Par ailleurs, la CNIL a demandé des définitions plus précises de catégories de données comme « *l'origine géographique* », les « *activités publiques* » ou les « *comportements* », notions que l'on retrouve notamment dans le fichier EASP, non définies.

Les données sont conservées pendant 10 ans après l'intervention du dernier événement de nature à faire apparaître un risque d'atteinte à la sécurité publique ayant donné lieu à un enregistrement. Concrètement, il suffit dans ces conditions que les agents de police ou de gendarmerie ajoutent des éléments avant le terme pour repousser l'effacement de toutes les données concernant une personne. Le Conseil d'État a d'ailleurs censuré une disposition similaire en précisant que la conservation des données ne saurait être prolongée à l'initiative de l'enquêteur[292].

Le droit d'accès aux données est réservé, pour le fichier PASP, « *dans la limite du besoin d'en connaître, y compris pour des enquêtes administratives* », aux agents individuellement désignés et spécialement habilités du service central du renseignement territorial de la direction centrale de la sécurité publique, des directions départementales de la sécurité publique ou des directions territoriales de la police nationale, les agents de la préfecture de police dans les services du renseignement, et le référent national. Bénéficient d'un accès indirect « *dans la limite du besoin d'en connaître, en vue de la réalisation d'enquêtes administratives* », les agents individuellement désignés et spécialement habilités

[291] V. Gautron, « Usages et mésusages des fichiers de police : la sécurité contre la sûreté ? », *AJ Pénal*, 2010, p. 266 [cité par V. Gautron, « Fichiers de police », *Répertoire de droit pénal et de procédure pénale*, avril 2015, point 193].
[292] CE, 10 mars 2011, n°2011-625 DC, cons. 72.

du Service national des enquêtes administratives, du Commandement spécialisé pour la sécurité nucléaire. « *Dans la limite du besoin d'en connaître* » seulement cette fois, peuvent également être destinataires des données les personnes ayant autorité tous les services susmentionnés, les procureurs de la République, les agents d'un service de la police nationale ou de la gendarmerie nationale chargés d'une mission de renseignement, ainsi que ces mêmes agents, non chargés d'une mission de renseignement, sur demande expresse cette fois. Concernant le fichier GIPASP, ont un accès direct « *dans la limite du besoin d'en connaître, y compris pour les enquêtes administratives* », les personnels de la gendarmerie nationale individuellement désignés et spécialement habilités et le référent national. « *Dans la limite du besoin d'en connaître, en vue de la réalisation d'enquêtes administratives* », peuvent être destinataires des données les agents du Service national des enquêtes administratives, les agents du Commandement spécialisé pour la sécurité nucléaire. Dans la limite du besoin d'en connaître encore, peuvent être destinataires les personnes ayant autorité sur les services susmentionnés, les procureurs de la République, les agents chargés d'une mission de renseignement ou ces mêmes agents sur demande expresse, s'ils·elles ne sont pas chargé·e·s d'une mission de renseignement.

Un « *référent national* », membre du Conseil d'État, mentionné aux articles R. 236-15 et R. 236-26 (I, 2°) pour le GIPASP, est chargé d'adresser des recommandations aux responsables des fichiers PASP et GIPASP et de produire un rapport annuel. Il dispose pour cela d'un accès direct aux données contenues dans les fichiers concernés. En violation de l'article R. 236-15, ce référent national n'a publié qu'un seul rapport relatif aux fichiers PASP et GIPASP, en 2017.

Encore une fois, les enregistrements des consultations de ces fichiers sont conservés moins longtemps que les données elles-mêmes, c'est-à-dire seulement 3 ans pour les fichiers PASP et GIPASP, alors que les données sont conservées 10 ans. Avant le décret 2020-1511 du 2 décembre 2020, ces enregistrements étaient conservés 5 ans.

Comme pour le fichier EASP, le décret n°2017-1216 du 2 août 2017 **a abrogé juste avant la création d'ACCReD les articles interdisant que les fichiers PASP et GIPASP fassent l'objet d'aucune interconnexion**, aucun rapprochement ni aucune mise en relation avec d'autres traitements ou fichiers. Le décret de décembre 2020, quant à lui, a supprimé la mention « le traitement ne comporte pas de dispositif de reconnaissance faciale à partir de la photographie » aux articles R. 236-11 et R. 236-21 du CSI.

VIII. Les fichiers de renseignements

A) GESTEREX - (GEStion du TERrorisme et des EXTrémismes à potentialité violente)

Il s'agit d'un fichier mis en œuvre par la sous-direction chargée de la lutte contre le terrorisme et les extrémismes à potentialité violente de la direction du renseignement de la préfecture de police de Paris, afin d'exercer ses missions couvertes par le secret. Ainsi le contenu de la délibération n°2017-157 du 18 mai 2017 de la CNIL est tenu secret, avec pour seule information qu'il s'agit d'un "avis favorable avec réserves".

Créé en 2008 (arrêté du 27 juin 2008 du ministre de l'Intérieur), GESTEREX serait resté illégal a priori jusqu'en 2017. En 2017, après avis de la CNIL un décret, tenu secret aussi (n°2017-1218 du 2 août 2017) aurait « recréé » GESTEREXT[293].

« *Aucune durée de conservation fixe n'est prévue : les données ne sont conservées qu'en fonction des finalités (très strictement délimitées) du fichier et donc, pour l'essentiel, de l'intérêt qu'elles présentent au regard de la sûreté de l'État et de la sécurité nationale* »[294]. Bien que le Conseil d'État ait validé cette possibilité (V. supra, n. 56), l'absence totale d'information sur les fichiers de renseignement seraient « *vraisemblablement sanctionnées par la Cour européenne des droits de l'homme au regard de sa jurisprudence en la matière, celle-ci admettant des limites à la transparence, mais non un secret absolu* »[295].

B) CRISTINA, Fichiers de la DGSE et SIREX (Système d'information du renseignement de contre-ingérence)

Concernant les fichiers de renseignement, le Conseil d'État a confié une marge d'appréciation absolue au pouvoir réglementaire concernant le fichier CRISTINA dès lors « *qu'aucun texte ni aucun principe ne fait obligation à un décret dispensant de publication [...] d'indiquer, même sommairement, les motifs de fait et de droit qui déterminent la décision*

[293] "*La folle envie de tout contrôler*", *op. cit.*, p. 78.
[294] Alain Bauer et Christophe Soullez, *Les fichiers de police et de gendarmerie*, *op.cit.*, p. 36.
[295] *Fichiers de police, op.cit*., p. 71.

de dispense de publication prise par l'autorité administrative ». Il ne doit pas non plus publier la teneur des réserves émises par la CNIL[296].

Ainsi, comme la plupart des fichiers de renseignement, les fichiers de la DGSE ont été créés par un décret non publié. D'après l'article 3 du décret n°2007-914 du 15 mai 2007, les fichiers de la DGSE ne sont pas soumis aux pouvoirs de contrôle de la CNIL. Concernant le SIREX, fichier de la direction du renseignement et de la sécurité de la défense, il est créé en 2014 par un décret non publié. On ne connaît son existence que grâce au décret n°2014- 957 du 20 août 2014 qui ajoute ce fichier à la liste des fichiers qui échappent au contrôle de la CNIL.

Nous ne disposons donc d'aucune information concernant les données collectées par la DGSE ou la DRSD, le nombre de personnes dont les informations sont collectées, les utilisations faites etc. Il est donc d'autant plus étonnant que les données de ces fichiers soient accessibles dans un traitement de données pour lequel autant d'autorités ont accès que l'ACCReD. **Ainsi, les autorités réalisant des enquêtes administratives ont accès à des informations dont les personnes concernées elles-mêmes ne sauraient disposer. Faute d'interdiction expresse, les interconnexions des données au sein de ces fichiers avec d'autres fichiers seraient – et seront – très probablement nombreuses et fréquentes**.

CHAPITRE 3 :
ACCRED ET LA MISE EN PERIL
DES LIBERTES INDIVIDUELLES ET CITOYENNES

Après avoir étudié les fichiers auxquels l'ACCReD donne accès, nous nous concentrons désormais sur le fonctionnement pratique d'ACCReD et comment ce traitement de données répond à notre définition de croisements (I). C'est finalement après avoir défini tout ce que contient l'ACCReD et son fonctionnement que nous pourrons réaliser à quel point ce type de base de données permettant des croisements presque infinis entre les fichiers viole nos libertés au nom de la sécurité (II).

[296] Conseil d'Etat, 16 avril 2010, n°320196

I. Le fonctionnement d'ACCReD : un idéal type de la construction de nouvelles « méga » bases de données ?

A) L'automatisation

Comme nous l'avons précisé, ACCReD est **un « logiciel de rapprochement », c'est-à-dire « *un logiciel qui permet, à travers une base de données aux entrées multiples, de créer des relations entre toutes les informations contenues dans différents fichiers : faciliter l'interconnexion de fichiers jusqu'alors séparés* »**[297]. C'est une sorte d'application utilisée par plusieurs services aux fins de collecter les informations nécessaires à la prise d'une décision dans le cadre d'une enquête administrative. En ce sens, c'est une forme matérialisée et légalisée des interconnexions en matière de fichiers de renseignement. Si les logiciels de rapprochement judiciaire comme SALVAC, CORAIL ou ANACRIM sont déjà connus et trouvent leur fondement légal dans la loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, dite « LOPPSI II »[298], cette pratique est plus innovante en matière administrative.

La stratégie de l'automatisation de l'interconnexion répond à différents besoins, et en premier lieu, s'agissant d'ACCReD, celui de **faciliter la réalisation d'enquêtes administratives**. La CNIL a donné un avis positif au projet de décret pour ACCReD, reconnaissant « *la nécessité d'accélérer et de faciliter les consultations réalisées dans le cadre de certaines enquêtes* »[299]. Si l'on s'arrête là, ACCReD est un simple outil pratique qui ne fait évoluer que le mode opératoire sans ouvrir de nouvelles possibilités.

Le gouvernement, dans sa demande d'avis n°17006644, adressée à la CNIL, estimait la création d'ACCReD nécessaire en raison d'un « *risque exceptionnel de menace terroriste* », ainsi que pour répondre à « *l'adoption de nouveaux dispositifs législatifs imposant la réalisation d'enquêtes administratives conditionnant l'accès à certains emplois ou sites sensibles* » et pour tenir compte « *de l'évolution des modalités de réalisation des*

[297] *Le fichage des mineurs : entre ordre public et libertés individuelles*, *op.cit*, p. 245.
[298] Sur le sujet, v. J. Buisson, « Preuve », *Répertoire de droit pénal et de procédure pénale*, octobre 2020, point 82 et suivants.
[299] CNIL, Délibération n°2017-152 du 18 mai 2017 portant avis sur un projet de décret portant création d'un traitement automatisé de données à caractère personnel dénommé « ACCRED ».

contrôles réalisés à l'occasion de ces enquêtes »[300]. Ces nouveaux cadres d'enquête administrative sont destinés à « *répondre à l'état de la menace terroriste* » : ces nouvelles enquêtes administratives concernent le secteur du transport public de personnes et de marchandises dangereuses (loi du 22 mars 2016) et le domaine des grands événements (loi du 3 juin 2016)[301].

En réalité, l'automatisation des recherches dans le cadre d'enquêtes administratives est le symptôme d'une politique de surveillance généralisée qui s'inscrit dans le cadre de la « *lutte contre le terrorisme* », une formule généralisante qui a déjà maintes fois été critiquée. Il s'agit de prévoir la « *radicalisation* », qui elle-même est entendue au sens large. Les enquêtes administratives répondent en effet à une logique de prévention : le but est d'« *anticiper sur un comportement futur* »[302], sauf que la lutte antiterroriste est devenue au fil des législations pénales le prétexte à la mise en place de dispositifs visant d'autres fins sécuritaires.

L'automatisation des interconnexions pourrait, en soi, permettre l'automatisation de l'accès aux droits et notamment à celui de l'effacement. En matière de durée de conservation des données, ACCReD respecte la jurisprudence de la CEDH et de la CJUE et prévoit des durées de conservation différentes en fonction des catégories de données[303] : les données qui peuvent être directement enregistrées dans la racine d'ACCReD, c'est-à-dire les données relatives à la demande d'avis ou de décision, les données relatives à la personne faisant l'objet de l'enquête, et les données relatives aux résultats de l'enquête, sont conservées 5 ans, tandis que les données issues des autres fichiers peuvent être conservées « *jusqu'à expiration du délai de recours contentieux dirigé contre l'avis ou la décision ou, en cas de recours, jusqu'à ce qu'il ait été définitivement statué sur le litige* ». Les données relatives aux consultations

[300] W. Azoulay, « Du panoptique au technoptique : renforcement de l'arsenal de collecte de données », *Dalloz Actualités*, 19 septembre 2017.

[301] Assemblée Nationale, Audition de Mme Carine Vialatte, cheffe du service national des enquêtes administratives de sécurité (SNEAS), Compte-rendu de la Commission d'enquête chargée de faire la lumière sur les dysfonctionnements ayant conduit aux attaques commises à la préfecture de police de Paris le jeudi 3 octobre 2019, présidence de M. Eric Ciotti, mercredi 15 janvier 2020. Disponible en ligne : https://www.assemblee-nationale.fr/dyn/15/comptes-rendus/ceprefpol/l15ceprefpol1920020_compte-rendu?fbclid=IwAR3abjJYdHWmMh0BtFpKnlgw4Bb--W-0g7lXDSmvekjO4duxeZYzfhzmcMk.

[302] B. Schmaltz, « Les consultations de fichiers de police pour enquête administrative », in *Les fichiers de police*, dir. E. Debaets, A. Duranthon, M. Sztulman, ed. Institut Universitaire Varenne, coll. Colloques & Essais, 2019, p. 200 [Cité par M. Cottereau, « Le 'super fichier' des enquêtes administratives passe le contrôle de proportionnalité du Conseil d'Etat », *AJDA*, n°32, septembre 2019, p. 1879.].

[303] M. Cottereau, « Le 'super fichier' des enquêtes administratives passe le contrôle de proportionnalité du Conseil d'Etat », *AJDA*, n°32, septembre 2019, p. 1879.

sont enregistrées et conservées pendant une durée de six ans (article 6 du décret). **Mais rien n'indique que l'automatisation permet une meilleure gestion de l'expiration des délais, en prévoyant par exemple une suppression automatique des informations pour laquelle la durée maximale de conservation est expirée.**

B) Les modes de consultation des données

Il n'est *a priori* pas obligatoire, au sens juridique, de passer par le logiciel ACCReD pour réaliser une enquête administrative. Toutefois, **vraisemblablement, tous les services y ayant accès l'utilisent pour leur travail d'enquête administrative**. Les personnes avec un accès sont les agents du Service national des enquêtes administratives de sécurité (SNAES), les agents du Commandement spécialisé pour la sécurité nucléaire (CoSSeN) ; s'y ajoutent les destinataires d'informations « *dans la limite du besoin d'en connaître* », c'est-à-dire les agents chargés d'effectuer des enquêtes administratives au ministère de l'Intérieur (seulement pour les données relatives au sens de l'avis ou de la décision) ou dans les services spécialisés de renseignement du ministère de la Défense (seulement pour le document de synthèse des éléments pertinents de l'enquête), les personnes morales ou l'autorité administrative à l'origine de la demande (seulement pour le sens de l'avis ou de la décision), le préfet de département du lieu d'exercice de l'emploi, de la mission ou de la fonction (Article 5 du décret). L'audition de la directrice du SNAES, Carine Vialatte, laisse penser que les agents de ce service passent systématiquement par ACCReD[304].

L'utilisation d'ACCReD permet un accès semi direct aux autres fichiers interconnectés via ce logiciel. Concrètement, l'utilisation de l'application donne directement accès à l'information suivante : **la personne concernée par l'enquête administrative est-elle inscrite dans l'un des 9 fichiers interconnectés, et si oui, lesquels ?** Cette consultation « *est effectuée aux seules fins de vérifier si l'identité de la personne concernée par l'enquête administrative y est ou non enregistrée* »[305]. L'information ainsi recueillie ne suffit pas, en principe, à tirer des conclusions dans le cadre de l'enquête, puisque celle-ci « *ne peut aboutir à un avis défavorable sans procéder à un complément d'information, par consultation dudit*

[304] Assemblée Nationale, Audition de Mme Carine Vialatte, *op.cit.*
[305] CE, 9e et 10e chambres réunies, 11 juillet 2018, n°414827.

traitement ou par la saisine préalable du responsable dudit traitement »[306], précision qui n'est toutefois pas inscrite dans le décret publié. **L'enquête administrative se poursuit donc par la saisine des services émetteurs, enquêteurs ou des autorités ou institutions administratives ou judiciaires aux fins d'investigations plus poussées. A ce stade, la consultation est indirecte : le service enquêteur ayant accès à ACCReD sollicite le service de renseignement gestionnaire du fichier où la personne concernée par l'enquête est enregistrée, ce service consulte par la suite le fichier et transmet les informations qu'il estime pertinentes au regard des objectifs de l'enquête annoncés par le service demandeur**[307]. Par ce biais, la SNAES peut être destinataire des informations des fichiers CRISTINA, GESTEREXT, et SIREX depuis peu, ce qui présente parfois un intérêt notable du point de vue du périmètre d'investigation pour les enquêtes administratives, puisque ce sont des fichiers auxquels les services de police et les unités de gendarmerie n'ont pas accès[308.]

Ce sont les services recevant la demande qui jugent de la nécessité de transmettre les informations enregistrées dans les fichiers qu'ils gèrent. Il n'existe pas de directive claire quant aux informations devant être transmises, le cadre étant par définition souple, afin de pouvoir s'adapter aux différents motifs des enquêtes administratives. Concrètement, cela signifie que le service recevant la demande peut décider de transmettre toutes les informations qu'il a à sa disposition, d'autant plus que les institutions en jeu se trouvent *a priori* dans un rapport de confiance mutuelle. Ces informations seraient alors enregistrées dans ACCReD et directement comparées aux informations disponibles provenant d'autres fichiers.

Au fond, le risque est celui du modèle proposé par ACCReD : une centralisation d'informations par l'interconnexion de multiples fichiers, prêtes à être comparées et analysées pour en tirer des profils, prédire des comportements. Or, de plus en plus d'enquêtes administratives passent par la consultation du fichier ACCReD, et de plus en plus de situations, emplois, fonctions, sont soumis à la réalisation d'une enquête administrative, au nom de la lutte contre le terrorisme (emplois dans les transports publics, lors d'événements sportifs, y compris des emplois éloignés de la sécurité privée). Or, prévoir une enquête administrative préalable, c'est ouvrir l'accès à ACCReD dans un nombre croissant de

[306] *Op. cit.*, CNIL, Délibération n°2017-152 du 18 mai 2017.
[307] Assemblée Nationale, Audition de Mme Carine Vialatte, *op.cit.*
308
308 Rapport parlementaire Paris-Morel-à-L'Huissier, *op.cit*.

situations, donc augmenter le nombre de personnes enregistrées dans ce fichier et dont les informations peuvent être interconnectées.

C) Illégalismes

Il est extrêmement difficile d'identifier des illégalismes[309] dans les usages des fichiers. En réalité, le plus inquiétant est la souplesse permise par le cadre réglementaire : **il semble qu'il est très aisé de modifier le régime juridique d'un fichier, notamment pour pouvoir le croiser avec d'autres**. Ainsi, alors que les fichiers PASP et GIPASP étaient soumis à l'interdiction d'être interconnectés, le décret 2017-1216 du 2 août 2017 a abrogé les articles prévoyant cette interdiction. La voie était alors libre pour la mise en place d'ACCReD, de sorte qu'il puisse organiser le croisement des fichiers PASP et GIPASP avec d'autres fichiers sensibles. **Les garanties peuvent manifestement disparaître d'un jour à l'autre et les garde-fous sont fragiles**. Le cadre juridique des fichiers peut être modifié très vite et l'organisation des usages peut changer radicalement du jour au lendemain. En réalité, il est souvent possible pour le pouvoir réglementaire d'arriver à ses fins sans tomber dans l'illégalité car le cadre juridique est complexe, donc difficile d'accès ; souple, donc facile à modifier ; et flou, donc ouvert à des interprétations évolutives.

II. La violation de nos libertés au nom de la sécurité

Le traitement automatisé ACCReD n'est qu'un symptôme **d'une politique ancrée dans la lutte contre un ennemi par une surveillance accrue des individus, au nom de la liberté**. Cette philosophie de l'ennemi, qui s'applique aujourd'hui autour de la figure du radicalisé et du djihadiste, n'est nouvelle ni dans l'histoire française ni dans la philosophie politique.

[309] Utilisée par Michel Foucault, la notion d'illégalisme recouvre l'ensemble des pratiques qui soit transgressent délibérément, soit contournent ou même détournent la loi.

A) L'ennemi

Dans la philosophie hobbesienne, une différence essentielle est faite entre le délinquant et l'ennemi. Le premier commet une transgression de la loi civile et doit être sujet à une réponse de droit, malgré son statut de délinquant ou criminel, il est toujours détenteur de son statut de citoyen avec des droits. Et le deuxième, considéré comme une menace pour le pouvoir du souverain, le souverain se doit de répondre à cette injure mais non pas via le droit, l'ennemi ne peut en bénéficier car il n'est plus considéré comme un citoyen.

Cet ennemi n'est pas identifié en réaction à un acte commis, mais étant susceptible de, ayant l'intention de. De telle sorte que rien, mis à part la parole du souverain peut légitimer – ou non - qui est l'ennemi, et cette parole ne peut être questionnée, étant représentative de la multitude. De la même manière que de nos jours, pour être inscrit dans un fichier de personnes recherchées avec des mesures de surveillance particulières, seul un soupçon est nécessaire. Ou encore, il suffit d'un avis défavorable lors d'une enquête administrative pour se voir refuser un titre de séjour, un asile politique ou un travail.

Hobbes précise dans *Léviathan* l'importance des ennemis extérieurs, communs à tou·te·s les citoyen·ne·s : la peur interne est transférée à l'extérieur, une étape nécessaire pour que les citoyen·ne·s acceptent que le souverain les protège de l'étranger, l'ennemi, l'autre.

Cela nous amène à la pensée de Carl Schmitt, qui affirme que le choix de l'ennemi par l'État souverain est le fondement du politique. Dans les ouvrages *La notion du politique* et la *Théorie du partisan*, il propose le critère d'ami-ennemi comme expression de la nécessité de différenciation, une forme d'affirmation face à l'autre. L'ennemi est pour lui un individu ou un groupe affrontant un ensemble de même nature, de l'ordre public et non pas privé, – *hostis* et non pas *inimicus* – qui, pour diverses raisons, s'opposent à l'État, engagé dans une lutte pour le moins virtuelle, c'est-à-dire effectivement possible. C'est grâce à l'identification du *nous* face *aux autres* qu'il y a union à l'intérieur de l'État. Néanmoins, l'ennemi peut être à l'intérieur du corps social, comme c'est le cas avec les *terroristes, les radicalisés*, sans pour autant aboutir à une guerre civile, car il est ennemi et non pas adversaire, ce n'est pas un conflit entre partis.

L'État a le devoir d'éliminer ces ennemis, le cas contraire reviendrait à mettre des limites à son propre pouvoir, s'automutiler. Ce ne sont plus les actes de l'ennemi qui sont sanctionnés, mais sa dangerosité, sa potentielle menace. Paradoxalement le droit se suspend pour assurer sa propre existence, pour garantir sa conduite. Ce comportement est défini par Derrida comme l'Auto-immunité : *Vivant peut spontanément détruire de façon autonome même ce qui en lui se destine à le protéger ou à l'immuniser conte l'intrusion agressive de l'autre.* Ce serait par exemple nier la démocratie au nom de celle-ci, ruiner les libertés dont elle se prétend garante suspendre le droit pour assurer sa propre existence, justifier une surveillance massive et incontrôlable au nom de la liberté.

Comme nous l'avons vu avec l'exemple des « carnets B » et des « listes S », l'usage des fichiers pour l'identification des ennemis et la justification de leur surveillance et de mesures contraignantes n'est pas une pratique moderne. **Ces techniques ne sont effectivement pas des conséquences de l'essor technologique**. Il existe évidemment une corrélation entre la massification de la surveillance, son étendue et les outils technologiques dont l'automatisation des traitements de données, mais il ne s'agit pas de la cause principale.

Il en va de même avec le traitement de données ACCReD, qui peut être considéré comme un symptôme d'une politique tout comme d'un outil qui simplifie et normalise l'identification de suspects, de potentiels dangers et leur surveillance.

B) Enquêtes administratives

Les enquêtes administratives ont depuis quelques années été un moyen et un outil de plus en plus utilisé pour **identifier de potentielles menaces pour la sécurité intérieure**. Effectivement, depuis 2016, les domaines et situations faisant appel aux enquêtes administratives se sont étendus.

Tout d'abord, au lendemain des attentats du 13 novembre 2015, une nouvelle loi loi dite « Savary » promulguée le **22 mars 2016** a étendu le champ des enquêtes administratives aux décisions de recrutement et d'affectation concernant les emplois en lien direct avec la sécurité des personnes et des biens au sein d'une entreprise de transport public de personnes

ou d'une entreprise de transport de marchandises dangereuses, via l'article L.114-2 du code de la sécurité intérieure.

Le **3 juin 2016**, ces contrôles ont été étendus aux établissements ou installations accueillant des évènements de grande ampleur, avec pour finalité de renforcer la lutte contre le crime organisé, le terrorisme et leur financement et améliorant l'efficacité et les garanties de la procédure pénale (article L. 211-11-1 du code de la sécurité intérieure)[310].

Le **27 avril 2017** est créé le Service National des enquêtes administratives de sécurité (SNEAS), chargé des enquêtes administratives prévues par les articles L.114-1, L.114-2 et L.211-11-1 du code de la sécurité intérieure.

Le **2 août 2017**, le décret n° 2017-1216 modifiant les traitements automatisés de données à caractère personnel prévus aux articles R. 236-1, R. 236-11 et R. 236-21 du code de la sécurité intérieure abroge l'ancien article R236-8 qui expliquait que le traitement des enquêtes administratives liées à la sécurité publique ne pouvait faire « *l'objet d'aucune interconnexion, aucun rapprochement ni aucune forme de mise en relation avec d'autres traitements ou fichiers* »[311].

Le **3 août 2017** est créé le traitement automatisé de données à caractère personnel ACCReD, qui sera désormais l'outil de référence pour les enquêtes administratives. En plus d'être un traitement qui interconnecte 9 fichiers, l'ACCReD passe outre la restriction de l'article 8 de la loi de 1978 qui interdit « *de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci* ». En effet, il est désormais possible de collecter des données dites sensibles mais « *à la condition que leur collecte soit indispensable à la réalisation des enquêtes administratives et dans les seuls cas où ces données se rapportent à des opinions politiques, philosophiques ou religieuses* »[312].

[310] Rapport parlementaire Diard-Poulliat, nº2082, 27 juin 2019, p.28.
[311] Marc Rees, "Dans la torpeur de l'été, la grande foire aux fichiers de sécurité", *Next Inpact*, Aout 2017
[312] Décret n° 2017-1224 du 3 août 2017 portant création d'un traitement automatisé de données à caractère personnel dénommé « Automatisation de la consultation centralisée de renseignements et de données » (ACCReD).

Le **30 octobre 2017** est publié la loi nº2017-1510 renforçant la sécurité intérieure et la lutte contre le terrorisme, permettant aux enquêtes administratives de consulter des « *traitements automatisés de données à caractère personnel relevant de l'article 26 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, à l'exception des fichiers d'identification. Les conditions dans lesquelles les personnes intéressées sont informées de cette consultation sont précisées par décret* ». Ce même décret permet de pratiquer des enquêtes administratives non plus seulement pour l'obtention d'un contrat, mais durant l'exécution du contrat, à la simple demande de l'employeur.

Le **10 septembre 2018**, la loi n° 2018-778 pour une immigration maîtrisée, un droit d'asile effectif et une intégration réussie, permet la réalisation d'enquêtes administratives « *pour la délivrance, le renouvellement ou le retrait d'un titre ou d'une autorisation de séjour sur le fondement des articles L. 121-4, L. 122-1, L. 311-12, L. 313-3, L. 314-3 et L. 316-1-1 du code de l'entrée et du séjour des étrangers et du droit d'asile ou des stipulations équivalentes des conventions internationales ainsi que pour l'application des articles L. 411-6, L. 711-6, L. 712-2 et L. 712-3 du même code* ».

Il ne s'agit là que de quelques exemples qui permettent de signifier l'importance des enquêtes administratives de nos jours. ACCReD n'est qu'un outil au service d'une logique politique beaucoup plus ample, avec néanmoins des conséquences indéniables : 1) parce qu'il permet une interconnexion de différents fichiers interdite jusqu'à la publication d'un décret la veille de celui créant l'ACCReD – ce qui, d'ailleurs, pose la question du contrôle des fichiers lorsqu'ils ne sont qu'un maillon d'une longue chaîne de décrets qui ne sont à aucun moment contrôlés – ; ou 2) parce qu'il permet l'accès et la conservation de données sensibles ; ou encore 3) parce qu'il permet, à lui seul, une généralisation dramatique des enquêtes administratives.

Pour comprendre cela, il suffit d'ailleurs de jeter un œil sur l'évolution du nombre d'enquêtes réalisées par le SNEAS, en 2017 et 2018 grâce à ACCReD :

- 2017[313] : 91 798 enquêtes en 5 mois
- 2018[314] : 318 464 enquêtes
- 2019[315]: 409 018 enquêtes

[313] Rapport parlementaire Diard-Poulliat, *op.cit.*
[314] *Ibid.*

C) Les conséquences des discriminations fondées sur la prédiction d'un comportement

L'accès ainsi que la conservation de données sensibles telles que des opinions politiques, religieuses et philosophiques, constituent une violation des libertés individuelles. **Ces données deviennent en outre également le fondement d'avis favorables ou défavorables à l'issue d'enquêtes administratives**, ce qui peut avoir des conséquences défavorables sur la vie d'une personne.

Ce point est fondamental car ces informations sensibles ne sont pas rattachées à des actions, à des faits réels, objectifs et libérés d'une quelconque interprétation. Au contraire, il s'agit de données éminemment subjectives, pouvant être interprétées différemment de leur signification initiale, influencées par l'objectif de rechercher des personnes potentiellement radicalisées ou terroristes. Nous avons déjà fait référence aux signes de radicalisation dénombrés par le gouvernement, exemple parfait pour comprendre l'impact de l'interprétation sur des faits au nom d'une finalité politique. L'exemple du port de la barbe, ou même d'une pratique exacerbée de la religion lors d'une période de ramadan ne peuvent et ne devraient en aucun cas être considérés comme objectivement, des signes de radicalisation, même s'ils sont accompagnés d'autres éléments.

Les données sensibles recueillies par ACCReD lors des enquêtes administratives sont interprétables et constituent **un indice de prévention, de prédiction du comportement de l'individu**. Ainsi, on empêche les individus d'avoir accès à un emploi ou à un titre de séjour parce qu'ils pourraient, dans le futur, être un potentiel danger pour la sécurité de l'État. Or, cet avis est fondé sur des données personnelles relatives et parfaitement interprétables sans aucun contrôle de véracité.

Une fois qu'un avis défavorable est rendu, il semble impossible d'espérer un autre avis. En effet, les données de conservation s'élèvent à 5 ans pour l'ACCReD.

D'autant plus si une enquête s'appuie sur un résumé/procès-verbal d'une précédente enquête avec avis défavorable, archivée et consultable via le fichier EASP, comment sortir de ce déterminisme ? **Ou plus simplement, comment le contester, demander un deuxième avis, vérifier les informations, contrôler les analyses qui sont réalisées par les**

[315] Assemblée Nationale, Audition de Mme Carine Vialatte, *op.cit.*

enquêteurs, vérifier leur objectivité et leur impartialité ? Impossible. Ni pour l'individu concerné qui d'ailleurs n'est même pas au courant, ni par une autorité extérieure et indépendante.

D) L'absence totale de contrôle de la CNIL

Le champ d'application de la CNIL est très limité, surtout parce qu'il se concentre uniquement sur le contenu d'un texte législatif et non pas sur l'enchaînement de décrets et d'ordonnances qui, dans leur ensemble, amènent à des violations de droits individuels, **une surveillance massive et l'exclusion de certains individus sur le fondement de leurs opinions personnelles et d'une analyse prédictive et subjective de leur comportement**.

Comme nous l'avons vu, ACCReD n'existe que grâce à un agencement de modifications juridiques amenant à un bouleversement du cadre légal qui, dorénavant, permet un usage abusif de la surveillance et des données personnelles.

ACCReD est pour autant un traitement de données légales, établi par un cadre réglementaire, mais qui n'en demeure pas moins abusif. Le droit est la meilleure des armes pour légitimer ses pratiques abusives, et la CNIL, plutôt que de protéger la société de ces pratiques, protège ces pratiques en participant à leur légitimation.

BIBLIOGRAPHIE

Ouvrages

Alain Bauer, Christophe Soullez, *Les fichiers de police et de gendarmerie*, éd. Presses Universitaires de France, coll. « Que sais-je ? », 2011.

Jean-Louis Bergel, *Méthodologie juridique*, ed. PUF, coll « Thémis », 2018.

Claire Bruggiamosca et Christophe Daadouch, *Le fichage des mineurs : entre ordre public et libertés individuelles*, 20 juin 2019, Berger-Levrault.

Jean Buisson, *Force publique*, Rép. Pénal, oct. 2019.

Emilie Debaets, Arnaud Duranthon, Marc Sztulman, *Les fichiers de police*, ed. Institut Universitaire Varenne, coll. Colloques & Essais, 2019.

Virginie Gautron, *Fichiers de police*, Dalloz, Rép. Pénal, avr. 2015.

Jean Mafart, *Carnet B*, Hugues Moutouh éd., *Dictionnaire du renseignement*, Perrin, 2018, pp. 134-136. Disponible en ligne : https://www-cairn-info.faraway.parisnanterre.fr/dictionnaire-du-renseignement--9782262070564-page-134.htm.

Phillipe Pédrot, *Traçabilité et responsabilité*, ed. Economica, 2003.

Gildas Roussel, *Police judiciaire*, Rép. Pénal, oct. 2020.

Articles de doctrine

Warren Azoulay, « Du panoptique au technoptique : renforcement de l'arsenal de collecte de données », 19 septembre 2017, *Dalloz Actualité*.

Gérald Bégranger, « Le contrôle des fichiers de police par les juges », *AJ Pénal*, 2014, p. 176.

Céline Bloud-Rey, « Quelle place pour l'action de la CNIL et du juge judiciaire dans le système de protection des données personnelles ? », Analyse et perspectives, *Recueil Dalloz*, 2013.

Lisa Carayon, « Quelle folie ! A propos de l'interconnexion entre le fichier des personnes hospitalisées sans consentement en psychiatrie (HOPSYWEB) et celui des personnes soupçonnées de radicalisation terroriste (FSPRT) », *La Revue des droits de l'homme*, Actualités Droits-Libertés. Disponible en ligne : http://journals.openedition.org/revdh/9746.

Marc Cottereau, « Le 'super fichier' des enquêtes administratives passe le contrôle de proportionnalité du Conseil d'Etat », *AJDA*, n°32, septembre 2019, p. 1879.

Jean-Pierre Deschodt, « La preuve par le carnet B », *Les Cahiers du Centre de Recherches Historiques*, 45 | 2010, 181-193.

Jean Frayssinet, « Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques », *J.-Cl. Pénal*, fasc. 20, mars 2010.

Virginie Gautron, « La prolifération incontrôlée des fichiers de police », *AJ Pénal*, 2007.

Virginie Gautron, « Surveiller, sanctionner et prédire les risques : les secrets impénétrables du fichage policier », *Champ pénal*, 2019, vol. n°17.

Virginie Gautron, « Usages et mésusages des fichiers de police : la sécurité contre la sûreté ? », *AJ Pénal*, 2010.

Éric Heilmann, « Le désordre assisté par ordinateur. L'informatisation des fichiers de police en France (1968-1988) », *Les Cahiers de la sécurité*, 2005, n°56.

Pierre Januel, « Fichiers de police partout », 19 octobre 2018, *Dalloz Actualité*.

G. Koubi, « Les données à caractère personnel, outil des services de renseignements », *JCP Adm.*, 2009, p. 2264.

David Larbre, « Les fichiers de police : une catégorie juridique incertaine ? », *Technologie de l'information, culture et société,* 2011, vol. 108-109, p. 141-151.

Olivier Le Bot, « Le contentieux du renseignement devant la formation spécialisée du Conseil d'État », *RFDA*, 2017.

Danièle Lochak, « Des fichiers pour gérer, contrôler, surveiller les étrangers », *Plein droit*, n°71, 2006, p. 24-25.

Articles de presse

BugBrother, « En 2008, la CNIL a constaté 83% d'erreurs dans les fichiers policiers », *Le Monde*, 21 janvier 2009.

Antoine Lafébure, « Fiches S, carte d'identité et ancêtre du numéro de Sécu, quand Vichy inventait les moyens de surveiller la population », *Slate*, 3 juin 2018.

Yoann Nabat, « Cnil, Conseil d'Etat, Conseil constitutionnel… : comment est contrôlé le fichage policier en France », *Journal du Dimanche*, 18 décembre 2020.

Marc Rees, « Dans la torpeur de l'été, la grande foire aux fichiers de sécurité », *Next INpact,* août 2017.

Mars Rees, « Psychiatrie et radicalisation : un croisement de fichiers qui ne passe pas », *Next INpact*, 14 mai 2019.

Rapports et documents institutionnels

Assemblée Nationale, Question N° 24092 de Momain Grau, *Logiciel rédaction de procédure de la police*, déc. 2019.

CNIL, *Conclusions du contrôle des fichiers d'antécédents du ministère de l'intérieur*, 13 juin 2013.

CNIL, *Sécurité : Tracer les accès et gérer les incidents*. Disponible en ligne : https://www.cnil.fr/fr/securite-tracer-les-acces-et-gerer-les-incidents.

Communication de la Commission au Parlement européen et au Conseil sur des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité, COM (2016) 205 final

Délibération n° 2013-357 du 14 novembre 2013 portant avis sur un projet d'arrêté portant autorisation à titre expérimental d'un traitement automatisé de données à caractère personnel dénommé « Fichier des objets et des véhicules signalés » (FOVeS) (demande d'avis n° 1301197)

Délibération n° 2017-152 du 18 mai 2017 portant avis sur un projet de décret portant création d'un traitement automatisé de données à caractère personnel dénommé « ACCRED » (demande d'avis n° 17006644), CNIL, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000035467065/

Délibération n° 2018-354 du 13 décembre 2018 portant avis sur un projet de décret modifiant le décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement (demande d'avis n° 18020552)

Rapport de l'école Nationale Supérieure de la Police, *Former au LRPPN, une étape cruciale du dispositif*, 21 novembre 2013. Disponible en ligne : https://www.ensp.interieur.gouv.fr/Actualites/Former-au-LRPPN-une-etape-cruciale-du-dispositif.

Rapport parlementaire Pillet, nº219, 19 déc. 2019.

Rapport parlementaire Batho-Bénisti, n°4113, 21 déc. 2011.

Rapport parlementaire Paris-Morel-à-L'huissier, n°1335, 17 oct. 2018.

Rapport n° 484 (2016-2017) de M. François-Noël BUFFET, fait au nom de la commission d'enquête, déposé le 29 mars 2017, Circuler en sécurité en Europe : renforcer Schengen. Disponible en ligne : https://www.senat.fr/rap/r16-484/r16-484.html.

Secrétariat général de la défense et de la sécurité nationale, Note technique, No DAT-NT-012/ANSSI/SDE/NP, le 2 décembre 2013.

Sénat, Question écrite N° 13314 de M. Jean-Pierre Grand, *Dysfonctionnements des fichiers de police*, oct. 2014.

UNSA Police, *Dématérialisation de la procédure pénale / Logiciel Scribe,* févr. 2019. Disponible en ligne : http://police.unsa.org/dossiers/procedure-penale/article/dematerialisation-de-la-procedure-penale-logiciel-scribe.

Autres

Patrick Canin, Le décret ACCRED ou comment automatiser le traitement de données à caractère personnel, Lettre d'information de la Ligue des droits de l'Homme, 20 septembre 2017, https://www.ldh-france.org/decret-3-aout-2017/**.**

Camille Gosselin, *La police prédictive : enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique*, Institut d'Aménagement et d'Urbanisme, avril 2019.

La Quadrature du Net, *Gendnotes, faciliter le fichage policier et la reconnaissance faciale*, 25 février 2020. Disponible en ligne : https://www.laquadrature.net/2020/02/25/gendnotes-faciliter-le-fichage-policier-et-la-reconnaissance-faciale.