EXPÉDITEUR :

Direction centrale de la Police judiciaire
Ministère de l'intérieur
Place BEAUVAU
75800 PARIS CEDEX 08

Par lettre recommandée avec accusé de réception

LIEU, le DATE

Objet : Rectification/effacement de données du Système national du système d'information Schengen (N-SIS II)

Madame, Monsieur,

Je soussigné(e) M./Mme XXX, né(e) le XXX à XXX, domicilié(e) au XXX, exerce par la présente mon droit de rectification/d'effacement d'informations me concernant contenues dans le Système d'information Schengen (N-SIS II).

En conséquence et en application de l'article 106 de la loi n°78-17 du 6 janvier 1978 et de l'article R231-12 du code de la sécurité intérieure, je vous demande de rectifier/d'effacer les informations suivantes me concernant contenues dans le Système d'information Schengen (N-SIS II) :

LISTE DES INFORMATIONS CONCERNÉES

En application de la loi du 6 janvier 1978, je vous demande de bien vouloir m'informer de l'issue donnée à cette demande.

Je vous prie d'agréer, Madame, Monsieur, l'expression de mes salutations distinguées.

Pièce-jointe : copie de ma pièce d'identité

La folle volonté de tout contrôler

Les fichiers d'identification administrative, de police, de justice et de renseignement :

Utilisation des données de plus de 100 fichiers actifs et procédures pour leur suppression

Caisse de solidarité de Lyon
caissedesolidarite@riseup.net
06.43.08.50.32
@CaissedesoLyon

Avril 2024
Version 4

Table des matières

EXPÉDITEUR :

Direction centrale de la Police judiciaire
Ministère de l'intérieur
Place BEAUVAU
75800 PARIS CEDEX 08

Par lettre recommandée avec accusé de réception

LIEU, le DATE

Objet : Accès aux données du Système national du système d'information Schengen (N-SIS II)

Madame, Monsieur,

Je soussigné(e) M./Mme XXX, né(e) le XXX à XXX, domicilié(e) au XXX, exerce par la présente mon droit d'accès aux informations me concernant contenues dans le Système d'information Schengen (N-SIS II).

En conséquence et en application des articles 104 et 105 de la loi n°78-17 du 6 janvier 1978 et de l'article R231-12 II du code de la sécurité intérieure, je vous demande de me communiquer les informations me concernant contenues dans le Système d'information Schengen (N-SIS II).

Je vous remercie de m'envoyer ces informations par courrier à mon adresse, ci-dessus.

Je vous prie d'agréer, Madame, Monsieur, l'expression de mes salutations distinguées.

Pièce-jointe : copie de ma pièce d'identité

En application de la loi du 6 janvier 1978, je vous demande de bien vouloir m'informer de l'issue donnée à cette demande.

Je vous prie d'agréer, Monsieur le Ministre, l'expression de mes salutations distinguées.

Pièce-jointe : copie de ma pièce d'identité

EXPÉDITEUR

Monsieur le Ministre de l'Intérieur
Place BEAUVAU
75800 PARIS CEDEX 08

Par lettre recommandée avec avis de réception

LIEU, le DATE

Objet : Rectification/Effacement de données me concernant contenues dans le TAJ, LRPPN, LRPGN, DPIO, LUPIN, iGAV, OSIRIS, LAPI

Monsieur le Ministre,

Je soussigné(e) M./Mme XXX, né(e) le XXX à XXX, domicilié(e) au XXX, exerce par la présente mon droit de rectification/effacement des informations me concernant contenues dans les fichiers suivants :

- Le Traitement des Antécédents judiciaires (TAJ, article R40-33 II du code de procédure pénale) :

LISTE DES INFORMATIONS CONCERNÉES

- Le Logiciel de rédaction des procédures de la police nationale (LRPPN, décret n°2011-110 du 27 janvier 2011 et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) :

LISTE DES INFORMATIONS CONCERNÉES

- Le Logiciel de rédaction des procédures de la gendarmerie nationale (LRPGN, décret 2011-111 du 27 janvier 2011 et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) :

LISTE DES INFORMATIONS CONCERNÉES

- Diffusion de l'information opérationnelle (DPIO, décret n°2014-187 du 20 février 2014 et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) :

LISTE DES INFORMATIONS CONCERNÉES

- Logiciel d'uniformisation des procédures d'identification (LUPIN, arrêté du 15 octobre 2014 et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) :

LISTE DES INFORMATIONS CONCERNÉES

- Informatisation de la gestion des gardes à vue (iGAV, article R15-33-82 du code de procédure pénale mais articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) :

LISTE DES INFORMATIONS CONCERNÉES

- Outil et Système d'Informations Relatives aux Infractions à la législation sur les stupéfiants (OSIRIS, arrêté du 12 janvier 2016 et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) :

LISTE DES INFORMATIONS CONCERNÉES

- Lecture Automatisée des Plaques d'Immatriculation (LAPI, arrêté du 18 mai 2009 et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) :

LISTE DES INFORMATIONS CONCERNÉES

EXPÉDITEUR

Monsieur le Ministre de l’Intérieur
Place BEAUVAU
75800 PARIS CEDEX 08

Par lettre recommandée avec avis de réception

LIEU, le DATE

Objet : Consultation des données me concernant contenues dans le TAJ, LRPPN, LRPGN, DPIO, LUPIN, iGAV, OSIRIS, LAPI

Monsieur le Ministre,

Je soussigné(e) M./Mme XXX, né(e) le XXX à XXX, domicilié(e) au XXX, exerce par la présente mon droit de consultation des informations me concernant contenues dans les fichiers suivants :

- Le Traitement des Antécédents judiciaires (TAJ, article R40-33 II du code de procédure pénale) ;
- Le Logiciel de rédaction des procédures de la police nationale (LRPPN, décret n°2011-110 du 27 janvier 2011 et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) ;
- Le Logiciel de rédaction des procédures de la gendarmerie nationale (LRPGN, décret 2011-111 du 27 janvier 2011 et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) ;
- Diffusion de l’information opérationnelle (DPIO, décret n°2014-187 du 20 février 2014 et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) ;
- Logiciel d’uniformisation des procédures d’identification (LUPIN, arrêté du 15 octobre 2014 et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) ;
- Informatisation de la gestion des gardes à vue (iGAV, article R15-33-82 du code de procédure pénale mais articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) ;
- Outil et Système d’Informations Relatives aux Infractions à la législation sur les stupéfiants (OSIRIS, arrêté du 12 janvier 2016 et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) ;
- Lecture Automatisée des Plaques d’Immatriculation (LAPI, arrêté du 18 mai 2009 et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978).

Je vous remercie de m’envoyer ces informations par courrier à mon adresse, ci-dessus.

Je vous prie d’agréer, Monsieur le Ministre, l’expression de mes salutations distinguées.

Pièce-jointe : copie de ma pièce d’identité

Utilisation du dossier

Bienvenue dans la 4e version (28 avril 2024) d'analyse des fichiers de police, de justice et de renseignement. Outre les mises à jour des informations des fichiers déjà décrits, le dossier prend en compte les dernières évolutions sur l'utilisation des images des drones, des hélicoptères et des caméras piétons utilisés par différents acteurs de la surveillance. Dans la même thématique, ont été ajoutées les différentes images prises par les gendarmes mobiles (camionnettes spécialisées dans la surveillance, réseaux de caméras temporaires, caméscopes utilisés pendant les manifestations, etc), dans la partie 6.

Certains fichiers sont également apparus depuis la dernière version, en particulier sur l'échange des données des casiers judiciaires au niveau européen (le système ECRIS et ECRIS-TCN, partie 10), le fichage des enfants revenant de Syrie (MRZOGT, partie 9), le fichage par la justice dans le domaine de la criminalité organisée (SIROCCO) et celui, clandestin, par les procureurs de la République pendant les mouvements sociaux (partie 13). Dans la foulée, un autre fichier a vu le jour (SISPoPP), le 10 octobre 2023, pour légaliser cette pratique : le fichier, accessible aux magistrats et personnels d'enquête, contient notamment des données sur l'appartenance syndicale ou les opinions politiques des personnes mises en cause dans des violences sur personnes dépositaires de l'autorité publique (partie 13).

RINC, un fichier de renseignements utilisé dans la « *cyber-défense* » a aussi été créé (partie 9).

Enfin, des fichiers qui existaient auparavant mais n'étaient pas mentionnés ici ont été ajoutés dans le dossier : CANONGE et GASPARD-NG, des fichiers reliés au TAJ (le fichier d'antécédents de la police et de la gendarmerie) mais dont le rôle est assez obscur (partie 3) et PARAFE, censé faciliter le passage rapide des frontières (partie 12) et qui utilise la reconnaissance faciale.

Comme dans les trois éditions précédentes, le dossier s'ouvre sur des schémas. Ils permettent de montrer dans quels fichiers on est susceptible d'être répertorié·e, et quels fichiers sont consultés, dans quelques situations. Ça donne une compréhension globale, sans pouvoir entrer dans le détail.

Chaque schéma correspond à une situation dans laquelle la police, la gendarmerie, les services de renseignement, de l'administration ou la justice intervient : arrestation, enquête, procès, vie militante, vie professionnelle, ainsi que certaines situations de la vie quotidienne. Ça ne veut pas dire que les fichages n'interviennent que lors de ces situations, loin de là. Nous avons choisi ces situations parce qu'elles sont relativement critiques ou courantes… Aussi, il s'agit de schémas : ils ne sont pas très précis, un certain nombre d'informations sont perdues. Mieux vaut se reporter au texte général ci-dessous pour avoir plus d'informations sur un fichier en particulier.

Expéditeur :

Direction générale de la Police judiciaire
Ministère de l'intérieur
Place BEAUVAU
75800 PARIS CEDEX 08

Par lettre recommandée avec accusé de réception

LIEU, le DATE

Objet : Rectification/Effacement de données du Fichier des personnes recherchées (FPR)

Madame, Monsieur,

Je soussigné(e) M./Mme XXX, né(e) le XXX à XXX, domicilié(e) au XXX, exerce par la présente mon droit de rectification / d'effacement d'informations me concernant contenues dans le Fichier des personnes recherchées.

En conséquence et en application de l'article 106 de la loi n°78-17 du 6 janvier 1978 et de l'article 9 alinéa 1 du décret n°2010-569 du 28 mai 2010, je vous demande de rectifier/effacer les informations suivantes me concernant contenues dans le Fichier des personnes recherchées :

LISTE DES INFORMATIONS CONCERNÉES

En application de la loi du 6 janvier 1978, je vous demande de bien vouloir m'informer de l'issue donnée à cette demande.

Je vous prie d'agréer, Madame, Monsieur, l'expression de mes salutations distinguées.

Pièce-jointe : copie de ma pièce d'identité

Expéditeur :

Direction générale de la Police judiciaire
Ministère de l’intérieur
Place BEAUVAU
75800 PARIS CEDEX 08

Par lettre recommandée avec accusé de réception

LIEU, le DATE

Objet : Accès aux données du Fichier des personnes recherchées (FPR)

Madame, Monsieur,

Je soussigné(e) M./Mme XXX, né(e) le XXX à XXX, domicilié(e) au XXX, exerce par la présente mon droit d’accès aux informations me concernant contenues dans le Fichier des personnes recherchées.

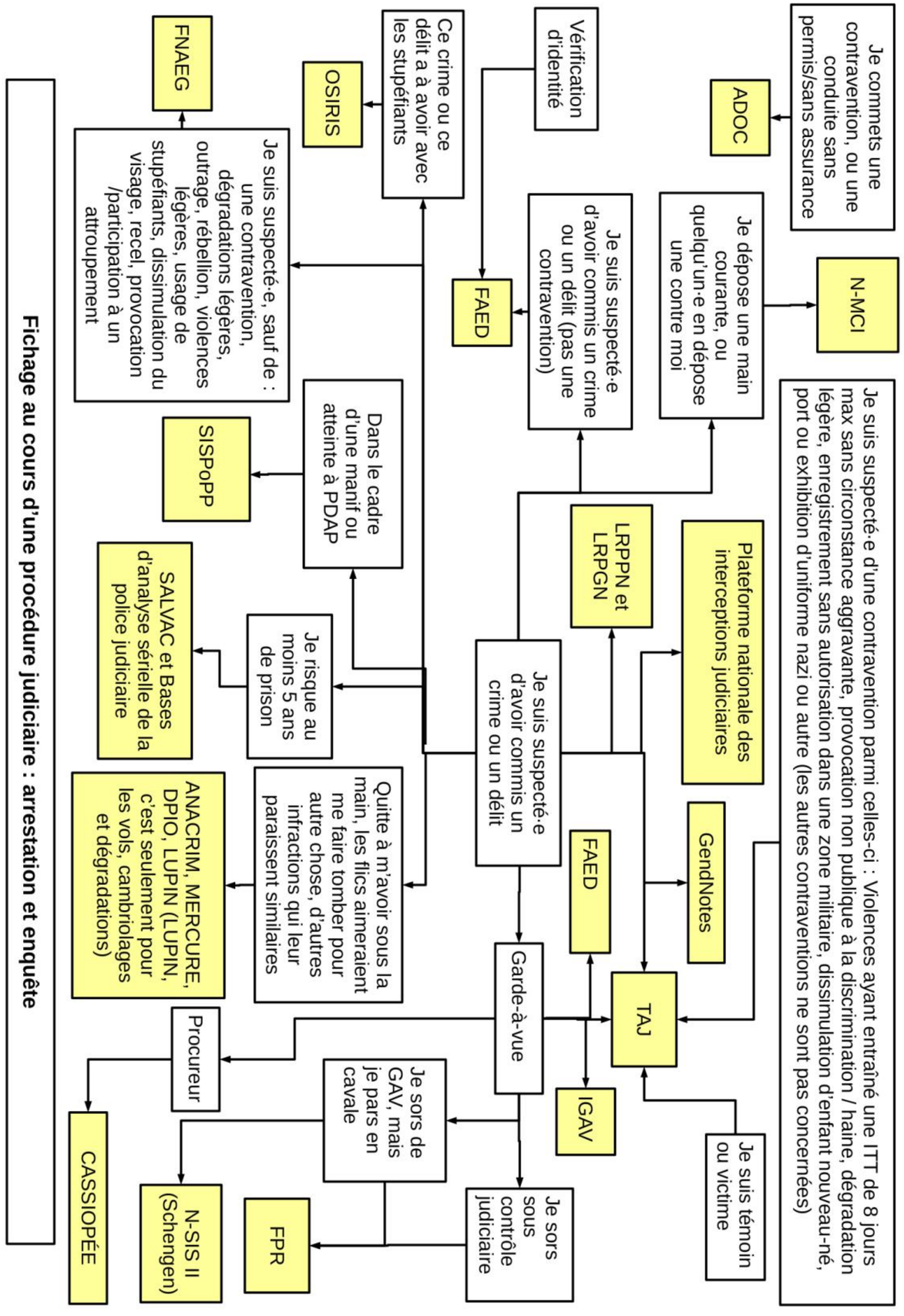
En conséquence et en application des articles 104 et 105 dernier alinéa de la loi n°78-17 du 6 janvier 1978 et de l’article 9 alinéa 1 du décret n°2010-569 du 28 mai 2010, je vous demande de me communiquer les informations me concernant contenues dans le Fichier des personnes recherchées.

Je vous remercie de m’envoyer ces informations par courrier à mon adresse, ci-dessus.

Je vous prie d’agréer, Madame, Monsieur, l’expression de mes salutations distinguées.

Pièce-jointe : Copie de ma pièce d’identité

Merci à tou·te·s les camarades qui nous ont fait des retours d’expériences et qui nous ont signalé les erreurs et les changements de législation depuis la dernière édition !



Expéditeur :

Procureur de la République compétent
En fonction du domicile du demandeur

Par lettre recommandée avec accusé de réception

LIEU, le DATE

Objet : Accès au Bulletin n°1 du casier judiciaire

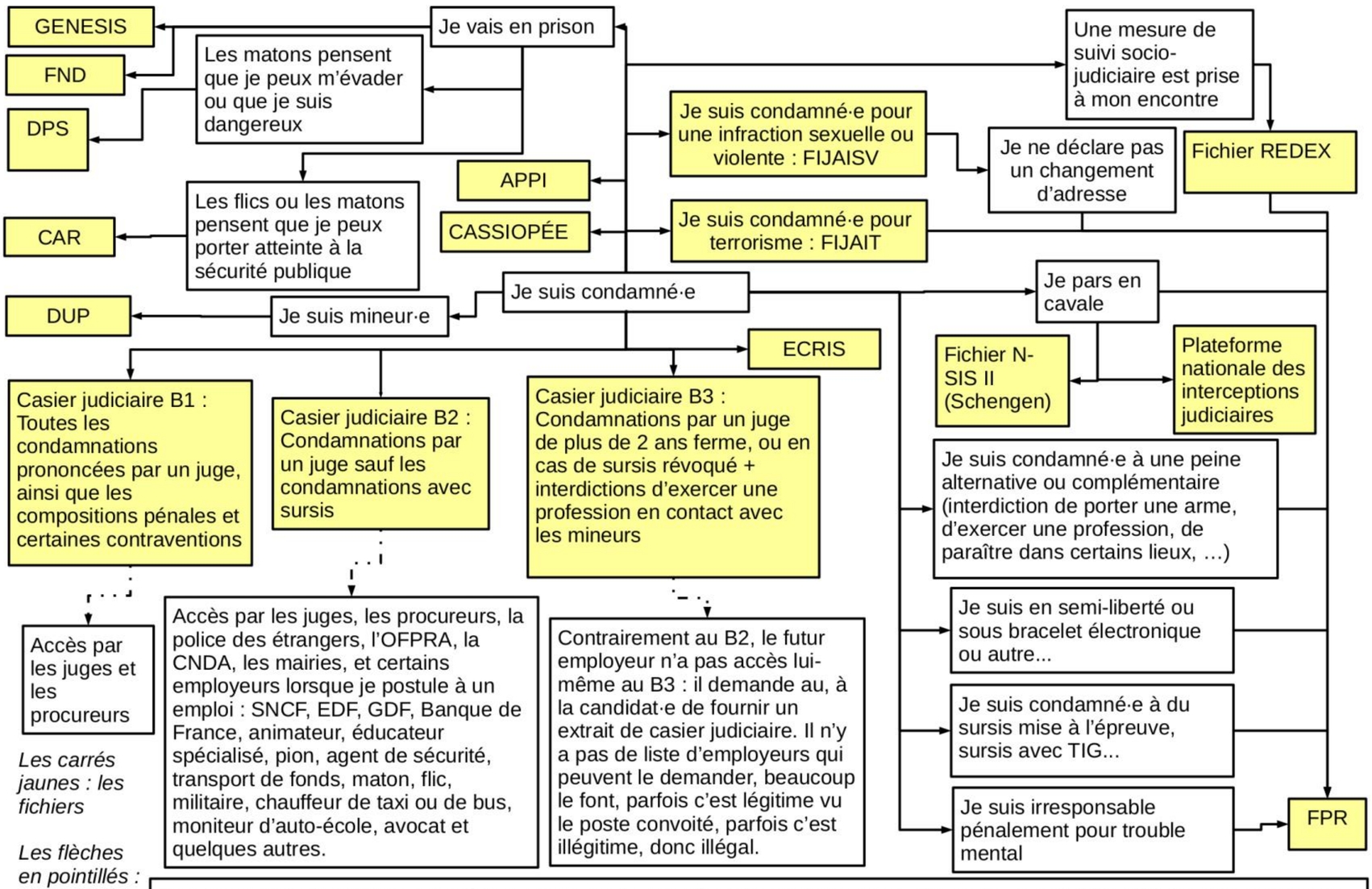
Madame, Monsieur le procureur de la République,

Je soussigné·e M./Mme XXX, né(e) le XXX à XXX, domicilié(e) au XXX, exerce par la présente mon droit d'accès au Bulletin n°1 du casier judiciaire.

En conséquence et en application de l'article 777-2 du code de procédure pénale, je vous demande de bien vouloir me recevoir pour la communication des données me concernant contenues dans le Bulletin n°1 du casier judiciaire.

Je vous prie d'agréer, Madame, Monsieur le procureur, l'expression de ma plus haute considération.

Pièce-jointe : Copie de ma pièce d'identité



Expéditeur :

Préfet du domicile

Par lettre recommandée avec accusé de réception

LIEU, le DATE

Objet : Rectification/Effacement de données du Fichier National des Permis de Conduire

Madame, Monsieur le Préfet

Je soussigné(e) M./Mme XXX, né(e) le XXX à XXX, domicilié(e) au XXX, exerce par la présente mon droit de rectification/d'effacement des informations me concernant contenues dans le Fichier National des Permis de Conduire.

En conséquence et en application de l'article L225-2 du code de la route, je vous demande de rectifier/d'effacer les informations suivantes me concernant contenues dans le Fichier National des Permis de Conduire :

LISTE DES INFORMATIONS CONCERNÉES

En application de la loi du 6 janvier 1978, je vous demande de bien vouloir m'informer de l'issue donnée à cette demande.

Je vous prie de bien vouloir agréer, Madame, Monsieur, le Préfet, l'expression de ma plus haute considération.

Pièce-jointe : Copie de ma pièce d'identité

Expéditeur :

Préfet du domicile

Par lettre recommandée avec accusé de réception

LIEU, le DATE

Objet : Accès aux données du Fichier National des Permis de Conduire

Madame, Monsieur le Préfet

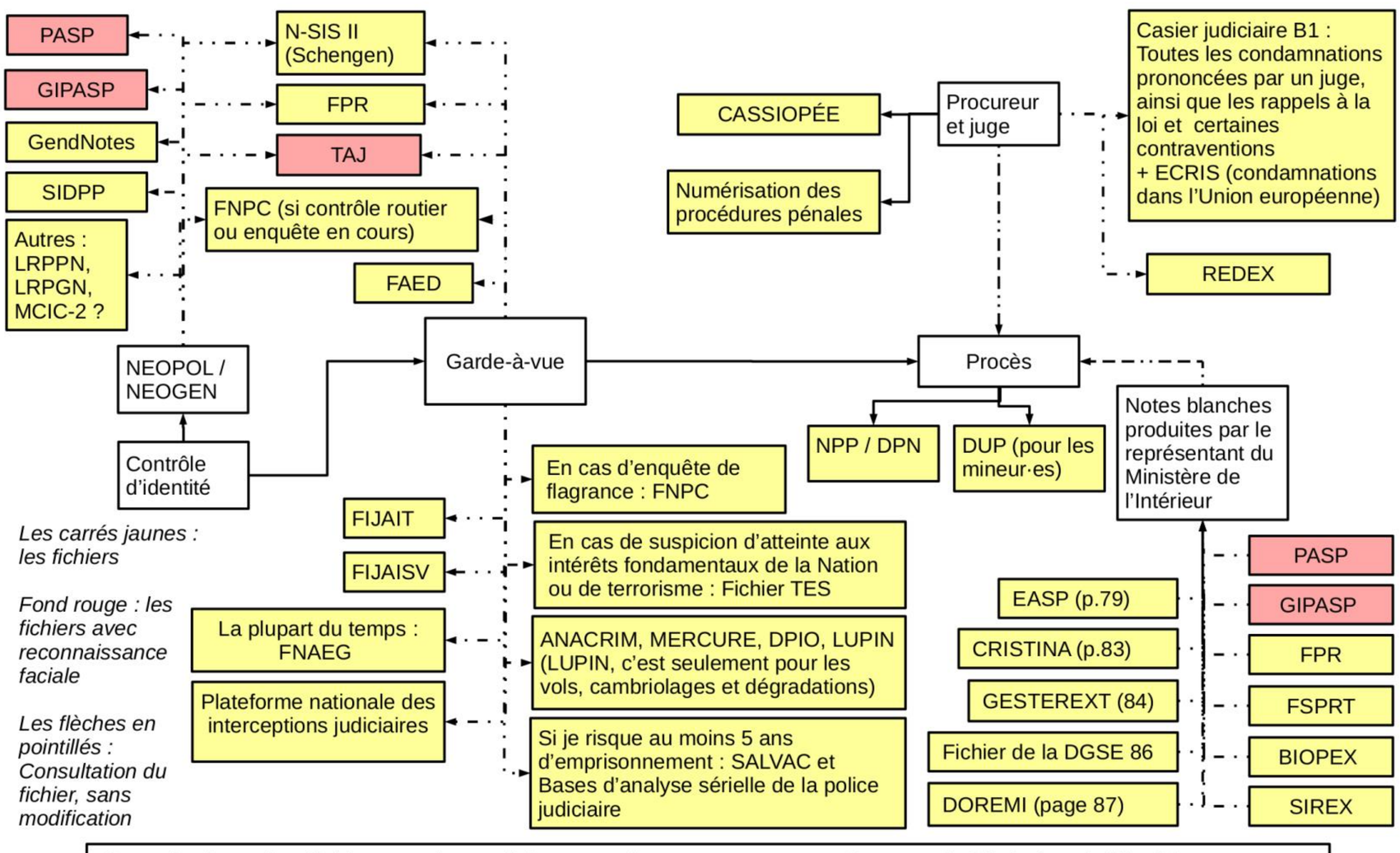
Je soussigné(e) M./Mme XXX, né(e) le XXX à XXX, domicilié(e) au XXX, exerce par la présente mon droit d'accès aux informations me concernant contenues dans le Fichier National des Permis de Conduire.

En conséquence et en application de l'article L225-3 du code de la route, je vous demande de me communiquer les informations me concernant contenues dans le Fichier National des Permis de Conduire.

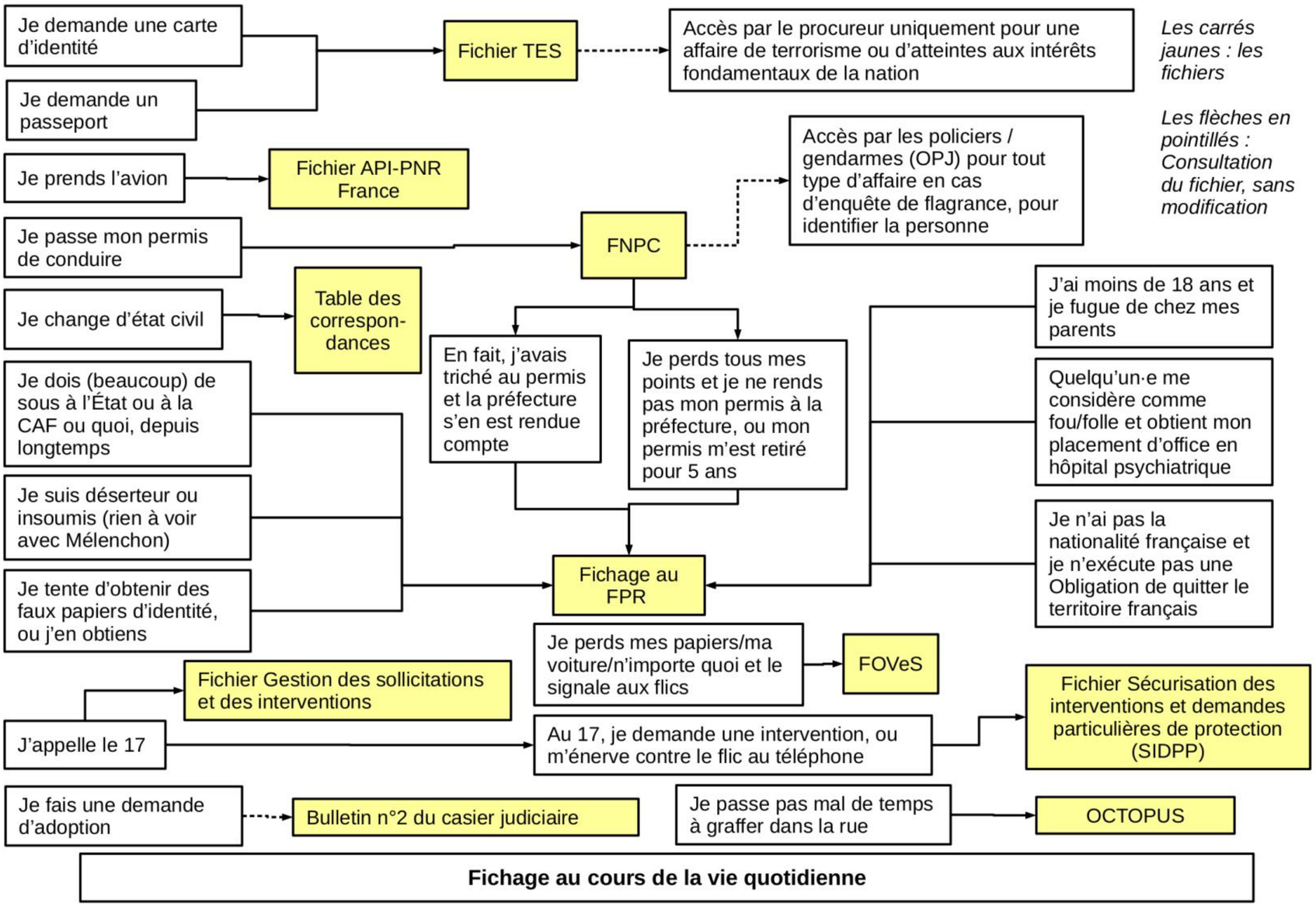
Je vous remercie de m'envoyer ces informations par courrier à mon adresse, ci-dessus.

Je vous prie de bien vouloir agréer, Madame, Monsieur, le Préfet, l'expression de ma plus haute considération.

Pièce-jointe : Copie de ma pièce d'identité



Consultations des fichiers par les policiers, gendarmes, procureurs, juges et le Ministère de l'intérieur au cours de la procédure pénale : il y a ici seulement des traits en pointillés, parce qu'il s'agit de la consultation des fichiers et non de leur modification. Attention, pour certains fichiers, leur consultation équivaut à l'entrée de nouvelles données (par exemple FAED, FNAEG, et sûrement ANACRIM, SALVAC et consorts.



Expéditeur :

Préfecture ayant délivré le passeport
Ou Mairie ayant délivré la carte nationale d'identité

Par lettre recommandée avec avis de réception

LIEU, le DATE

Objet : Suppression de données du fichier des Titres Électroniques Sécurisés

Madame, Monsieur,

Je soussigné(e) M./Mme XXX, né(e) le XXX à XXX, domicilié(e) au XXX, exerce par la présente mon droit d'effacement/de rectification de certaines informations me concernant contenues dans le fichier des Titres Électroniques Sécurisés.

En conséquence et en application de l'article 11 du décret n°2016-1460 du 28 octobre 2016, je vous demande d'effacer/de rectifier les informations suivantes me concernant contenues dans le Fichier des Titres Électroniques Sécurisés :

LISTE DES INFORMATIONS CONCERNÉES

En application de la loi du 6 janvier 1978, je vous demande de bien vouloir m'informer de l'issue donnée à cette demande.

Je vous prie d'agréer, Madame, Monsieur le Ministre, l'expression de ma haute considération.

Pièce-jointe : Copie de ma pièce d'identité

Expéditeur :

Préfecture ayant délivré le passeport
Ou Mairie ayant délivré la carte nationale d'identité

Par lettre recommandée avec avis de réception

LIEU, le DATE

Objet : Accès aux données du fichier des Titres Électroniques Sécurisés

Madame, Monsieur,

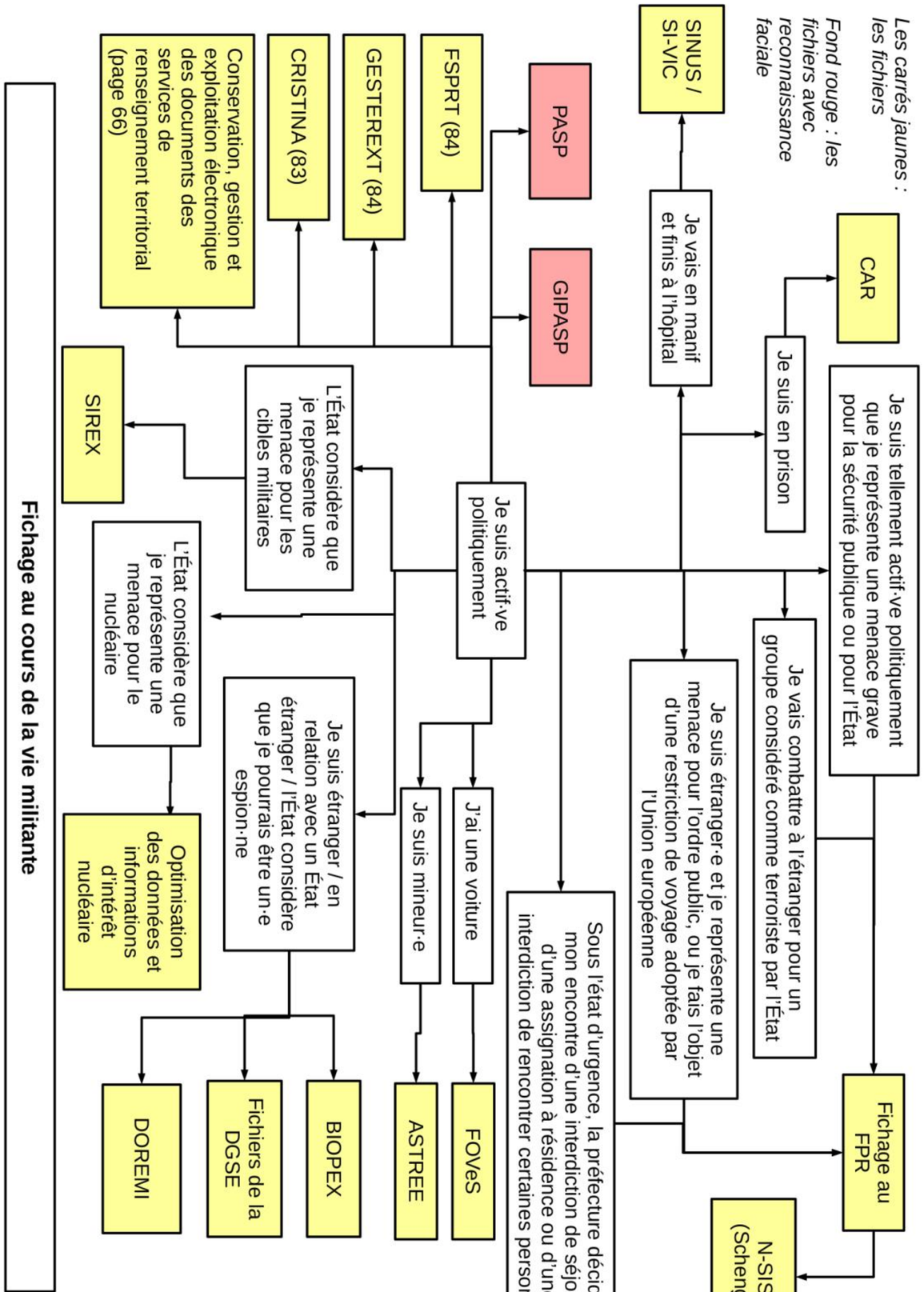
Je soussigné(e) M./Mme XXX, né(e) le XXX à XXX, domicilié(e) au XXX, exerce par la présente mon droit d'accès aux informations me concernant contenues dans le fichier des Titres Électroniques Sécurisés.

En conséquence et en application de l'article 11 du décret n°2016-1460 du 28 octobre 2016, je vous demande de me communiquer les informations me concernant contenues dans le Fichier des Titres Électroniques Sécurisés.

Je vous remercie de m'envoyer ces informations par courrier à mon adresse, ci-dessus.

Je vous prie d'agréer, Madame, Monsieur le Ministre, l'expression de ma haute considération.

Pièce-jointe : copie de ma pièce d'identité



Nous sommes là pour vous aider

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA JUSTICE

cerfa

n° 12411*02

Demande d'effacement d'un signalement au fichier national automatisé des empreintes génétiques adressée au Procureur de la République

(Article R53-13-1 du code de procédure pénale)

Votre identité :

☐Madame ☐Monsieur

Votre nom (de naissance): _____

Votre nom d'usage (ex. nom d'épouse) _____

Vos prénoms : _____

Votre date et lieu de naissance : |__|__|__|__|__|__|__|__| à _____

Votre adresse : _____

_____

Code postal |__|__|__|__|__| Commune : _____

Pays: _____

Adresse courriel : _____@_____

Numéro de téléphone: |__|__|__|__|__|__|__|__|__|__|

Votre demande :

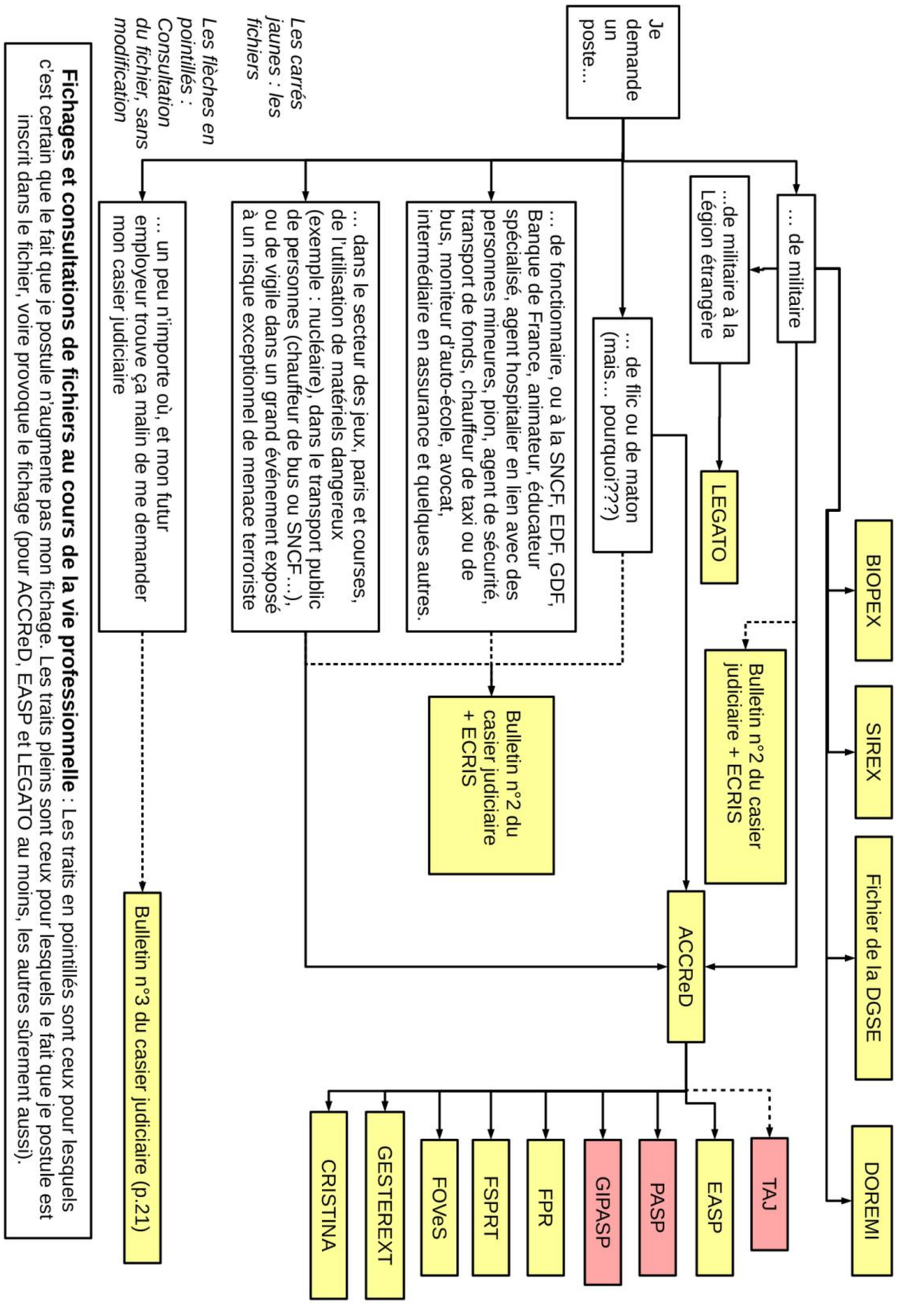
Vous demandez au Procureur de la République d'ordonner l'effacement au fichier national automatisé des empreintes génétiques d'un signalement vous concernant.

Précisez si vous pouvez l'affaire dans laquelle vous avez fait l'objet du prélèvement d'empreinte génétique *(date et nature de l'affaire)* :

_____

_____

_____



Les différentes catégories de fichiers et leur utilisation

On va se lancer dans la lecture de plein de pages consacrées à la surveillance et au fichage. Le but n'est pas d'alimenter la paranoïa sur la police ou le sentiment de toute-puissance de l'État : Oui, l'État a des moyens pour se protéger, mais visibiliser ces moyens et les connaître permet d'abord de mieux les combattre et y faire face. De plus, ici, on a essayé de trier un peu, mais à l'arrivée des fichiers très différents sont mélangés : de fait, il n'y a pas grand-chose à voir entre le TES (qui rassemble les données de toutes les personnes ayant une carte d'identité ou un passeport, mais qui n'est théoriquement pas consultable par les juges ou par les services de renseignement sauf « terrorisme »), le FPR et CRISTINA (qui ont, eux, vocation à surveiller l'activité et les opinions des personnes) et le casier judiciaire (qui recense les condamnations des personnes). Les différents services ont le droit à accéder à certains fichiers, pas à d'autres. Quand ils peuvent accéder à un fichier, c'est souvent pour un objectif précis. Dans la pratique, n'importe quel flic ne peut pas accéder à toutes les informations sur une personne. Il y a une certaine imperméabilité des différents systèmes de fichage.

Les fichiers peuvent être utilisés pour les enquêtes administratives pour l'accès à certaines professions : recrutement de personnels pour la souveraineté de l'État, recrutement privé ou public dans le domaine de la sécurité ou de la défense, dans le domaine des jeux, paris et courses, l'accès à des zones protégées ou l'utilisation de matières dangereuses. Dans le cadre de ces enquêtes, de nombreux fichiers peuvent être consultés (fichiers administratifs, fichiers d'antécédent, fichiers de rapprochement, fichiers de renseignement dans certains cas), mais pas les fichiers d'identification (article L114-1 du code de la sécurité intérieure).

Ici, de nombreux fichiers ne sont pas évoqués : les fichiers de personnes étrangères par exemple, et les innombrables fichiers relatifs aux droits sociaux des personnes (numéro de sécurité sociale, CAF, etc.). De la même manière, certains fichiers tenus secrets ne sont pas mentionnés (par exemple STARTRAC opéré par TRACFIN contre l'évasion fiscale ou LEGATO créé le 24 mai 2018 pour les recrutements à la légion étrangère).

Différents types de fichiers suivent donc :

- Les fichiers d'identification administrative (qui ne sont pas des fichiers de police et qui sont tenus par l'administration), qui comportent le plus grand nombre de personnes (Partie 1) ;
- Suivent les fichiers d'antécédents (le casier judiciaire en premier lieu) et les principaux fichiers de justice (Partie 2) ;

Expéditeur :

Procureur de la République compétent
En fonction de l'autorité de police qui a émis chaque mention au fichier.

Par lettre recommandée avec accusé de réception

LIEU, le DATE

Objet : Suppression de la mention n° [identification de la mention] au FAED

Madame, Monsieur le procureur de la République,

Je soussigné(e) M./Mme XXX, né(e) le XXX à XXX, domicilié(e) au XXX, exerce par la présente mon droit de supprimer certaines mentions me concernant contenues dans le Fichier Automatisé des Empreintes Digitales.

En conséquence et en application de l'article 106 de la loi n°78-17 du 6 janvier 1978 et des articles 7-1 et 7-2 du décret n°87-249 du 8 avril 1987, je vous demande de supprimer les mentions suivantes me concernant contenues dans le Fichier Automatisé des Empreintes Digitales :

[LISTE DES MENTIONS]

En application de l'article 7-2 du décret n°87-249 susmentionné, je vous remercie de me faire parvenir votre réponse dans un délai de 3 mois, par lettre recommandée avec accusé de réception, à mon adresse : [ADRESSE]

Je vous prie d'agréer, Madame, Monsieur le procureur, l'expression de ma plus haute considération.

Pièce-jointe : copie de ma pièce d'identité

Expéditeur :

Chef du service central de la police technique et scientifique
Ministère de l’intérieur
Place BEAUVAU
75800 PARIS CEDEX 08

Par lettre recommandée avec accusé de réception

LIEU, le DATE

Objet : Accès aux données du FAED et du FNAEG

Madame, Monsieur,

Je soussigné(e) M./Mme XXX, né(e) le XXX à XXX, domicilié(e) au XXX, exerce par la présente mon droit d’accès aux informations me concernant contenues dans le Fichier Automatisé des Empreintes Digitales et dans le Fichier National Automatisé des Empreintes Génétiques.

En conséquence et en application des articles 104 et 107 de la loi n°78-17 du 6 janvier 1978 et de l’article 6 du décret n°87-249 du 8 avril 1987, je vous demande de me communiquer les informations me concernant contenues dans le Fichier Automatisé des Empreintes Digitales.

En outre, en application des articles 104 et 107 de la loi n°78-17 du 6 janvier 1978 et de l’article R53-15 du code de procédure pénale, j’exerce mon droit d’accès aux informations me concernant contenues dans le Fichier National Automatisé des Empreintes Génétiques.

Je vous remercie de m’envoyer ces informations par courrier à mon adresse, ci-dessus.

Je vous prie d’agréer, Madame, Monsieur, l’expression de mes salutations distinguées.

Pièce-jointe : Copie de ma pièce d’identité

- Les principaux fichiers utilisés au quotidien par la police qui recensent par exemple le Traitement des antécédents judiciaires et certains fichiers aisément accessibles via les tablettes et smartphones de type NEOGEND et NEOPOL (Partie 3) ;
- Les principaux fichiers d’identification, en particulier ceux des empreintes digitales et des empreintes génétiques (Partie 4) ;
- Les fichiers de renseignement tenus par les services de police et de gendarmerie (Partie 5) ;
- Les fichiers rassemblant les images et les sons captés par les services de police et de gendarmerie (Partie 6) ;
- Ensuite viennent les logiciels d’analyse de données utilisés par les services de police et de gendarmerie (Partie 7) ;
- Les fichiers de renseignement utilisés pour les enquêtes administratives, par exemple quand une personne postule à un poste d’enseignant, ou quand un·e étranger·e demande un titre de séjour (Partie 8) ;
- Les « vrais » fichiers de renseignement, utilisés par les services de renseignement type DGSI et DGSE (Partie 9) ;
- Les principaux fichiers européens et internationaux (Partie 10) ;
- Les fichiers de police secondaires, qui servent principalement au fonctionnement de l’institution policière (Partie 11) ;
- Les fichiers de police secondaires thématiques, par exemple relatifs aux interdictions de stade ou aux interdictions de porter une arme (Partie 12) ;
- Les fichiers de justice secondaires, qui servent principalement au fonctionnement de l’institution judiciaire (Partie 13).

Après cette longue liste, une partie est consacrée au récapitulatif du droit d’accès et de suppression (Partie 14). Il s’agit de rassembler les informations utiles pour comprendre les procédures relatives à chaque fichier, pour pouvoir plus facilement demander l’accès aux données et leur suppression.

Enfin, pour rendre encore plus faciles les démarches de consultation, de rectification et de suppression des données, un certain nombre de lettres-types sont rassemblées (Annexes).

Partie 1 : Fichiers d'identification administrative

Voici quatre fichiers d'identification administrative.

Ces fichiers n'ont pas pour vocation principale d'identifier une personne lorsqu'une infraction a été commise. Il s'agit plutôt d'identifier une personne que les services de police ont sous la main – par exemple, en cas de doute sur l'identité d'une personne, ils consultent systématiquement le Fichier National des Permis de Conduire. Ils peuvent aussi accéder à DOCVERIF pour vérifier que le passeport, la carte d'identité ou le permis de conduire n'est pas un faux. De plus, en cas de menace d'atteinte contre la nation ou en cas de terrorisme, les services de police peuvent accéder à toutes les données contenues dans ces fichiers.

Pour cette mise à jour, il a été décidé d'intégrer le Répertoire national des personnes physiques (RNIPP) en raison de ses liens de plus en plus nombreux avec des fichiers de police.

1. Répertoire national des personnes physiques (RNIPP)

L'idée de tenir un répertoire général de la population remonte à loin (voir par exemple le Fichier des personnes sans domicile ni résidence fixe, partie 12, sous-partie 13, héritier d'une demande du ministère de l'Intérieur aux préfets du 20 mars 1895 de recenser les « bohémiens » selon le terme employé à l'époque, puis le carnet anthropométrique créé par la loi du 16 juillet 1912 qui visait les « nomades »). Sous Vichy, et plus précisément en 1941 le numéro que l'on connaît désormais comme numéro de la sécurité sociale est mis en place, aux fins de fichage de toute la population[1]. Qui se souvient qu'à part le 1 ou le 2 initiaux (homme ou femme français.e), étaient prévus le 3 et 4 pour les « indigènes musulmans » et le 5 et 6 pour les « indigènes juifs » ?

Après la deuxième guerre mondiale, l'INSEE est créé en 1946 et il lui est très rapidement donné pour mission, par l'article 6 du décret n°47-834 du 13 mai 1947 de tenir un répertoire de la population née en France ou vivant en France.

En 1970, l'INSEE lance le sulfureux projet SAFARI, qui prévoit l'interconnexion de ce fichier de tous les Français avec les fichiers de police. Scandale. Le projet est abandonné en 1974.

Finalement le répertoire est transformé en un fichier informatique par le décret n°83-103 du 22 janvier 1982 créant le Répertoire national des personnes physiques (RNIPP), toujours tenu par l'INSEE.

1.1 – Données concernées

Il concerne toutes les personnes qui sont nées en France. Les personnes non nées en France peuvent également y être inscrites (par exemple les personnes dont la naissance a été déclarée à un consulat français,

1 Sur cette histoire controversée, voir notamment : Monique Méron, « Statistiques ethniques : tabous et boutades », *Travail, genre et sociétés*, 2009/1 (Nº 21), p. 55-68.

- les données contenues dans le fichier Application relative à la prévention des atteintes à la sécurité publique (PASP, article R236-19 du code de la sécurité intérieure) intéressant la sûreté de l'État (article 118 de la loi du 6 janvier 1978) ;
- les données contenues dans le fichier Gestion de l'information et la prévention des atteintes à la sécurité publique (GIPASP article R236-29 du code de la sécurité intérieure) intéressant la sûreté de l'État (article 118 de la loi du 6 janvier 1978) ;
- Conservation, gestion et exploitation électroniques des documents des services de renseignement territorial, article R236-51 du code de la sécurité intérieure ;
- CRISTINA, décret du 27 juin 2008 et article R841-2 1° du code de la sécurité intérieure ;
- Gestion du terrorisme et des extrémismes à potentialité violente (GESTEREXT, décret n°2017-1218 du 2 août 2017 et article R841-2 10° du code de la sécurité intérieure) ;
- Fichier des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT, décret n°2015-252 du 4 mars 2015 et article R841-2 5° du code de la sécurité intérieure) ;
- Fichier du renseignement pénitentiaire, décret n°2023-795 du 18 août 2023 ;
- ASTREE, décret n°2017-154 du 8 février 2017 ;
- BIOPEX, décret n°2017-1231 du 4 août 2017 et article R841-2 11° ;
- TREX, article R841-2 2° du code de la sécurité intérieure et article 1 2° du décret n°2007-914 du 15 mai 2007 ;
- Fichier de la DGSE, article 1 6° du décret n°2007-914 du 15 mai 2007 ;
- DOREMI, article R841-2 4° du code de la sécurité intérieure et article 1 4° du décret n°2007-914 du 15 mai 2007 ;
- Fichier des personnes étrangères de la Direction du renseignement militaire, article 1 8° du décret n°2007-914 du 15 mai 2007 ;
- SIREX, article R841-2 3° du code de la sécurité intérieure ;
- BCR-DNRED, article R841-2 9° du code de la sécurité intérieure ;
- Outil de Centralisation et de Traitement Opérationnel des Procédures et des Utilisateurs de Signatures (OCTOPUS) de la Direction de police urbaine de proximité de la Préfecture de police de Paris (Service régional de police des transports – Brigade des réseaux ferrés d'Île-de-France – Cellule tags).

Je vous prie d'agréer, Madame la Présidente, l'expression de mes salutations distinguées.

Pièce-jointe : Copie de ma pièce d'identité

Expéditeur :

Commission Nationale Informatique et Libertés
Service du droit d’accès indirect
3, Place de Fontenoy
TSA 80715
75334 PARIS CEDEX 07

Par lettre recommandée avec accusé de réception

LIEU, le DATE

Objet : Effacement d’informations de certains fichiers de l’État

Madame la Présidente,

En application de la loi du 6 janvier 1978 et de la directive n°2016/680 (directive « police-justice »), je soussigné(e) M./Mme XXX, né(e) le XXX à XXX, domicilié(e) au XXX, exerce par la présente mon droit d’effacement des informations me concernant contenues dans les fichiers suivants :

- les données contenues dans le Fichier des personnes recherchées (FPR, article 9 du décret n°2010-569 du 28 mai 2010) intéressant la sûreté de l’État (article 118 de la loi du 6 janvier 1978) ;
- les données contenues dans le fichier Automatisation de la consultation centralisée de renseignements et de données (ACCReD, article 8 du décret n°2017-1224 du 3 août 2017) intéressant la sûreté de l’État (article 118 de la loi du 6 janvier 1978) ;
- les données contenues dans le Fichier des Objets et Véhicules Signalés (FOVeS, article 8 de l’arrêté du 7 juillet 2017) intéressant la sûreté de l’État (article 118 de la loi du 6 janvier 1978) ;
- les données contenues dans le Fichier du Système d’informations Schengen N-SIS II, article R231-12 du code de la sécurité intérieure intéressant la sûreté de l’État (article 118 de la loi du 6 janvier 1978) ;
- European Criminal Records Information System / Système européen d’information sur les casiers judiciaires (ECRIS, article 25 du règlement européen 2019/816 du 17 avril 2019) ;
- les fichiers gérés par Europol (article 36 du règlement 2016/794 du 11 mai 2016) ;
- l’ensemble des fichiers européens interconnectés (Bases de données Prüm, article 31 de la décision 2008/615/JAI du 23 juin 2008) ;
- Fichier Central de la Criminalité Organisée (F2CO) et Fichier des Brigades Spécialisées ;
- les données contenues dans le fichier Enquêtes administratives liées à la sécurité publique (EASP, article R236-9 du code de la sécurité intérieure) intéressant la sûreté de l’État (article 118 de la loi du 6 janvier 1978) ;

les personnes étrangères ayant bénéficié d’un accord de regroupement familial pour rejoindre des proches vivant en France, ou les personnes qui travaillent en France ou sont affiliées à un organisme de sécurité sociale (article R161-1 du code de la sécurité sociale)).

Il contient l’ensemble de leurs données d’état civil, ainsi qu’un numéro d’inscription qui est en fait le numéro de sécurité sociale.

Les modifications de l’état civil (changements de nom, de prénom, de sexe) y sont inscrites.

1.2 – Connexions avec d’autres fichiers

Le RNIPP n’est pas à proprement parler un fichier de police, toutefois ses connexions avec d’autres fichiers justifient qu’il apparaisse ici.

Il est en effet lié au casier judiciaire dans la mesure où l’INSEE communique au Service du casier judiciaire national le nom, les prénoms, les dates et lieu de naissance et le sexe de l’ensemble des personnes inscrites au RNIPP de plus de douze ans (article R64 du code de procédure pénale).

Cela permet la constitution des fiches du casier judiciaire. Ainsi, lorsque le procureur de la République consulte le casier judiciaire, s’il constate qu’il n’y a aucune fiche existante pour une personne née en France, il y a de fortes probabilités qu’il s’agisse d’une fausse identité.

Le RNIPP est également en lien indirect avec le fichier ACCReD (utilisé dans de nombreuses enquêtes administratives, lorsqu’une personne postule à un emploi considéré comme sensible) car celui-ci permet d’interroger le casier judiciaire et d’obtenir un retour si la personne n’y est pas inscrite, ce qui signifie (si elle est née en France) qu’elle n’est pas non plus au RNIPP.

Le RNIPP est, enfin, lié à la Table de correspondance des noms et prénoms créée par un arrêté du 19 décembre 2023. Cette table, plus communément appelée « Fichier des personnes trans », permet de conserver les correspondances des personnes ayant changé de nom, de prénom, de sexe et est consultable par de nombreux services de police (voir partie 4) .

1.3 – Durée de conservation des données

Il semble qu’aucune durée de conservation des données n’est prévue, de telle sorte qu’elles ne sont jamais effacées.

1.4 – Droits d’accès aux données

Ce droit s’exerce auprès des directions régionales de l’INSEE pour les personnes résidant en France, et auprès de la direction générale de l’INSEE pour celles résidant à l’étranger (article 8 du décret n°83-103 du 22 janvier 1982).

Aucun droit de rectification ou d’effacement n’est prévu.

2. Fichier des Titres Électroniques Sécurisés (TES)

Il a été créé en 2016 (décret n°2016-1460 du 28 octobre 2016). Il rassemble les données du Fichier National de Gestion (FNG), qui concernait la carte d'identité, et de l'ancien TES, qui concernait les passeports. Ce fichier est géré par la direction des libertés publiques et des affaires juridiques du ministère de l'intérieur et par l'agence nationale des titres sécurisés (ANTS). Sa création en 2016, et sa modification en 2018, ont été combattues, en particulier par La Quadrature du Net[2].

Le TES a été modifié en 2021 (décret n°2021-279 du 13 mars 2021) notamment suite à l'entrée en vigueur du règlement européen n°2019/1157 du 20 juin 2019[3]. Cette modification a été largement critiquée[4].

Parallèlement à la réforme du TES, en 2021 est apparue une nouvelle carte d'identité, au format carte bleue. Cette carte d'identité, contrairement à la précédente, comporte une puce électronique qui contient les mêmes informations que celles qui apparaissent sur la carte d'identité (comme pour les passeports). En plus de ces informations, cette puce électronique contient les empreintes digitales de deux doigts (les deux index, si impossibilité le majeur et l'annulaire de la même main, sinon de l'autre main – article 4-3 du décret du 22 octobre 1955).

Cette nouvelle carte d'identité comprend, comme l'ancienne, une zone de lecture automatique (appelée « bande MRZ ») qui contient le nom, les prénoms, la date de naissance, le sexe et la nationalité du titulaire, le type du document, l'État émetteur (la France), le numéro du titre et sa date de fin de validité (article 1-2 du décret du 22 octobre 1955).

Elle comprend, en plus de l'ancienne, un « cachet électronique visible » (un QR code), qui comprend à peu près les mêmes informations que la bande MRZ (à la différence de la bande MRZ, le QR code contient seulement le premier prénom, il ajoute le nom d'usage, il ne contient pas le pays de délivrance, et la date de fin de validité est remplacée par la date de délivrance) (article 1-3 du décret du 22 octobre 1955).

La bande MRZ peut être lue automatiquement lors d'un contrôle d'identité par les tablettes NEOGEND (gendarmerie) et NEOPOL (police). Cela entraîne une consultation automatique, au minimum, du TAJ et du FPR. Il est difficile de savoir si d'autres fichiers sont consultés automatiquement à cette étape[5].

2 La Quadrature du Net, *Fichier TES, danger pour les libertés! https://www.laquadrature.net/2016/11/14/oln-fichier-tes-danger-pour-libertes/ ; Le fichier TES, prémisse à la reconnaissance faciale de masse, arrive devant le Conseil d'État* https://www.laquadrature.net/2018/09/26/audience_tes/

3 Une autre modifications non substantielle a eu lieu depuis par décret (le 2 novembre 2023)

4 Voir par exemple https://www.nextinpact.com/article/46457/la-cnil-retoque-encore-mega-fichier-biometrique-gens-honnetes

5 Voir Libération, Checknews, Gilets jaunes : les forces de l'ordre peuvent-elles prendre en photo les pièces d'identité ?, https://www.liberation.fr/checknews/2019/01/24/gilets-jaunes-les-forces-de-l-ordre-peuvent-elles-prendre-en-photo-les-pieces-d-identite_1704376/m

- les données contenues dans le fichier Gestion de l'information et la prévention des atteintes à la sécurité publique (GIPASP article R236-29 du code de la sécurité intérieure)intéressant la sûreté de l'État (article 118 de la loi du 6 janvier 1978) ;
- Conservation, gestion et exploitation électroniques des documents des services de renseignement territorial, article R236-51 du code de la sécurité intérieure ;
- CRISTINA, décret du 27 juin 2008 et article R841-2 1° du code de la sécurité intérieure ;
- Gestion du terrorisme et des extrémismes à potentialité violente (GESTEREXT, décret n°2017-1218 du 2 août 2017 et article R841-2 10° du code de la sécurité intérieure) ;
- Fichier des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT, décret n°2015-252 du 4 mars 2015 et article R841-2 5° du code de la sécurité intérieure) ;
- Fichier du renseignement pénitentiaire, décret n°2023-795 du 18 août 2023 ;
- ASTREE, décret n°2017-154 du 8 février 2017 ;
- BIOPEX, décret n°2017-1231 du 4 août 2017 et article R841-2 11° ;
- TREX, article R841-2 2° du code de la sécurité intérieure et article 1 2° du décret n°2007-914 du 15 mai 2007 ;
- Fichier de la DGSE, article 1 6° du décret n°2007-914 du 15 mai 2007 ;
- DOREMI, article R841-2 4° du code de la sécurité intérieure et article 1 4° du décret n°2007-914 du 15 mai 2007 ;
- Fichier des personnes étrangères de la Direction du renseignement militaire, article 1 8° du décret n°2007-914 du 15 mai 2007 ;
- SIREX, article R841-2 3° du code de la sécurité intérieure ;
- BCR-DNRED, article R841-2 9° du code de la sécurité intérieure ;
- Outil de Centralisation et de Traitement Opérationnel des Procédures et des Utilisateurs de Signatures (OCTOPUS) de la Direction de police urbaine de proximité de la Préfecture de police de Paris (Service régional de police des transports – Brigade des réseaux ferrés d'Île-de-France – Cellule tags).

Je vous remercie de m'envoyer ces informations par courrier à mon adresse, ci-dessus.

Je vous prie d'agréer, Madame la Présidente, l'expression de mes salutations distinguées.

Pièce-jointe : Copie de ma pièce d'identité

Expéditeur :

Commission Nationale Informatique et Libertés
3, Place de Fontenoy
TSA 80715
75334 PARIS CEDEX 07

Par lettre recommandée avec accusé de réception

LIEU, le DATE

Objet : Accès aux informations me concernant contenues dans certains fichiers de l'État

Madame la Présidente,

En application de la loi du 6 janvier 1978 et de la directive n°2016/680 (directive « police-justice »), je soussigné(e) M./Mme XXX, né(e) le XXX à XXX, domicilié(e) au XXX, exerce par la présente mon droit d'accès aux informations me concernant contenues dans les fichiers suivants :

- les données contenues dans le Fichier des personnes recherchées (FPR, article 9 du décret n°2010-569 du 28 mai 2010) intéressant la sûreté de l'État (article 118 de la loi du 6 janvier 1978) ;.
- les données contenues dans le fichier Automatisation de la consultation centralisée de renseignements et de données (ACCReD, article 8 du décret n°2017-1224 du 3 août 2017) intéressant la sûreté de l'État (article 118 de la loi du 6 janvier 1978) ; ;
- les données contenues dans le Fichier des Objets et Véhicules Signalés (FOVeS, article 8 de l'arrêté du 7 juillet 2017) intéressant la sûreté de l'État (article 118 de la loi du 6 janvier 1978) ;.
- les données contenues dans le Fichier du Système d'informations Schengen N-SIS II (article R231-12 du code de la sécurité intérieure) intéressant la sûreté de l'État (article 118 de la loi du 6 janvier 1978) ;.
- European Criminal Records Information System / Système européen d'information sur les casiers judiciaires (ECRIS, article 25 du règlement européen 2019/816 du 17 avril 2019) ;
- l'ensemble des fichiers européens interconnectés (Bases de données Prüm, article 31 de la décision 2008/615/JAI du 23 juin 2008) ;
- les fichiers gérés par Europol (article 36 du règlement 2016/794 du 11 mai 2016) ;
- Fichier Central de la Criminalité Organisée (F2CO) et Fichier des Brigades Spécialisées ;
- les données contenues dans le fichier Enquêtes administratives liées à la sécurité publique (EASP, article R236-9 du code de la sécurité intérieure) intéressant la sûreté de l'État (article 118 de la loi du 6 janvier 1978) ;
- les données contenues dans le fichier Application relative à la prévention des atteintes à la sécurité publique (PASP, article R236-19 du code de la sécurité intérieure) intéressant la sûreté de l'État (article 118 de la loi du 6 janvier 1978) ; ;

2.1 – Données concernées par le TES

Ces données sont listées à l'article 2 du décret n°2016-1460 du 28 octobre 2016. Elles n'ont pas été modifiées par la réforme de 2021.

Quiconque demande une carte d'identité ou un passeport voit les données suivantes déposées dans le TES : tout l'état civil bien sûr, ainsi que la couleur des yeux, la taille, le domicile, la filiation, les images numérisées du visage, des empreintes digitales (des deux index, et si impossibilité du majeur et de l'annulaire) et de la signature, l'email ou le téléphone si la personne l'a donnée et a souhaité être informée par ce biais.

Il était possible, jusqu'en 2021 (la date dépend des départements), d'obtenir une carte d'identité (mais pas un passeport) en refusant la numérisation de ses empreintes digitales. Cette possibilité a été supprimée. **Toutefois, c'est toujours possible de limiter les dégâts en demandant à ce que la conservation des empreintes digitales soit limitée à 90 jours, au lieu de 15 ans** (article 4-3 I bis du décret n°55-1397 du 22 octobre 1955 et article 9 I bis du décret du 28 octobre 2016). Dans ce cas-là, il faut faire la demande en même temps que la demande de carte d'identité. Alors, les empreintes digitales sont versées dans le TES, puis elles sont copiées sur un document papier, et supprimées du TES (normalement). En théorie, tout le monde est informé de cette possibilité au moment de la demande de carte d'identité (article 10 I 3° du décret du 28 octobre 2016). On n'a pas trouvé à ce jour de formulaire de demande d'effacement des empreintes digitales dans ce cadre… Mais des retours d'expérience nous indiquent que les mairies disposent d'un formulaire prévu à cet effet, à remplir au moment de la demande de renouvellement.

Dans tous les cas, quand on effectue une telle demande que les empreintes ne soient conservées que 90 jours, il apparaît pertinent de faire une demande d'accès aux informations contenues dans le TES à l'issue de ces 90 jours (voir plus bas, et les modèles en annexe).

Enfin, il n'est pas possible de faire cette demande pour un passeport.

2.2 – Utilisation du fichier TES et personnes y ayant accès

Les personnes qui peuvent avoir accès à ce fichier sont listées aux articles 3 à 5 du décret du 28 octobre 2016. L'accès de toutes ces personnes se fait pour toutes les données, à l'exclusion de l'image numérisée des empreintes digitales.

Il s'agit des agents du ministère de l'intérieur qui sont affectés au service des passeports et de la carte d'identité, des agents de la préfecture et agents consulaires chargés de la délivrance des passeports et des cartes d'identité, ainsi que des agents des communes habilités pour recueillir les demandes et délivrer les titres. Ont été ajoutés en 2021 les agents de l'agence nationale des titres sécurisés (ANTS). Pour les passeports de mission (délivrés aux agents de l'État partant en mission à l'étranger), certains agents du ministère des armées peuvent aussi accéder aux données.

Mais ces personnes ne sont pas les seules à avoir accès à ce fichier. Certains policiers et militaires de la gendarmerie, ainsi que la DGSI, la DGSE et la DNRED (genre de super-douanes) peuvent y accéder pour prévenir et réprimer les atteintes aux intérêts fondamentaux de la nation, et c'est large (article L.811-3 du code de la sécurité intérieure et décision du Conseil constitutionnel n°2015-713 du 23 juillet 2015) :

- les atteintes à l'indépendance nationale, intégrité du territoire, défense nationale, intérêts majeurs de la politique étrangère, etc (trahison, espionnage, complot, mouvement insurrectionnel, atteinte au secret de la défense nationale…),
- les atteintes aux intérêts économiques, industriels et scientifiques majeurs,
- la prévention du terrorisme,
- la prévention des atteintes à la forme républicaine des institutions,
- la prévention de la reconstitution de groupements dissous,
- la prévention des violences collectives de nature à porter gravement atteinte à la paix publique (ce qui comprend l'ensemble des délits des articles 431-1 à 431-10 du code pénal, y compris l'entrave concertée à la liberté du travail par des menaces ou des violences, l'entrave concertée à l'exercice de la fonction d'enseignant par des menaces ou des violences, l'attroupement, la provocation à l'attroupement, l'organisation d'une manifestation interdite ou sans déclaration préalable, la dissimulation du visage en manifestation),
- la prévention de la criminalité et de la délinquance organisée (ce qui comprend les infractions prévues à l'article 706-73 du code pénal, dont le trafic de stupéfiants en bande organisée, le vol en bande organisée, les destructions ou détériorations en bande organisée, l'aide à l'entrée ou au séjour irrégulier d'un étranger en France en bande organisée),
- la prévention de la prolifération des armes de destruction massive.

De même, les agents français en relation avec INTERPOL et avec N-SIS II (le système d'information Schengen) peuvent accéder aux données.

Même si la reconnaissance faciale est interdite dans le TES (article 2 II du décret du 28 octobre 2016), aucune disposition n'interdit l'utilisation de la reconnaissance faciale à partir des photographies contenues dans le TES. Ces accès au fichier engendrent donc des **risques importants que la reconnaissance faciale soit utilisée** par le versement de ces photographies dans un autre fichier de police (par exemple le Traitement des antécédents judiciaires, TAJ), qui, lui, permet la reconnaissance faciale[6] ou sur réquisition de la photographie au cours d'une enquête.

6 La Quadrature du Net, *Le fichier TES, prémisse à la reconnaissance faciale de masse, arrive devant le Conseil d'État* https://www.laquadrature.net/2018/09/26/audience_tes/

Partie 15 : Annexes : Modèles de lettres

En général, la procédure pour obtenir la rectification ou l'effacement des données s'effectue en 2 étapes : il faut d'abord demander l'accès aux données, puis leur rectification ou leur effacement. Voici donc des lettres-types pour un grand nombre de fichiers. Il faut noter qu'ici, il n'y a pas certains fichiers : Le fichier judiciaire national automatisé des auteurs d'infractions terroristes, le fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes. En effet, quand on est présent dans ces fichiers on le sait, et les procédures d'effacement se font devant un juge (soit celui qui nous a condamné, soit celui qui mène l'instruction). En conséquence, il vaut mieux voir avec son avocat·e que se lancer dans la procédure seul·e.

Aussi, ces modèles sont pour chaque fichier : la lettre pour demander l'accès aux informations, puis la lettre pour demander leur suppression. Les lettres de recours en cas de refus ne sont pas dedans, car ça dépend plus de chaque cas, et souvent il vaut mieux faire appel à un·e avocat·e.

Quand on envoie la lettre pour demander l'accès aux informations ou la limitation du traitement, il faut toujours, sauf exception, l'envoyer en **recommandé avec accusé de réception**. De plus, il faut toujours joindre une **photocopie d'une pièce d'identité**.

Quand on envoie la lettre pour demander la rectification ou la suppression des informations, le mieux c'est de mentionner précisément quelles informations (en les désignant par exemple avec le n° de mention). Il faut toujours, là aussi, envoyer la lettre en recommandé avec accusé de réception et joindre une photocopie d'une pièce d'identité. Ajouter une photocopie des informations communiquées à l'étape précédente peut aider.

Aussi, pour de nombreux fichiers, notamment ceux classés « secret-défense » (donc les fichiers de renseignement) il y a de fortes chances d'obtenir un refus. Dans ce cas-là, si on veut continuer, il faut contester le refus de communication des données et demander l'effacement des données illégales devant la formation spécialisée du Conseil d'État, mais il faut vraiment l'aide d'un·e avocat·e !

Enfin, on ne peut pas assurer qu'effectuer toutes ces démarches n'énerve pas un peu les services de renseignement… peut-être le seul fait de demander à connaître les informations qui nous concernent peut provoquer la création d'une fiche à notre nom !

Dans cette nouvelle version (2024), on a considérablement diminué cette partie des modèles de lettres, pour conserver celles

fichiers concernés figure à l'article R841-2 du code de la sécurité intérieure, et parmi les fichiers qu'on a étudié, il s'agit de ceux-ci : Fichier de la DGSI, fichier de la DGSE, fichier SIREX, DOREMI, FSPRT, Fiches S du FPR, N-SIS II (Schengen), TRACFIN, BCR-DNRED, GESTEREXT, BIOPEX, LEGATO (fichier des membres de la Légion étrangère) et une partie de ACCReD.

L'article L773-8 du code de la justice administrative prévoit que la procédure appliquée au contentieux issu des décisions de la CNIL est la même que celle appliquée au contentieux issu des décisions de la CNCTR. En conséquence, voilà comment est organisée la justice classée « secret-défense » à la française :

Les membres de la formation spécialisée sont peu nombreux et habilités au secret de la défense nationale (article L773-2 du code de la justice administrative). En ce qui concerne le contradictoire, celui-ci est réduit à néant : pour protéger le secret-défense, le requérant (qui demande l'effacement des données) n'a ni accès aux données dont il demande la suppression, ni accès à l'argumentation de l'administration. Les audiences ne sont pas publiques, et lorsque l'administration s'exprime et présente sa défense, le requérant doit sortir de la salle.

Si le juge constate qu'il y a eu une illégalité, il informe le requérant qu'il y a eu une illégalité et qu'il a fait supprimer des données… sans pour autant donner aucune précision (article L773-8 du CJA).

Si le juge considère qu'aucune donnée contenue dans le fichier n'est illégale, ou que le requérant ne figure pas dans le fichier, il ne donne aucune précision au requérant (CÉ, 19 octobre 2016, n°396503).

Enfin, pour se donner une idée, le 19 octobre 2016 le Conseil d'État a rendu ses 11 premières décisions relatives à la demande d'effacement de données contenues dans les fichiers de renseignement : 5 portaient sur des fichiers de la DGSE, 5 sur des fichiers de la DPSD (qui est devenue depuis la DRSD, ministère des armées) et 1 sur des fichiers de la DRM (Direction du renseignement militaire, ministère des armées aussi, fichier remplacé par DOREMI depuis). Sur tout ça, le juge n'a trouvé aucune irrégularité, et n'a donc rien effacé… Ce qui n'a pas empêché beaucoup d'autres de continuer à demander ! Du coup, quelques mois plus tard, cette formation spécialisée du Conseil d'État a, pour la première fois, ordonné l'effacement des données contenues dans un de ces fichiers secrets, le SIREX (CÉ, 5 mai 2017, n°396669).

Enfin, les membres de la formation spécialisée du Conseil d'État se plaignaient, en 2020, de ne pas avoir l'expertise technique suffisante pour apprécier la légalité des données recueillies… et de n'avoir aucun personnel technique pour l'aider[86]. Elle est donc réduite à faire confiance à ce que lui racontent les services de renseignement.

Le 14 avril 2021, 17 personnes ont saisi la Cour européenne des droits de l'Homme pour contester cette procédure.

86 Rapport de la délégation parlementaire au renseignement pour l'année 2019-2020, enregistré à la présidence de l'Assemblée nationale et du Sénat le 11 juin 2020, pp, 106-107

De plus, les policiers et les gendarmes chargés du contrôle de l'identité des personnes et de la vérification de l'authenticité des cartes d'identité et des passeports peuvent accéder aux données contenues dans la puce du titre.

2.3 – Interconnexions du fichier TES

Depuis sa création en 2016, les interconnexions du fichier TES ont été élargies en 2019, 2021 et 2022. Dorénavant, il est en lien avec SGIN « Service de garantie de l'identité numérique » (qui remplace ALICEM, voir le décret n°2022-676 du 26 avril 2022), N-SIS II, DOCVERIF, LRPPN, LRPGN et le fichier SLTD d'INTERPOL… Autant dire que les recommandations successives de la CNIL, qui voulait que le TES ait le moins d'interconnexions possible, ont été superbement ignorées.

En 2019, une nouvelle interconnexion est créée : les données du fichier TES relatives au passeport, ainsi que les données relatives au titre de séjour d'une personne étrangère, peuvent être lues par l'application SGIN. Le but, c'est que chacun·e puisse se connecter à un service en ligne (public ou privé) à partir de son téléphone portable, et que son identité soit vérifiée par reconnaissance faciale (la comparaison entre la photo du passeport ou du titre de séjour et celle prise par l'appareil photo du téléphone portable au moment de la création du compte). Le fichage par SGIN est affiché comme seulement volontaire : si on ne crée pas un compte SGIN sur l'application (ou, peut-être, sur FranceConnect), a priori on ne rentre pas dans le fichier.

En cas de perte, vol ou invalidation de la carte d'identité ou du passeport, le numéro de ce document, le nom, le prénom, la date de naissance de son titulaire, ainsi que la date de délivrance du document, sont transmis au système d'informations Schengen (N-SIS II). Dans les mêmes cas de perte, vol ou invalidation du document, toutes ces données transmises à N-SIS II sont également transmises à INTERPOL pour être versées dans la Stolen and Lost Travel Documents Database (SLTD) (article 6 du décret du 28 octobre 2016 et délibération n°2021-022 du 11 février 2021 de la CNIL).

La réforme de 2021 a élargi les données transmises à INTERPOL (avant, ce n'était que le numéro du titre perdu ou volé, et la date de la perte ou du vol) et a ajouté deux nouvelles interconnexions :

- en cas de déclaration de vol de la carte d'identité ou du passeport, les informations contenues dans le TES sont transmises au logiciel de rédaction des procédures de la police nationale (LRPPN) et au logiciel de rédaction des procédures de la gendarmerie nationale (LRPGN). Alors, les données deviennent accessibles à l'ensemble des policiers et des gendarmes. Dans ce cas-là, la photographie est transmise à LRPPN et LRPGN mais elle ne doit pas y être enregistrée.
- un élargissement considérable de l'interconnexion avec le fichier national de contrôle de la validité des titres (fichier DOCVERIF). Dorénavant, le TES transmet à DOCVERIF le numéro de carte d'identité ou de passeport, la date de délivrance, le nom, le prénom, date et lieu de naissance du titulaire, ainsi que la mention de la validité ou de la non validité du document, ainsi que les raisons

de son caractère non valide et la date de son vol, perte, ou annulation. Le fichier DOCVERIF devient donc, de fait, un « fichier-miroir » du TES (sauf pour la photographie et les empreintes digitales qui ne sont pas transmises à DOCVERIF).

À côté de ces interconnexions, le Fichier des Personnes Recherchées (FPR) est consulté au moment de la demande d'une carte d'identité ou d'un passeport, pour vérifier qu'aucun élément ne s'oppose à sa délivrance (article 8 du décret n°2016-1460 du 28 octobre 2016). Ce qui explique parfois des délais de délivrance accrus.

2.4 – Durée de conservation des données

Les durées de conservation des données sont prévues par l'article 9 du décret n°2016-1460 du 28 octobre 2016.

Les données sont conservées 15 ans, que ce soit pour les cartes d'identité ou pour les passeports, à compter de la délivrance du titre. Si le titre n'a pas été délivré, le délai de 15 ans court à compter de l'enregistrement de la demande.

Ces durées sont différentes pour les anciennes cartes d'identité (grand format) : les données sont conservées 20 ans pour les majeurs et 15 ans pour les mineurs.

Toujours concernant les anciennes cartes d'identité, si celles-ci sont périmées au 1er janvier 2014, leurs données sont conservées 15 ans (même si elles ont été délivrées à des majeurs).

Pour les passeports délivrés à un mineur, la durée de conservation des données est de 10 ans.

Si le demandeur de la carte d'identité a demandé que ses empreintes digitales ne soient pas conservées au-delà de 90 jours au moment de sa demande, elles doivent être effacées à l'issue de ce délai (les empreintes sont alors copiées sur papier).

2.5 – Droits d'accès et de rectification

L'article 11 du décret n°2016-1460 du 28 octobre 2016 prévoit simplement que ces droits « s'exercent auprès de l'autorité de délivrance dans les conditions prévues respectivement aux articles 13,15,16 et 18 du règlement (UE) 2016/679 du 27 avril 2016 » !!! Autant dire que, au ministère de la justice, on a économisé de l'encre…

Pour les droits d'accès et de rectification, il faut donc s'adresser à la préfecture qui a délivré le passeport, ou à la mairie qui a délivré la carte d'identité.

3. DOCVERIF

Ce fichier a été créé par l'arrêté du 10 août 2016. Il est placé sous la responsabilité du ministère de l'intérieur, afin de faciliter la vérification de la validité des cartes d'identité et des passeports.

signalés, c'est à la CNIL. Pour les objets et véhicules perdus ou volés, il faut s'adresser à la Direction générale de la police nationale (Place Beauvau, 75800 PARIS CEDEX 08) ou à la Direction générale de la gendarmerie nationale (4 Rue Claude-Bernard, CS 60003, 92136 ISSY-LES-MOULINEAUX CEDEX) (article 8 alinéa 2 de l'arrêté du 7 juillet 2017).

- Système d'Information Schengen (N-SIS II) : Comme le FPR, une partie des informations est à demander à la CNIL, une autre partie au ministère de l'intérieur : Il y a un droit de communication direct auprès de la Direction centrale de la police judiciaire, ministère de l'Intérieur, Place Beauvau, 75800 PARIS Cedex 08 pour : l'état civil, le sexe, la nationalité, les signes physiques particuliers, la photographie et les motifs du signalement.
- Le système API-PNR France (Advance Passenger Information – Passenger Name Record) : Pour la plupart des données, il faut s'adresser directement au Directeur de l'Unité Information Passagers ou son adjoint : 11 Rue des Deux-Communes, 93558 MONTREUIL CEDEX. Pour le reste des données, il faut s'adresser à la CNIL (notamment le lien avec le FPR et N-SIS II).
- PASP : Il faut s'adresser à la fois à la Direction générale de la police nationale du ministère de l'intérieur et à la CNIL ;
- GIPASP : Il faut s'adresser à la fois à la Direction générale de la gendarmerie nationale du ministère de l'intérieur et à la CNIL ;
- EASP : Il faut s'adresser à la fois à la Direction générale de la police nationale du ministère de l'intérieur et à la CNIL.

2. La formation spécialisée du Conseil d'État, une justice classée « secret-défense »

Aux États-Unis ça existe depuis 1978 et le dispositif a été renforcé au cours des années 2000. La Cour FISA (Foreign Intelligence Surveillance Act) juge secrètement, les débats ne sont pas contradictoires, et elle autorise massivement la surveillance. Elle a reçu 33949 demandes de surveillance de la part des services de renseignement en 33 ans, et en a rejeté… 11. C'est ce tribunal qui a autorisé la surveillance globale mise en place par la NSA. En France, on n'en est pas là, mais le Conseil d'État a depuis quelques années sa formation spéciale pour juger secrètement.

Cette formation spéciale a été créée par la loi n°2015-912 du 24 juillet 2015 relative au renseignement. Elle est compétente pour 2 choses : d'une part pour le contentieux sur les décisions de la Commission nationale de contrôle des techniques de renseignement (CNCTR), à qui on s'adresse lorsqu'on soutient que les services de renseignement utilisent des techniques de surveillance illégales. D'autre part, et ce qui nous intéresse plus ici, pour le contentieux relatif aux données contenues dans les fichiers des services de renseignement, lorsqu'on considère que ces fichiers contiennent des informations illégales à notre égard, et que la CNIL n'en a pas ordonné l'effacement (article L841-2 du code de la sécurité intérieure). La liste des

- Fichier du système du contrôle automatique (radars routiers automatiques) : Il faut s'adresser au Centre national de traitement automatisé, CS 41101, 35911 RENNES Cedex 9 ;
- SINUS : Il faut s'adresser au Secrétariat général de la zone de défense de Paris, 1bis rue de Lutèce, 75004 PARIS (arrêté du 17 février 2010 du ministre de l'intérieur) ;
- Système d'information pour le suivi des victimes (SI-VIC) : Il faut s'adresser à la Direction générale de la santé, 14 avenue Duquesne, 75350 PARIS SP 07 (décret n°2018-175 du 9 mars 2018) ;
- Fichiers d'Interpol : Il faut s'adresser à la Commission de contrôle des fichiers d'Interpol, 200 quai Charles de Gaulle, 69006 LYON ;
- Pré-plainte en ligne : il faut s'adresser au commissariat ou à la gendarmerie sélectionné pour signer la plainte ;
- Fichier des appels à témoin : il faut s'adresser au commissariat ou à la gendarmerie qui a lancé l'appel à témoins ;
- SIVAC (Système d'information intermninistériel des victimes d'attentats et de catastrophes) : Il faut s'adresser au service d'aide aux victimes du secrétariat général du ministère de la justice.
- Fichier des personnes placées sous surveillance électronique, fichier des personnes placées sous surveillance électronique mobile, fichier des personnes placées sous bracelet anti-rapprochement : Il faut s'adresser à la direction de l'administration pénitentiaire ;
- SIAJ : Greffe du tribunal judiciaire où la demande d'aide juridictionnelle a été déposée ;
- RNIPP : Directions régionales de l'INSEE pour les personnes résidant en France, et direction générale de l'INSEE pour celles résidant à l'étranger (article 8 du décret n°83-103 du 22 janvier 1982).

1.3 – Fichiers pour lesquels les droits s'exercent auprès de la CNIL et du ministère de l'intérieur

Attention, pour 7 fichiers (FPR, API-PNR, N-SIS II, FoVES, PASP, GIPASP, EASP), la démarche auprès de la CNIL ne permet de demander l'accès qu'à certaines données. Pour les autres données, il faut s'adresser directement à l'institution qui gère le fichier (voir plus bas).

- Fichier des Personnes Recherchées (FPR) : Ça dépend, pour certaines informations (comme les Fiches S) il faut s'adresser à la CNIL, pour d'autres non. Pour certaines personnes, il leur a été notifié officiellement qu'elles ont fait l'objet d'une procédure qui les a inscrites dans le FPR (par exemple en cas de retrait de permis). Pour ces personnes, en ce qui concerne de nombreuses informations, le droit de communication et de rectification est direct, auprès de la Direction centrale de la police judiciaire, ministère de l'intérieur, Place Beauvau, 75800 PARIS Cedex 08.
- Fichier des Objets et Véhicules Signalés (FOVeS) : Comme le FPR, une partie des informations est à demander à la CNIL, une autre partie au ministère de l'intérieur : Pour les objets et véhicules

Jusqu'en 2021, DOCVERIF ne recevait des informations du TES que lorsqu'une carte d'identité ou un passeport était déclaré perdu ou volé. Dorénavant, le TES transmet automatiquement à DOCVERIF les données de tous les passeports et toutes les cartes d'identité (sauf la photographie et les empreintes digitales). DOCVERIF devient donc un fichier-miroir du TES.

Le champ des personnes autorisées à interroger le fichier pour constater la validité ou non d'un titre s'est élargi par l'arrêté du 28 avril 2022 : désormais les policiers municipaux, les garde-champêtres, les agents du SGIN (service de garantie de l'identité numérique) et les fournisseurs de moyen d'identification électronique ont le droit d'y accéder. L'identité des personnes qui consultent ces données est conservée trois ans. Sinon, évidemment les services de police et de gendarmerie, les administrations publiques, les agents de l'ANTS et les établissements de crédit y ont accès.

DOCVERIF, en cas de déclaration de vol ou de perte, transmet à INTERPOL le numéro du document perdu ou volé, et à N-SIS II (Schengen) de nombreuses informations (mais pas la photographie ni les empreintes digitales).

Les durées de conservation des données sont les mêmes que celles du TES.

Pour les demandes d'accès et de rectification des données, il faut s'adresser au secrétaire général du ministère de l'intérieur, direction de la modernisation et de l'action territoriale, Place Beauvau, 75800 PARIS CEDEX 08.

4. <u>Fichier National des Permis de Conduire (FNPC)</u>

Il a été créé en 1972. Les règles qui le concernent sont aux articles L225-1 et suivants et R225-1 et suivants du code de la route.

4.1 – Données concernées

L'article L225-1 du code de la route prévoit que tout un tas d'informations sont contenues dans ce fichier (identité, décisions de suppression, suspension du permis etc, retraits de points…).

Les personnes qui ont accès au fichier sont nombreuses : la police municipale pour vérifier l'authenticité du permis de conduire, la police et la gendarmerie lors des contrôles routiers, les compagnies d'assurance, les entreprises de transport public routier de voyageurs qui emploient des conducteurs… Y compris les autorités judiciaires et les OPJ dans le cadre d'une enquête de flagrance (article R225-4). Un décret du 24 mai 2018 a encore allongé la liste, avec la consultation par la police dans le cadre d'une enquête préliminaire, par les gardes champêtres pour constater les infractions qu'ils sont habilités à constater (article R225-5). C'est pourquoi lorsque quelqu'un·e donne une identité imaginaire et dit qu'il ou elle est titulaire du permis, la police ou le procureur se rend vite compte que l'identité est imaginaire.

Ce fichier est partagé au sein de l'Union européenne (plus la Norvège, le Royaume-Uni et la Suisse) à EUCARIS (European Car and Driving Licence Information System), créé par le traité *sur un*

système d'information européen concernant les véhicules et les permis de conduire du 29 juin 2000 et le règlement (UE) n°2018/858 du parlement européen et du conseil du 30 mai 2018. Ainsi, lorsqu'une personne titulaire d'un permis de conduire (quel que soit l'État de cette liste ayant délivré le permis) donne une identité imaginaire dans un de ces pays, il est possible que la police ou le procureur se rende également vite compte que cette identité est imaginaire.

Enfin, comme pour le fichier des Titres électroniques sécurisés (TES), certains policiers et militaires de la gendarmerie, ainsi que la DGSI, la DGSE et la DNRED (genre de super-douanes) peuvent y accéder pour prévenir et réprimer les atteintes aux intérêts fondamentaux de la nation (voir la longue liste dans la partie du TES : les atteintes aux intérêts fondamentaux de la nation désignent, par exemple et en vrac, les mouvements insurrectionnels, les intérêts économiques, industriels et scientifiques majeurs, les atteintes à la forme républicaine des institutions, la reconstitution de groupements dissous, les violences collectives de nature à porter gravement atteinte à la paix publique (dont l'entrave concertée à la liberté du travail par des menaces ou des violences, l'attroupement, la provocation à l'attroupement, l'organisation d'une manifestation interdite, la dissimulation du visage en manifestation), l'aide à l'entrée et au séjour des étrangers en bande organisée (article L811-3 du code de la sécurité intérieure et décision du Conseil constitutionnel n°2015-713 du 23 juillet 2015)), les destructions en bande organisée[7]. Ils peuvent aussi l'utiliser pour prévenir et réprimer les actes de terrorisme.

Il est relié à de nombreux fichiers, par exemple ADOC (fichier des contraventions).

4.2 – Durée de conservation des données

L'article L225-2 prévoit que les données relatives à des infractions sont conservées 10 ans sauf nouvelle infraction. Ce délai peut être plus long : l'interdiction définitive de passer le permis de conduire est inscrite dans le fichier jusqu'à ce que la personne ait atteint ses 80 ans. Ce délai peut aussi être plus court : en cas de retrait de points sur le permis, les points sont récupérés au bout de 2 ans sans nouvelle infraction, et l'information précisant qu'il y a eu retrait de point est effacée 1 an plus tard.

4.3 – Droits d'accès et de rectification

L'article L225-3 du code de la route renvoie au code des relations entre le public et l'administration (CRPA). Le relevé original des mentions apparaissant sur le permis de conduire peut donc être demandé à la préfecture. Il faut adresser une demande écrite à la préfecture, de préférence en lettre recommandée avec accusé de réception, accompagnée d'une photocopie du permis de conduire, d'une photocopie d'une pièce d'identité et d'une enveloppe affranchie au tarif recommandé avec accusé de réception.

La préfecture a 1 mois pour répondre (article R311-13 du CRPA). Si la préfecture n'a pas répondu au bout d'un mois, cela équivaut à un refus (article R311-12 du CRPA). Dans ce cas-là, on a 2 mois pour contester ce refus devant la Commission d'accès aux documents administratifs (article R311-15 du CRPA).

7 Infraction récemment mobilisée contre les intrusions écologistes sur des sites de Lafarge, en 2022 et 2023.

- SISPoPP (Système informatisé de suivi de politiques pénales prioritaires), lorsqu'il y a une enquête judiciaire, article 7 du décret n°2023-935 du 10 octobre 2023.

e – Fichiers à demander à la préfecture

2 fichiers suivants sont à demander à la préfecture.

- Le TES (Titres Électroniques Sécurisés) : En application de l'article 11 du décret n°2016-1460 du 28 octobre 2016, les droits d'accès et de rectification s'exercent directement auprès de la préfecture qui a délivré le passeport ou la carte nationale d'identité.
- Le Fichier National des Permis de Conduire (FNPC) : L'article L225-3 du code de la route renvoie au code des relations entre le public et l'administration (CRPA). Le relevé original des mentions apparaissant sur le permis de conduire peut donc être demandé à la préfecture. Il faut adresser une demande écrite à la préfecture de son domicile, de préférence en lettre recommandée avec accusé de réception, accompagnée d'une photocopie du permis de conduire, d'une photocopie d'une pièce d'identité et d'une enveloppe affranchie au tarif recommandé avec accusé de réception. La préfecture a 1 mois pour répondre (article R311-13 du CRPA). Si la préfecture n'a pas répondu au bout d'un mois, cela équivaut à un refus (article R311-12 du CRPA). Dans ce cas-là, on a 2 mois pour contester ce refus devant la Commission d'accès aux documents administratifs (article R311-15 du CRPA).

f – Fichiers à demander à d'autres institutions

Pour les 17 fichiers suivants, les démarches sont à adresser à d'autres institutions.

- Gestion nationale des personnes détenues en établissement pénitentiaire (GENESIS) : le droit d'accès et de rectification des données, s'exerce auprès du directeur de l'établissement pénitentiaire (article 57-9-24 du code de procédure pénale) ;
- MINOS : il faut s'adresser au greffe du tribunal de police saisi de la contestation de la contravention (arrêté du 22 février 2008) ;
- Dossier Unique de Personnalité (DUP) : Procédure effectuée par l'avocat·e auprès du Juge des enfants ;
- Fichier national automatisé des personnes incarcérées (FND) : Le droit d'accès et de rectification s'exerce, lorsque la personne est incarcérée, auprès du directeur de la taule ou auprès du directeur interrégional des services pénitentiaires. Lorsque la personne n'est pas incarcérée, il s'exerce auprès du procureur de la République du domicile de la personne concernée (article 2 de l'arrêté du 28 octobre 1996) ;
- Accès aux Dossiers des Contraventions (ADOC) : Il faut s'adresser au Centre national de traitement automatisé, CS 41101, 35911 RENNES Cedex 9. Attention, pour l'effacement après avoir été relaxé, il faut s'adresser au procureur de la République près le tribunal judiciaire de Rennes, 7 rue Pierre Abélard, CS73127, 35000 Rennes ;

- FAED pour les demandes de rectification et d'effacement des données ;
- FNAEG pour les demandes de rectification et d'effacement des données ;
- Dossier Pénal Numérique (DPN) : a priori, il faut s'adresser au procureur de la République en charge de la procédure (article R249-14 du code de procédure pénale).
- Répertoire des expertises (REDEX) : Le droit de communication des données s'exerce auprès du procureur de la République du domicile de la personne (article R53-21-10 du code de procédure pénale). Les droits de rectification et d'effacement s'exercent aussi auprès du procureur de la République (article R53-21-11). Pour les recours contre la décision du procureur, l'appel se forme auprès du JLD (articles R53-21-13 et suivants).
- Chaîne Applicative Supportant le Système d'Information Oriente Procédure pénale Et Enfants (CASSIOPÉE) : Le droit d'accès et de rectification des données s'exerce directement auprès du procureur de la République de notre domicile (article R15-33-66-10 du code de procédure pénale).
- Application des Peines, Probation et Insertion (APPI) : Le droit d'accès et de rectification des données s'exerce auprès du procureur de la République du tribunal qui a été saisi de la procédure, ou dans le ressort duquel est situé le SPIP chargé du suivi de la mesure (article R57-4-7 du code de procédure pénale).
- Fichier national automatisé des personnes incarcérées (FND) : Le droit d'accès et de rectification s'exerce, lorsque la personne est incarcérée, auprès du directeur de la taule ou auprès du directeur interrégional des services pénitentiaires. Lorsque la personne n'est pas incarcérée, il s'exerce auprès du procureur de la République du domicile de la personne concernée (article 2 de l'arrêté du 28 octobre 1996).
- Fichier judiciaire national automatisé des auteurs d'infractions terroristes (FIJAIT) : Quand on est fiché on le sait. Le droit de communication, de rectification et de suppression des données s'exerce auprès du procureur de la République près le Tribunal judiciaire dans le ressort duquel la personne réside (articles 706-25-12 du code de procédure pénale) ou auprès du juge d'instruction en cas d'instruction. En cas de refus, recours devant le JLD ou devant la chambre de l'instruction.
- Fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes (FIJAISV) : Quand on est fiché on le sait. La procédure est la même que pour le Fichier judiciaire national automatisé des auteurs d'infractions terroristes, mais en application des articles 706-53-9 et 706-53-10 du code de procédure pénale ;
- ANACRIM (article 230-23 du code de procédure pénale) ;
- MERCURE (article 230-23 du code de procédure pénale) ;
- BIE (Bureau informatisé des enquêtes) ;

Partie 2 : Fichiers de justice : Fichiers d'antécédents et principaux fichiers d'application des peines

Les fichiers rassemblés ici sont utilisés par l'institution judiciaire. Il s'agit d'abord du casier judiciaire, qui permet aux juges de savoir si une personne a déjà été condamnée auparavant, puis des principaux fichiers d'application des peines, utilisés par l'administration pénitentiaire.

Les fichiers secondaires sont décrits dans la partie 13.

1. Casier judiciaire national automatisé

Il a été créé au milieu du XIXe siècle. Le but, c'est de permettre aux flics, juges et autres de savoir à quoi une personne a été condamnée dans le passé. Les règles relatives au casier judiciaire sont aux articles 768 et suivants et R62 et suivants du code de procédure pénale. Il rassemble les condamnations pénales, mais aussi certaines condamnations commerciales et civiles (liquidation judiciaire, faillite personnelle…) et certaines décisions administratives. Il est organisé en 3 niveaux appelés « Bulletin » : B1, B2 et B3.

Selon le projet d'accord-cadre du Service des technologies et des systèmes d'information de la sécurité intérieure du 18 mai 2022[8], il y a 5,2 millions de personnes inscrites au casier judiciaire. Il en ressort aussi que le casier judiciaire national automatisé risque fort, à l'avenir, d'intégrer les photographies des personnes pour pouvoir effectuer des recherches par reconnaissance faciale au niveau européen et améliorer le fonctionnement de ECRIS et ECRIS-TCN (des fichiers de l'Union européenne relatifs au partage des antécédents judiciaires entre les différents Etats).

En application du règlement 2019/816 (créant ECRIS-TCN, concernant les ressortissants non européens) et de la directive 2019/884 (ECRIS, concernant les ressortissants européens), les différents États membres de l'Union européenne doivent pouvoir comparer les empreintes digitales des personnes condamnées à une peine privative de liberté d'au moins six mois, ou condamnées pour un délit punissable d'au moins douze mois. L'ordonnance n°2022-1524 du 7 décembre 2022 prévoit donc, en application de ces textes, que les empreintes des personnes condamnées sont versées au casier national judiciaire (article 771-2 du code de procédure pénale). Ainsi depuis fin 2022, toutes les empreintes des personnes condamnées figurent au casier judiciaire national.

De la même façon, sous impulsion européenne, le casier judiciaire national pourrait à terme intégrer une photographie du visage de la personne condamnée.

8 https://www.nextinpact.com/article/69249/le-fichier-empreintes-digitales-sera-interconnecte-avec-casier-judiciaire-13

1.1 – Bulletin n°1

a – Données concernées

Le bulletin n°1 rassemble toutes les informations contenues dans le casier : condamnations pénales, contraventions de la 5e classe (1500 euros d'amende), contraventions de la 1ère à la 4e classe lorsqu'elles entraînent une interdiction, une déchéance ou une incapacité, liquidation judiciaire, faillite personnelle, interdiction de gérer une entreprise, déchéance de l'autorité parentale, retrait de certains droits attachés à l'autorité parentale, arrêtés d'expulsion pris à l'encontre des étrangers, compositions pénales, dispenses de peine, grâces, réductions de peines, libérations conditionnelles, suspensions de peine.

Depuis décembre 2022, le casier contient aussi les empreintes digitales (cf. art. 777-3 du code de procédure pénale qui autorise l'interconnexion avec le fichier automatisé des empreintes digitales).

b – Utilisation du fichier

Il ne peut être consulté que par les juges, les procureurs et l'administration pénitentiaire.

c – Durée de conservation des données

Les condamnations pour contravention sont conservées 3 ans, tout comme les dispenses de peine, les mesures éducatives contre les mineurs (sauf nouvelle condamnation). Les liquidations judiciaires et autres sont conservées 5 ans.

Les condamnations prononcées pour des faits imprescriptibles (génocide et autres crimes contre l'humanité) ne sont jamais effacées du « B1 ».

Toutes les autres condamnations sont effacées au bout de 40 ans, sauf nouvelle condamnation.

d – Accès, rectification et effacement des données

L'article 777-2 du code de procédure pénale prévoit que quiconque peut demander la communication du Bulletin n°1 du casier judiciaire auprès du procureur de la République du Tribunal judiciaire qui est compétent sur son domicile. Il suffit pour cela de lui envoyer une lettre simple.

Le procureur convoque alors la personne à une audience et lui communique les données, sans lui en donner une copie. On peut venir avec un·e avocat·e.

De plus, quiconque de moins de 21 ans peut demander une suppression des mentions au B1. Au-delà de 21 ans, ce n'est plus possible.

1.2 – Bulletin n°2

a – Données concernées

Le bulletin n°2 rassemble toutes les informations du bulletin n°1 sauf les mesures éducatives à l'encontre des mineurs, les contraventions, les dispenses de peine, les compositions pénales, et les condamnations avec sursis lorsque le sursis est expiré et n'a pas été révoqué (article 775 du code de procédure pénale). Il peut être consulté par les administrations (préfectures, ministère des armées…).

En cas de refus de la DGGN ou de la DGPN, il est possible d'effectuer un recours devant la CNIL, ou devant le tribunal administratif de Paris.

c – Fichiers à demander au ministère de la justice

Pour 4 fichiers et le statut de DPS, les droits s'exercent auprès du ministère de la justice (toujours par LR/AR, avec une copie de la pièce d'identité, sauf pour le B3).

- Le Bulletin n°3 du casier judiciaire (B3) : Pour l'accès aux données conservées dans le Bulletin n°3 (B3), il suffit de se connecter ici, https://www.cjn.justice.gouv.fr . Pour la suppression des données, c'est comme le B2.
- Répertoire des Détenus Particulièrement Signalés (DPS) : La procédure est effectuée auprès du Ministre de la justice, puis du Tribunal administratif, avec un·e avocat·e.
- Données recueillies par l'Agence nationale des techniques d'enquêtes numériques judiciaires prévue à l'article 230-45 du code de procédure pénale et par la plate-forme nationale des interceptions judiciaires prévue à l'article 1er du décret n°2017-614 du 24 avril 2017 (article R40-55 du code de procédure pénale et ordonnance n°2018-1125 du 12 décembre 2018 ayant instauré un droit d'accès direct à tous les fichiers sauf ceux de renseignement) ;
- DataJust : auprès du ministère de la justice (décret n°2020-356 du 27 mars 2020) ;
- SISPoPP (Système informatisé de suivi de politiques pénales prioritaires), en l'absence d'enquête judiciaire, article 7 du décret n°2023-935 du 10 octobre 2023.

d – Fichiers à demander au procureur de la République

Pour 16 fichiers, les droits s'exercent auprès du procureur de la République, toujours par LR/AR. Suivant la situation, c'est soit le procureur du domicile de la personne qui fait la demande, soit le procureur qui s'est occupé de la procédure.

- Le Bulletin n°1 du casier judiciaire (B1) : L'article 777-2 du code de procédure pénale prévoit que quiconque peut demander la communication du Bulletin n°1 du casier judiciaire auprès du procureur de la République du Tribunal judiciaire qui est compétent sur son domicile. Il suffit pour cela de lui envoyer une lettre simple. Le procureur convoque alors la personne à une audience et lui communique les données, sans lui en donner une copie. On peut venir avec un·e avocat·e. De plus, quiconque de moins de 21 ans peut demander une suppression des mentions au B1. Au-delà de 21 ans, ce n'est plus possible. La suppression des données du B1 entraîne celle du B2 et du B3.
- Le Bulletin n°2 du casier judiciaire (B2) : Pour la demande de suppression, il faut s'adresser à un juge (article 775-1 du code de procédure pénale). Pour savoir à quel juge s'adresser, c'est l'article 702-1. Il vaut mieux l'aide d'un·e avocat·e. La suppression des données du B2 entraîne celle du B3.
- Numérisation des procédures pénales (NPP) : il faut s'adresser au procureur de la République en charge de la procédure (arrêté du 16 janvier 2008).

- Outil et Système d'Informations Relatives aux Infractions à la législation sur les stupéfiants (OSIRIS, arrêté du 12 janvier 2016 et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) ;
- Lecture Automatisée des Plaques d'Immatriculation (LAPI, arrêté du 18 mai 2009 et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) ;
- SIPol (Système d'information de la police nationale) ;
- Fichier des interdictions du territoire ;
- Images des caméras individuelles portées par les fonctionnaires de police et les militaires de la gendarmerie ;
- THESEE (plaintes en ligne).

b – Fichiers à demander à la Direction générale de la police nationale et à la Direction générale de la gendarmerie nationale

Les 9 fichiers suivants sont à demander à la DGGN ou à la DGPN, ou aux deux à la fois.

- Fichiers d'analyse sérielle prévus aux articles 230-12 à 230-18 du code de procédure pénale, dont SALVAC et les bases d'analyse sérielle de la police judiciaire : Il faut les demander à la DGPN ET à la DGGN (articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) ;
- Fichier Gestion des sollicitations et des interventions, à demander à la DGGN (articles 236-31 et suivants du code de la sécurité intérieure et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) ;
- Fichier Sécurisation des interventions et demandes particulières de protection (SIDPP), à demander à la DGGN (articles 236-38 et suivants du code de la sécurité intérieure et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) ;
- Fichier National des Interdits de Stade (FNIS), à demander à la DGPN (arrêté du 28 août 2007 et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) ;
- Nouvelle Main Courante Informatisée (N-MCI) : Il faut demander l'accès aux données à la DGPN (arrêté du 22 juin 2011 modifié par l'arrêté du 9 août 2016 et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) ;
- GendNotes : Il faut demander l'accès aux données à la DGGN (décret n°2020-151 du 20 février 2020) ;
- FNOS : Il faut demander l'accès à la DGPN et à la DGGN, et à la Direction générale des douanes et des droits indirects ;
- PEGASE II (Pilotage des événements, gestion de l'activité et sécurisation des équipages) : Il faut s'adresser à la la direction générale de la police nationale (article R236-60 du code de la sécurité intérieure) ;
- FOJ : Il faut demander l'accès à la DGPN, et à la DGGN, et à la Préfecture de police de Paris.

Au moment de la condamnation, le juge peut aussi décider que celle-ci ne sera pas inscrite au « B2 ».

b – Utilisation du fichier

Peuvent avoir accès au « B2 » certaines administrations (police des étrangers, juge commis à la surveillance du registre du commerce, collectivités publiques locales, contrôle de la profession de marin, OFPRA, CNDA, AMF, INPI), certains employeurs privés (SNCF, SNCF Réseau, SNCF Mobilités, EDF, GDF, Banque de France), ou intervenant dans le domaine de l'enfance (animateur, éducateur spécialisé, surveillant…) ou de la sécurité (agent de sécurité, transport de fonds, maton, flic, militaire…) ou autre (chauffeur de taxi, conducteur de bus, contrôleur, moniteur d'auto-école, agent immobilier, avocat, notaire). Cet accès se fait toujours pour des motifs précis (par exemple lors de l'accès à un emploi en contact avec des mineurs, travaux publics, marchés publics, poursuites disciplinaires, autorisation de port d'arme à des fins professionnelles, transport de matières nucléaires), le Conseil de l'ordre des médecins en cas de poursuites disciplinaires, commissions d'inscription sur la liste de commissaire aux comptes, administration pénitentiaire pour le recrutement et l'accès à la détention… L'ensemble est à l'article R79 du code de procédure pénale.

Depuis le décret n°2023-1388 du 29 décembre 2023, le bulletin n°2 du casier judiciaire est également consulté lors d'une recherche sur ACCReD (le fichier qui sert aux enquêtes effectuées lorsqu'une personne postule à un emploi, ou veut être bénévole aux JO).

c – Durée de conservation des données

Les condamnations à une peine de jour-amende sont conservées 3 ans. La liquidation judiciaire et la faillite personnelle, la condamnation à un stage de citoyenneté, à des TIG, à une interdiction de permis, à une confiscation d'un véhicule ou d'une arme sont conservées 5 ans (sauf si ces interdictions durent plus longtemps, alors elles sont conservées pour leur durée).

Toutes les autres sont effacées au bout de 40 ans, sauf nouvelle condamnation.

d – Accès, rectification et effacement des données

Pour l'accès au « B2 », c'est comme pour le « B1 » : il faut s'adresser au procureur, qui donne accès au « B1 » donc au « B2 » (le « B2 » étant une sorte d'extrait du « B1 »). Pour l'effacement du « B2 » avant la fin du délai de 40 ans, il faut s'adresser à un juge (article 775-1 du code de procédure pénale). Pour savoir à quel juge s'adresser, c'est l'article 702-1. Il vaut mieux l'aide d'un·e avocat·e.

Cet effacement des données du « B2 » est obtenu automatiquement 20 ans après la fin de la peine, s'il n'y a pas eu de nouvelle condamnation entre-temps, si la personne le demande (article 775-2).

1.3 – Bulletin n°3

a – Données concernées

Le bulletin n°3 concerne les condamnations pour crime ou pour délit à un emprisonnement de plus de 2 ans ferme, ou dont le sursis a été révoqué, les interdictions, les déchéances, le suivi socio-judiciaire, l'interdiction d'exercer une profession en contact avec les mineurs.

Le juge peut décider d'inscrire au bulletin n°3 les peines d'emprisonnement.

b – Utilisation du fichier

Le bulletin n°3 ne peut être communiqué qu'à la personne elle-même. L'employeur par exemple n'a jamais le droit de consulter le casier à l'insu d'une personne. Il n'y a pas de liste d'employeurs qui peuvent, ou non, demander une copie du « B3 » à l'embauche. Beaucoup le font, par exemple pour un poste de caissier, l'employeur considérant qu'une condamnation antérieure pour vol serait un obstacle…

c – Durée de conservation des données

Sauf amnistie ou réhabilitation judiciaire avec retrait du casier judiciaire, les données sont effacées au bout de 40 ans, sauf nouvelle condamnation.

d – Accès, rectification et effacement des données

Pour l'accès aux données conservées dans le Bulletin n°3 (B3), il suffit de se connecter ici, https://casier-judiciaire.justice.gouv.fr/pages/accueil.xhtml . C'est possible de faire la demande sans utiliser FRANCECONNECT.

Pour la demande de suppression avant la fin du délai de 40 ans, il faut s'adresser à un juge (article 777-1 du code de procédure pénale). Pour savoir à quel juge s'adresser, c'est l'article 702-1. Il vaut mieux l'aide d'un·e avocat·e.

2. Dossier Unique de Personnalité (DUP)

Il a été créé par l'article 28 de la loi n°2011-939 du 10 août 2011 et apparaît à l'article 5-2 de l'ordonnance n°45-174 du 2 février 1945. Il est transféré aux articles L322-8 et suivants du nouveau code de la justice pénale des mineurs. Il est précisé par le décret n°2014-472 du 9 mai 2014, transféré aux articles R322-11 du code de la justice pénale des mineurs.

Il concerne toutes les personnes mineures qui sont présentées à un juge des enfants.

2.1 – Données concernées

Les données recueillies sont l'ensemble des éléments relatifs à la personnalité du ou de la mineur·e, ce qui est très large : rapports de suivi des mesures éducatives, santé, expertises psychiatriques et psychologiques, examens médicaux, fréquentation scolaire, formation, antécédents et parcours judiciaire, situation matérielle et sociale de sa famille, conditions de vie, alternatives aux poursuites, composition pénale.

Paris (Service régional de police des transports – Brigade des réseaux ferrés d'Île-de-France – Cellule tags) ;

- Fichiers d'Euopol.

Pour contester les résultats obtenus par l'exercice du droit d'accès indirect auprès de la CNIL, il faut faire un recours devant le tribunal administratif de Paris.

Cependant, pour certains fichiers (par exemple les fichiers de la DGSI et de la DGSE, SIREX, FSPRT, Fiches S du FPR, …), le recours s'effectue devant une formation spécialisée du Conseil d'État – voir le II.

1.2 – Le droit d'accès, de rectification et d'effacement auprès de l'autorité chargée de la gestion des fichiers

Pour 29 fichiers, il faut s'adresser directement à l'administration qui gère le fichier pour avoir accès aux informations.

a – Fichiers à demander au ministère de l'intérieur

Les informations contenues dans 15 fichiers doivent être demandées au ministère de l'intérieur (toujours par LR/AR, avec une copie de la pièce d'identité) :

- DOCVERIF (article 11 de l'arrêté du 10 août 2016) ;
- Le Fichier Automatisé des Empreintes Digitales (FAED) : Il faut demander l'accès aux données au ministère de l'intérieur (article 6 du décret n°87-249 du 8 avril 1987) ;
- Le Fichier National Automatisé des Empreintes Génétiques (FNAEG) : Il faut demander l'accès aux données au ministère de l'intérieur (article R53-14-2 du code de procédure pénale) ;
- Le Traitement des Antécédents judiciaires (TAJ) : Il faut demander l'accès aux données au ministère de l'intérieur (article R40-33 II du code de procédure pénale) ;
- LRPPN : Il faut demander l'accès aux données au ministère de l'intérieur (décret n°2011-110 du 27 janvier 2011 et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) ;
- LRPGN : Il faut demander l'accès aux données au ministère de l'intérieur (décret 2011-111 du 27 janvier 2011 et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) ;
- DPIO : Il faut demander l'accès aux données au ministère de l'intérieur (décret n°2014-187 du 20 février 2014 et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) ;
- LUPIN : Il faut demander l'accès aux données au ministère de l'intérieur (arrêté du 15 octobre 2014 et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) ;
- Informatisation de la gestion des gardes à vue (iGAV, article R15-33-82 du code de procédure pénale mais articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) ;

en demander la rectification ou l'effacement, à chaque fois avec la copie de sa pièce d'identité. Un modèle de lettre est en pièce-jointe.

Il s'agit de ces 20 fichiers :

- European Criminal Records Information System / Système européen d'information sur les casiers judiciaires (ECRIS, article 25 du règlement européen 2019/816 du 17 avril 2019) ;
- l'ensemble des fichiers européens interconnectés (Bases de données Prüm, article 31 de la décision 2008/615/JAI du 23 juin 2008) ;
- N-SIS II (volet national du fichier Schengen) ;
- Fichier Central de la Criminalité Organisée (F2CO) et Fichier des Brigades Spécialisées ;
- Conservation, gestion et exploitation électroniques des documents des services de renseignement territorial, article R236-51 du code de la sécurité intérieure ;
- CRISTINA, décret du 27 juin 2008 et article R841-2 1° du code de la sécurité intérieure ;
- Gestion du terrorisme et des extrémismes à potentialité violente (GESTEREXT, décret n°2017-1218 du 2 août 2017 et article R841-2 10° du code de la sécurité intérieure) ;
- Fichier des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT, décret n°2015-252 du 4 mars 2015 et article R841-2 5° du code de la sécurité intérieure) ;
- Fichier de suivi des personnes placées sous main de justice pour la prévention des atteintes à la sécurité pénitentiaire et à la sécurité publique (CAR, décret n°2015-1465 du 10 novembre 2015) ;
- Fichier du renseignement pénitentiaire (qui a remplacé CAR), décret n°2023-795 du 18 août 2023 ;
- ASTREE, décret n°2017-154 du 8 février 2017 ;
- BIOPEX, décret n°2017-1231 du 4 août 2017 et article R841-2 11° ;
- Fichier d'informations nominatives de la DGSE, article R841-2 2° du code de la sécurité intérieure et article 1 2° du décret n°2007-914 du 15 mai 2007 ;
- Fichier de la DGSE, article 1 6° du décret n°2007-914 du 15 mai 2007 ;
- DOREMI, article R841-2 4° du code de la sécurité intérieure et article 1 4° du décret n°2007-914 du 15 mai 2007 ;
- Fichier des personnes étrangères de la Direction du renseignement militaire, article 1 8° du décret n°2007-914 du 15 mai 2007 ;
- SIRCID, article R841-2 3° du code de la sécurité intérieure ;
- BCR-DNRED, article R841-2 9° du code de la sécurité intérieure ;
- Outil de Centralisation et de Traitement Opérationnel des Procédures et des Utilisateurs de Signatures (OCTOPUS) de la Direction de police urbaine de proximité de la Préfecture de police de

Ce fichier est en lien avec CASSIOPÉE et peut être consulté via le logiciel WINEURS.

Par ailleurs, l'objet du fichier (réunir les données recueillies relatives à la personnalité du mineur au cours d'une procédure pénale) a pour conséquence que ses données sont de facto également présentes dans le Dossier pénal numérique (DPN), qui concerne toutes les personnes, y compris les majeurs, faisant l'objet d'une procédure pénale.

2.2 – Utilisation du DUP

Le DUP ne peut être utilisé que dans les procédures pénales (et non dans les procédures d'assistance éducative).

Ont accès au fichier : les avocat·es, la protection judiciaire de la jeunesse, les juges d'instruction et les juges des enfants (pas les policiers), les personnels de la protection judiciaire de la jeunesse, les personnels de l'association qui suit le mineur, ainsi que le mineur·e lui-même s'il est devenu majeur et s'il n'a pas d'avocat.

Le psychologue désigné en tant qu'expert dans le cadre d'une mesure judiciaire concernant le mineur peut aussi être autorisé à avoir accès au DUP par le juge des enfants.

2.3 – Conservation des données

Les données sont conservées jusqu'à la majorité du ou de la mineur·e. Cependant, si il y a encore une procédure ouverte contre lui au moment où il atteint 18 ans, les données sont conservées jusqu'au jugement ou jusqu'à ce que la peine ait été exécutée.

2.4 – Droit de communication, de rectification et d'effacement

Avant l'ordonnance du 11 septembre 2019 qui a créé le code de la justice pénale des mineurs, il s'agissait surtout d'un droit de consultation : le juge des enfants pouvait autoriser l'avocat à transmettre le dossier au mineur·e lui-même, à ses parents ou à son tuteur (article 5-2 de l'ordonnance du 2 février 1945, qui a été supprimée entièrement).

Aujourd'hui cela a disparu du code de la justice pénale des mineurs. À la place, la personne mineure n'a accès aux données que lorsqu'elle est devenue majeure et à la condition qu'elle n'ait pas d'avocat, et ses parents ne peuvent plus du tout avoir accès aux données (article L322-10 du code de la justice pénale des mineurs qui en vigueur depuis le 1er octobre 2020).

De plus, aucun droit de rectification et d'effacement n'est prévu. Peut-être un décret va être publié pour remplacer celui du 9 mars 2014, et mettre en place une procédure pour les droits de rectification et d'effacement des données du Dossier Unique de Personnalité.

3. GENESIS

Gestion nationale des personnes détenues en établissement pénitentiaire (GENESIS) a été créé par le décret n°2014-558 du 30 mai 2014. Il remplace GIDE (Gestion Informatisée des Détenus en Établissement) depuis le 1er janvier 2017. Il a été entièrement refondé par le décret n° 2022-479 du 30 mars 2022.

3.1 – Données concernées

Le but est l'exécution des peines, la gestion des détenus, la sécurité des matons, la gestion des formalités d'écrou, la prévention des comportements à risques, la tenue de la commission pluridisciplinaire, la gestion des audiences, des requêtes, des rendez-vous, du courrier, de l'argent des détenus, des fouilles, de l'isolement, la réinsertion, les activités socioculturelles… Au final, il s'agit de ficher tous les détenus de la manière la plus complète, et pas seulement : Il permet aussi de « r*ecueillir des informations permettant la prévention des actes susceptibles de porter atteinte à la sécurité publique et à la sécurité des établissements et des services pénitentiaires, mais aussi d'assurer la surveillance des personnes détenues, des groupes ou organisations et phénomènes précurseurs de menaces*[9] ». Donc toute personne qui serait soupçonnée de porter atteinte à la sécurité des taules est susceptible d'être fichée dans GENESIS.

Les données concernées sont innombrables : nom, prénom, nom d'usage, sexe, numéro d'écrou, date et lieu de naissance, nationalité, numéro de pièce d'identité, photographie numérisée, filiation, situation familiale, adresse avant l'incarcération, lieux d'assignation à résidence, nom et adresse de la personne qui reçoit le détenu en permission, niveau d'études, langues parlées, lieu de scolarité, test lecture population pénale, profession, formation professionnelle, type de contrat de travail avant la détention… Ainsi que la condamnation, les réductions de peine, la période de sûreté, les condamnations pénales sans incarcération, l'inscription ou non au FNAEG, au FIJAIS, les interdictions de séjour et de droits civiques, civils et de famille, le fichage au DPS, plein d'infos de la commission pluridisciplinaire (dangerosité, vulnérabilité, prévention du suicide, SMPR et UMD antérieurement, hospitalisation d'office antérieure, suivi somatique, régime alimentaire, grève de la faim, fumeur, aptitude au sport et au travail, conseiller SPIP), risques de suicide (antécédents familiaux, deuil d'un·e proche, situation irrégulière, rupture conjugale, maltraitance parentale, victime d'abus physique ou sexuel, addictions, automutilation…), dangerosité (condamnation pour viol, agression sexuelle, violences graves aux personnes, torture, barbarie, assassinat, meurtre, criminalité organisée, terrorisme), vulnérabilité (profession ciblée en détention : flic, juge, maton, politique, affaire médiatisée, victime de violence en détention), soutien financier extérieur, ensemble des décisions du directeur de la taule concernant le détenu, historique des décisions d'affectation en cellule, fouille, tous les rendez-vous/entretiens/convocations, tous les expéditeurs et destinataires de courriers postaux, les

9 Délibération n°2013-405 du 19 décembre 2013 de la CNIL *portant avis sur un projet de décret portant création d'un traitement de données à caractère personnel relatif à la gestion nationale des personnes détenues en établissement pénitentiaire dénommé GENESIS (demande d'avis n° 13032517)*

Partie 14 : Récapitulatif du droit d'accès, de rectification et d'effacement

La loi informatiques et libertés de 1978, la directive « police justice » n°2016/680 du 27 avril 2016, et le règlement général sur la protection des données n°2016/679 du 27 avril 2016 prévoient que les personnes concernées disposent d'un droit d'accès aux informations les concernant. Pour certaines informations, ce droit existe à peu près – encore faut-il savoir qu'une institution a rassemblé ces informations et les conserve, ce qui est l'objet de ce dossier. Il est aussi possible de demander leur rectification et leur effacement (ce qui est toujours un peu plus compliqué). **Surtout, le droit européen a introduit une autre possibilité, mal nommée « limitation du traitement »** : il s'agit ici, pour une personne qui souhaite pouvoir utiliser ses données personnelles devant un tribunal, de demander à ce qu'elles soient conservées, gelées (la personne n'y a donc pas accès directement, mais au moins elles ne sont pas effacées et pourront être utilisées).

Ces procédures existent même pour les fichiers classés « *secret* » et « *très secret* » (l'ancien « *confidentiel défense* »)… mais de là à réussir à les mettre en œuvre, et à obtenir véritablement l'accès ou la suppression des données, c'est une autre affaire !

Voici donc d'abord le récapitulatif des institutions à qui s'adresser pour l'accès et la suppression des données (I). Pour de nombreux fichiers, en cas de refus, la contestation du refus se fait par un recours classique, devant un juge. Par contre, pour de nombreux autres fichiers, classés « secret-défense », le recours se fait devant une juridiction secrète, dont personne n'a accès aux jugements… même pas la personne qui a fait un recours ! On la verra donc plus bas (II).

1. Récapitulatif des institutions à qui s'adresser pour le droit d'accès, de rectification et de suppression des données

Pour exercer son droit d'accès, de rectification et de suppression des informations, ça serait trop simple de n'avoir à demander qu'à une personne. Voilà donc un petit récapitulatif pour s'y retrouver : sur tous les fichiers qu'on a vus, pour 20 d'entre eux il faut s'adresser à la CNIL et pour 37 autres il faut s'adresser à d'autres institutions. Pour 4 d'entre eux, il faut s'adresser à la CNIL et au ministère de l'intérieur.

1.1 – Droit d'accès via la CNIL

Pour les fichiers suivants, le droit d'accès s'effectue auprès de la CNIL. Il faut envoyer un courrier en lettre recommandée avec avis de réception à la CNIL (Commission Nationale Informatique et Libertés, 3 Place de Fontenoy, TSA 80715, 75334 PARIS CEDEX 07) pour demander un accès aux données, puis pour

Il est possible de demander l'accès et la rectification des données concernées auprès du ministre de la justice, 13 Place Vendôme, 75042 PARIS cedex 01.

procédures disciplinaires, l'application des peines, la liste des personnes ayant un permis de parloir, nom des juges ayant rendu les décisions, des avocats aussi, des intervenants extérieurs en détention… (article R57-9-20).

Les empreintes digitales prises lors de l'incarcération ne sont pas conservées dans GENESIS, mais dans le FAED (article 3 4° du décret n°87-249 du 8 avril 1987).

3.2 – Utilisation de GENESIS

Les données sont accessibles à l'administration pénitentiaire et à certains matons ainsi qu'aux greffiers et juges, aux membres de la commission pluridisciplinaire, aux membres de la commission d'application des peines, aux SPIP, à la protection judiciaire de la jeunesse, aux agents de l'éducation nationale intervenant en détention, à certains personnels privés (intervenants sportifs, personnel d'entretien, personnel de la cantine…).

Elles sont aussi accessibles aux personnels des UCSA, SMPR, UHSI, UHSA, mais aussi aux préfets, aux avocats, et même aux maires (seulement dans le cadre des modifications d'état civil, et seulement les données relatives à l'identité et au lieu d'incarcération), aux flics quand il y a une permission de sortie ou pour prendre l'ADN, aux juridictions étrangères, au service national du casier judiciaire et même à Pôle Emploi et aux Missions locales (qui ont accès seulement à l'état civil, au lieu de détention, aux dates de sortie, de permission ou d'aménagement de peine), aux douanes, à la CAF (pour certaines informations aussi), à la sécurité sociale, aux institutions de retraite et aux organismes de formation (idem).

3.3 – Conservation des données

Les données sont conservées 2 ans à compter de la levée d'écrou (article R240-4 du code pénitentiaire). Elles sont gelées en cas de contentieux avec l'administration pénitentiaire, jusqu'à l'extinction du recours.

3.4 – Droit d'accès, de rectification et d'effacement

En ce qui concerne le droit d'accès, de rectification et d'effacement des données, il s'exerce (selon l'article R240-7) directement auprès du directeur de la prison.

Par contre, ce même directeur a des pouvoirs importants (article R240-7). Lorsqu'on demande à exercer ces droits, le directeur peut refuser au détenu l'accès aux données concernant les dates prévues pour les transferts et les extractions, le régime de détention, les locaux de la taule, et les mouvements de la personne en détention.

Lorsqu'il oppose un tel refus, le directeur de la taule doit fonder son refus sur les motifs listés à l'article 107 II, 2° et 3°, et III de la loi du 6 janvier 1978 (par exemple éviter de nuire à l'exécution des sanctions pénales, protéger la sécurité publique, protéger la sécurité nationale, protéger les droits et libertés d'autrui). En ce cas, le directeur peut refuser de transmettre ces informations.

En cas de refus de transmettre ces informations, le détenu peut faire un recours à la CNIL (article 108 de la loi du 6 janvier 1978 et article R240-7 du code pénitentiaire). Cependant la loi a tout prévu : le directeur de la prison peut même refuser d'informer la personne de son refus de rectification ou d'effacement des données (article 107 II 3° de la loi du 6 janvier 1978) ! En conséquence, ça devient compliqué de saisir la CNIL pour contester une décision dont on n'a même pas connaissance…

4. Répertoire des Détenus Particulièrement Signalés (DPS)

Sa création est permise par l'article D276-1 du code de procédure pénale. Le Répertoire DPS existe depuis 1967, puis a été développé surtout par des circulaires : 2 en 1970, puis 1971, 1975, 2 circulaires du 19 mai 1980, 18 décembre 2007, 18 septembre 2012, 15 octobre 2012, 8 novembre 2013, 19 janvier 2015, et la dernière 11 janvier 2022.

Ça concerne les détenu·es, alors l'État joue sur les mots : il s'agit d'un répertoire, non d'un fichier, et la CNIL n'a jamais eu son mot à dire dessus.

Il vise à appliquer un régime spécial à certains détenus considérés comme dangereux. Il s'agit de renforcer la surveillance : contrôle d'œilleton systématique (ce qui entraîne un réveil toutes les 2 heures : bruit de l'œilleton et lumière allumée), consultations médicales menotté·e et sous la surveillance des matons, ceinture abdominale et « chaîne de conduite » pendant les déplacements, etc (voir le point 4.2 de la circulaire du 11 janvier 2022).

Selon l'OIP, en 2014, il y avait environ 300 personnes concernées par ce régime d'exception en prison[10]. Au 31 août 2018, il y avait 274 DPS.

Depuis la création du code pénitentiaire (par ordonnance n°2022-478 du 30 mars 2022), c'est l'article D223-11 de ce code qui encadre l'inscription et la radiation des personnes, par le ministre de la justice.

4.1 – Personnes concernées

Les personnes concernées sont les détenu·es qui remplissent au moins l'un des critères suivants (point 1.1 de la circulaire du 11 janvier 2022) :

- Appartenant à la criminalité organisée locale, régionale, nationale ou internationale, ou aux mouvances terroristes, appartenance établie par la situation pénale, par un signalement des autorités judiciaires et administratives ou des forces de sécurité intérieure,
- Signalées ou ayant été signalées pour une évasion réussie, tentée ou projetée,
- Susceptibles de mobiliser par tout moyen, un soutien humain, logistique ou financier extérieur en vue de s'évader et/ou de causer un trouble grave au bon ordre de l'établissement,

10 https://oip.org/analyse/detenus-particulierement-signales-surveillance-permanente-et-contrainte-maximale/

GIDE (Gestion Informatisée des Détenus en Établissement), qui avait été opportunément créé en juillet 2011).

Dorénavant, CEL n'existe donc plus en tant que tel. Le GIDE non plus, d'ailleurs : il a été remplacé par GENESIS.

18. Système d'information de l'aide juridictionnelle (SIAJ)

Il a été créé par l'arrêté du 19 mars 2021 et est mis en œuvre par le ministère de la justice. Il sert au traitement des demandes d'aide juridictionnelle, en particulier lorsqu'elles sont déposées par voie dématérialisée. Les informations collectées sont celles relatives à la demande d'aide juridictionnelle. Les informations sont conservées 5 ans et 2 mois à compter de la date de la décision sur la demande d'aide juridictionnelle.

L'accès aux informations se fait soit sur le portail internet qui permet de déposer une demande d'aide juridictionnelle ou au greffe du tribunal où la demande a été déposée.

19. DataJust

Il a été créé par le décret n°2020-356 du 27 mars 2020, en pleine période de confinement et d'état d'urgence sanitaire. Il permet de rassembler l'ensemble des arrêts des cours d'appel rendus en 2017, 2018 et 2019, pour en extraire les données relatives aux montants de dommages-intérêts demandés par les victimes et aux montants alloués par les juges. Mais, pour rassembler ces données, le logiciel enregistre nécessairement les nom, prénom, adresse, etc de toutes les personnes concernées.

Les données sont conservées pendant 2 ans afin de créer un algorithme permettant, notamment, la création d'un logiciel permettant d'évaluer automatiquement le montant de dommages-intérêts auquel une victime peut prétendre. Le but affiché est d'éviter le passage devant un juge en facilitant la médiation (l'idée est que si les parties savent à quoi s'attendre, elles préféreront se mettre d'accord plutôt que de faire un long et coûteux procès). Cela permettra aussi d'automatiser les décisions de justice avec une décision automatique du montant des dommages-intérêts. Dans tous les cas, l'objectif est de dissuader d'aller en justice. Aussi, on peut difficilement imaginer un algorithme créé en 2021 à partir des données récoltées en 2017… en effet, dans 5 ou 8 ans, les données seront datées – on s'achemine donc vers un fichier pérenne, qui récolte en permanence les décisions de justice.

Enfin, les personnes concernées par ce fichier ne sont pas informées de l'utilisation de leurs données personnelles… cela constituerait un « effort disproportionné » pour le ministère. Ainsi, les services du ministère peuvent créer et alimenter un énième fichier, mais prévenir les personnes concernées est au-delà de leur capacité. On ne peut pas non plus s'opposer au traitement.

Les enregistrements des conversations sont conservés 3 mois. Les données du système d'identification biométrique de la voix sont effacées à la fin de la mesure de placement sous surveillance électronique mobile.

En revanche, **toutes les autres données du système sont conservées 10 ans à compter de la fin de la mesure de placement sous surveillance électronique mobile.**

Pour avoir accès aux données ou les faire rectifier, il faut s'adresser au directeur de l'administration pénitentiaire (13 place Vendôme, 75042 PARIS CEDEX 01).

15. Fichier Bracelet anti-rapprochement

Ce dispositif est prévu aux articles R24-14 et suivants et R61-43 du code de procédure pénale, et aux articles R631-6 et suivants du code pénitentiaire. Son objectif est, par la pose d'un bracelet sur l'auteur, et le port d'un téléphone doté d'un système de géolocalisation par la victime de faits de violences, qu'une alerte se déclenche si les deux personnes se rencontrent.

Il est mis en œuvre par la direction de l'administration pénitentiaire.

Le fichier contient de nombreuses données sur l'auteur et la victime, ainsi que les données permettant leur géolocalisation, l'enregistrement de leurs communications avec les agents de l'administration pénitentiaire. **Il est doté d'un système de reconnaissance biométrique de la voix.**

Aucune disposition ne permet l'utilisation de ces données pour constater des faits (notamment des infractions) autres que le contact entre l'auteur et la victime.

Les données sont conservées 6 ans après la fin de la mesure (sauf les données relatives à la reconnaissance biométrique de la voix et l'enregistrement des conversations, qui sont conservées un et deux mois).

Pour avoir accès aux données ou les faire rectifier, il faut s'adresser au directeur de l'administration pénitentiaire (13 place Vendôme, 75042 PARIS CEDEX 01).

16. Gestion Informatisée des Détenus en Établissement (GIDE)

Il a été remplacé par GENESIS le 1er janvier 2017 (article 11 du décret n°2011-817 du 6 juillet 2011).

17. Cahier Électronique de Liaison (CEL)

Il a été créé, en toute illégalité, par une note de service de l'administration pénitentiaire du 24 décembre 2008 (joyeux noël!). Le 4 juin 2012, le Conseil d'État a constaté que le CEL était complètement illégal. Mais il n'a pas ordonné la destruction des données : au lieu de cela, elles sont transférées dans le

- Dont la soustraction à la justice, en raison de leur personnalité et/ou des faits pour lesquels elles sont écrouées pourraient avoir un impact important sur l'ordre public,
- Susceptibles d'actes de grandes violences, ou ayant commis des atteintes graves à la vie d'autrui, des viols, actes de torture et de barbarie ou prises d'otage en établissement pénitentiaire,
- Signalées ou ayant été signalées pour avoir été à l'initiative d'un mouvement collectif, d'une mutinerie ou d'actes de dégradations de grande ampleur en établissement, ou d'avoir participé à plusieurs reprises à de tels incidents.

La circulaire du 11 janvier 2022 prévoit que l'inscription au répertoire DPS est contradictoire, donc que la personne détenue est informée de son inscription et de son maintien, de ses conséquences, et peut faire valoir ses observations (point 1.2.3).

Les conséquences d'une inscription au répertoire DPS sont une atteinte encore plus grave aux libertés : cellule individuelle, fouilles répétées, surveillance nocturne avec lumière allumée.

4.2 – Données concernées

Le statut DPS a pour conséquence une alimentation beaucoup plus importante de GENESIS. Sont versées dans ce fichier, chaque jour (point 4.1.2.1 de la circulaire du 11 janvier 2022) :

- Le comportement de la personne avec les personnels et les partenaires,
- Les relations en détention et le positionnement de la personne avec les autres détenu·es,
- Les demandes d'échanges et de dons,
- Les liens entretenus avec l'extérieur,
- Les habitudes de vie en détention,
- Les changements de comportement et les changements d'apparence,
- Les éléments d'information importants recueillis à l'occasion du contrôle des communications écrites, téléphoniques, et des mandats.

Le préfet, les autorités judiciaires et les personnels hospitaliers sont informés du statut DPS (point 4.1.2.3).

4.3 – Conservation des données

Le tour de passe-passe de la création d'un « répertoire » et non d'un « fichier » a pour conséquence que les données ne sont pas vraiment collectées : le FND et GENESIS comportent seulement la mention « Détenu Particulièrement Signalé », et cette mention est retirée lorsque le ou la détenu·e sort du DPS.

4.4 – Droit de communication, de rectification et d'effacement

Il ne s'agit donc pas de l'effacement des données, mais d'une demande de sortie du statut de DPS. Le point 2.4 de la circulaire du 11 janvier 2022 prévoit que la demande est à formuler au ministre de la

justice. En cas de silence de l’administration pendant 2 mois (qui vaut refus), ou en cas de décision de refus, c’est possible de contester cette décision devant le tribunal administratif (plutôt avec l’aide d’un·e avocat·e).

Les données du fichier sont accessibles par les personnels de l’administration pénitentiaire, par les magistrats, et par les officiers de police judiciaire.

Les enregistrements des conversations sont conservés 3 mois. Les données du système d’identification biométrique de la voix sont effacées à la fin de la mesure de placement sous surveillance électronique mobile.

En revanche, toutes les autres données du système sont conservées 12 mois à compter de la fin de la mesure de placement sous surveillance électronique mobile.

Pour avoir accès aux données ou les faire rectifier, il faut s’adresser au directeur de l’administration pénitentiaire (13 place Vendôme, 75042 PARIS CEDEX 01).

14. Fichier des personnes placées sous surveillance électronique mobile

Ce fichier est prévu par les articles 763-13 et R61-12 et suivants du code de procédure pénale, et aux articles L544-2, L544-3, R544-7 et R544-18 et suivants du code pénitentiaire. Il vise à contrôler à distance la localisation de la personne condamnée ou mise en examen qui est placée sous surveillance électronique mobile (à la différence du précédent, ce bracelet électronique permet de géolocaliser la personne).

Il est mis en œuvre par le directeur de l’administration pénitentiaire (ministère de la justice).

Il vise les personnes placées sous bracelet électronique doté d’un système de géolocalisation, en application soit d’une mesure d’assignation à résidence, d’un suivi socio-judiciaire, d’une surveillance judiciaire, d’une surveillance de sûreté, d’une libération conditionnelle, d’une permission de sortie au cours d’une rétention de sûreté, soit d’une décision de la cour de cassation ordonnant la suspension de l’exécution de la condamnation, ou du placement sous assignation à résidence d’un étranger en situation irrégulière, ou de décision du ministre de l’intérieur de prononcer certaines obligations à l’encontre d’une personne pour prévenir la commission d’actes de terrorisme (MICAS, en application des articles L228-1 et suivants, R228-1 et suivants du code de la sécurité intérieure, et R641-1 et suivants du code pénitentiaire).

Ce fichier rassemble beaucoup d’informations sur l’identité et les procédures judiciaires concernant les personnes placées sous surveillance électronique mobile. Il rassemble aussi le relevé de la localisation de ces personnes, la liste des alarmes déclenchées, les enregistrements des communications émises via le bracelet entre la personne et les agents de l’administration pénitentiaire. Il contient aussi un **système d’identification biométrique de la voix**.

Les données du fichier sont accessibles par les personnels de l’administration pénitentiaire, par les magistrats, et par les officiers de police judiciaire. Elles peuvent permettre de **constater d’autres infractions** que celles résultant du non respect de ses obligations par la personne porteuse du bracelet (article 763-13 du code de procédure pénale).

date de fin de peine, la date de libération, le nom du juge d'instruction, les remises de peine, la situation professionnelle, les langues parlées.

12.2 – Utilisation du FND

Les personnes qui ont accès aux informations sont l'administration pénitentiaire, les directeurs de taule, les magistrats, les greffiers, les flics.

12.3 – Conservation des données

On n'a pas trouvé d'informations certaines. Ce qui est étonnant, voire complètement illégal, c'est que l'arrêté du 20 février 2003 ne prévoit aucune durée de conservation des données, et qu'il semble qu'aucun autre texte ne prévoit cette durée.

12.4 – Droit de communication, de rectification et d'effacement

L'article 2 de l'arrêté du 20 février 2003 précise les modalités d'exercice de ce droit :

Le droit d'accès et de rectification s'exerce, lorsque la personne est incarcérée, auprès du directeur de la taule ou auprès du directeur interrégional des services pénitentiaires.

Lorsque la personne n'est pas incarcérée, il s'exerce auprès du procureur de la République du domicile de la personne concernée.

13. <u>Fichier des personnes placées sous surveillance électronique</u>

Ce bracelet électronique ne géolocalise pas la personne : il est seulement lié à un boîtier fixe, et une alarme se déclenche lorsque la personne s'éloigne de ce boîtier au-delà de la zone autorisée (le domicile) à une heure à laquelle cela lui est interdit.

Il est prévu par les articles 723-9 et R57-30-1 du code de procédure pénale et par les articles R622-1 et R622-22 et suivants du code pénitentiaire. Il est mis en œuvre par la direction de l'administration pénitentiaire.

Il concerne les personnes condamnées à une peine de détention à domicile sous surveillance électronique. Le fichier permet de contrôler que la personne condamnée est présente à son domicile aux heures prévues par le juge. Il permet aussi de contrôler, pour toute autre enquête, à quels moments une personne est à son domicile. Il est interconnecté avec le fichier APPI (Application des peines, probation et insertion).

Ce fichier rassemble beaucoup d'informations sur l'identité et les procédures judiciaires concernant les personnes placées sous surveillance électronique mobile. Il rassemble aussi, la liste des alarmes déclenchées, les enregistrements des communications émises via le bracelet entre la personne et les agents de l'administration pénitentiaire. Il contient aussi un **système d'identification biométrique de la voix**.

Partie 3 : Fichiers de police : Principaux fichiers du quotidien

Les principaux fichiers de police sont les fichiers d'antécédents (le traitement des antécédents judiciaires, TAJ), ainsi que d'autres fichiers qui rassemblent énormément d'informations : la main-courante informatisée (N-MCI), les logiciels de prise de notes et de rédaction des procédures des gendarmes et des policiers (GendNotes, LRPPN, LRPGN), le FOVeS (ancien fichier des véhicules volés)…

Vous trouverez aussi des informations sur les smartphones et tablettes NEOGEND et NEOPOL, des outils de plus en plus performants pour la consultation et l'alimentation des fichiers, même à l'extérieur des locaux de police et de gendarmerie, et toujours plus rapidement.

Une des évolutions les plus notables ces dernières années est le recours massif à la reconnaissance faciale par le biais du TAJ : possible depuis 2011, cet usage se multiplie, dans les enquêtes ou lors de simples contrôles d'identité.

1. <u>Traitement d'Antécédents judiciaires (TAJ)</u>

C'est un fichier de police judiciaire (ministère de l'intérieur). Il remplace depuis 2012 l'ancien STIC (police nationale) et l'ancien JUDEX (gendarmerie nationale). Il est prévu aux articles 230-6 et suivants et R40-23 et suivants du code de procédure pénale.

C'est le fichier de référence pour les policiers, et ils en font bien n'importe quoi : les faits divers relèvent fréquemment des consultations non autorisées. Ainsi, de la nièce de Gérald Darmanin, placée en garde à vue en mars 2023 pour accès illégal au fichier à l'aide de son ancien compagnon, gendarme[11]. Mais les flics s'en servent aussi pour vérifier le passé de leurs voisins… ou pour arrondir leurs fins de mois et vendre des informations : cette pratique est tellement répandue qu'elle a un nom, « la tricoche »[12]. Une policière a ainsi récupéré le 06 de Darmanin pour lui envoyer un SMS sur l'état de délabrement de son commissariat[13]. Un autre est suspecté de s'être fait environ 10.000 euros sur deux ans grâce à la revente de fichiers[14] (dont le FPR aussi).

1.1 – Données concernées

Ces règles sont dans l'article 230-7 du code de procédure pénale : Le TAJ concerne les personnes suspectées d'avoir commis une infraction en tant qu'auteur ou complice, ainsi que les victimes.

11 https://www.lejdd.fr/societe/la-niece-de-gerald-darmanin-placee-en-garde-vue-pour-avoir-consulte-illegalement-des-fichiers-de-police-134169

12 https://www.lemonde.fr/societe/article/2024/03/13/au-tribunal-de-paris-la-tricoche-de-deux-policiers-qui-monnayaient-des-fichiers-confidentiels_6221733_3224.html?random=446963116&random=1303040225

13 https://www.leparisien.fr/faits-divers/tours-une-policiere-condamnee-pour-avoir-consulte-un-fichier-a-des-fins-personnelles-31-01-2023-MSLRO3DT4RF4VI7O6BRH4Z4MQY.php

14 https://www.laprovence.com/article/france-monde/12575616997006/bientot-un-an-de-detention-provisoire-pour-un-policier-qui-vendait-des-fichiers-confidentiels

Attention, en ce qui concerne les contraventions, le fichage au TAJ ne concerne normalement que celles-ci : violences ayant entraîné une ITT de 8 jours max, provocation non publique à la discrimination/haine…, dégradation légère, port ou exhibition d'uniforme rappelant ceux d'organisations ou de personnes responsables de crimes contre l'humanité, enregistrement sans autorisation dans une zone militaire, dissimulation d'enfant nouveau-né trouvé. En conséquence, les autres contraventions ne doivent pas apparaître au TAJ.

En ce qui concerne les données enregistrées, elles sont très nombreuses : l'identité de la personne, sa profession, sa situation familiale, sa nationalité, ses adresse, numéro de téléphone, adresse électronique, sa photographie, les faits qui lui sont reprochés, ses caractéristiques physiques, les dates des infractions supposées, les données et images relatives à ces faits, etc.

Le TAJ est alimenté via l'application GASPARD NG, qui permet d'alimenter simultanément le TAJ et le FAED (mais pas le FNAEG).

1.2 – Utilisation du TAJ et reconnaissance faciale

Le TAJ peut être consulté par la police nationale, la gendarmerie nationale, la douane, les services de renseignement, certains agents du fisc, et les procureurs. La police municipale n'y a pas accès.

Il peut être consulté au cours d'une enquête de police, mais aussi au cours d'une enquête administrative pour l'accès à certaines professions (agent de police, gardiennage, surveillance, militaire, secteur du nucléaire, intervention dans des grands événements, (par exemple les Jeux Olympiques), etc) et lors des demandes de titre de séjour et de nationalité française. Dans certains cas (notamment en cas de classement sans suite), il est prévu que les données fassent l'objet d'une « *mention* » du procureur de la République, qui interdit leur consultation pour les enquêtes administratives (voir Conseil d'État, 17 avril 2023, n°463359, Publié).

Le TAJ c'est LE fichier qui sert à faire de la reconnaissance faciale en France. Elle est mentionnée depuis 2013 (article R40-26 1° et 3° du code de procédure pénale, qui autorise la conservation d'une « photographie comportant des caractéristiques techniques permettant de recourir à un dispositif de reconnaissance faciale »), mais on peine à trouver une réelle base légale à la reconnaissance faciale et les modalités d'exécution ne sont de toutes façons pas encadrées. Ainsi, si la police a un doute sur l'identité d'une personne, elle peut faire une comparaison automatique de sa photographie avec les photos contenues dans le TAJ. Le TAJ contient ainsi le logiciel de reconnaissance faciale FaceVACS-DBScan de la société COGNITEC[15]. Il ressort de l'avis n°3404 sur le volet sécurité de la loi de finances pour 2021, déposé à l'Assemblée nationale le 13 octobre 2020 par le député Stéphane Mazars au nom de la commission des lois,

15 https://www.nextinpact.com/lebrief/44501/la-reconnaissance-faciale-policiere-boostee-pendant-confinement?fbclid=IwAR0jhquJbzx7cfyLoecW5A2u5S5he8SbrHWW7Y4hNwF7z75whzpY59HtzDc%3Ffbclid%3DIwAR0jhquJbzx7cfyLoecW5A2u5S5he8SbrHWW7Y4hNwF7z75whzpY59HtzDc

11.1 – Données concernées

Les données concernées sont l'identité complète des personnes, leurs documents d'identité et titres de séjour, permis de conduire, livret de famille, etc, adresse, adresse des personnes qui les hébergent, niveau d'étude, ressources financières, prestations sociales.

Le fichier répertorie aussi les avocats, les experts, les victimes, les proches.

Le fichier rassemble enfin toutes les données relatives à l'exécution de la peine : aménagements de peine, suivi médical, obligation de soins, lieux d'incarcération, liens familiaux, activités, postes de travail, incidents, évaluation par le SPIP.

11.2 – Utilisation de APPI

Peuvent accéder aux données : les procureurs, les juges, les juges d'application des peines, les juges des libertés et de la détention, les juges d'instruction, les SPIP, les directeurs de prison, la protection judiciaire de la jeunesse et les greffiers (articles R113-53 et R113-54 du code pénitentiaire).

11.3 – Durée de conservation des données

Les données sont conservées 5 ans à compter de la fin de la peine (article R113-52 du code pénitentiaire).

11.4 – Accès, rectification et effacement des données

Le droit d'accès et de rectification des données s'exerce auprès du procureur de la République du tribunal qui a été saisi de la procédure, ou dans le ressort duquel est situé le SPIP chargé du suivi de la mesure (article R113-55).

12. Fichier National des Détenus (FND)

Aussi appelé Fichier National Informatisé des Personnes Incarcérées, il a été créé par l'arrêté du 28 octobre 1996 et réactualisé par l'arrêté du 20 février 2003. Il est sous la responsabilité de l'administration pénitentiaire (ministère de la justice).

Il a pour objectif la gestion des affectations pénitentiaires.

Il est alimenté par l'application Gestion nationale des personnes détenues en établissement pénitentiaire (GENESIS) qui a remplacé GIDE. À terme, GENESIS devrait remplacer également le FND.

12.1 – Données concernées

Les données collectées sont : tout ce qui concerne l'identité des personnes incarcérées, le statut marital, le nombre d'affaires pour lesquelles la personne est incarcérée, les mesures d'éloignement, le statut DPS, le suivi médical, les situations de handicap, l'établissement d'incarcération et les taules précédentes, les sorties, les numéros d'écrou, la catégorie pénale, les infractions, la procédure, la date de condamnation, la

port d'arme de catégorie A ou B, enlèvement et séquestration, destruction de biens par explosif, diffusion de procédés permettant de fabriquer des explosifs, terrorisme.

Il rassemble les expertises, évaluations et examens psychiatriques, médico-psychologiques, psychologiques et pluridisciplinaires réalisés au cours d'une enquête, d'une instruction, d'un jugement ou de l'exécution d'une peine. Les données ne peuvent être consultées que par les autorités judiciaires et par les experts désignés par elle.

10.7 – Utilisation de REDEX

Les juges et procureurs peuvent avoir accès au REDEX.

10.8 – Conservation des données

Les données sont immédiatement supprimées en cas de classement sans suite, de non-lieu, de relaxe ou d'acquittement (sauf irresponsabilité pénale due à un trouble mental).

Si la personne est majeure, les informations sont conservées pendant 30 ans à compter du jour de l'examen, de l'expertise ou de l'évaluation (15 ans si la personne est mineure).

10.9 – Droit de communication, de rectification et d'effacement

Le droit de communication des données s'exerce auprès du procureur de la République du domicile de la personne (article R53-21-10). Les droits de rectification et d'effacement s'exercent aussi auprès du procureur de la République (article R53-21-11). Pour les recours contre la décision du procureur, l'appel se forme auprès du juge des libertés et de la détention (R53-21-13 et suivants).

11. Application des Peines, Probation et Insertion (APPI)

Il est régi par les articles R57-4-1 du code de procédure pénale et R113-49 et suivants du code pénitentiaire. Il est placé sous l'égide du ministère de la justice.

Ce fichier a pour objectif de suivre les condamnations des personnes, l'exécution de leur peine, le travail des services pénitentiaires d'insertion et de probation y compris pour la mise en œuvre des mesures de sûreté.

APPI est en lien avec CASSIOPÉE, GENESIS, le casier judiciaire, le fichier des personnes placées sous surveillance électronique mobile et celui des personnes placées sous surveillance électroniques (bracelet électronique).

Ce fichier buggue tout le temps, et il est prévu de le remplacer par le logiciel PRISME (Probation, insertion, suivi, mesure et évaluation), des essais étant programmés à la fin de l'année 2023.

que la reconnaissance faciale est utilisée massivement[16] : 375'747 requêtes de reconnaissance faciale ont été effectuées en 2020 pour les seuls services de la police nationale. Cette utilisation est en très forte augmentation (207'584 requêtes du 1er janvier au 17 juin 2020). **En 2021, la police procédait en moyenne à 1680 reconnaissances faciales par jour**[17].

C'est une drôle d'interprétation de la « nécessité absolue » requise pour son utilisation selon l'article 88 de la loi du 6 janvier1978.

De plus, depuis novembre 2019, **la reconnaissance faciale peut être utilisée à partir de n'importe quelle photographie (surveillances, images postées sur les réseaux sociaux, glanées sur internet, ou provenant de vidéos)[18].**

La reconnaissance faciale peut ainsi être mise en œuvre à partir de photographies prises par les policiers et les gendarmes, en particulier à partir des tablettes NEOPOL (police) et NEOGEND (gendarmerie). Par conséquent, il est techniquement facile, au cours d'un contrôle d'identité, **de prendre en photo une personne avec NEO, de verser sa photographie dans le TAJ, et de faire tourner le logiciel de reconnaissance faciale pour retrouver son identité.** Cette pratique semble déjà être très répandue[19] et pourtant sans fondement légal. En effet, la prise de photographie (de même que la prise d'empreintes) au cours d'une vérification d'identité ne peut se faire que dans un cadre précis :

- refus de décliner son identité ou éléments d'identité manifestement inexacts,
- autorisation nécessaire du procureur ou du juge d'instruction,
- rédaction d'un procès-verbal qui justifie le contrôle et informe la personne de ses droits (etc.).

On est bien loin donc de la pratique de prises de photo à la volée, lorsque les gens sont alignés contre un mur lors d'un contrôle. Par ailleurs, les flics utilisent vraisemblablement fréquemment leur propre téléphone portable à cet usage.

Le 26 avril 2022, le Conseil d'État, saisi par la Quadrature du Net qui demandait la suppression de la reconnaissance faciale dans le TAJ, a jugé que celle-ci était légale et a rejeté le recours[20]. La Quadrature a déposé un nouveau recours, cette fois sous la forme d'une plainte collective auprès de la CNIL en septembre 2022 concernant la vidéosurveillance, le fichage de masse et la reconnaissance faciale[21]. Cette plainte est toujours en cours d'instruction.

16 Voir notamment Christophe-Cécil GARNIER, *Dans tous les commissariats de France, la reconnaissance faciale est utilisée facilement*, STREETPRESS, 7 avril 2021
17 https://technopolice.fr/plainte/
18 https://www.assemblee-nationale.fr/dyn/15/rapports/cion_lois/l15b3404-tvii_rapport-avis#
19 Voir par exemple à Montreuil : https://fr.squat.net/2021/02/27/montreuil-93-expulsion-du-marbre/
20 Conseil d'État, 26 avril 2022, n°442364, La Quadrature du Net
21 https://www.nextinpact.com/article/70034/la-quadrature-net-porte-plainte-contre-technopolice-ministere-interieur

La reconnaissance faciale a aussi fait son entrée dans les tribunaux, par exemple à Lyon le 17 septembre 2019[22]. Elle a récemment servi à condamner un gilet jaune le 22 juin 2023 à Niort, reconnu sur cette base à sa participation à la manifestation à Sainte-Soline du 25 mars 2023[23], et de nouveau, toujours à Niort et pour les mêmes faits, le 28 mars 2024.

Concernant la reconnaissance faciale, un récent arrêt de la CEDH pourrait s'évérer pertinent : dans l'affaire Glukhin c. Russie, la Cour a estimé que le recours à la reconnaissance faciale pour la répression d'un manifestant était disproportionné, s'agissant de simples faits de manifestation sans violences[24].

Enfin, le TAJ, c'est énormément de fiches, 15,6 millions en 2016 (une même personne pouvant avoir plusieurs fiches). Selon la CNIL, il y avait environ 9,5 millions de personnes fichées dans le TAJ en 2015 dont 3,4 millions avec photographie. En 2020, 19 millions de fiches et 8 millions de photographies figuraient au TAJ[25].

Il est interconnecté avec les fichiers d'Europol et d'Interpol (article R40-29 III).

1.3 – Conservation des données

Le délai de conservation des données par défaut pour une personne majeure mise en cause (donc suspectée ou condamnée) est de 20 ans (article R40-27 du code de procédure pénale).

Ce délai est plus court, 5 ans, pour les délits prévus au code de la route et pour certains autres délits (genre homicide involontaire, coups et blessures involontaires, racolage (délit abrogé, qui n'existe plus), non-versement de pension alimentaire, vol simple, détournement de gage, détournement d'objet saisi, entrave à la liberté d'expression, d'association, de travail, des débats d'une assemblée parlementaire etc, participation non armée à un attroupement visage masqué ou découvert, délit de fuite d'un conducteur de véhicule après un accident, usage de stupéfiants), et pour les contraventions concernées par le fichage au TAJ (violences ayant entraîné une ITT de 8 jours max, provocation non publique à la discrimination/haine…, dégradation légère, port ou exhibition d'uniforme/… rappelant ceux d'organisations ou de personnes responsables de crimes contre l'humanité, enregistrement sans autorisation dans une zone militaire, dissimulation d'enfant nouveau-né trouvé).

Ce délai est plus long, 40 ans, pour certaines infractions : administration de substances nuisibles, détournement de moyen de transport, empoisonnement, enlèvement, séquestration, exploitation de la mendicité aggravée ou en bande organisée, crime contre l'humanité, meurtre, assassinat, menace de mort, torture, acte de barbarie, violence volontaire ayant entraîné la mort ou une mutilation ou une infirmité permanente, vol avec violence, agression sexuelle, atteinte sexuelle sur mineur de moins de 15 ans,

22 https://rebellyon.info/A-Lyon-la-gendarmerie-utilise-la-21118
23 https://www.infolibertaire.net/niort-deux-sevres-letat-se-venge-suite-a-sainte-soline/#/
24 blob:https://hudoc.echr.coe.int/a1ad9fee-ff92-4526-b53b-815d80ea8ee9
25 https://www.laquadrature.net/2020/08/07/nous-attaquons-la-reconnaissance-faciale-dans-le-taj/

Ce fichier est automatiquement interconnecté avec LRPPN et LRPGN pour les affaires classées sans suite et les alternatives aux poursuites.

Il permet aussi aux magistrats d'interroger le TAJ, le casier judiciaire, le FAED, le FNAEG, CASSIOPEE et WINEURS.

10.3 – Durée de conservation des données

Les données sont conservées jusqu'à l'extinction de l'action publique (donc jusqu'à la prescription des faits, soit plusieurs années), ou jusqu'à la fin de l'exécution de la peine (paiement de l'amende, fin des 5 ans de la durée du sursis, sortie de détention) et si la peine n'est pas exécutée jusqu'à sa prescription (3 ans pour les contraventions, 6 ans en principe pour les délits mais 20 ans pour certains, 30 ans pour les crimes) (article R249-12 du code de procédure pénale).

Les minutes d'un jugement (retranscription des débats) sont conservées 6 ans après le prononcé du jugement.

À l'issue de ces délais, les données ne sont pas effacées, mais archivées « en base inactive pour leur durée d'utilité administrative ». Si on ne comprend pas ce que ça veut dire, c'est normal. Le gouvernement a simplement dit à la CNIL qu'une solution sera mise en place en 2021 (Délibération de la CNIL n°2020-036 du 12 mars 2020, point 47).

10.4 – Accès, rectification, effacement des données personnelles

Le nouvel article R249-14 du code de procédure pénale est tout à fait obscur quant aux modalités d'exercice du droit d'accès, de rectification et d'effacement des données personnelles, ça vaut le coup de le citer : « l'accès aux données et les conditions de leur rectification ou de leur effacement sont régis par les dispositions du présent code. » Donc, il suffit de trouver la procédure parmi le bon millier d'articles du code.

Il s'agit, en fait, des dispositions relatives à l'accès au dossier par le prévenu lui-même (article 279 du code de procédure pénale devant la cour d'assises, article 388-4 devant le tribunal correctionnel, article 533 devant le tribunal de police par exemple), ou par le témoin assisté (article 113-3), la partie civile et la personne mise en examen (article 114) pendant l'instruction.

10.5 – Répertoire des expertises (REDEX)

REDEX est prévu par les articles 706-56-2 et R53-21-1 et suivants du code de procédure pénale.

Il est tenu par le Service du casier judiciaire (ministère de la justice).

10.6 – Données concernées

Il concerne toutes les personnes poursuivies ou condamnées pour l'une des infractions dans lesquelles le suivi socio-judiciaire est encouru : homicides volontaires, viols et agressions sexuelles, tortures, violences domestiques, corruption de mineur, atteinte sexuelle sur mineur, pédopornograhie, trafic d'armes,

NPP rassemblait tous les actes composant un dossier de procédure (procès-verbaux, pièces de la procédure, décisions des procureurs et des juges, etc).

Les données étaient conservées jusqu'à la fin de l'exécution de la peine (paiement de l'amende, fin de l'emprisonnement, stage de citoyenneté, etc).

Avaient accès aux données les magistrats, greffiers, avocats, huissiers qui signifient les actes, etc.

On pouvait demander l'accès aux informations au procureur de la République qui est saisi du dossier (par exemple le procureur de la République du Tribunal judiciaire de Bordeaux si on est jugé·e à Bordeaux).

10. <u>Dossier pénal numérique (DPN)</u>

Il est créé par le décret n°2020-767 du 23 juin 2020 et va être mis en place progressivement sur le territoire, en commençant par Blois et Amiens, pour remplacer NPP. En juin 2023, il concerne 55 tribunaux sur 164 et devrait être généralisé fin 2025. Il est mis en œuvre par chaque tribunal, par les cours d'appel et par la cour de cassation, et apparaît aux articles R249-9 et suivants du code de procédure pénale.

10.1 – Données concernées

Les données concernées sont listées par l'article R249-11 du code de procédure pénale. Comme NPP, il concerne tous les actes composant un dossier de procédure, du début de l'enquête jusqu'aux notes prises par les greffiers au cours d'une audience devant le tribunal et la peine prononcée. Il comporte des photographies (le nouvel article R249-11 du code de procédure pénale précise qu'aucune reconnaissance faciale ne pourra être mise en œuvre), des empreintes digitales et des empreintes génétiques. Il rassemble des informations aussi sur toutes les personnes concernées par une procédure : mis en cause, condamné·e, victime, témoin, expert, avocat, enquêteur, etc. Il est même prévu que les magistrats puissent remplir des « commentaires libres » à propos d'une personne, mais que personne d'autre qu'eux n'y auront accès.

Pour les mineurs, DPN permet l'accès au Dossier unique de personnalité (DUP).

10.2 – Accès aux informations

Ont accès à DPN les magistrats (juges, procureurs) pour les procédures dont ils sont saisis, les greffiers, les délégués du procureur chargés de la mise en œuvre des alternatives aux poursuites (par exemple en Maison de la justice et du droit), les avocats.

Ont aussi accès aux informations les parties à la procédure (les personnes mises en cause et les parties civiles).

Concernant le volet Dossier unique de personnalité, ont accès aux informations les avocats du mineur, ses parents, ses représentants légaux, les professionnels de la protection judiciaire de la jeunesse et les personnels de l'association assurant le suivi du mineur.

corruption de mineur, proxénétisme, viol, trafic de stupéfiants, traite des êtres humains, abus de confiance aggravé, détérioration par substance explosive ou incendie, escroquerie aggravée, extorsion, vol en bande organisée, vol avec arme, blanchiment, falsification de monnaie etc, faux en écritures publiques, abus de biens sociaux, délit d'initié, atteinte aux systèmes de traitement automatisé de données, terrorisme, association de malfaiteurs, évasion, infraction au régime des armes (sauf catégorie D), recel de malfaiteurs, violation de secret professionnel ou bancaire, atteinte aux intérêts fondamentaux de la nation (voir la longue liste dans la partie dédiée au fichier TES).

Si la personne est mineure, en principe c'est 5 ans, mais il y a des dérogations : il peut être allongé à 10 ou 20 ans (voir article R40-27).

Si la personne est victime, c'est 5 ans. Une victime peut aussi demander son effacement du TAJ dès que l'auteur de l'infraction a été condamné.

Dans certains cas, le TAJ doit être automatiquement mis à jour (les données doivent être effacées), ou la mise à jour est automatique lorsqu'on la demande (article 230-8 du code de procédure pénale) :

- S'il y a eu relaxe, acquittement, ou condamnation avec dispense de peine : l'affaire est effacée, sauf si le procureur de la République s'oppose à l'effacement (alors, elle reste inscrite, mais la loi prévoit que la fiche est inaccessible lors d'une enquête administrative).
- S'il y a eu ordonnance de non-lieu ou classement sans suite : en principe, c'est noté qu'il y a eu non-lieu ou classement sans suite, mais on peut demander au procureur de la République l'effacement.

1.4 – Droit de communication, de rectification et d'effacement

L'exercice de ce droit est assez complexe (et cette complexité semble avoir été décidée volontairement pour décourager les tentatives), mais c'est possible de s'y retrouver.

Le droit d'information et d'accès aux données

Le droit de communication des données s'effectue soit auprès du procureur de la République « territorialement compétent » (article R40-33 II du code de procédure pénale, normalement c'est le procureur du tribunal qui a jugé l'affaire, ou le procureur du tribunal dans le ressort duquel les faits ont eu lieu, mais c'est souvent difficile à définir) soit auprès du ministre de l'intérieur (article R40-33 II du même code). On n'a pas comparé les 2 voies différentes, donc on ne peut pas orienter vers l'une plus que l'autre. Cependant, pour beaucoup d'affaires, elles ne vont pas jusqu'au tribunal, donc on ne sait pas à quel procureur s'adresser. Du coup, demander au ministre de l'intérieur paraît être une bonne option.

De plus, demander au ministre de l'intérieur permet aussi de demander la finalité du TAJ, sa base juridique, les données concernées, les destinataires à qui les données nous concernant ont été communiquées, la durée de conservation des données (article 105 de la loi du 6 janvier 1978).

Si le ministère de l'intérieur ne répond pas dans un délai de 2 mois, ou s'il refuse l'accès, c'est possible de faire un recours devant la CNIL (3 place de Fontenoy, TSA 80715, 75334 PARIS CEDEX 07) (article 105 de la loi du 6 janvier 1978).

Lorsqu'on fait une demande au ministre de l'intérieur, on reçoit 2 lettres en réponse : l'une de la gendarmerie nationale (pour la partie gendarmerie du TAJ) et l'autre de la police nationale (pour la partie police du fichier). La gendarmerie a tendance à répondre assez rapidement (1 mois environ après la réception de la demande), mais la police nationale est beaucoup moins rapide (jusqu'à 4 mois après la réception de la demande).

Habituellement, les retours de courrier de la gendarmerie et de la police nationale ne comprennent pas les photographies. C'est contestable car l'ensemble des données doivent être communiquées aux personnes qui en font la demande. Cette réponse partielle peut donc être considérée comme un refus : on a alors un délai de deux mois après cette réponse pour effectuer un recours devant la CNIL.

La rectification et l'effacement des données

On a le choix pour demander la rectification et l'effacement des données :

- On peut s'adresser au procureur territorialement compétent (articles 230-8 et R40-31) ou au magistrat référent du TAJ (article 230-9 et R40-31), ou au ministre de l'intérieur (article 106 de la loi du 6 janvier 1978). Pareil que précédemment, c'est souvent difficile de savoir quel est le procureur territorialement compétent.
- C'est possible de se tourner vers le magistrat référent du TAJ : Magistrat référent TAJ, Secrétariat général – ministère de la justice, 13 place Vendôme, 75042 PARIS CEDEX 01.
- Ça paraît mieux de s'adresser au ministère de l'intérieur : Place Beauvau, 75800 PARIS CEDEX 08. Alors, la procédure est plus simple (en cas de refus le recours se fera devant la CNIL, sans avocat, et non devant le président de la chambre de l'instruction).

Différentes situations se présentent pour ce qui est de la rectification et de l'effacement. Par exemple, si vous vous rendez compte que vous apparaissez dans le TAJ comme coupable de « vol avec arme » mais que le tribunal vous a condamné pour « vol », c'est possible d'exiger que la circonstance aggravante (« avec arme ») disparaisse. Même chose si vous apparaissez dans le TAJ pour « violences » mais qu'à l'arrivée vous avez été condamné·e pour « dégradations ».

On peut aussi former une demande de rectification ou d'effacement si on n'a jamais été présenté à un juge (ni en audience, ni par la procédure de l'ordonnance pénale), y compris s'il y a eu un classement sans suite.

Si les faits qui apparaissent dans le TAJ ont fait l'objet d'un jugement, on obtiendra obligatoirement l'effacement si on a été relaxé·e, acquitté·e, condamné·e avec dispense de peine, condamné·e avec dispense de mention au casier judiciaire, ou s'il y a eu une ordonnance de non-lieu.

8. Données recueillies par l'Agence nationale des techniques d'enquêtes numériques judiciaires et par la plate-forme nationale des interceptions judiciaires

L'agence nationale des techniques d'enquêtes numériques judiciaires a été créée par l'article 230-45 du code de procédure pénale et par le décret n°2017-614 du 24 avril 2017. Elle est rattachée au ministère de la justice. Elle effectue certains actes d'enquêtes elle-même (article 2 du décret du 24 avril 2017), et d'autres via la plate-forme nationale des interceptions judiciaires (articles R40-42 et suivants du code de procédure pénale).

8.1 – Ce qui peut être intercepté

Les données susceptibles d'être recueillies sont vraiment très nombreuses (article R40-46 CPP). La possibilité de recueillir ces données, selon leur type, dépend de l'enquête[85]. Ces enquêtes sont prévues à l'article R40-43 du code de procédure pénale. Ce sont celles relatives à toute personne en fuite (article 74-2 CPP), les personnes disparues (article 80-4 CPP), et les personnes qui font l'objet d'une instruction et qui encourent une peine d'au moins 3 ans d'emprisonnement (article 100 CPP).

En cas d'enquête dans le cadre de la délinquance et de la criminalité organisée, peuvent également être enregistrées des courriers électroniques et autres correspondances électroniques accessibles par mot de passe (articles R40-43 et 706-95) des captations de données informatiques (enregistrement à distance des frappes de clavier, de l'affichage de l'écran, des contenus audiovisuels, du contenu de la mémoire d'appareils informatiques, articles R40-43 et 706-102-1 CPP).

L'article 2 du décret du 24 avril 2017 énumère d'autres catégories de données concernées. Il s'agit du déchiffrement de données informatiques (articles 230-1 et 230-2 CPP), les courriers électroniques et autres correspondances électroniques accessibles par mot de passe dans le cadre d'une information judiciaire, les captations d'images et de sons dans les véhicules et dans les lieux publics et privés dans le cadre d'une information judiciaire, les captations de données informatiques dans le cade d'une information judiciaire.

8.2 – Droit d'accès et de rectification

L'article R40-55 du code de procédure pénale prévoit que ces droits s'exercent auprès de la CNIL concernant les données de la plate-forme nationale des interceptions judiciaires.

9. Numérisation des procédures pénales (NPP)

Ce fichier a été créé par l'arrêté du 16 janvier 2008. Il était géré par le ministère de la justice et servait au suivi des procédures pénales dans les tribunaux. Ce fichier a été supprimé par l'article 3 du décret n°2020-767 du 23 juin 2020, qui a remplacé NPP par le Dossier pénal numérique (DPN).

85 Pour une lecture en tableaux des différentes possibilités d'enquête et leurs moyens : voir le rapport législatif de 2018 sur le projet de loi de renforcement de l'organisation des juridictions
https://www.senat.fr/rap/l18-011-1/l18-011-122.html

6. Bureau informatisé des enquêtes (BIE)

BIE est le deuxième module, avec VIGIE, des « Logiciels métier du parquet » (LMP). Il est prévu par le décret n°2017-1194 du 26 juillet 2017 et est mis en œuvre par le ministère de la justice.

Il sert au suivi calendaire des enquêtes pénales par les magistrats du parquet (les procureurs).

Les informations échangées sont seulement celles ayant trait au suivi des enquêtes, donc la date de la demande d'un acte par le parquet, le nom de cet acte, la date de la réalisation de l'acte et le numéro de procès-verbal. Elles sont conservées 5 ans à compter du dernier acte d'enquête.

Le droit d'accès et de rectification s'exerce auprès du procureur de la République.

7. Minos

Il a été créé par l'arrêté du 22 février 2008 (pour sa version 2). Minos est géré par le ministère de la justice et sert au traitement des contraventions par les tribunaux de police.

7.1 – Données concernées

L'ensemble des données de la contravention (identité complète de la personne concernée, catégorie socio-professionnelle de cette personne, permis de conduire, etc.).

Il concerne seulement les contraventions qui font l'objet d'une contestation devant le tribunal de police.

7.2 – Utilisation de Minos

Minos est utilisé par les greffes et les magistrats des tribunaux de police, devant lesquels on conteste les contraventions.

7.3 – Durée de conservation des données

Les données sont conservées pendant 5 ans à compter de la date à laquelle la décision du tribunal de police ou de la cour d'appel est devenue définitive.

7.4 – Accès, rectification et effacement des données

On ne peut pas s'opposer au traitement. Pour demander l'accès et la rectification des informations contenues dans Minos, il faut s'adresser au greffe du tribunal saisi de la contestation de la contravention concernée (par exemple, si on est suspecté d'avoir commis une contravention routière à Poitiers, on la conteste devant le tribunal de police de Poitiers, et c'est là qu'il faut s'adresser pour exercer son droit d'accès et de rectification des données).

Attention, en cas de condamnation avec mention au casier judiciaire, il faut d'abord demander l'effacement du bulletin n°2 du casier, puis demander l'effacement du TAJ (article 230-8 du code de procédure pénale).

Enfin, rien n'est indiqué en cas d'avertissement pénal probatoire. A priori, c'est possible de demander un effacement dans ce cas (et ça ne coûte rien d'essayer de toutes façons).

Si le procureur refuse d'effectuer les modifications demandées, on a 1 mois pour faire appel devant le président de la chambre de l'instruction, appel qui doit être motivé. Si on a formé la demande au magistrat référent chargé du TAJ, les délais sont les mêmes et l'appel doit être effectué auprès du président de la chambre de l'instruction de Paris. Dans les deux cas, il vaut mieux avoir l'aide d'un·e avocat·e. Si on a formé la demande au ministre de l'intérieur, et que ce dernier refuse de modifier les mentions contestées, il faut faire un recours à la CNIL (et on n'a pas besoin d'avocat pour cela).

En l'absence de réponse sous 2 mois du procureur (ou du magistrat référent du TAJ), on a 1 mois pour faire appel devant le président de la chambre de l'instruction. Le délai d'1 mois court à partir du jour où l'absence de réponse est effective. Il faut donc compter 2 mois à compter de la date à laquelle le procureur a reçu la demande, date qui figure sur l'avis de réception de la lettre recommandée avec avis de réception. En l'absence de réponse sous 2 mois du ministre de l'intérieur, c'est la même chose, mais le recours doit être fait devant la CNIL.

En cas de nouveau refus du président de la chambre de l'instruction, un pourvoi en cassation est possible, mais c'est pareil : il vaut vraiment mieux avoir l'aide d'un·e avocat·e.

2. CANONGE et GASPARD-NG

Ces deux fichiers sont fortement liés au TAJ, et spécifiquement sur la question de la reconnaissance faciale. Officiellement CANONGE et GASPARD-NG ne sont pas des fichiers mais des logiciels, dont l'utilisation n'est pas reconnue par les services de police. Autant dire qu'on procède à tâtons.

CANONGE est un logiciel de traitement des données qui fonctionnait a priori avec l'ancêtre du TAJ : le STIC. Canonge, c'est aussi le nom d'un inspecteur de police marseillais des années 1950 qui a créé un fichier manuel pour trier les personnes mises en cause d'après des « types raciaux » : « caucasien, gitan, moyen-oriental, nord-africain-maghrébin, » etc.[26] Ces données ont continué à figurer dans ce fichier, ou ce logiciel de traitement de données. CANONGE recensait donc le signalement d'auteurs d'infractions, et plus précisément la couleur des yeux, de cheveux, le « type ethnique » et les détails particuliers (par exemple les tatouages). Il n'est pas certain que CANONGE ait disparu avec le remplacement du STIC par le TAJ.

26 https://www.lemonde.fr/societe/article/2010/10/07/le-fichier-de-police-stic-canonge-contient-deja-des-caracterisques-ethno-raciales_1421666_3224.html

GASPARD-NG (« gestion automatisée des signalements et des photographies anthropométriques répertoriés et distribuables nouvelle génération ») pourrait être l'héritier de CANONGE, ou s'est simplement rajouté à celui-ci. Avec des objectifs similaires, GASPARD puis GASPARD-NG semblent toutefois exister depuis au moins 2008. Lors d'un reportage de Mediapart sur la police technique et scientifique, le logiciel GASPARD-NG apparaît à l'écran d'un des flics[27]. On peut en déduire que les données collectées sont (au moins) : le type ethnique, la pilosité, yeux cheveux, les signes particuliers, les accents, forme du visage et des photos. Dans sa plainte, la Quadrature du Net cite un rapport qui recense les outils de la police :

> « *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.*»[28]

On peut légitimement supposer que c'est l'outil GASPARD-NG qui permet d'effectuer des rapprochements biométriques entre des photos extraites d'une vidéo où des infractions seraient commises par exemple, et les fiches photographiques du TAJ.

La conservation des données devrait être la même que pour l'ensemble des données du TAJ.

Un arrêt du Tribunal des conflits, saisi pour l'effacement des données du TAJ et celles de CANONGE, ne s'est prononcé que concernant le TAJ[29]. Il semble considérer que les données de CANONGE sont dépendantes du TAJ. Il semble donc pertinent de suivre la procédure prévue pour le TAJ, d'adresser les demandes d'effacement au procureur de la République et, en cas de refus de celui-ci, d'introduire un recours devant la Chambre de l'instruction. Le même raisonnement peut être fait pour GASPARD-NG.

Concernant l'accès aux données, comme pour le TAJ, il semble pertinent de s'adresser au ministre de l'Intérieur.

3. Fichier des Objets et Véhicules Signalés (FOVeS)

Il a été créé en 2014 (arrêté du 17 mars 2014) à titre expérimental, et est définitif depuis 2017 (arrêté du 7 juillet 2017). Il remplace l'ancien Fichier des véhicules volés.

Il est mis en œuvre par la Direction générale de la police nationale (ministère de l'intérieur).

Son objectif est double : retrouver les objets et les véhicules volés (et même les animaux!), et surveiller les objets et les véhicules signalés. De plus, il peut être consulté en cas d'enquête administrative sur une personne qui veut être flic, gendarme, militaire, travailler dans les secteurs dits sensibles (nucléaire,

27 http://owni.fr/2012/06/01/deux-millions-de-controles-de-facies/index.html
28 https://www.laquadrature.net/wp-content/uploads/sites/8/2022/09/Plainte_TKPL_TAJ_anon.pdf
29 http://www.tribunal-conflits.fr/PDF/4134_Decision_decision_4134.pdf

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, profession, situation d'emploi, nom de l'employeur, langue parlée, données bancaires (sauf pour les témoins).

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, …

Des données sont aussi recueillies concernant les avocats et le personnel du ministère de la justice.

4.2 – Utilisation de CASSIOPÉE

Les données ne peuvent pas être directement consultées par les flics : seuls les juges, les procureurs, les greffiers et les éducateurs de la protection judiciaire de la jeunesse y ont accès. De plus, les avocats, les juges d'instruction et les flics qui agissent sous leur contrôle, certains membres d'associations d'aide aux victimes, et l'administration pénitentiaire ont accès à certaines données (articles R15-33-66-8 et R15-33-66-9).

4.3 – Durée de conservation des données

En principe, pour ce qui est des procédure pénales, les données sont conservées 10 ans à partir de la dernière modification du fichier, mais des durées plus longues sont prévues : 20 ans voire 30 ans en cas de condamnation à une peine criminelle, ou en cas de crime imprescriptible, ou en cas de terrorisme ou de trafic de stupéfiants.

Pour ce qui est des autres procédures, la durée de conservation des données est de 10 ans (article R15-33-66-7 du code de procédure pénale).

4.4 – Accès, rectification et effacement des données

Le droit d'accès et de rectification des données s'exerce directement auprès du procureur de la République de notre domicile (article R15-33-66-10).

5. Veille informatisée de gestion de informations et des évènements (VIGIE)

VIGIE est un des deux modules des « Logiciels métier du parquet » (LMP). Il est prévu par le décret n°2017-1194 du 26 juillet 2017 et est mis en œuvre par le ministère de la justice.

Il sert aux échanges entre les magistrats du parquet (les procureurs) et les services d'enquête de police et de gendarmerie.

Les informations échangées sont toutes celles ayant trait aux enquêtes, donc c'est extrêmement large. Elles sont conservées un an.

Le droit d'accès et de rectification s'exerce auprès du procureur de la République.

3.2 – Utilisation de SIROCCO

SIROCCO est utilisé seulement par les magistrats des JIRS et de la JUNALCO : Juges d'instruction et membres du parquet.

Il n'est pas accessible aux policiers, gendarmes et douaniers.

3.3 – Durée de conservation des données

L'article 3 du décret n°2023-309 du 25 avril 2023 prévoit que les données sont conservées dix ans à compter du dernier enregistrement, et, en cas de condamnation, dix ans si celle-ci est relative à un délit et quinze ans si celle-ci est relative à un crime, ces deux durées débutant à la date de la fin de l'exécution de la peine.

Les données sont effacées en cas de relaxe ou d'acquittement.

3.4 – Accès, rectification et effacement des données

Les données relatives aux procédures pénales peuvent être consultées selon les règles relatives à l'accès aux procédures pénales (différentes selon la situation : la procédure est en cours d'enquête de police, d'information judiciaire, ou si une juridiction de jugement est saisie ou a statué définitivement).

Les demandes de copie et d'effacement des données autres que celles inclues dans la procédure pénale elle-même peuvent être formulées auprès de la Direction des affaires criminelles et des grâces du ministère de la Justice. En cas de refus, il est possible de s'adresser à la CNIL.

4. CASSIOPÉE

Il s'agit de la Chaîne Applicative Supportant le Système d'Information Oriente Procédure pénale Et Enfants, qui est prévue aux articles 48-1 et R15-33-66-4 et suivants du code de procédure pénale.

Elle dépend du ministère de la justice. L'objectif est le 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.

CASSIOPÉE est directement reliée au fichier Application des Peines, Probation et Insertion (APPI, mis en œuvre par le ministère de la justice), ainsi qu'au casier judiciaire (également mis en œuvre par la ministère de la justice).

4.1 – Données concernées

CASSIOPÉE est alimenté automatiquement par le Logiciel de Rédaction des Procédures de la Police Nationale (LRPPN) et par celui de la Gendarmerie Nationale (LRPGN).

Les données recueillies sont, en ce qui concerne les personnes mises en cause, condamnées, victimes ou témoins : nom, prénom, nom d'usage, sexe, date de naissance, lieu de naissance, nationalité,

transport public de personnes, jeux, paris, utilisation de matières dangereuses, grand événement exposé à un risque terroriste, coucou les JO 2024…). Ce sont les activités citées aux articles L114-1, L114-2 et L211-11-1 du code de la sécurité intérieure. C'est donc à la fois un fichier de police et un fichier de renseignement.

3.1 – Données concernées

Les données recueillies sont 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.

Plus précisément, ces données sont :

- En cas de vol : nature de l'objet, numéro de série, photos de l'objet ou du véhicule, date et heure du vol, date et heure de la plainte, état civil et coordonnées du plaignant, identité de la personne susceptible d'utiliser le véhicule ou l'objet, descriptif et caractéristiques de l'objet ou du véhicule, conduite à tenir en cas de découverte.
- En cas de perte : la même chose qu'en cas de vol, sans l'identité de la personne susceptible d'utiliser le véhicule ou l'objet.
- En cas de surveillance : la même chose qu'en cas de vol, avec en plus le cadre juridique et la date de la mise sous surveillance.

Les personnes qui ont accès à ce fichier sont nombreuses : n'importe quel flic ou gendarme, les douanes, la Direction des libertés publiques et des affaires juridiques du ministère de l'intérieur, le Commandement spécialisé pour la sécurité nucléaire, la préfecture pour l'immatriculation des véhicules, la police municipale, les juges et procureurs, etc.

3.2 – Durée de conservation des données

En ce qui concerne les objets et véhicules volés, les données sont concernées pendant : 50 ans pour les armes, munitions, explosifs, bijoux, montres, objets d'art ; 20 ans pour les billets de banque ; 10 ans pour les véhicules, containers, documents, plaques d'immatriculation, moteurs de bateau ; 5 ans pour tout le reste.

En ce qui concerne les objets et véhicules perdus, les données sont conservées pendant 50 ans pour les armes, 10 ans pour les documents.

En ce qui concerne les objets et véhicules surveillés, les données sont conservées pendant 6 mois renouvelables.

Enfin, du moment de la découverte du véhicule ou de l'objet perdu / volé, les données sont encore conservées pendant 4 mois (5 ans si c'est un véhicule terrestre, un bateau ou un moteur de bateau)… et si c'est un véhicule ou objet signalé, les données sont effacées à la fin de la surveillance (elles sont conservées pendant 4 mois si la surveillance est arrêtée avant la fin de la période de 6 mois).

Mais ce n'est pas tout. L'État n'aime pas oublier : en fait, au moment de l'effacement des données, celles-ci ne sont pas supprimées… elles sont archivées pour une durée de 10 ans ! (article 5 de l'arrêté du 7 juillet 2017).

3.3 – Droits d'accès et de rectification

En ce qui concerne la procédure pour la consultation et l'effacement des données, comme pour le FPR, l'État n'aime pas faire les choses simplement. Donc pour ce qui est des données relatives à un véhicule ou un objet signalé, il faut s'adresser à la CNIL (article 8 de l'arrêté du 7 juillet 2017). Cette procédure semble être en contradiction avec les nouvelles dispositions des articles 105 et suivants de la loi du 6 janvier 1978. C'est possible qu'il faille s'adresser à la Direction générale de la police nationale ou à la Direction générale de la gendarmerie nationale.

Pour ce qui est des données relatives à un véhicule ou un objet perdu ou volé, il faut s'adresser directement à la Direction générale de la police nationale (Place Beauvau, 75800 PARIS CEDEX 08) ou à la Direction générale de la gendarmerie nationale (4 Rue Claude-Bernard, CS 60003, 92136 ISSY-LES-MOULINEAUX CEDEX) (article 8 alinéa 2 de l'arrêté du 7 juillet 2017).

4. Nouvelle Main courante informatisée (N-MCI / MCPN)

Il s'agit d'un fichier qui permet l'informatisation de l'enregistrement des mains courantes par les services de la police nationale. Il a pour but le suivi des mains courantes et le contrôle de l'activité des policiers. Il est régi par l'arrêté du 22 juin 2011 modifié par l'arrêté du 9 août 2016 (avis de la CNIL n°2016-091 du 7 avril 2016), puis par l'arrêté du 29 janvier 2024 (qui intègre simplement des modifications de noms de service dans la lignée de la réforme de la police judiciaire).

Au-delà des seules mains-courantes, le fichier est alimenté par les appels « police-secours » au 17, les appels aux commissariats, les appels provenant du SAMU, des taxis, des téléalarmes. Ce fichier a un rôle important dans l'élaboration des statistiques des infractions[30].

Tous les policiers ont accès aux données de N-MCI, ainsi que les « intervenants sociaux dans les commissariats » (souvent des travailleurs sociaux qui orientent les personnes vers des associations, ou qui peuvent rechercher un hébergement pour des personnes à la rue, ou formés aux violences conjugales).

Les magistrats du parquet (les procureurs) n'ont pas officiellement accès à N-MCI. Toutefois, il semble qu'ils utilisent ce fichier très souvent pour savoir si une personne est connue ou non des services de police.

Il y avait plus d'un million de fiches dans N-MCI en 2014.

30 Frédéric OCQUETEAU, *La main-courante informatisée, outil méconnu de la sécurité publique*, Questions pénales, CESDIP, https://www.cesdip.fr/wp-content/uploads/2015/10/QP_08_2015.pdf

2.3 – Durée de conservation des données

L'article 3 du décret prévoit une conservation des données de 3 mois pour les personnes signalées à l'autorité judiciaire mais non poursuivies, et de 3 ans pour les personnes mises en cause ou victimes d'infractions en présence d'une procédure judiciaire.

2.4 – Accès, rectification et effacement des données

Quand il y a une enquête judiciaire et/ou un jugement, les règles relatives à l'accès, la rectification et l'effacement des données sont celles applicables à la copie du dossier en cours d'enquête et après l'enquête. Il s'agit donc de s'adresser au procureur de la République du Tribunal judiciaire dans le ressort duquel se sont produits les faits.

Lorsqu'il n'y a pas eu d'enquête judiciaire, les demandes d'accès, de rectification et d'effacement des données sont à adresser à la Direction des affaires criminelles et des grâces, ministère de la Justice, 13 place Vendôme, 75042 Paris cedex 01.

3. SIROCCO

Il s'agit du Système Informatisé de Recoupement, d'Orientation et de Coordination des procédures de Criminalité Organisé, créé par le décret n°2023-309 du 25 avril 2023. Ce fichier est utilisé par les juges d'instruction au sein des Juridictions Interrégionales Spécialisées (JIRS) et de la Juridiction Nationale chargée de la Lutte contre la Criminalité Organisée (JUNALCO), qui sont donc chargés d'enquêter sur les dossiers de criminalité organisée qui ont une certaine ampleur et qui dépassent les limites d'une juridiction.

Le décret a été précédé d'un avis n°2022-105 de la CNIL du 20 octobre 2022.

Il est relié au Dossier pénal numérique (DPN) qui permet la numérisation des procédures pénales et à CASSIOPEE (Chaîne Applicative Supportant le Système d'Information Oriente Procédure pénale Et Enfants), qui concerne les éléments de base des procédures pénales.

3.1 – Données concernées

L'ensemble d'une procédure pénale (en criminalité organisée) est susceptible d'entrer dans SIROCCO : Procès-verbaux, documents annexes non versés dans la procédure, nom, prénom, surnoms, sexe, date et lieu de naissance, infractions, saisies, coopération internationale concernant les personnes mises en cause, mises en examen, placées sous statut de témoin assisté, poursuivies ou condamnées. S'agissant des victimes et des témoins, les données sont celles apparaissant dans la procédure pénale.

En cas de nécessité absolue, ces données peuvent concerner « *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* ».

stupéfiants, radicalisation violente, atteintes aux personnes dépositaires de l'autorité publique (PDAP), « *infractions commises dans le cadre ou en marge des événements de nature à entraîner un danger grave et imminent pour la sécurité ou l'ordre public* » (notamment les manifestations), radicalisation violente…

Sa création a été précédée d'un avis de la CNIL n°2023-055 du 15 juin 2023.

2.1 – Données concernées

Les données recueillies peuvent concerner à la fois les personnes mises en cause pour une infraction, les personnes victimes, celles qui ont été signalées auprès de l'institution judiciaire (ex : suspicion de maltraitance d'enfants), mais aussi les personnes qui sont apparues dans la procédure (par exemple les témoins).

Les données concernées apparaissent à l'article 3 du décret, liste précisée par un tableau en annexe. Il s'agit de :

- toutes les données d'état civil (nom, prénom, date et lieu de naissance, filiation), adresse, numéro de téléphone, adresse mail,

- en plus, pour les personnes mises en cause : toutes les données relatives à la procédure (garde à vue, orientation pénale, antécédents judiciaires, mesures prises, condamnations etc.), la situation patrimoniale (numéro de compte en banque), professionnelle et familiale, mais aussi des éléments médicaux : suivi médical, expertise psy, hospitalisation sans consentement, addictions.

Ce n'est pas inscrit dans les articles du décret, mais on découvre en annexe que les données relatives aux opinions politiques, à l'appartenance syndicale mais aussi à l'orientation sexuelle, aux convictions religieuses ou à l'origine ethnique peuvent être collectées (seulement concernant les violences intrafamiliales pour l'orientation sexuelle, et seulement concernant les atteintes aux personnes dépositaires de l'autorité publique, les infractions à la sécurité et l'ordre public et la radicalisation violente pour les opinions politiques).

2.2 – Utilisation de SISPoPP

Le fichier est accessible aux magistrats, personnel judiciaire, greffe, délégué du procureur, ainsi qu'à l'administration pénitentiaire et aux services de protection judiciaire de la jeunesse (quand un mineur est impliqué).

L'accès aux données peut également être accordée par le procureur, de manière limitée, aux policiers et gendarmes qui mènent les enquêtes, mais aussi aux préfets et aux élus locaux (en particulier les maires).

4.1 – Données concernées

Outre les données relatives à l'agent qui remplit la fiche, N-MCI contient, concernant les personnes qui déposent une main courante ou qui sont concernées par celle-ci, leur état civil, filiation, et contact.

Lorsqu'une personne se rend dans un commissariat, N-MCI enregistre également son état civil et le motif de sa visite. Les agents ont un champ libre pour décrire les détails qu'ils veulent sur l'événement enregistré dans la fiche.

4.2 – Conservation des données

Les données recueillies lorsqu'une personne se rend dans un commissariat sans déposer de main courante ou de plainte sont conservées pendant 1 an, puis elles sont anonymisées et conservées à des fins statistiques.

Les autres données sont conservées pendant 5 ans.

4.3 – Droit de communication, de rectification et d'effacement

On peut demander les informations nous concernant contenues dans N-MCI directement à la Direction Générale de la Police Nationale, Place Beauvau, 75800 PARIS CEDEX 08. Pour l'effacement, il faut également s'adresser à la Direction Générale de la Police Nationale.

5. GendNotes

Il s'agit d'une application mobile de prise de notes, créée par le décret n°2020-151 du 20 février 2020. L'idée, c'est de permettre aux gendarmes de prendre des notes sur leur smartphone au cours de toutes leurs missions et de leur donner la possibilité de les transmettre aux procureurs.

À sa création, le fichier GendNotes devait être interconnecté avec un nombre indéterminé d'autres fichiers. Cela a été annulé par un arrêt du Conseil d'État du 13 avril 2021 (n°439360) suite au recours de plusieurs associations.

5.1 – Données concernées

C'est extrêmement large : les gendarmes peuvent noter « l'ensemble des éléments relatifs aux personnes, aux lieux ou aux objets qui sont recueillis », donc tout et n'importe quoi, mais c'est pas tout. Les gendarmes peuvent aussi recueillir toutes les informations relatives aux différentes procédures, lors de gardes à vue (donc on peut imaginer qu'à côté des PV d'audition et autres, on se retrouve avec des notes éparses des gendarmes dans les dossiers de procédure au pénal) et « lors du traitement de certaines infractions relatives à la police de la route » (l'arrêté ne dit pas lesquelles, le gendarme appréciera?).

Donc c'est open bar. Mais ça va plus loin que l'open bar :

Le fichier contient aussi la photographie de la personne et même selon l'article 2 du décret du 20 février 2020, les données relatives à « *la prétendue* ***origine raciale ou ethnique***, *aux* ***opinions politiques***,

philosophiques ou religieuses, à l'appartenance ***syndicale****, à la santé ou à la* ***vie sexuelle ou l'orientation sexuelle*** ».

D'habitude, ce genre de données sont réservées aux services de renseignement. Là, on appréciera que tout gendarme peut faire ce qu'il veut (avec la seule limite du « strictement nécessaire », mais on voit bien que les juges ne le contrôleront jamais et que si d'aventure un dossier leur arriverait entre les mains ils seront bienveillants à l'égard des cognes).

5.2 – Utilisation des données

Bien sûr, les gendarmes peuvent consulter toutes ces données qu'ils ont eux-mêmes collectées, ainsi que les procureurs à qui ils les ont envoyés. Mais ça va beaucoup plus loin :

Le préfet, et même le maire peuvent en avoir connaissance !

5.3 – Durée de conservation des données

Les données sont conservées 3 mois et cette durée peut être prolongée à chaque fois qu'un nouveau fait est consigné dans la même fiche dans ce délai. Donc, si un gendarme écrit une note le 1er janvier, les données sont effacées le 1er avril, sauf si, par exemple le 29 mars, le gendarme ajoute quelque chose.

La limite est d'un an : le 1er janvier suivant, les données sont effacées.

5.4 – Consultation, rectification et effacement des données

Les droits de consultation, de rectification et d'effacement des données s'exercent directement auprès de la Direction Générale de la Gendarmerie Nationale, 4 rue Claude-Bernard, CS 60003, 92136 Issy-les-Moulineaux Cedex.

6. ARDOISE et ICARE, remplacés par LRPPN et LRPGN

ARDOISE et ICARE n'étaient pas des fichiers, mais plutôt des logiciels. ARDOISE pour la police nationale, ICARE pour la gendarmerie, servaient à accéder au STIC et à JUDEX. Avec le TAJ, ARDOISE a été remplacé par LRPPN (Logiciel de Rédaction des Procédures de la Police Nationale) et ICARE par LRPGN (Logiciel de Rédaction des Procédures de la Gendarmerie Nationale).

LRPPN et LRPGN sont donc des fichiers jumeaux, l'un côté police, l'autre côté gendarmerie. Bizarrement, LRPGN a été réformé en 2021 (décret n°2021-928 du 12 juillet 2021), mais pas LRPPN – LRPPN ayant eu vocation à être remplacé par SCRIBE, mais ce projet semble avoir été abandonné en 2022.

LRPPN et LRPGN alimentent automatiquement le TAJ, FOVeS et CASSIOPEE, et échangent des informations avec GASPARD NG (le logiciel qui permet de remplir simultanément le TAJ et le FAED).

Les règles relatives à ces fichiers sont dans les décrets n°2011-110 et 2011-111 du 27 janvier 2011.

Partie 13 : Fichiers de justice : Fichiers de fonctionnement et fichiers secondaires

Ces fichiers sont utilisés en interne par les magistrats. Ils servent soit au fonctionnement de la justice (CASSIOPÉE, VIGIE, SIAJ et SIROCCO par exemple), soit à l'existence des dossiers de procédure (« Numérisation des procédures pénales », REDEX par exemple), soit à l'application des peines (APPI et autres).

Ils ont moins d'importance pour les personnes concernées que les fichiers d'antécédents et d'application des peines de la partie 2.

Les seules modifications notables depuis la dernière mise à jour concerne les fichiers clandestins créés par les parquets pendant le mouvement contre la réforme des retraites en 2023, et leur légalisation par la création de SISPoPP (Système informatisé de suivi de politiques pénales prioritaires) par le décret n°2023-935 du 10 octobre 2023.

1. Fichiers clandestins créés par les parquets

Comme si la panoplie à leur disposition ne suffisait pas, les procureurs de la République ont tendance, lors de mouvements sociaux, à créer des fichiers sauvages et clandestins de manifestant.es, par exemple sur des tableaux Excel qu'ils se partagent entre eux.

La plupart du temps ces fichiers restent secrets et personne n'en connaît l'existence à part les personnels des tribunaux, mais des fois il y a des loupés.

Par exemple, pendant le mouvement contre la réforme des retraites en 2023, le parquet de Lille a créé un tableau Excel enregistrant sur des bases politiques les identités des manifestants interpellés. le Tribunal administratif de Lille a enjoint, en référé liberté, à la procureure de la République près le Tribunal judiciaire de Lille et au ministre de la justice d'effacer les données contenues dans ce fichier intitulé « suivi des procédures pénales : mouvement de la réforme des retraites » (TA Lille, 19 mai 2023, n°2304177 et 2304186).

2. Système informatisé de suivi de politiques pénales prioritaires (SISPoPP)

Après le scandale du fichage illégal des manifestants par le procureur de la République de Lille pendant le mouvement contre la réforme des retraites en 2023, le gouvernement a créé SISPoPP (Système informatisé de suivi de politiques pénales prioritaires) pour légaliser le fichage des manifestants, dans l'avenir, avec le décret n°2023-935 du 10 octobre 2023. Ce fichier est censé représenter un outil de pilotage et d'évaluation des politiques pénales considérées comme prioritaires : violences intra-familiales, trafics de

De nombreuses personnes peuvent accéder à ces données, dont les magistrats, les policiers et les gendarmes, les préfets, les associations d'aides aux victimes, certains personnels de l'assurance maladie, certains personnels des services des impôts, certains personnels de la caisse nationale d'allocation familiale.

Il est possible de s'opposer à ce que ses données soient transmises à certains de ces destinataires. Pour l'exercice de ce droit, ainsi que de l'accès, la rectification, et la limitation du traitement, il faut s'adresser au service en charge de l'aide aux victimes du secrétariat général du ministère de la justice.

13. Fichier des personnes sans domicile ni résidence fixe (SDRF)

Le fichage des « gens du voyage » est un précurseur de tous les fichiers qui existent aujourd'hui. Il a débuté avec une demande du ministère de l'intérieur aux préfets, le 20 mars 1895, de recenser les « bohémiens » selon le terme employé à l'époque. Est ensuite apparu le carnet anthropométrique qui visait les « nomades » (loi du 16 juillet 1912), remplacé en 1969 par le livret spécial de circulation, le livret de circulation et le carnet de circulation qui visent les « gens du voyage » (loi du 3 août 1969). Le carnet de circulation a été supprimé par une décision du Conseil constitutionnel du 5 octobre 2012. En parallèle, le fichier SDRF a été créé en 1994 (arrêté du 22 mars 1994). Il servait à assurer le suivi des titres de circulation délivrés aux personnes circulant en France sans domicile ni résidence fixe et visait surtout les « gens du voyage ». Ces titres de circulation (livret de circulation et livret spécial de circulation) ont été supprimés par l'article 195 de la loi n°2017-86 du 27 janvier 2017. En conséquence, l'arrêté du 19 septembre 2017 supprime le fichier SDRF. Enfin, le fichier MENS (Minorités Ethniques Non Sédentarisées), a existé illégalement pendant longtemps, principalement géré par l'Office central de lutte contre la délinquance itinérante (OCLI) de la gendarmerie nationale[84]. Ça ne veut pas dire que d'autres fichiers ne continuent pas d'exister illégalement.

84 https://www.liberation.fr/societe/2010/10/08/un-fichier-bien-cache-stigmatise-les-roms_684944/

6.1 – Données concernées

LRPPN et LRPGN agrègent tout un tas de données, semblables à celles du TAJ : l'état civil des personnes mises en cause, victimes et témoins des infractions, leur surnom, date de naissance, lieu de naissance, filiation, nationalité, nom du ou de la partenaire/conjoint·e, nationalité, diplômes, permis de conduire, adresse, adresses électronique, numéros de téléphone, ainsi que les informations relatives aux gardes à vue éventuelles.

Côté LRPPN, il est précisé qu'il peut comporter des photographies des personnes mises en cause et des victimes, et que **les caractéristiques techniques de ces photographies permettent de recourir à la reconnaissance faciale**.

Côté LRPGN, le décret du 12 juillet 2021 a permis de préciser que les photographies des personnes mises en cause et des victimes peuvent être versées dans le fichier. Il ne précise pas la possibilité de mettre en œuvre la reconnaissance faciale. Côté LRPGN toujours, le décret du 12 juillet 2021 a ajouté les empreintes digitales des personnes mises en cause.

6.2 – Utilisation de LRPPN et LRPGN

Ils sont utilisés par la police et la gendarmerie, ainsi que par les magistrats (juges et procureurs), au cours des enquêtes judiciaires. Ils peuvent être utilisés aussi pour certaines enquêtes administratives (pour l'accès à certains emplois, par exemple dans la sécurité, le nucléaire ou autres secteurs sensibles, et l'acquisition de la nationalité française).

6.3 – Conservation des données

Les textes ne prévoient pas de durée maximale de conservation des données. Ils prévoient seulement que les données sont effacées 5 ans (côté LRPPN) et 3 ans (côté LRPGN) après la transmission de la procédure à l'autorité judiciaire ou à l'autorité administrative… **donc si la procédure n'est jamais transmise, les données ne sont jamais effacées.**

6.4 – Droit de communication, de rectification et d'effacement

L'article 6 du décret n°2011-110 du 27 janvier 2011 (LRPPN) prévoit que ces droits s'exercent auprès de la CNIL. Cependant, cela est en contradiction avec les articles 104 à 106 de la loi n°78-17 du 6 janvier 1978 tels que modifiés par l'ordonnance n°2018-1125 du 12 décembre 2018, qui prévoient qu'il faut s'adresser au responsable du traitement. Ça a été corrigé côté LRPGN, mais pas côté LRPPN.

En conséquence, il faut appliquer les articles 104 à 108 de la loi du 6 janvier 1978, et s'adresser, pour LRPPN, à la direction générale de la police nationale du ministère de l'intérieur (Place Beauvau, 75800 PARIS CEDEX 08).

Pour LRPGN, il faut s'adresser à la direction générale de la gendarmerie nationale du ministère de l'intérieur (Place Beauvau, 75800 PARIS CEDEX 08).

On peut ainsi demander la communication de l'ensemble des données nous concernant dans le LRPPN et dans le LRPGN (article 105 de la loi n°78-17 du 6 janvier 1978), ainsi que des précisions concernant les finalités de ces fichiers (article 105 1° de la même loi), les catégories de données concernées (article 105 2°), les destinataires français et étrangers des données nous concernant (article 105 3°), la durée de conservation des données (article 105 4°), l'existence du droit de demander la rectification et l'effacement des données nous concernant (article 105 5°), et la communication des données en cours de traitement et leur source (article 105 7°).

Côté LRPGN (mais pas côté LRPPN), il est prévu que la direction générale de la gendarmerie nationale peut refuser de donner les informations personnelles contenues dans LRPGN, ou n'en donner qu'une partie (article 107 I et II 2° de la loi du 6 janvier 1978 et article 7 II du décret n°2011-111 du 27 janvier 2011). Elle doit alors en informer la personne (article 107 III de la loi du 6 janvier 1978). Quand on demande la rectification ou l'effacement des données, la direction générale de la gendarmerie nationale peut refuser de le faire, et même ne pas informer la personne de son refus (article 7 II du décret n°2011-111 du 27 janvier 2011 et article 107 II 2° et 3° et III de la loi du 6 janvier 1978). Quand la direction générale de la gendarmerie nationale refuse de communiquer certaines informations, ou refuse de rectifier ou d'effacer des informations, il est possible soit de contester ce refus devant la CNIL (3 place de Fontenoy, TSA 80715, 75334 PARIS CEDEX 07) en application des articles 104 et 108 de la loi du 6 janvier 1978 et de l'article 7 du décret n°2011-111 du 27 janvier 2011, soit de contester ce refus devant le tribunal administratif de Paris. Il vaut mieux demander à un·e avocat·e.

Côté LRPPN, la direction générale de la police nationale n'a pas le droit de refuser à une personne qui en fait la demande l'accès à ses informations personnelles. Elle peut toujours refuser la rectification ou l'effacement de ces informations. Pour faire la demande, il faut s'adresser à la direction générale de la police nationale, ministère de l'intérieur (Place Beauvau, 75800 PARIS CEDEX 08). En cas de refus ou de silence gardé pendant 2 mois par l'administration, c'est possible d'exercer un recours auprès de la CNIL (3 place de Fontenoy, TSA 80715, 75334 PARIS CEDEX 07). C'est aussi possible de contester ce refus devant le tribunal administratif de Paris. Il vaut mieux demander à un·e avocat·e.

Toutes ces demandes sont à envoyer par lettre recommandée avec accusé de réception, accompagnées d'une copie de pièce d'identité.

Il a été créé par le décret n°2018-175 du 9 mars 2018 et s'insère dans le dispositif ORSAN (à la base, l'organisation des secours en cas de catastrophe climatique, d'épidémie ou d'attentat). Les dispositions qui l'encadrent sont aux articles L3131-9-1 et R3131-14-10 et suivants du code de la santé publique.

SI-VIC (ou SIVIC, SiVic) est utilisé par les personnels soignants (SAMU, médecins, personnels hospitaliers, etc) et est placé sous la responsabilité du ministère de la santé.

Cependant il a toute sa place ici en raison de son utilisation pendant les manifestations pour ficher les manifestants qui se rendent à l'hôpital (nom, prénom, etc, blessure, origine supposée de la blessure, voire le signalement de la personne jusqu'à la couleur de ses chaussettes[83]). SI-VIC est donc un outil efficace qui permet à l'hôpital de devenir un auxiliaire de la police nationale.

Il utilise le même numéro d'identification que le fichier SINUS, qui permet de délivrer à chaque victime un numéro unique et est géré par le ministère de l'intérieur. Pour le fichier SINUS (arrêté du 17 février 2010 du ministre de l'intérieur), les données sont conservées 1 mois à compter de la dernière mise à jour de la fiche.

Pour le fichier SI-VIC, il était prévu que les données soient conservées le temps de la prise en charge de la personne dans le système de santé (donc le temps de sa présence à l'hôpital, mais on ne sait pas si ce temps est prolongé en cas de consultations ultérieures)… Cette limite a été supprimée par le décret n°2022-1109 du 2 août 2022, de telle sorte qu'on ne sait pas combien de temps les données sont conservées.

Pour le fichier SI-VIC, on peut demander l'accès et la rectification des données à la Direction générale de la santé, 14 avenue Duquesne, 75350 PARIS SP 07.

Pour le fichier SINUS, il faut s'adresser au Secrétariat général de la zone de défense de Paris, 1bis rue de Lutèce, 75004 PARIS.

12. Système d'information interministériel des victimes d'attentats et de catastrophes (SIVAC)

Ce fichier a été créé par le décret du 13 septembre 2021 et il apparaît aux articles R2-15 et suivants du code de procédure pénale. Il est géré par le ministère de la justice. Son but est de rassembler les données sur les personnes concernées par les accidents, sinistres, catastrophes ou infractions, y compris les actes de terrorisme, susceptibles de provoquer de nombreuses victimes (c'est large), d'améliorer l'information et la prise en charge des victimes, et de produire des statistiques.

Les données collectées sont nombreuses, y compris celles concernant les personnes prenant attache avec les cellules d'information (conservées 6 mois), les personnes présentes sur les lieux et leurs proches (conservées 10 ans), et les victimes et leurs proches (conservées 10 ans, 15 ans en cas d'acte terroriste).

83 Le Canard Enchaîné, 24 avril 2019

d'appel). La demande doit être formulée par lettre recommandée avec accusé de réception, ou par déclaration au greffe (article R53-8-27 du code de procédure pénale). Si la personne est mise en examen, la demande doit être faite au juge d'instruction.

Le procureur ou le juge d'instruction a 2 mois pour se prononcer. En cas de silence du procureur ou du juge d'instruction pendant 2 mois, ou en cas de refus du procureur ou du juge d'instruction, il est possible de contester cette décision. Avant la loi n°2020-1672 du 24 décembre 2020, il fallait passer par le juge des libertés et de la détention. La loi semble avoir supprimé cette étape (mais les articles R53-8-27 et suivants du code de procédure pénale n'ont pas été modifiés), et ce recours doit être exercé devant le président de la chambre de l'instruction (article 706-53-10) dans un délai de dix jours. Il vaut mieux l'assistance d'un·e avocat·e.

10. MISP-PJ

Ce fichier a été créé par un arrêté du 22 décembre 2021 et est géré par la direction générale de la police nationale.

Il a pour but de lutter contre les atteintes aux traitements automatisés de données (les autres fichiers).

Il regroupe des informations issues de sources ouvertes (publiques) et des informations relatives aux procédures judiciaires ouvertes (informations sur les victimes d'attaques informatiques, les numéros de procédures, les faits, et concernant les auteurs, leurs adresses IP, adresses électroniques, etc).

Peuvent accéder aux données les agents de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (DCPJ), ceux du Centre de lutte contre les criminalités numériques (DGGN), ceux de la Brigade de lutte contre la cybercriminalité (Préfecture de police de Paris), les magistrats du parquet ainsi que les enquêteurs (dans la limite de leur besoin) et les organismes de coopération internationale.

Les données sont enregistrées 6 ans à compter de leur enregistrement.

Les droits de consultation, de rectification et d'effacement des données s'exercent auprès de la Direction centrale de la police judiciaire, Place Beauvau, 75800 PARIS CEDEX 08.

11. Fichiers SINUS et SI-VIC (Système d'information pour le suivi des victimes)

À l'origine ce n'est pas un fichier de police mais de santé. Cependant son utilisation lors de manifestation, notamment au cours du mouvement des Gilets Jaunes, en a fait un mouchard des flics à l'intérieur des hôpitaux[82].

82 https://rebellyon.info/Fichier-SIVIC-et-fichage-des-manifestant-20576

7. Le système d'information et de communication de l'État (smartphones et tablettes NEOPOL et NEOGEND)

Le système d'information et de communication de l'État a été créé par le décret n°2014-879 du 1er août 2014, remplacé ensuite par le décret n°2019-1088 du 25 octobre 2019, lui-même profondément modifié par le décret n°2022-513 du 8 avril 2022. Un « avis sur le projet de mobilité des forces de sécurité intérieure NEOPOL-NEOGEND » du directeur interministériel du numérique daté du 20 avril 2016 précise que l'équipement des policiers et des gendarmes en smartphones et en tablettes numériques est une des applications de ce système d'information et de communication[31].

Au début de l'année 2022, il a été décidé de doter les personnels de police et de gendarmerie de nouveaux smartphones (110'000 pour la gendarmerie et 116'000 pour la police nationale) et de nouvelles tablettes (20'000 au total)[32].

Ces terminaux informatiques disposent de nombreuses applications, par exemple :

- GOPSERVE : géolocalisation des gendarmes et des policiers
- PRATICp (Photographie Rapide et Adaptée pour les TICp) et NEO DK : prise de photos et d'empreintes digitales, consultation et alimentation de fichiers, en cours de déploiement en 2023
- GendSafe : Secourisme,
- GENDNOTES : Prise de notes (voir le fichier GENDNOTES plus haut).

Ils permettent ainsi, pour les gendarmes, de se connecter à BDSP (base de données de la sécurité publique) qui regroupe les fichiers GSI (gestion des sollicitations et des interventions), SIDPP (sécurisation des interventions et demandes particulières de protection), GEA (gestion des évènements d'ampleur). Les gendarmes habilités ont aussi accès au GIPASP.

8. ADOC (Accès aux Dossiers des Contraventions)

Le fichier a été créé par l'arrêté du 13 octobre 2004. Il s'agissait d'enregistrer les infractions des radars automatiques (excès de vitesse, feux rouges).

Il est géré par le ministère de l'intérieur, et plus précisément par le Centre national de traitements de Rennes.

Pendant le confinement en 2020, il a été utilisé illégalement pour enregistrer les contraventions de non-respect de confinement, afin de pouvoir mettre en prison les personnes qui étaient verbalisées à 4 reprises pendant 30 jours. Cependant cette utilisation était illégale.

31 https://www.numerique.gouv.fr/uploads/neopol_neogend_art_3.pdf
32 https://www.gendarmerie.interieur.gouv.fr/gendinfo/actualites/2022/neo-2-une-manaeuvre-strategique-technologique-et-logistique-d-ampleur

Du coup, le 14 avril 2020, un nouvel arrêté est publié. Désormais, ce fichier peut enregistrer toutes les infractions faisant l'objet d'une procédure d'amende forfaitaire (contraventionnelle et délictuelle).

Les délits concernés ne sont pas nombreux, mais très courants: conduite sans permis, conduite sans assurance, violation du confinement, vol à l'étalage et consommation de stupéfiants.

Il s'agit donc d'un fichier renouvelé qui permet de ficher tous les consommateurs de stupéfiants.

8.1 – Données concernées

Le fichier ADOC concerne maintenant presque toutes les contraventions, et même certains délits (voir plus haut).

Il rassemble les photographies des véhicules prises par les radars automatiques, leur lieu, heure, plaque d'immatriculation des véhicules, nature de l'infraction, nom des agents verbalisateurs, nom, prénom et identité des personnes ayant commis la contravention, informations relatives au permis de conduire, au véhicule, au paiement des amendes, au retrait de points, aux contestations de l'infraction, montant de l'amende, etc.

Il permet même de ficher les ascendants du conducteur.

8.2 – Utilisation des données

Les données sont utilisées par les agents du Centre national de traitements, les juges et procureurs, les OPJ et APJ, les APJ adjoints, les gardes champêtres (seulement pour les contraventions routières), les agents de surveillance de la voie publique (ASVP, pour les contraventions routières), les préfets (pour la délivrance des cartes grises), le ministère de l'intérieur (pour la délivrance des permis de conduire).

Elles peuvent être communiquées à l'étranger, en particulier aux États membres de l'Union européenne.

Le fichier est interconnecté avec le fichier national des immatriculations, le fichier national des permis de conduire (FNPC), les fichiers des entreprises de location de voiture (Hertz, Europcar et autres), le fichier Minos (ordonnances pénales et jugements des tribunaux de police), « Numérisation des procédures pénales », le Système d'immatriculation des véhicules (SIV), la base satellite des véhicules volés, le TAJ, le fichier des véhicules terrestres à moteur assurés, CASSIOPÉE.

8.3 – Durée de conservation des données

Les données sont conservées pendant 10 ans pour les délits et les contraventions au code de la route. Les données relatives aux autres contraventions sont conservées 5 ans.

8.4 – Droit d'accès, de rectification et d'effacement des données

Il faut s'adresser au Centre national de traitement automatisé, CS 41101, 35911 RENNES Cedex 9 pour accéder aux données.

9. Fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes (FIJAISV)

Il a été créé en 2004 par la loi Perben II et est tenu par le Service du casier judiciaire (ministère de la justice). Les règles qui le régissent sont aux articles 706-53-1 et suivants et R53-8-1 et suivants du code de procédure pénale.

9.1 – Données contenues dans le fichier

Il concerne les personnes ayant fait l'objet d'une 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).

Les mineurs de moins de 13 ans ne sont pas inscrits dans le fichier. Pour les mineurs de 13 à 18 ans, ils sont inscrits dans le fichier sur décision du juge ou du procureur de la République.

Les personnes fichées le savent et doivent déclarer leurs changements d'adresse.

Le fichier peut être consulté par les préfectures, l'éducation nationale, les rectorats, les académies, la protection judiciaire de la jeunesse, l'administration pénitentiaire, la direction de la jeunesse et de l'éducation populaire et la direction des sports, les directeurs généraux des agences régionales de santé, et les directions régionales de l'économie, de l'emploi, du travail et des solidarité, les directions départementales de la cohésion sociale, pour les procédures de recrutement concernant une activité ou une profession impliquant un contact avec des mineurs.

9.2 – Durée de conservation des données

Les informations sont conservées pendant 20 ans, et 30 ans s'il s'agit d'un crime ou d'un délit puni de 10 ans d'emprisonnement. Elles sont conservées pendant 10 ans lorsque l'auteur est un mineur.

Si une personne exécute une peine privative de liberté, ces délais débutent à compter de sa libération.

9.3 – Droit de communication, de rectification et d'effacement des données

Le droit de communication des données s'exerce auprès du procureur de la République près le tribunal judiciaire dans le ressort duquel la personne réside (article 706-53-9 du code de procédure pénale). Les données la concernant lui seront communiquées comme il est fait pour le volet B1 du casier judiciaire : la personne est convoquée au tribunal, et elle peut consulter ces informations, sans pouvoir les copier ou les prendre en photo (elle peut normalement prendre des notes).

En ce qui concerne la rectification et l'effacement des données, la demande doit être portée au procureur de la République près le tribunal judiciaire qui a prononcé la dernière condamnation (si c'est une cour d'appel, c'est le procureur de la République près le tribunal judiciaire où se situe le siège de la cour

- le fait de quitter le territoire malgré une interdiction de sortie du territoire prise à l'encontre d'une personne de nationalité française dont il existe des raisons sérieuses de penser qu'elle projette d'aller à l'étranger pour participer à des activités terroristes ou de rejoindre un théâtre d'opération de groupements terroristes en application de l'article L224-1 du code de la sécurité intérieure ;
- le fait de ne pas respecter une décision de contrôle administratif (interdiction de quitter un périmètre géographique, pointer au commissariat, etc) prise à l'encontre d'une personne partie à l'étranger, vers un théâtre d'opérations de groupements terroristes, et qui en revient (articles L225-1 et suivants du code de la sécurité intérieure) ;
- les personnes condamnées pour provocation ou apologie d'un acte de terrorisme (article 421-2-5 du code pénal) ;
- les personnes condamnées pour l'extraction, la reproduction ou la transmission de données faisant l'apologie d'actes de terrorisme (article 421-2-5-1 du code pénal).

Attention, en cas d'exécution d'une peine privative de liberté, ces délais ne commencent à courir qu'à compter de la libération de la personne.

8.3 – Droit de communication, de rectification et d'effacement des données

Le droit de communication des données s'exerce auprès du procureur de la République près le tribunal judiciaire dans le ressort duquel la personne réside (article 706-25-11 du code de procédure pénale). Les données la concernant lui seront communiquées comme il est fait pour le volet B1 du casier judiciaire : la personne est convoquée au tribunal, et elle peut consulter ces informations, sans pouvoir les copier ou les prendre en photo (elle peut normalement prendre des notes).

En ce qui concerne la rectification et l'effacement des données, la demande doit être portée au procureur de la République près le tribunal judiciaire qui a prononcé la dernière condamnation (si c'est une cour d'appel, c'est le procureur de la République près le tribunal judiciaire où se situe le siège de la cour d'appel). La demande doit être formulée par lettre recommandée avec accusé de réception, ou par déclaration au greffe (article R50-55 du code de procédure pénale). Si la personne est mise en examen, la demande doit être faite au juge d'instruction.

Le procureur ou le juge d'instruction a 3 mois pour se prononcer. En cas de silence du procureur ou du juge d'instruction pendant 3 mois, ou en cas de refus du procureur ou du juge d'instruction, il est possible de contester cette décision. Avant la loi n°2020-1672 du 24 décembre 2020, il fallait passer par le juge des libertés et de la détention. La loi semble avoir supprimé cette étape (mais les articles R50-56 et suivants du code de procédure pénale n'ont pas été modifiés), et ce recours doit être exercé devant le président de la chambre de l'instruction (article 706-25-12) dans un délai de dix jours. Il vaut mieux l'assistance d'un·e avocat·e.

Pour obtenir l'effacement, il faut en faire la demande au procureur de la République de Rennes, et avoir eu une décision de relaxe pour la contravention ou le délit pour lequel on est fiché (article 3 de l'arrêté du 13 octobre 2004). C'est aussi possible de demander l'effacement si la personne a récupéré ses points au permis de conduire (qui entraîne, pour les infractions routières, un classement sans suite).

Ainsi, si la procédure est classée sans suite et ne concerne pas une infraction routière, on n'a pas la possibilité de faire effacer ses données… Cette disposition a été annulée par l'arrêt n°441317 du Conseil d'État du 22 septembre 2021 précisément car il n'est pas prévu de procédure d'effacement en cas de classement sans suite. Du coup, on peut considérer que c'est possible de demander l'effacement, également auprès du procureur de la République, en cas de classement sans suite d'une infraction autre que routière.

Il reste un problème car rien n'est prévu en cas de refus du procureur de la République ! L'État, ça ne lui pose aucun problème d'étendre énormément l'utilisation d'un fichier… mais prévoir une procédure pour assurer les droits des personnes, il est moins fan. Alors, il vaut mieux demander conseil à un·e avocat·e qui saisira, par exemple, le Tribunal judiciaire dans son ensemble, ou le Juge des libertés et de la détention, voire la chambre de l'instruction, par analogie avec d'autres fichiers (par exemple le TAJ).

Partie 4 : Fichiers de police : Principaux fichiers d'identification

Ces fichiers-là servent à identifier une personne. Le plus simple pour comprendre le fonctionnement, c'est : les gendarmes relèvent une empreinte digitale sur une voiture volée, puis ils cherchent dans leur fichier (le FAED) une empreinte digitale similaire. Ils ne cherchent alors que dans leurs fichiers de gendarmerie et de police, pas dans tous les fichiers, donc pour pouvoir retrouver à qui appartient l'empreinte, il faut que la personne ait déjà, dans le passé, au cours de n'importe quelle enquête, donné ses empreintes aux forces de l'ordre.

Il est question, ici, du fichier des empreintes digitales (le FAED), du fichier des empreintes génétiques (le FNAEG), et du lecteur automatique des plaques d'immatriculation (LAPI) qui est aussi très utilisée pour identifier des personnes.

Une remarque sur les empreintes digitales, qui apparaissent aussi dans le fichier des cartes d'identité et des passeports (le TES) : si une personne a seulement un passeport biométrique et est fichée au TES, sans n'avoir jamais donné ses empreintes à la police ou à la gendarmerie (elle n'est donc pas au FAED), les gendarmes ne la retrouveront pas en consultant le FAED. Bien sûr, il y a une exception : en cas d'atteinte aux intérêts fondamentaux de la nation ou en cas de terrorisme, les gendarmes peuvent consulter le TES (fichier des passeports et des cartes d'identité, article L222-1 du code de la sécurité intérieure). Et ces atteintes, ça recouvre beaucoup de choses (voir le TES dans la partie 1). Enfin, c'est possible d'obtenir une carte d'identité (mais pas un passeport) en refusant la conservation de la numérisation de ses empreintes digitales au-delà de 90 jours (voir le TES dans la partie 1).

1. Fichier automatisé des empreintes digitales (FAED)

C'est un fichier très ancien. Les premiers fichiers de police utilisant les empreintes digitales en France remontent à 1904-1907. Il est régi par plusieurs articles du code de procédure pénale et par le décret n°87-249 du 8 avril 1987.

Il est géré par le service national de police scientifique du ministère de l'intérieur, qui ne fait pas de zèle dans le respect de la loi : la CNIL a constaté le 24 septembre 2021 que ce service conserve dans le FAED des données non prévues par la loi, qu'il les conserve au-delà des délais autorisés, qu'il s'abstient de les effacer après une décision d'acquittement, de non-lieu, de relaxe ou de classement sans suite, qu'il s'abstient d'informer les personnes concernées, et que les mots de passe utilisés sont trop faibles[33].

33 Délibération du 24 septembre 2021, https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000044115170

8.1 – Données contenues dans le fichier et utilisation

Le fichier recense les personnes ayant fait l'objet d'une condamnation pour des faits de terrorisme (articles 421-1 et suivants du code pénal) ou d'une interdiction de sortie du territoire en lien avec des activités terroristes (articles L225-1 et L225-7 du code de la sécurité intérieure). Il a pour but d'augmenter leur contrôle, pendant l'exécution de leur peine et après celle-ci. Ça concerne les personnes condamnées majeures et mineures, les personnes ayant fait l'objet d'une décision d'irresponsabilité pénale pour trouble mental, et même au stade de l'instruction (article 706-25-4). En 2021, en ce qui concerne les personnes mises en examen (instruction), la demande du juge d'instruction a été supprimée ; l'inscription au FIJAIT est donc automatique. Ça concerne également les personnes condamnées par un tribunal étranger pour ces faits.

En 2021, ont été ajoutées à cette liste les personnes condamnées pour provocation au terrorisme, apologie du terrorisme, ou transmission d'apologie du terrorisme.

L'inscription au fichier des personnes condamnées, ou déclarées irresponsables pénalement, et des personnes mises en examen, peut être écartée par le juge qui prononce la condamnation ou la mise en examen.

Concernant les mineurs, ils ne sont pas inscrits dans le FIJAIT en-dessous de 13 ans. À partir de 13 ans, ils sont inscrits si la juridiction qui les condamne l'ordonne, ou si le procureur de la République l'ordonne lorsqu'ils ont été condamnés à l'étranger ou reconnus irresponsables pénalement (article 633-2 du code de justice pénale des mineurs et dernier alinéa de l'article 706-25-4 du code de procédure pénale).

Outre n'importe quel type de flic, les maires y ont accès.

Les personnes fichées le savent et doivent déclarer leurs changements d'adresse et déplacements à l'étranger.

Le FIJAIT est utilisé, outre les contrôles auxquels la personne doit se soumettre, par les préfectures, les services des ressources humaines de l'éducation nationale, les rectorats, les services départementaux de l'éducation nationale, la protection judiciaire de la jeunesse, l'administration pénitentiaire, la police nationale, la gendarmerie et la DGSI pour toute demande de recrutement dans la fonction publique, tout emploi dans une installation classée SEVESO, tout emploi dans la sécurité, l'éducation et les transports, et tout emploi auprès d'un « opérateur d'importance vitale » (c'est défini par l'article R1332-2 du code de la défense et c'est large : justice, armées, sécurité civile, santé, gestion de l'eau, énergie, communications audiovisuelles et électroniques, etc).

8.2 – Durée de conservation des données

Les données sont conservées pendant 20 ans pour les majeurs, 10 ans pour les mineurs.

La durée de conservation des données est plus courte (5 ans pour les majeurs, 3 ans pour les mineurs à compter de la condamnation) pour les infractions suivantes :

responsable du traitement. Il faut donc appliquer ces nouvelles dispositions et s'adresser à la Direction générale de la police nationale, Place Beauvau, 75800 PARIS CEDEX 08.

7. Fichier des interdictions de sortie du territoire

Il a été créé par l'arrêté du 7 août 2017 *portant autorisation d'un traitement de données à caractère personnel relatif à l'instruction et au suivi des interdictions de territoire*. Il est géré par la direction des libertés publiques et des affaires juridiques du ministère de l'intérieur.

Il concerne tout ressortissant français ayant fait l'objet d'une interdiction de sortie du territoire national lorsqu'il existe des raisons sérieuses de penser qu'il projette des déplacements à l'étranger pour participer à des activités terroristes, ou pour rejoindre un théâtre d'opérations de groupements terroristes, en application de l'article L224-1 du code de la sécurité intérieure.

Les personnes qui font l'objet d'une telle interdiction de sortie du territoire en sont informées.

Ce fichier contient tout l'état civil de la personne concernée, les données relatives à l'interdiction de sortie du territoire (sa date, la mention de la restitution de sa carte d'identité et de son passeport aux autorités, le numéro du récépissé justifiant de son identité qui lui a été remis, etc).

Il n'est interconnecté avec aucun autre fichier. Il contient seulement la mention de l'inscription de la personne au FPR et au FOVeS.

Ce fichier est utilisé par les policiers et les gendarmes chargés de la procédure d'interdiction de sortie. Peuvent y avoir aussi accès tous les policiers et les gendarmes chargés des contrôles d'identité, et les agents chargés de la délivrance des cartes d'identité et des passeports.

Les données sont conservées 3 ans à compter de la décision de l'interdiction de sortie du territoire, durée renouvelée à chaque nouvelle interdiction de sortie du territoire, avec un maximum de 20 ans.

Pour l'accès et la rectification des données, il faut s'adresser au ministère de l'intérieur.

8. Fichier judiciaire national automatisé des auteurs d'infractions terroristes (FIJAIT)

Il a été créé en 2015 (décret n°2015-1840 du 29 décembre 2015) et est tenu par le Service du casier judiciaire (ministère de la justice). Les règles qui le régissent sont aux articles 706-25-3 et suivants du code de procédure pénale, et R50-30 et suivants du même code.

Il a été modifié en 2021, dans le sens d'un élargissement des cas dans lesquels une personne entre dans ce fichier, et d'une restriction des possibilités d'en sortir (article 8 de la loi n°2021-1109 du 24 août 2021 confortant le respect des principes de la République).

Selon le projet d'accord-cadre du Service des technologies et des systèmes d'information de la sécurité intérieure du 18 mai 2022[34], 6,7 millions de personnes sont enregistrées dans le FAED, 8,5 millions d'identités et il y a en tout 14,9 millions de signalisations. Environ 1,2 million de signalements s'ajoutent chaque année (soit 1,2 million de prises d'empreintes et de traces recueillies pendant les enquêtes pénales). Il est également prévu que, à terme, le FAED soit interconnecté avec le casier judiciaire pour permettre les échanges de données au niveau européen (les fichiers ECRIS et ECRIS-TCN en particulier, voir ces fichiers).

Attention, la Cour de justice de l'Union européenne a jugé, le 26 janvier 2023, dans l'affaire V.S c. Ministerstvo na vatreshnite raboti, C 205-21, concernant la Bulgarie, que la prise d'empreintes systématiques des personnes mises en examen est contraire à la directive 2016/680 du 27 avril 2016[35]. Cette décision peut également être utile pour contester le fichage systématique dans le FAED en France.

1.1 – Données concernées

Aujourd'hui, il permet d'enregistrer les empreintes digitales de quiconque soupçonné d'un crime ou d'un délit dans une enquête de flagrance (article 55-1 du code de procédure pénale), une enquête préliminaire (article 76-2 du code de procédure pénale), ou condamné pour un crime ou un délit, ou lors d'une vérification d'identité au commissariat d'une personne française (article 78-3 du code de procédure pénale) ou étrangère (articles L813-10, L142-2, L142-3 du code de l'entrée et du séjour des étrangers et des demandeurs d'asile). Il contient également les empreintes prises lors de l'incarcération d'une personne (article 3 4° du décret n°87-249 du 8 avril 1987).

Les empreintes peuvent aussi être prises sur une personne décédée, pour l'identifier.

Quand une personne est placée en garde à vue pour une enquête de flagrance ou pour une enquête préliminaire (c'est le cas dans la plupart des gardes à vue), les policiers ou les gendarmes prennent systématiquement ses empreintes et sa photographie. C'est possible de refuser, mais ça constitue un délit puni d'un an d'emprisonnement et de 15.000 euros d'amende (article 55-1 du code de procédure pénale). Ça ne veut pas dire que la personne va systématiquement être condamnée à cette peine, mais la peine prononcée varie beaucoup, de presque rien lorsqu'elle est relaxée pour le délit pour lequel elle est entrée en garde à vue, à quelques centaines d'euros d'amende et quelques mois de prison, le plus souvent avec sursis, lorsqu'elle est condamnée pour le délit principal.

Enfin, depuis la loi n°2022-52 du 24 janvier 2022 (article 55-1 alinéa 4 du code de procédure pénale et, pour les mineurs, article L413-17 du code de justice pénale des mineurs), lorsqu'une personne est placée en garde à vue ou en « audition libre », la prise d'empreintes digitales peut être effectuée de force.

34 Voir la série d'articles de NEXTINPACT: https://www.nextinpact.com/article/69249/le-fichier-empreintes-digitales-sera-interconnecte-avec-casier-judiciaire-13

35 Voir https://consultation.avocat.fr/blog/alexis-baudelin/article-46402-la-cour-de-justice-de-l-union-europeenne-interdit-la-collecte-systematique-des-donnees-biometriques-et-genetiques-de-toute-personne-mise-en-cause-dans-une-affaire-penale.html

Dès les premiers mois, cela a été un nouveau prétexte pour la police de tabasser et taser des personnes en garde-à-vue[36].

La prise d'empreintes forcée peut être effectuée aux conditions cumulatives suivantes :

- C'est l'unique moyen d'identifier la personne,
- Elle est entendue pour un crime ou un délit puni d'au moins trois ans d'emprisonnement,
- Elle refuse de justifier de son identité ou elle fournit des éléments d'identité manifestement inexacts.

Pour les mineurs, les conditions de la prise d'empreintes forcée sont les suivantes :

- C'est l'unique moyen d'identifier le mineur,
- Celui-ci est soupçonné d'un crime ou un délit puni d'au moins cinq ans d'emprisonnement,
- Il refuse de justifier de son identité ou il fournit des éléments d'identité manifestement inexacts,
- Il apparaît manifestement âgé d'au moins treize ans.

Le Conseil constitutionnel a ajouté que l'avocat·e de la personne doit être présent·e ainsi que, si elle est mineure, son représentant légal (10 février 2023, n°2022-1034).

Bien sûr, quand les empreintes sont prises de force, ça ne fait pas obstacle à des poursuites pour le refus de donner ses empreintes !

Ce fichier est accessible à un très grand nombre de policiers et gendarmes.

1.2 – Interconnexions du FAED avec d'autres fichiers

Le FAED est en lien avec CASSIOPEE (article 9 du décret du 8 avril 1987) et avec le casier judiciaire national (articles 771-1 et 771-2 du code de procédure pénale tels que modifiés par l'ordonnance n°2022-1524 du 7 décembre 2022).

Il est aussi en lien avec des fichiers européens et internationaux (article 9-1 du décret du 8 avril 1987) :

- les fichiers européens des bases de données prévues par le traité de Prüm du 27 mai 2005, pour lutter notamment contre le terrorisme, la criminalité transfrontalière et les migrations irrégulières ; cela inclut les manifestations de grande envergure, qu'elles soient politiques ou sportives (article 1er de la décision 2008/615/JAI du Conseil du 23 juin 2008) ;
- EURODAC, qui organise la conservation des empreintes digitales pour appliquer la procédure « Dublin » dans l'Union européenne (qui concerne les ressortissants étrangers qui veulent déposer une demande d'asile) (article 20 du règlement n°603/2013 du 26 juin 2013) ;
- tous les fichiers pris en application du titre V de la 3e partie du traité sur le fonctionnement de l'Union européenne, donc qui concernent l'espace de liberté, de sécurité et de justice de l'Union

36 Voir sur le sujet : https://www.laquadrature.net/2023/05/12/en-gav-tes-fiche%C2%B7e-episode-2-les-empreintes/

4.3 – Droit d'accès et de rectification indirect

En l'absence de texte l'ayant légalisé, le droit d'accès et de rectification s'effectue de manière indirecte, via la CNIL.

5. Fichier national des interdits d'acquisition et de détention d'armes (FINIADA)

Il est prévu aux articles L312-16 et R312-77 et suivants du code de la sécurité intérieure. Rien ne le précise explicitement, mais il doit être géré par le ministère de l'intérieur. Son but est de recenser les personnes qui font l'objet d'une décision d'interdiction d'acquisition et de détention d'armes.

L'article L312-3 du code de la sécurité intérieure prévoit une longue liste d'infractions qui, si elles apparaissent dans le bulletin n°2 du casier judiciaire, entraînent l'interdiction d'acquérir ou de détenir des armes. Par exemple, les violences volontaires, les menaces d'atteintes aux personnes, la participation à un attroupement ou à une manifestation en étant porteur d'une arme, etc.

Avant la condamnation, le préfet peut interdire à la personne d'acquérir ou de détenir une arme en application de l'article L312-3-1 du code de la sécurité intérieure, ce qui entraîne son inscription dans FINIADA.

La loi n°2022-52 du 24 janvier 2022 a introduit une interconnexion automatique entre le fichier du casier judiciaire et le FINIADA, pour que les condamnations à une peine d'interdiction de détenir une arme soient systématiquement inscrites au FINIADA (article L312-16-1).

La durée de l'inscription dans FINIADA correspond à la durée de l'interdiction de détention d'arme. Ça peut être long (l'inscription au volet B2 du casier judiciaire, c'est 40 ans).

C'est possible de demander l'effacement de l'inscription au B2, ce qui entraînera l'effacement de FINIADA (ce qu'il faudra peut-être demander au ministère de l'intérieur et à la CNIL).

Concernant l'interdiction par le préfet, c'est possible de contester cette décision du préfet, devant le tribunal administratif.

6. Fichier National des Interdits de Stade (FNIS)

Il a été créé par l'arrêté du 28 août 2007 du Ministre de l'intérieur. Il est mis en œuvre par la Direction générale de la police nationale. Il concerne les personnes visées par une interdiction de stade suite à une décision judiciaire ou administrative (articles L332-11 et suivants du code du sport). Les données sont conservées pendant 5 ans à compter de la fin de la dernière interdiction de stade.

L'article 8 de l'arrêté du 28 août 2007 prévoit que ces droits s'exercent auprès de la CNIL. Cependant, cela est en contradiction avec les articles 104 à 106 de la loi n°78-17 du 6 janvier 1978 tels que modifiés par l'ordonnance n°2018-1125 du 12 décembre 2018, qui prévoient qu'il faut s'adresser au

3.2 – Utilisation des données

Le SAS PARAFE interroge le FPR, SIS Schengen et le fichier des documents perdus ou volés d'Interpol. Si l'on figure au FPR, il y a de bonnes chances que le SAS ne s'ouvre pas, et clignote en rouge. Les personnes qui peuvent utiliser PARAFE sont les ressortissantes de l'Union Européenne ou de Suisse, Etats-Unis, Grande Bretagne, Canada, Japon (liste complète à l'article R232-6 du CSI). Peuvent avoir accès aux données les agents de la PAF et des douanes habilités dans les aéroports, ports maritimes et gares concernés.

3.3 – Conservation des données

Les images de vidéosurveillance du SAS, transmises en temps réel au poste de contrôle, sont effacées normalement à la sortie du SAS (R 232-8 du CSI). Sont conservées par contre pendant deux ans les informations sur le fait qu'on est passé.e par PARAFE, avec la date et l'heure.

3.4 – Accès, rectification et effacement

Les conditions relatives à l'accès, la rectification et l'effacement des données, prévues par l'article R232-10 du code de la sécurité intérieure, ont été modifiées par le décret n°2023-544 du 30 juin 2024. Dorénavant l'exercice de ces droits s'effectue auprès du ministère de l'Intérieur, ce qui est plus simple qu'auparavant (il fallait s'adresser à chaque gare ou aéroport dans lequel la personne était passée). Par contre, le décret a supprimé la mention relative à la demande d'effacement de données, semble-t-il en raison du fait que l'État considère ces données comme nécessaires pour une mission d'intérêt public. Cela n'empêche pas de le demander quand même.

4. Outil de Centralisation et de Traitement Opérationnel des Procédures et des Utilisateurs de Signatures (OCTOPUS)

Il est géré par la Direction de police urbaine de proximité de la Préfecture de police de Paris (Service régional de police des transports – Brigade des réseaux ferrés d'Île-de-France – Cellule tags). Ce fichier a été créé en 2008 et n'a aucune existence légale. Il a peut-être été supprimé depuis, peut-être pas, en tout cas rien ne dit qu'il a été légalisé. Il a pour but de recouper les informations concernant les tags et d'identifier les tagueurs et tagueuses pour pouvoir les condamner sur le fondement des articles 322-1 al.2 et R635-1 du code pénal.

4.1 – Données concernées

Il regroupe les lieux des tags, les constatations, les signatures, les crews et, quand c'est possible, l'identité des tagueuses et tagueurs.

4.2 – Durée de conservation des données

Aux dernières nouvelles, aucun texte n'a légalisé OCTOPUS, donc on ne sait pas.

(contrôle aux frontières, asile, immigration, coopération judiciaire en matière pénale, coopération policière) ;

- les fichiers d'INTERPOL et d'Europol.

Il y a pour projet d'interconnecter le FAED avec le FPR, le FNAEG, AGDREF 2 (le fichier des ressortissants étrangers en France), le FND, iGAV et VISABIO[37].

1.3 – Durée de conservation des données

Elle est régie par l'article 5 du décret n°87-249 du 8 avril 1987.

La durée de conservation est par défaut de **15 ans**. Cependant elle peut être de 25 ans dans certaines situations, par exemple pour toute personne suspectée de viol, ou de meurtre/assassinat sur mineur, de torture, etc. (liste à l'article 706-47 du code de procédure pénale), trafic de stupéfiants, vol en bande organisée, terrorisme, aide à l'entrée ou au séjour des étrangers en bande organisée, et autres (article 706-73 du code de procédure pénale). Cette durée est à calculer à compter de l'inscription des empreintes dans le fichier. Or la CNIL a constaté que dans les faits, le ministère de l'intérieur calcule cette durée à compter de la dernière inscription dans le fichier (donc, si quelqu'un a été inscrit en 1995, ses données doivent être effacées en 2010 ; or dans les faits, si les empreintes de cette personne sont à nouveau versées au fichier en 2005, alors même celles de 1995 sont conservées jusqu'en 2020, ce qui est illégal).

Si la personne est mineure, les empreintes sont conservées 10 ans, mais il y a des exceptions aussi.

Enfin, si la personne fait l'objet d'une décision de non-lieu ou si la procédure est classée sans suite, les données sont effacées à moins que le procureur ne s'y oppose (article 7-1 II du décret du 8 avril 1987).

1.4 – Droit d'accès et de rectification

Le droit d'accès et de rectification s'exerce désormais auprès du ministère de l'intérieur, place Beauvau, 75800 PARIS Cedex 08 (article 6 du décret n°87-249 du 8 avril 1987 et article 106 de la loi du 6 janvier 1978). **Attention, depuis 2023**, il ne faut plus envoyer le courrier au Service national de la police technique et scientifique (qui est à la même adresse que celle du ministre de l'intérieur), car la lettre est alors refusée par le destinataire. Voir un modèle de lettre en annexes. En 2023, la réponse est transmise en 3 semaines environ.

Attention, lorsque le ministère répond, il propose de se rendre au commissariat ou à la gendarmerie pour donner ses empreintes et vérifier qu'elles ne sont pas présentes dans le fichier sans être reliées à une identité, ou en étant reliées à une autre identité. Il ne faut bien évidemment pas le faire ! Cela serait une occasion pour la police de mettre sur le dos de la personne une infraction constatée dans le passé, ou de générer une nouvelle trace inscrite dans le fichier !

37 https://www.nextinpact.com/article/69295/le-fichier-empreintes-digitales-sera-interconnecte-avec-casier-judiciaire-33

Pour demander la rectification ou la suppression des données, il faut envoyer une deuxième lettre recommandée avec accusé de réception. Cette fois, ça dépend du domicile de la personne : il faut regarder quel est le tribunal judiciaire compétent sur ce domicile, puis envoyer la demande au procureur de la République de ce Tribunal judiciaire (article 7-2 du décret n°87-249 du 8 avril 1987). Voir un modèle de lettre en annexe.

Si le procureur refuse la suppression, la personne a 10 jours pour contester ce refus (article 7-2 du décret n°87-249 du 8 avril 1987). Donc s'il y a refus expresse (réponse du procureur qui dit « non »), la personne a 10 jours à compter de la date de ce refus. S'il n'y a pas eu de réponse, ça vaut refus implicite, qui est effectif 3 mois après que la lettre avec accusé de réception de l'étape précédente a été réceptionnée par le procureur. Donc il faut compter cette date + 3 mois et contester sous 10 jours.

Pour contester cet éventuel refus du procureur, il faut envoyer une lettre recommandée avec accusé de réception au Juge de la liberté et de la détention (JLD) compétent pour les décisions du procureur dont on conteste le refus (donc le JLD du même tribunal judiciaire). À cette étape, ça vaut le coup de demander l'aide d'un avocat. On peut citer l'arrêt de la CEDH, 18 avril 2013, *M. K. contre France*. On peut citer aussi la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel* du Conseil de l'Europe du 28 janvier 1981. Et l'arrêt de la CJUE du 26 janvier 2023 concernant le cas bulgare mentionné plus haut.

Si le JLD refuse aussi, ou s'il ne répond pas sous 2 mois, c'est possible de faire appel, avec le même délai de 10 jours. Il faut s'adresser au Président de la chambre de l'instruction de la Cour d'appel dont dépend le Tribunal judiciaire. Mais là, il faut vraiment un·e avocat·e.

2. Fichier national automatisé des empreintes génétiques (FNAEG)

Il a été créé en 1998, et depuis il n'a cessé de prendre de l'ampleur. Par exemple, pendant l'année 2002 environ 4100 fiches ont été enregistrées dans le FNAEG ; sur l'année 2010 1,5 millions de personnes ont été enregistrées, et sur l'année 2015, 2,75 millions de fiches sont rentrées dans le fichier. Au début de l'année 2016, le fichier rassemblait 3 millions de fiches sur environ 2,2 millions personnes, et une personne peut être fichée plusieurs fois, si son ADN a été prélevé sur plusieurs affaires. En 2020, plus de 4,8 millions de personnes étaient fichées dans le FNAEG[38].

Les règles qui l'organisent sont aux articles 706-54 et suivants et R53-9 et suivants du code de procédure pénale. Il est géré par le service national de police scientifique du ministère de l'intérieur.

Lors de sa création, il concernait les infractions sexuelles graves, les atteintes volontaires à la vie, les actes de torture et de barbarie… puis il a été élargi plusieurs fois (environ 7 fois) et aujourd'hui les agents de police et les gendarmes peuvent faire un prélèvement d'ADN presque pour un oui ou pour un non.

38 Jean-Marc MANACH, *Plus d'un tiers des Français sont fichés dans le FNAEG*, NEXTIMPACT, 27 septembre 2021 https://www.nextinpact.com/article/48209/plus-dun-tiers-francais-sont-fiches-dans-fnaeg

En l'absence d'infraction, les données doivent être supprimées sous 24 heures. Ce délai n'est pas non plus respecté, la CNIL ayant constaté que ces données étaient conservées plus de 13 mois.

Les droits d'information, d'accès, de rectification et d'effacement s'exercent auprès du Centre national de traitement automatisé, CS 41101, 35911 RENNES Cedex 9.

Par ailleurs, un arrêté du 14 avril 2020 a prévu qu'il est possible de demander l'effacement en cas de décision de relaxe ou, pour les infractions routières, en cas de récupération des points perdus sur le permis de conduire. Cet arrêté a été annulé par le Conseil d'État (arrêt n°441317 du 24 septembre 2021) en raison du fait qu'il ne prévoyait pas de possibilité de demander l'effacement en cas de classement sans suite d'infractions non routières. On peut donc penser pouvoir demander l'effacement dans tous ces cas de figure (sans garantie de l'obtenir).

Il a fallu attendre deux ans et l'entrée en vigueur d'un arrêté du 15 novembre 2023 pour la mise en conformité de la procédure. L'article 3 de l'arrêté du 13 octobre 2004 prévoit dorénavant qu'il est possible de demander au procureur de la République d'ordonner l'effacement des données en cas de décision définitive de relaxe ou de classement sans suite, ainsi que lorsque la personne a récupéré les points ayant été retirés de son permis.

3. Passage rapide aux frontières extérieures (PARAFE)

Créé par décret n°2007-1182 du 3 août 2007, PARAFES (qui a depuis perdu son S final pour "Schengen" au fil du temps) est un traitement automatisé de données qui intervient dans les aéroports et certaines gares (à Paris, pour l'Eurostar par exemple). Il est dorénavant prévu par les articles L232-1 à L232-6 et R232-6 et suivants du code de la sécurité intérieure. Il vise à accélérer le franchissement de frontières et donc à remplacer le contrôle humain, réalisé par des gardes frontières, par une identification biométrique via un SAS automatique. Concrètement, il s'agit de scanner son passeport à l'entrée du SAS, puis de prendre position dedans : une caméra relève les traits du visage et confirme par la reconnaissance faciale l'identité du porteur ou de la porteuse du titre. Le recours à PARAFE est volontaire et facultatif dans la mesure où l'article R232-6 du code de la sécurité intérieure prévoit les conditions dans lesquelles une personne peut bénéficier de ce dispositif, ce qui n'est donc pas une obligation : on peut toujours ne pas emprunter ce SAS et choisir le contrôle à la guérite par les policiers aux frontières.

3.1 – Données concernées

Les données traitées sont l'image numérisée du visage du porteur du document, prise par la caméra dans le SAS, et possiblement l'empreinte de deux doigts pour les personnes de certaines nationalités (UE et États faisant partie de l'accord sur l'espace économique européen).

1.3 – Durée de conservation des données

Les données sont conservées pendant 30 ans, mais les données personnelles sont effacées au bout d'un an.

Cependant, vu que le fichier a été mis en place pendant 10 ans de manière illégale, et que son utilisation comme fichier d'antécédents judiciaires est toujours illégale, on peut difficilement faire confiance aux stups pour effacer les données personnelles au bout d'un an.

1.4 – Accès, rectification, effacement des données

On ne peut pas demander l'effacement des données personnelles contenues dans ce fichier.

Concernant l'accès et la rectification, l'arrêté du 12 janvier 2006 n'a pas été modifié. La procédure est donc contraire au règlement européen 2016/680 du 27 avril 2016 et aux articles 104 et suivants de la loi du 6 janvier 1978.

On peut quand même affirmer que le droit d'accès et de rectification des données s'exerce directement auprès du ministère de l'intérieur (Place Beauvau, 75800 PARIS CEDEX 08). Il n'est pas certain que le ministère puisse refuser l'accès aux informations. Toujours est-il que s'il refuse l'accès ou la rectification, ou s'il garde le silence pendant deux mois, c'est possible de contester ce refus devant la CNIL (3 place de Fontenoy, TSA 80715, 75334 PARIS CEDEX 07). C'est aussi possible de contester ce refus devant le tribunal administratif de Paris (mais il vaut mieux faire appel à un·e avocat·e).

2. <u>Fichier du système de contrôle automatisé (radars routiers automatiques)</u>

Il est prévu par l'arrêté du 13 octobre 2004 et est géré par le ministère de l'intérieur. L'objectif de ce fichier est de constater des infractions à l'aide des radars automatiques, identifier les véhicules concernés, émettre des contraventions, gérer les réponses des destinataires des contraventions, faciliter les opérations de paiement, transmettre les informations aux autorités judiciaires (les tribunaux).

Ce fichier concerne aussi les infractions non routières soumises à la procédure d'amende forfaitaire (c'est par ici que transitent les informations nécessaires à la verbalisation pour usage de stupéfiants).

Il est interconnecté avec le fichier national des immatriculations, le fichier national des permis de conduire, les fichiers des entreprises de location de véhicules, le fichier Minos (tribunaux de police), CASSIOPÉE (tribunaux judiciaires), Numérisation des procédures pénales, le SIV, la base satellite des véhicules volés, le TAJ et le fichier des véhicules terrestres à moteur assurés.

Les données sont conservées 10 ans (pour les délits et les contraventions au code de la route) ou 5 ans (pour les autres contraventions). Ces délais ne sont pas respectés : en 2019, la CNIL a constaté que des données étaient conservées plus de 13 ans.

Ce fichier très large et particulièrement intrusif a amené la France à être condamnée en 2017 par la Cour européenne des droits de l'Homme. En fait, dès 2010, le Conseil constitutionnel a considéré que ce fichier devait prévoir des durées de conservation des empreintes génétiques différentes selon la gravité de l'infraction reprochée à la personne[39]… pourtant le gouvernement a maintenu une durée de conservation des données pendant 40 ans, quelle que soit l'infraction reprochée à la personne. En 2017, la Cour européenne des droits de l'Homme est revenue à la charge en condamnant la France en raison de cette durée de conservation des données pendant 40 ans, quelle que soit l'infraction reprochée, et en raison de l'absence de procédure permettant à une personne de demander l'effacement des données si elle a été condamnée[40].

Ce n'est qu'en 2019 que la loi a été modifiée, pour permettre aux personnes condamnées de demander l'effacement de leurs données (nouvel article 706-54-1 du code de procédure pénale) mais le gouvernement s'est abstenu de prendre un décret d'application, ce qui rendait cette procédure inexistante ! Finalement celui-ci est paru… le 30 octobre 2021 (décret n°2021-1402 du 29 octobre 2021 et délibération de la CNIL n°2021-009 du 7 janvier 2021). Et il pose toujours de nombreux problèmes (voir ci-dessous).

Concernant les personnes seulement suspectées (et non condamnées) des faits ayant donné lieu au prélèvement génétique, la procédure pour demander l'effacement des données existe depuis 2004 au moins.

Les objectifs du fichier ont été précisés (et élargis) par le décret n°2021-1402 du 29 octobre 2021 (nouvel article R53-9 du code de procédure pénale). Il s'agit de :

- Faciliter la recherche et l'identification de crimes et délits (voir la liste plus bas), y compris par la **recherche en parentèle** (donc en analysant les données du fichier pour savoir si une trace non identifiée peut correspondre à celle d'un frère, d'une sœur, d'un parent, etc d'une personne fichée),
- Faciliter la recherche des mineurs et majeurs protégés disparus, et des personnes faisant l'objet d'une disparition inquiétante,
- Faciliter l'identification d'une personne décédée.

Par ailleurs, la loi du 3 juin 2016 a rendu possible la recherche en parentèle en cas de crime (et non de délit) : quand une trace d'ADN est recueillie sur le lieu d'une infraction, et que cette trace ADN ne permet pas d'identifier directement la personne à partir des profils génétiques enregistrés dans le FNAEG, le procureur de la République ou le juge d'instruction peut demander à ce que soient recherchées les parents, grands-parents, enfants et petits-enfants inscrits dans le fichier (article 706-56-1-1).

39 Conseil constitutionnel, 16 septembre 2010, n°2010-25 QPC
40 CEDH, 22 juin 2017, *Aycaguer contre France*

Enfin, la loi du 22 décembre 2021 a modifié l'article 706-54 du code de procédure pénale et a encore élargi un peu le fichage : dans les enquêtes sur certains crimes (voir l'article 706-106-1 : meurtre, tortures, viol, enlèvement et séquestration) sériels ou dont l'auteur n'a pas pu être identifié sous 18 mois (les « *cold case* »), il contient également l'ADN des victimes et, avec leur consentement, des ascendants, descendants et collatéraux (frères et sœurs) des victimes.

2.1 – Données concernées

La liste des personnes concernées par un prélèvement ADN est à l'article 706-55 du code de procédure pénale. Plutôt que de faire la liste de tous les cas susceptibles d'entraîner un prélèvement ADN, on va citer quelques situations dans lesquelles le prélèvement est illégal :

- Les dégradations légères (plus légères que celles de l'article 322-1 du code pénal) ;
- Outrage à l'encontre d'un policier ou d'un gendarme (article 433-5 du code pénal) ou au drapeau (433-5-1) ;
- Rébellion (articles 433-6 et suivants du code pénal) ;
- Les violences n'ayant entraîné aucune ITT ou ayant entraîné une ITT inférieure à 8 jours sans aucune circonstance aggravante (la liste des circonstances aggravantes est longue, voir l'article 222-13 du code pénal) ;
- Groupement (article 222-14-2 du code pénal, qui est inclus dans la liste des articles 222-1 à 222-18 de ce code mais qui ne constitue pas une violence, et qui n'apparaît pas dans les articles R53-14 et suivants du code de procédure pénale) ;
- La provocation et participation délictueuse à un attroupement avec ou sans arme (articles 431-3 et suivants du code pénal) ;
- La dissimulation du visage dans l'espace public, y compris en manifestation (article 1er de la loi du 11 octobre 2020 et article R645-14 du code pénal) ;
- Tous les délits involontaires (par exemple : violences involontaires) ;
- L'usage de stupéfiants (puni d'un an d'emprisonnement, article L3421-1 du code de la santé publique), mais la détention de stupéfiants peut justifier le prélèvement de l'ADN ;
- Faux, usage de faux (articles 441 et suivants du code pénal) ;
- Le maintien d'un étranger sur le territoire national après une assignation à résidence ou une rétention, soustraction à une mesure d'éloignement du territoire (articles L824-3, L824-9 du CESEDA) ;
- L'aide à l'entrée, à la circulation ou au séjour irrégulier d'un étranger en France ou dans l'espace Schengen (articles L823-1 et suivants du CESEDA).

Partie 12 : Fichiers de police : Fichiers secondaires thématiques

Comme dans la partie précédente, ces fichiers sont utilisés par la police et la gendarmerie et servent principalement au fonctionnement interne de ces institutions. Ils paraissent donc avoir moins d'importance, pour les personnes visées par les forces de police ou de gendarmerie, que les fichiers précédemment étudiés dans les parties 3, 4 et 5.

Dans cette partie, il s'agit des fichiers thématiques en ce qu'ils sont spécifiques à un type d'infractions.

1. OSIRIS (Stupéfiants)

Le fichier a été créé clandestinement en 2006, et il a été officialisé par l'arrêté du 12 janvier 2016 du ministre de l'Intérieur.

Il est géré par le ministère de l'intérieur.

Officiellement, il s'agit d'évaluer la situation nationale sur l'activité des services de police en matière de stupéfiants et d'établir des statistiques. Cependant, l'Office central pour la répression du trafic illicite de stupéfiants (OCRTIS) le présentait lui-même comme un fichier d'antécédents judiciaires, nominatif. En 2020, l'OCRTIS a été remplacé par l'office anti-stupéfiants de la direction centrale de la police judiciaire (OFAST), qui a récupéré OSIRIS et en 2023, la direction centrale de la police judiciaire a été remplacée par la direction nationale de la police judiciaire, qui a donc récupéré l'OFAST, et OSIRIS.

La légalisation du fichier en 2016 n'empêche donc pas la continuation de l'utilisation illégale de celui-ci : aux stups, on n'est pas très regardant.

1.1 – Données concernées

Tout un tas de données nominatives (nom, adresse, etc, nombre d'heures de garde à vue), saisies (quantité et type de drogue, armes, en cas de trafic pays de provenance et de destination, etc), informations sur la procédure (date, numéro, service interpellateur, blanchiment, zone de sécurité prioritaire etc).

1.2 – Utilisation des données

Officiellement, statistique ; en vrai, c'est un fichier d'antécédents parallèle au TAJ.

Tous les policiers et les gendarmes n'ont pas accès à ce fichier : les données sont accessibles à l'OFAST, au service technique de recherches judiciaires et de documentation de la gendarmerie nationale, et à la brigade des stupéfiants de Paris.

Ils contiennent de nombreuses informations personnelles relatives aux personnes qui font l'objet d'une enquête. Ils permettent qu'une alerte se déclenche lorsqu'un enquêteur saisit un nom, un numéro de téléphone, une adresse électronique, une adresse postale, un numéro d'immatriculation d'un véhicule ou un numéro de boîtier de téléphone portable qui apparaît déjà dans une autre enquête.

Pour le FNOS, les droits d'accès et de rectification des informations s'exercent auprès du directeur général de la police nationale, du directeur général de la gendarmerie nationale, et du directeur général des douanes et des droits indirects (articles 104 et suivants de la loi du 6 janvier 1978).

Pour les FOJ, il faut s'adresser au directeur général de la police nationale, au directeur général de la gendarmerie nationale et au préfet de police de Paris (articles 104 et suivants de la loi du 6 janvier 1978).

10. Le sommier de police technique

Ce fichier a été créé par le décret n°59-1562 du 28 décembre 1959, et il ne semble pas avoir été modifié depuis. Il est placé sous la responsabilité du ministère de l'intérieur et il recense l'ensemble des condamnations à une peine privative de liberté pour un crime ou un délit.

Il a pour objectif l'identification des délinquants, mais s'il n'a pas été informatisé, il ne doit plus servir à grand-chose… mais l'article 773-1 du code de procédure pénale prévoit toujours qu'une copie de chaque fiche de condamnation à une peine privative de liberté est transférée au sommier, et on ne voit pas pourquoi ils auraient arrêté.

Aucune interconnexion avec d'autres fichiers n'est prévue (surtout que le fichier est peut-être toujours sous format papier).

Les droits de consultation, de rectification et d'effacement des données personnelles ne sont pas prévus. Il est toujours possible d'envoyer un courrier au ministère de l'intérieur pour essayer, avec ce problème que si le fichier n'est pas informatisé, il n'est pas automatisé, et la loi du 6 janvier 1978 (en particulier ses articles 105 et 106) ne s'appliquent pas.

11. STIC

Supprimé, remplacé par le TAJ (décret n°2012-652 du 4 mai 2012, article 2).

12. JUDEX

Supprimé, remplacé par le TAJ (décret n°2012-652 du 4 mai 2012, article 2).

13. Fichier des cartes d'identité (FNG) et Fichier relatif aux passeports (ancien TES)

Remplacés par le nouveau TES (décret n°2016-1460 du 28 octobre 2016).

C'est possible de refuser ce prélèvement ADN, mais ça constitue un délit puni d'un an d'emprisonnement et de 15.000 euros d'amende (article 706-55 du code de procédure pénale). Ça ne veut pas dire que la personne va prendre systématiquement cette peine, mais la peine prononcée varie beaucoup, de presque rien (souvent lorsqu'elle est relaxée pour le délit pour lequel elle est rentrée en garde-à-vue), à quelques centaines d'euros d'amende et quelques mois de prison, le plus souvent avec sursis. Pour un exemple de relaxe dans une affaire des « décrocheurs de portraits » du président de la République : Cass, crim, 22 septembre 2021, n°20-80.489. Voir aussi, pour une relaxe d'une personne qui a été condamnée par ailleurs pour la participation à un groupement et pour rébellion, le fichage ayant été considéré comme une atteinte disproportionnée à son droit à mener une vie privée et familiale normale au sens de l'article 8 de la CEDH : Cour d'appel de Grenoble, 20 octobre 2022, n°22/00681.

Aussi, si une personne refuse le prélèvement ADN alors qu'elle est déjà condamnée, cela enlève tout droit à des réductions de peine (mais elle peut encore bénéficier d'aménagements de peine) (article 706-55 III du code de procédure pénale). Cela a été supprimé par l'article 11 de la loi n°2021-1729 du 22 décembre 2021, mais c'est surtout parce que cette loi a supprimé les réductions de peine automatiques (crédits de réduction de peine).

Si la personne refuse de donner son ADN, les gendarmes ou les policiers peuvent le prendre par ruse (en récupérant de la salive sur un gobelet ou un mégot, un cheveu à condition qu'il soit tombé naturellement). Ils peuvent le prendre de force uniquement si la personne est condamné·e (et non pas seulement soupçonné·e) pour un crime ou un délit puni d'une peine de 10 ans d'emprisonnement.

Par ailleurs, certaines données génétiques doivent fait l'objet d'un enregistrement distinct des autres données. Il s'agit des traces issues des cadavres non identifiés, de celles des personnes disparues, et de celles des ascendants et descendants de victimes de catastrophes naturelles (article R53-10 IV).

2.2 – Sur le délai qu'ont les services de police et de gendarmerie pour procéder à un prélèvement ADN lorsqu'il n'a pas été effectué au cours de l'enquête

Si la personne a refusé de donner son ADN pendant l'enquête de police, cela constitue une infraction (voir ci-dessus). Les services de police et de gendarmerie peuvent, alors, la convoquer pour procéder au prélèvement de son ADN. Mais pas n'importe quand (article R53-20) :

- En cas de condamnation à une peine, les services de police et de gendarmerie peuvent la convoquer pendant 1 an à compter de l'exécution de la peine : ce délai d'un an commence à compter de la sortie de détention (s'il y a eu une peine d'emprisonnement), ou à compter du paiement de l'amende, à compter du jour où les travaux d'intérêt généraux ont été effectués, ou à compter de la fin du stage de citoyenneté ou autre, ou à la fin du suivi socio-judiciaire…

- En cas de condamnation à un emprisonnement avec sursis ou à une amende avec sursis, le délai d'un an commence à compter du jour où la peine est non avenue, donc 5 ans après la condamnation. Par conséquent, en cas de condamnation à une peine avec sursis, les services de police et de gendarmerie ont 6 ans pour convoquer la personne pour prélever son ADN.
- En cas de décision d'irresponsabilité pénale, le délai d'un an commence à courir au jour du caractère définitif de la condamnation (donc 10 jours après la condamnation par un tribunal, 5 jours après la condamnation par une cour d'appel).
- En cas d'hospitalisation sous contrainte ou de mesure de sûreté, le délai d'un an commence à courir à la fin de l'exécution de cette mesure.

2.3 – Interconnexions du FNAEG avec d'autres fichiers

Le FNAEG est en lien avec des fichiers européens et internationaux (article R53-19-1 du code de procédure pénale) :

- les fichiers européens des bases de données prévues par le traité de Prüm du 27 mai 2005, pour lutter notamment contre le terrorisme, la criminalité transfrontalière et les migrations irrégulières ; cela inclut les manifestations de grande envergure, qu'elles soient politiques ou sportives (article 1er de la décision 2008/615/JAI du Conseil du 23 juin 2008) ;
- l'article R53-19-1 du code de procédure pénale vise les fichiers pris en application « des titres IV ou VI du traité sur l'Union européenne » mais il semble que ce soit une erreur. Par analogie avec le FAED, on peut supposer qu'en fait il s'agit des fichiers pris en application du titre V de la 3e partie du traité sur le fonctionnement de l'Union européenne, donc qui concernent l'espace de liberté, de sécurité et de justice de l'Union (contrôle aux frontières, asile, immigration, coopération judiciaire en matière pénale, coopération policière) ;
- les fichiers d'Interpol.

Le décret du 30 octobre 2021 a permis l'interconnexion du FNAEG avec des fichiers nationaux, et il n'a pas fait les choses à moitié (article R53-19 du code de procédure pénale). Dorénavant, le FNAEG est aussi interconnecté avec :

- le fichier CASSIOPÉE, du ministère de la justice, qui permet le suivi des procédures pénales dans les tribunaux ;
- LRPPN et LRPGN, en particulier concernant le « numéro d'identification » dit IDPP créé par le LRPPN et LRPGN commun à plusieurs fichiers de police ;
- la passerelle internationale en matière d'ADN d'Interpol.

Une autre interconnexion est étrange : le nouvel article R53-19 cite le fichier prévu à l'article R249-9 du code de procédure pénale… mais cet article n'existe plus depuis 2020, et il n'a jamais été la base

curatelle, les représentants légaux s'il s'agit d'un mineur. La liste est prévue par l'article R15-33-78 du code de procédure pénale.

8.2 – Utilisation des données

Les personnes qui ont accès aux données sont les flics et gendarmes qui interviennent dans la garde à vue, leurs supérieurs, l'IGGN, l'IGPN, le contrôleur général des lieux de privation de liberté (CGLPL), le défenseur des droits (DDD) et les magistrats qui contrôlent la garde à vue.

8.3 – Durée de conservation des données

Les données sont conservées pendant 10 ans.

Pendant la première année, toutes les personnes citées plus haut y ont accès.

Pendant les 9 années suivantes, seuls les supérieurs des flics et gendarmes, l'IGGN, l'IGPN, le CGLPL, le défenseur des droits et les magistrats chargés de contrôler la garde à vue y ont accès.

Toutefois, concernant les mesures de retenue aux fins de vérification d'identité et celles de retenue aux fins de vérification du droit au séjour des étrangers, les données doivent être effacées dès la remise en liberté s'il n'y a eu ni procédure d'enquête, ni procédure d'exécution adressée à l'autorité judiciaire (article R15-33-80 du code de procédure pénale).

8.4 – Droit de consultation, de rectification et d'effacement des données

Le décret du 9 octobre 2023 a (enfin) mis en conformité les procédures de demande de consultation, de rectification et d'effacement des données avec l'ordonnance n°2018-1125 du 12 décembre 2018 modifiant la loi n°78-17 du 6 janvier 1978. Les droits d'accès, de rectification, d'effacement et de limitation des données (c'est-à-dire le droit d'une personne de demander à ce que les données ne soient pas effacées pour pouvoir les utiliser dans ses intérêts) s'exercent auprès de la direction générale de la police nationale (place Beauvau, 75800 PARIS CEDEX 08), de la direction générale de la gendarmerie nationale (4 rue Claude Bernard, 92130 ISSY-LES-MOULINEAUX) et de la préfecture de police de Paris (1bis rue de Lutèce, 75004 PARIS).

9. Les fichiers des objectifs judiciaires (FNOS et FOJ)

L'objectif de ces fichiers est d'éviter que des enquêteurs des services de police et de gendarmerie enquêtent sur une même personne, ou sur une même affaire, sans s'en rendre compte.

Le premier à avoir été créé est le fichier national des objectifs en matière de stupéfiants (FNOS, arrêté du 11 juillet 2012).

L'arrêté du 5 mai 2017 (avis de la CNIL n°2016-321 du 13 octobre 2016) autorise la création de ces fichiers pour tous les types d'infractions. Il ne s'agit pas d'un seul fichier, mais de fichiers locaux.

7. Fichier des appels à témoins

Il a été créé par l'arrêté du 22 août 2012 et est placé sous l'autorité du directeur général de la police national et du directeur général de la gendarmerie nationale.

Il regroupe l'identité des personnes qui répondent à l'appel à témoins et les informations qu'elles transmettent. Ces données sont conservées un an. Seuls les policiers et les gendarmes qui ont lancé l'appel à témoins y ont accès.

Pour accéder ou rectifier les informations contenues dans le traitement, la personne doit s'adresser à l'unité de gendarmerie ou au service de police qu'elle a appelé pour répondre à l'appel à témoins.

8. Informatisation de la gestion des gardes à vue (iGAV)

iGAV a été créé par le décret n°2016-1447 du 26 octobre 2016 et apparaît aux articles R15-33-77 et suivants du code de procédure pénale. Initialement et comme son nom l'indique, il était réservé aux mesures de garde-à-vue. Le décret n°2023-932 l'a étendu aux mesures de retenue judiciaire des mineurs (l'équivalent de la garde-à-vue pour les mineurs âgés de 10 à 13 ans), aux mesures de retenue aux fins de vérification d'identité et aux mesures de retenue administrative des étrangers aux fins de vérification de leur droit au séjour.

Il est mis en œuvre par le ministère de l'Intérieur et a pour objet la gestion et le suivi des gardes à vue.

8.1 – Données concernées

Elles sont nombreuses : état civil de la personne, photographie, antécédents judiciaires, état de santé, raisons de la garde à vue, circonstances de l'interpellation, de nombreuses informations relatives à la garde à vue (heure de début, durée, numéro de procédure, fouilles, repas, etc), nom de l'avocat et du médecin, avis du médecin…

Le fichier peut également contenir des données 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.* »

Les données pouvant être enregistrées ont été encore augmentées par le décret n°2023-932 pour intégrer notamment les éléments relatifs à la dangerosité de la personne (comportement agressif, risque d'évasion), à sa vulnérabilité (risque d'auto-mutilation ou de suicide), des éléments relatifs à la santé (affection déclarée, traitement médical), sa profession, sa filiation, l'existence d'une tutelle ou d'une

légale d'un fichier de police ou de justice. Or, la CNIL indique dans son avis de janvier 2021 que le projet de décret (qui sera le décret du 30 octobre 2021) prévoyait une interconnexion avec le TAJ et le FAED. Donc, aujourd'hui, le FNAEG n'est pas interconnecté avec ces fichiers, mais ça ne semble être qu'une erreur de rédaction, et il est probable qu'elle soit rapidement corrigée.

2.4 – Durée de conservation des données

Le décret du 29 octobre 2021 a modifié la durée de conservation des données. Auparavant, celles-ci étaient conservées 40 ans en cas de condamnation de la personne, et 25 ans si la personne suspectée n'a pas été condamnée.

Dorénavant les règles dépendent aussi de la gravité de l'infraction… même si ces durées restent extrêmement longues. Attention, elles peuvent être effacées avant l'écoulement de ces durées (voir plus bas). Les durées de conservation de base sont prévues à l'article R53-14 du code de procédure pénale :

- Les profils génétiques des personnes **suspectées** (et non condamnées) d'une infraction concernée par le fichage au FNAEG sont conservées :
  - **25 ans** pour les personnes **majeures** (à compter du prélèvement), lorsqu'elles sont suspectées de ces infractions :
    - crime contre l'humanité, meurtre ou assassinat, tortures, violences volontaires (sauf les violences volontaires n'ayant entraîné aucune ITT ou une ITT inférieure ou égale à 8 jours sans aucune circonstance aggravante) ;
    - viol, agression sexuelle, proxénétisme, recours à la prostitution de mineurs, mise en péril de mineurs,
    - trafic de stupéfiants ;
    - enlèvement et séquestration, détournement de moyen de transport, traite des êtres humains ;
    - vol ou extorsion avec violences ayant entraîné une mutilation ou une infirmité permanente, vol ou extorsion avec violences ayant entraîné la mort, vol ou extorsion à main armée, vol ou extorsion en bande organisée, extorsion avec violences ayant entraîné plus de 8 jours d'ITT, incendie volontaire, incendie (et incendie avec circonstances aggravantes) ;
    - trahison, espionnage, attentat, complot, mouvement insurrectionnel, terrorisme, provocation au terrorisme, fausse monnaie, participation à une association de malfaiteurs ;
    - crimes et délits de guerre ;
    - certaines infractions au régime des armes et munitions, par exemple la fabrication d'explosifs, l'acquisition, le transport ou la détention d'explosifs, acquisition, détention ou trafic d'armes de catégories A ou B.

- **15 ans** pour les personnes **majeures** (à compter du prélèvement) suspectées d'une autre infraction ;
- **15 ans** pour les personnes **mineures** (à compter du prélèvement) suspectées d'une infraction citée dans la liste précédente ;
- **10 ans** pour les personnes **mineures** (à compter du prélèvement) suspectées d'une autre infraction.

- Les profils génétiques des personnes **condamnées** d'une infraction concernée par le fichage au FNAEG, ou reconnues irresponsables pénalement sont conservées :
  - **40 ans** pour les personnes **majeures** (à compter de la condamnation) condamnées pour une infraction citée dans la liste précédente ;
  - **25 ans** pour les personnes **majeures** (à compter de la condamnation) condamnées pour une autre infraction ;
  - **25 ans** pour les personnes **mineures** (à compter de la condamnation) condamnées pour une infraction citée dans la liste précédente ;
  - **15 ans** pour les personnes **mineures** (à compter de la condamnation) condamnées pour une autre infraction.
  - Les traces recueillies au cours des enquêtes, sans que la personne ayant laissé cette trace soit identifiée, et les traces recueillies dans les enquêtes pour recherche des causes de la mort sont conservées :
    - **40 ans** lorsqu'elles ont été recueillies au cours d'une enquête pour une infraction citée dans la liste précédente ;
    - **25 ans** lorsqu'elles ont été recueillies au cours d'une enquête pour une autre infraction.
  - Les traces génétiques issues des cadavres non identifiés, les traces génétiques issues ou susceptibles d'être issues des personnes disparues, ainsi que les traces génétiques des parents, enfants, sœurs et frères des personnes disparues, sont conservées 40 ans ;
  - Les traces génétiques transmises par des États étrangers, par Europol ou par Interpol sont conservées 25 ans.

Donc on constate que les durées sont les mêmes pour une personne condamnée pour des coups avec un rouleau à pâtisserie (une arme) n'ayant entraîné aucune ITT, pour un trafic d'armes de guerre ou pour du proxénétisme… La différenciation entre la gravité des infractions est toute relative !

Les personnes qui ont accès à ces données sont en nombre assez limité, et seulement à l'échelon central de la police nationale : : directeur général, DNSP (direction nationale de la sécurité publique), DNPJ (police judiciaire), DNPAF (police aux frontières), CRS, coopération internationale, protection du président de la République et des ministres, UCLAT (lutte anti-terroriste). Peuvent aussi avoir accès à certaines données du fichier d'autres policiers et gendarmes, ainsi que les agents de la DGSI.

Les informations sont conservées pendant 6 ans.

L'article 6 du décret du 22 mai 2018 prévoit que le droit d'accès, de rectification et d'effacement des informations s'exerce auprès de la CNIL. Cependant, cela est en contradiction avec les articles 104 à 106 de la loi n°78-17 du 6 janvier 1978 tels que modifiés par l'ordonnance n°2018-1125 du 12 décembre 2018, qui prévoient qu'il faut s'adresser au responsable du traitement. Il faut appliquer les dispositions de la loi et non celles du décret.

En conséquence, il faut s'adresser au ministère de l'intérieur, Place Beauvau, 75800 PARIS CEDEX 08.

5. Pré-plainte en ligne

Le traitement de données permettant de déposer une pré-plainte sur internet a été permis par le décret n°2018-388 du 24 mai 2018. Il est géré par le ministère de l'intérieur (DGPN, DGGN et préfecture de police de Paris). Il contient toutes les données saisies par la personne déposant la pré-plainte.

Les données sont conservées jusqu'au dépôt de la plainte. En l'absence de dépôt de la plainte, elles sont effacées 30 jours après la déclaration en ligne. Le droit d'accès et de rectification s'exerce auprès du service de police ou de gendarmerie choisi par la personne pour signer la plainte.

6. Plainte en ligne et Traitement harmonisé des enquêtes et signalements pour les e-escroqueries (THESEE)

Le dispositif est prévu aux articles 15-3-1, 15-3-1-1, D8-2-1 et suivants et A 1er et suivants du code de procédure pénale, et par l'arrêté du 26 juin 2020 portant création de THESEE.

Il servait initialement à donner la possibilité aux victimes de faits d'escroquerie, de chantage ou d'extorsion (si celle-ci est connexe à l'accès frauduleux à un fichier), de discrimination ou de provocation à la discrimination, de déposer plainte en ligne, mais il a été étendu aux victimes de n'importe quels faits par la loi n°2023-22 du 24 janvier 2023 (article 15-3-1-1 du code de procédure pénale).

Les informations enregistrées sont toutes celles saisies par la victime. Elles sont conservées 6 ans. Il est possible de demander l'accès, la rectification ou l'effacement des données à la direction centrale de la police judiciaire.

Le fichier contient toutes les informations données pendant l'appel « 17 », le nom du fonctionnaire ayant réceptionné l'appel, l'indicatif de l'équipage avisé de l'appel, et les données de géolocalisation des véhicules de police. Il contient également le numéro de téléphone ayant appelé le « 17 », l'identité et les coordonnées de la personne ayant appelé, la localisation du téléphone utilisé, ainsi que de nombreuses informations concernant les personnes mises en cause, témoin ou victime de l'infraction, mais aussi les photographies des lieux de l'intervention prises par les personnels de la police nationale.

Il est précisé que le fichier peut comporter des données relatives à l'origine raciale ou ethnique, aux opinions politiques, aux convictions religieuses ou philosophiques, à l'appartenance syndicale, mais qu'il ne peut pas enregistrer de données génétiques ou biométriques (article R236-56 du code de la sécurité intérieure).

En réalité, et a minima pendant que PEGASE était utilisé, les informations sont plus nombreuses car c'est dans PEGASE que les policiers remplissent une « fiche d'intervention ». Par exemple, les policiers qui ont été filmés en train d'assassiner Nahel le 27 juin 2023 à Nanterre ont rempli une fausse « fiche d'intervention » dans PEGASE pour tenter de se couvrir[81].

Les autres sont conservées 2 ans, sauf les données de localisation (2 mois), celles relatives à la localisation des véhicules de police et des policiers et les photographies qu'ils ont prises (un an).

L'accès aux informations peut être demandé à la direction générale de la police nationale (article R236-60 du code de la sécurité intérieure).

4. Système d'information de la police nationale (fichier SIPol)

Il a existé un temps indéterminé de manière illégale (avis de la CNIL n°2018-049 du 8 février 2018), puis a été légalisé par le décret n°2018-377 du 22 mai 2018. Il est placé sous la responsabilité de la direction générale de la police nationale.

Ce fichier a pour objet de faciliter les remontées d'informations aux services nationaux de la police nationale. Du coup, les événements qui sont documentés dans le fichier doivent avoir des répercussions au niveaux des services nationaux de la police nationale (l'avis de la CNIL prend l'exemple d'une intervention du RAID).

Les informations conservées sont nombreuses et particulièrement intrusives : tout l'état civil et de nombreux éléments relatifs à l'identité des personnes concernées. Il peut aussi contenir la photographie, ainsi que les origines raciales ou ethniques des personnes, leurs opinions politiques, philosophiques ou religieuses, leur appartenance syndicale, leur santé et leur vie sexuelle.

81 https://www.huffingtonpost.fr/faits-divers/article/mort-de-nahel-les-policiers-ont-ils-menti-la-fiche-d-intervention-seme-le-trouble_220257.html

Enfin, ces durées peuvent être raccourcies en application de l'article R53-14-1 : le procureur de la République ou le juge d'instruction peut ordonner à tout moment l'effacement des données, notamment lorsque l'infraction est prescrite (on aimerait bien voir les statistiques de l'utilisation de cette disposition dans 5 ans pour constater qu'elle ne sera jamais utilisée).

Les données sont effacées en cas de relaxe ou d'acquittement… mais pas en cas de non-lieu !

Lorsque la personne décédée a été identifiée ou lorsque la personne disparue a été retrouvée, son profil génétique est effacé.

Attention, en cas de relaxe ou d'acquittement, en cas d'identification de la personne décédée ou de découverte de la personne disparue, cet effacement est censé être automatique, mais il y a de fortes chances que ça ne soit pas le cas, et qu'il faille le demander.

2.5 – Droit d'accès, de rectification et d'effacement

Le décret du 29 octobre 2021 a changé les procédures pour demander l'accès, la rectification et l'effacement des données dans le FNAEG.

Pour **l'accès aux données**, il faut envoyer une lettre recommandée avec accusé de réception au ministère de l'intérieur, place Beauvau, 75800 PARIS Cedex 08 (article 6 du décret n°87-249 du 8 avril 1987 et article 106 de la loi du 6 janvier 1978). Attention, depuis 2023, il ne faut plus envoyer le courrier au Service national de la police technique et scientifique (qui est à la même adresse que celle du ministre de l'intérieur), car la lettre est alors refusée par le destinataire. Voir un modèle de lettre en annexes. En 2023, la réponse est transmise en 3 semaines environ.

Attention, lorsque le ministère répond, il propose de se rendre au commissariat ou à la gendarmerie pour donner son ADN et vérifier qu'il n'est pas présent dans le fichier sans être relié à une identité, ou en étant relié à une autre identité. Il ne faut bien évidemment pas le faire ! Cela serait une occasion pour la police de mettre sur le dos de la personne une infraction constatée dans le passé, ou de générer une nouvelle trace inscrite dans le fichier !

Aussi, lorsque le ministère répond, il semble que les données communiquées soient incomplètes. En effet, il indique que la nature de l'infraction ne serait pas disponible dans le FNAEG, alors même que celle-ci doit être renseignée en application du III de l'article R53-11 du code de procédure pénale (ne serait-ce que pour que le gestionnaire du fichier sache combien de temps il peut conserver ces données!). Par ailleurs, il ne donne pas le numéro de la procédure et le nom de la personne ayant procédé à l'analyse, qui sont pourtant enregistrées en application du I de l'article R53-11.

Pour **la rectification des données**, il faut s'adresser au procureur de la République compétent, c'est-à-dire regarder où l'ADN a été prélevé, regarder quel tribunal judiciaire est compétent à cet endroit, et

l'envoyer au procureur de ce tribunal judiciaire en lettre recommandée avec accusé de réception (article R53-15 du code de procédure pénale).

Pour **l'effacement des données, concernant une personne suspectée (non condamnée) :** la personne peut soit s'adresser au procureur de la République de son domicile, soit s'adresser au procureur de la République du tribunal judiciaire compétent où l'ADN a été prélevé (article R53-14-2 du code de procédure pénale). La demande se fait par lettre recommandée avec accusé de réception.

Si la personne a été relaxée ou acquittée, le procureur de la République doit effacer les données.

Si la personne a fait l'objet d'une ordonnance de non-lieu, ou si la procédure a fait l'objet d'un classement sans suite pour absence d'infraction, d'un classement sans suite pour insuffisance de charges, ou d'un classement sans suite pour auteur inconnu, le procureur de la République peut refuser d'effacer les données. Par contre, si les faits sont prescrits, il doit effacer les données.

Ces règles s'appliquent aussi pour les prélèvements génétiques sur les parents, enfants, sœurs et frères d'une personne disparue ou victime de catastrophe naturelle.

Pour **l'effacement des données, concernant une personne condamnée** (ou déclarée irresponsable pénalement), elle peut s'adresser au procureur de la République du tribunal judiciaire de son domicile ou à celui du tribunal judiciaire du lieu où le prélèvement a été effectué. La demande se fait par lettre recommandée avec accusé de réception.

Elle ne peut demander l'effacement des données qu'à l'issue d'un certain délai après la condamnation : si ses données peuvent être conservées 15 ans, elle doit attendre 3 ans pour demander leur effacement ; si ses données peuvent être conservées 25 ans, elle doit attendre 7 ans ; si ses données peuvent être conservées 40 ans, elle doit attendre 10 ans.

Si le procureur refuse de faire procéder à l'effacement des données, il faut attendre un an avant de faire une nouvelle demande.

Le procureur de la République doit donner sa réponse sous 3 mois.

S'il ne répond pas dans ce délai, les données ne sont pas effacées… sauf si la personne suspectée a fait l'objet d'une décision de non-lieu, ou si la procédure a été classée sans suite pour certains motifs (voir plus haut), alors, en cas d'absence de réponse du procureur de la République, les données sont effacées (ça vaut le coup de vérifier en demandant l'accès aux données quelques mois plus tard!).

En cas de refus du procureur de la République, ou en cas d'absence de réponse sous 3 mois, la personne peut exercer un recours devant le président de la chambre de l'instruction par lettre recommandée

1.3 – Droit d'accès, rectification et effacement

L'article R236-37 du code de la sécurité intérieure prévoit que ces droits s'exercent auprès de la Direction générale de la gendarmerie nationale, 4 rue Claude Bernard, CS60003, 92136 ISSY-LES-MOULINEAUX CEDEX.

2. Sécurisation des interventions et demandes particulières de protection (SIDPP)

Il est géré par la Direction générale de la gendarmerie nationale (ministère de l'intérieur) et est prévu par les articles R236-38 et suivants du code de la sécurité intérieure. Il est intégré à la Base de données de la sécurité publique (BDSP) et est communément appelé SIP[80].

2.1 – Objectifs et données collectées

Ce fichier regroupe les personnes dont la dangerosité ou l'agressivité, à travers des manifestations de violence physique ou verbale, a été déjà constatée lors d'une précédente intervention, les personnes demandant une intervention, et les personnes se trouvant dans une situation de vulnérabilité particulière.

Il concerne tout le monde à partir de 13 ans.

2.2 – Durée de conservation des données

Les données sont conservées 10 ans à compter de la date de l'enregistrement, ou la durée pour laquelle a été demandée la protection. Pour les mineurs, les données sont effacées à leur majorité.

2.3 – Droit d'accès

L'article R236-45 du code de la sécurité intérieure prévoit que ces droits s'exercent auprès de la CNIL. Cependant, cela est en contradiction avec les articles 104 à 106 de la loi n°78-17 du 6 janvier 1978 tels que modifiés par l'ordonnance n°2018-1125 du 12 décembre 2018, qui prévoient qu'il faut s'adresser au responsable du traitement. Il faut donc appliquer ces nouvelles dispositions et s'adresser à la Direction générale de la gendarmerie nationale, 4 rue Claude Bernard, CS60003, 92136 ISSY-LES-MOULINEAUX CEDEX.

3. Pilotage des événements, gestion de l'activité et sécurisation des équipages (PEGASE)

C'est l'équivalent des deux fichiers précédents, mais côté police. Il sert à la gestion des appels « 17 » et à la géolocalisation des véhicules de police. Il est géré par le ministère de l'intérieur et autorisé par l'arrêté du 21 janvier 2008. Le fichier PEGASE a été créé par l'arrêté du 21 janvier 2008.

Il aurait vocation à être remplacé par le système MCIC 2, mais PEGASE a déjà été remplacé par PEGASE II par le décret n°2024-155 du 27 février 2024, et apparaît dorénavant aux articles R236-54 et suivants du code de la sécurité intérieure.

80 https://www.gendarmerie.interieur.gouv.fr/gendinfo/sur-le-terrain/immersion/2018/allo-le-17

Partie 11 : Fichiers de police : Fichiers secondaires généraux

Ces fichiers sont utilisés par la police et la gendarmerie. Ils servent principalement au fonctionnement interne de ces institutions, et paraissent donc avoir moins d'importance, pour les personnes visées par les forces de police ou de gendarmerie, que les fichiers précédemment étudiés dans les parties 3, 4 et 5.

Dans cette partie, il s'agit des fichiers généraux en ce qu'ils ne sont pas spécifiques à un type d'infractions.

Les principales modifications depuis la dernière édition concernent le fichier PEGASE, relatif aux appels au « 17 », qui a été remplacé par PEGASE II, l'adaptation du fichier relatif aux plaintes en ligne (THESEE) au fait que cette procédure est désormais ouverte pour tout type d'infraction, et l'élargissement de l'utilisation de iGAV (gestion informatisée des garde-à-vue) à d'autres mesures privatives de liberté.

1. Gestion des sollicitations et des interventions

Ce fichier est prévu par les articles R236-31 et suivants du code de la sécurité intérieure. Il est mis en œuvre par la Direction générale de la gendarmerie nationale (ministère de l'intérieur).

1.1 – Objectifs et données collectées

Ce fichier contient les enregistrement des appels vers les centres d'appel de la gendarmerie. Le décret n°2023-205 du 27 mars 2023 a considérablement élargi les données pouvant être enregistrées dans ce fichier.

Il concerne ainsi les photographies de la personne recherchée ou disparue, les photographies d'un véhicule recherché, les informations de localisation de l'appel vers le centre d'appel, les photographies de la scène d'intervention prises par les gendarmes et les positions GPS des véhicules des gendarmes sur l'intervention.

Il peut contenir des informations concernant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses, l'appartenance syndicale, la vie sexuelle et l'orientation sexuelle des personnes.

1.2 – Durée de conservation des données

Les données sont conservées 2 ans.

Toutefois, le décret n°2023-205 du 27 mars 2023 a tout prévu pour protéger les gendarmes : les donnés relatives aux positions GPS des véhicules des gendarmes en intervention ne sont pas conservées, et si jamais elles le sont quand même, c'est 30 minutes maximum ! Comme ça, si ils ont quelque chose à se reprocher, ils peuvent dormir tranquilles : le gouvernement a fait en sorte que les preuves soient effacées.

avec accusé de réception, ou par déclaration au greffe, sous 10 jours (article R53-14-3). Il vaut mieux demander de l'aide à un·e avocat·e.

Ici, il y a un arrêt intéressant de la cour de cassation (crim, 8 décembre 2021, n°20-84.201, Publié) selon lequel tous les prélèvements effectués avant l'entrée en vigueur du décret du 29 octobre 2021 l'ont été en contrariété avec la Convention européenne des droits de l'Homme…

3. Lecture Automatisée des Plaques d'Immatriculation (LAPI)

LAPI est régi par l'arrêté du 18 mai 2009, modifié plusieurs fois. Il est à la disposition des flics, des gendarmes et des services de douanes. Il a pour but la répression du terrorisme, de la criminalité organisée, du vol et du recel de véhicules.

Il a aussi des objectifs de police administrative de préservation de l'ordre public en cas d'évènements particuliers ou de grands rassemblements de personnes (par exemple de grands festivals ayant un risque terroriste, ou de sommets internationaux ayant un risque de contre-sommet).

Les « radars » permettant la lecture des plaques d'immatriculation peuvent être fixes – au bord des routes – ou mobiles (dans des voitures, sur le toit dans la barre du gyrophare). Le fichier est interconnecté avec le FoVES et N-SIS II.

Cependant, LAPI ne permet pas une consultation et une gestion centralisées des données. Il avait été question que le LAPI soit donc rendu encore plus efficace avec le Système de Traitement Central LAPI (STCL). La CNIL a été saisie d'une demande d'avis à l'automne 2019 sur le STCL, mais nous n'avons pas trouvé d'informations sur la suite du projet.

3.1 – Données concernées

Le fichier contient les 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.

Si le numéro d'immatriculation correspond à un véhicule enregistré dans le FoVES ou dans N-SIS II, le fichier contient également le motif du signalement au FoVES ou dans N-SIS II et la conduite à tenir pour les flics face au véhicule[41].

Il semble que le fichier soit en relation automatique avec le système d'immatriculation des véhicules (SIV) des articles L330-1 et suivants et R330-1 et suivants du code de la route. Il contiendrait alors plus de données que celles qui sont collectées légalement : par exemple le modèle du véhicule, le numéro de châssis et autres, ainsi que le nom de son propriétaire ou du locataire du véhicule et les données collectées par les loueurs des véhicules. La connexion de LAPI avec le SIV est susceptible d'être illégale.

41 Pour des exemples de conduites à tenir, voir le document partagé par Marc Rees sur : https://www.nextinpact.com/article/29066/107466-lapi-futurs-lecteurs-automatiques-plaques-dimmatriculation-forces-ordre

3.2 – Durée de conservation des données

Les données sont conservées 8 jours. En cas de rapprochement avec le FoVES ou N-SIS II, elles sont conservées 1 mois.

3.3 – Droit de communication, de rectification et d'effacement

L'article 6 de l'arrêté du 18 mai 2009 prévoit que ces droits s'exercent auprès de la CNIL. Cependant, cela est en contradiction avec les articles 104 à 106 de la loi n°78-17 du 6 janvier 1978 tels que modifiés par l'ordonnance n°2018-1125 du 12 décembre 2018, qui prévoient qu'il faut s'adresser au responsable du traitement. Même si l'arrêté n'a pas été mis à jour depuis l'adoption de la loi, cette dernière doit s'appliquer. En conséquence, il faut s'adresser au ministère de l'intérieur, Place Beauvau, 75800 PARIS CEDEX 08.

4. Table de correspondance des noms et prénoms

Ce fichier a été dénoncé par de nombreuses associations de défense des droits des personnes transgenres et a fait l'objet d'un article fourni de la Quadrature du Net[42] car il instaure *de facto* un fichage policier des personnes trans et des personnes immigrées ayant choisi de modifier leur nom.

Il a été créé par l'arrêté du 19 décembre 2023. Il permet un accès des policiers au RNIPP (au moins à une partie), géré par l'INSEE (répertoire national à des fins statistiques et administratives). Le RNIPP c'est le descendant du projet SAFARI qui avait fait scandale dans les années 70 et conduit à la création de la CNIL (à l'époque la perspective d'un fichage de toute la population mobilisait encore, on en parlait partie 1).

Ce décret permet concrètement aux policiers, gendarmes, agents du service national des enquêtes administratives de sécurité, agents des préfectures et sous-préfectures d'accéder à une liste de personnes qui ont changé de nom ou de prénom.

4.1 – Données concernées

Les données qui figurent au fichier sont : nom de famille antérieur et postérieur au changement de nom, les prénoms antérieur et postérieur au changement de prénom, date et lieu de naissance, date du changement de nom ou prénom, sexe et filiation.

4.2 – Durée de conservation des données

La durée maximum affichée dans l'arrêté est de 6 ans.

4.3 – Droit de communication, rectification et effacement

On n'a pas le droit de s'opposer à ce fichage, ni visiblement de demander l'effacement de ses données.

42 https://www.laquadrature.net/2024/01/30/la-france-cree-un-fichier-des-personnes-trans/

l'accès aux fichiers d'Interpol). Il existe un guide de procédure à l'intention des demandeurs qui saisissent la Commission[79].

C'est possible d'utiliser le formulaire de demande d'accès et/ou de rectification/effacement, disponible ici : https://www.interpol.int/fr/content/download/15565/file/CCF-Application-General-French.pdf

79 https://www.interpol.int/fr/content/download/13876/file/19Y2244%20F%20Procedural_Guidelines_Applicants_CCF-FR.pdf

La réponse d'Europol doit intervenir sous 4 mois. En cas de refus, la personne concernée peut introduire un recours devant le Centre européen de protection des données, rue Wiertz 60, B-1047 BRUXELLES, BELGIQUE.

6. Les fichiers d'Interpol

Interpol est un organisme international de coopération policière basé à Lyon. Il dispose d'un système d'information qui lui est propre et qui comprend 19 fichiers alimentés par les informations qui lui sont transmises par les États. Il est difficile de déterminer les articles de loi et les décrets qui permettent leur application en France. Il s'agit par exemple de la Stolen and Lost Travel Documents Database (fichier des documents de voyage perdus et volés, SLTD), qui est interconnecté avec le fichier français ACCReD (utilisé pour enquêter sur les personnes pour l'accès à certains emplois).

Un des autres fichiers d'Interpol est le fichier « Gestion électronique des demandes d'arrestation provisoire en vue d'extradition » (GERRPOL), régi en France par le décret n°2018-376 du 22 mai 2018.

Interpol gère également un fichier de notices (où sont conservées, par exemple, les « notices rouges »), un fichier des personnes faisant l'objet d'une demande de coopération policière internationale, une base de données sur l'exploitation sexuelle des enfants, un fichier d'empreintes digitales (système automatisé de reconnaissance d'empreintes digitales, AFIS), un fichier de profils ADN (non nominatif, il ne permet pas de relier un profil ADN à une identité), un système de reconnaissance faciale (IFRS), etc. La liste est ici : https://www.interpol.int/fr/Notre-action/Bases-de-donnees/Nos-19-bases-de-donnees

Concernant la reconnaissance faciale (IFRS), le système d'Interpol est alimenté, en France, par les photographies des personnes recherchées en vue de leur extradition et par le TAJ. La connexion avec le TAJ n'est pas automatique – les photographies sont versées manuellement dans IFRS lorsqu'il y a besoin. Les policiers français ne peuvent pas, eux-mêmes, faire tourner le logiciel de reconnaissance faciale d'Interpol ; ils doivent adresser une requête au Bureau central national d'Interpol en France, qui transmet au Secrétariat général d'Interpol, qui traite la demande[78].

Au niveau d'Interpol, ces fichiers sont régis par le règlement sur le traitement des données adopté par l'assemblée générale d'Interpol en 2011.

Il est possible de s'adresser à la Commission de contrôle des fichiers d'Interpol (200 quai Charles de Gaulle, 69006 LYON) pour demander l'accès, la rectification et l'effacement des données (article 18 du règlement sur le traitement des données d'Interpol, et règlement relatif au contrôle des informations et à

78 Avis au nom de la commission des lois sur le projet de loi de finances pour 2021, Assemblée nationale, https://www.assemblee-nationale.fr/dyn/15/rapports/cion_lois/l15b3404-tvii_rapport-avis#

Les demandes d'accès, de rectification ou de limitation sont à adresser au secrétariat général du ministère de l'intérieur.

Partie 5 : Fichiers de renseignement policier

Ces fichiers-là sont beaucoup utilisés par les gendarmes et les policiers. Ils sont accessibles à partir des tablettes NEOPOL et NEOGEND. Il s'agit de fichiers de renseignement, mais ils ne sont pas tenus par les véritables services de renseignement (DGSI et DGSE). Le FPR est le plus connu et le plus utilisé. Il sert à énormément de choses, de la gestion des interdictions de sortie du territoire aux contrôles judiciaires, en passant par les fiches « S » concernant les personnes que les services de police estiment qu'il faut surveiller.

Parmi ces fichiers de renseignement policier, on trouve aussi le PASP et GIPASP, qui rassemblent aussi énormément d'informations. Surtout, PASP et GIPASP permettent de noter finement le mode de vie d'une personne, jusqu'à ses opinions politiques, ses engagements syndicaux et ses convictions philosophiques et religieuses. PASP et GIPASP sont très liés à EASP, qui lui sera vu dans la partie 8 (fichiers servant aux enquêtes administratives).

1. Fichier des Personnes Recherchées (FPR)

C'est un fichier de police judiciaire (ministère de l'intérieur), créé en 1996, commun à la police nationale et à la gendarmerie nationale. Il est géré par la Direction centrale de la police judiciaire (DCPJ). En 2018, au moins 580.000 personnes étaient inscrites au FPR, et le FPR, à la même date, était consulté plus de 100.000 fois par jour.

1.1 – Données concernées

Il est divisé en 21 sous-fichiers, chacun identifié par une ou deux lettres (par exemple, « S » pour Sûreté de l'État, « V » pour Évadé, « CJ » pour Contrôle judiciaire, « E » pour la police des Étrangers, « I » pour les Interdictions judiciaires et interdictions de sortie du territoire, « J » pour les personnes recherchées par la Justice, « M » pour les Mineurs en fugue, « T » pour les débiteurs envers le Trésor, « TE » pour les personnes interdites d'entrée en France, « AL » pour les personnes recherchées en vue d'un placement en hôpital psychiatrique (« ALiéné »)…). Les données concernées sont très très nombreuses et tout peut paraître bien fouillis. Pour essayer de s'y retrouver, voici un tableau qui tente de les trier par thèmes. La liste des personnes et des situations concernées est à l'article 230-19 du code de procédure pénale et à l'article 2 du décret n°2010-569 du 28 mai 2010. L'ensemble du FPR a été révisé par le décret n°2023-979 du 23 octobre 2023. Cette mise à jour ajoute trois catégories de personnes :

- les personnes assujetties aux MICAS[43] (mesures individuelles de contrôle administratif et de surveillance), c'est-à-dire dont l'administration estime, préventivement, qu'il faut les surveiller pour éviter

43 Articles L.228-1 et suivants du code de la sécurité intérieure

5.3 – Durée de conservation des données

Elle est organisée à l'article 31 du règlement.

Les données sont conservées « *pour la durée nécessaire et proportionnée aux finalités pour lesquelles ces données sont traitées.* » Autant dire que c'est vague. À l'issue du délai de 3 ans de conservation, les données sont automatiquement effacées sauf si Europol reconduit ce délai de 3 ans. Ça laisse de grandes marges de manœuvres pour la conservation.

Plutôt, lorsqu'un État transmet des données à Europol, il peut définir un délai au-delà duquel elles sont effacées (article 19 du règlement 2016/794). Au passage, il n'est pas certain que la France, par exemple, définisse systématiquement ce délai, par exemple en prenant en compte le délai de conservation des informations dans les fichiers nationaux. Si l'État qui a fourni les informations a indiqué un tel délai au-delà duquel elles doivent être effacées, à l'issue de ce délai, Europol peut demander à cet État l'autorisation de continuer à les conserver.

De la même manière, l'État qui efface des données dans ses fichiers nationaux doit en informer Europol, qui les efface à son tour, sauf s'il demande à cet État l'autorisation de les conserver.

5.4 – Droit d'accès, de rectification et d'effacement des données

L'article 36 du règlement prévoit que les personnes concernées peuvent demander l'accès aux informations qui les concernent sont traitées par Europol. Elles peuvent s'adresser aux autorités de l'État de leur choix, qui fait suivre à Europol sous le délai d'un mois. Il semble qu'en France, il soit possible de s'adresser à la CNIL, à la direction générale de la police nationale ou à la direction générale de la gendarmerie nationale. Europol doit répondre dans un délai de 3 mois à compter de la réception de la demande.

Europol, avant de donner l'accès aux données à la personne concernée, interroge les États membres, qui peuvent s'opposer à la transmission des informations. En cas de refus, la personne en est informée par Europol. Europol peut aussi décider d'informer la personne uniquement du fait qu'il a effectué les vérifications nécessaires. La personne peut introduire un recours devant le Centre européen de protection des données, rue Wiertz 60, B-1047 BRUXELLES, BELGIQUE.

L'article 37 du règlement prévoit qu'une personne peut aussi demander la limitation du traitement (la conservation des données détenues par Europol pour qu'elle puisse s'en servir comme preuve), la rectification et l'effacement des données la concernant. Elle peut s'adresser à l'État de son choix (en France, ça doit être la CNIL, la DGPN et la DGGN). Pour la rectification et l'effacement, la personne doit avoir eu préalablement accès aux données la concernant.

Ses objectifs sont aujourd'hui très larges : ont été rajoutés la répression des faits de meurtre et de violences graves, d'enlèvement et séquestration, de racisme et de xénophobie, de vol aggravé, d'escroquerie, d'extorsion de fonds, de faux et usage de faux documents administratifs, de criminalité informatique, de corruption, de trafic d'armes, d'abus sexuel et exploitation sexuelle, de pédopornographie (annexe I du règlement 2016/794). Pour entrer dans les objectifs d'Europol, ces faits doivent affecter au moins deux États membres, ou porter atteinte à un intérêt commun faisant l'objet d'une politique de l'Union européenne (par exemple la pédopornographie, les abus sexuels sur les enfants, le trafic d'armes, la criminalité informatique…). Le terrorisme est toujours de la compétence d'Europol, même si les faits ne sont commis qu'à l'échelle nationale.

Le fichier Europol est alimenté par les États membres, via l'unité nationale de contact avec Europol présente dans chaque État membre.

5.1 – Données concernées

Les données collectées sont celles relatives aux personnes soupçonnées d'avoir commis ou condamnées pour les infractions ci-dessus, ainsi que les personnes dont il existe des indices concrets ou de bonnes raisons de croire qu'elles commettront ces infractions.

Il s'agit de tout l'état civil, le numéro de sécurité sociale, les papiers d'identité, les faits reprochés, les moyens utilisés, l'appartenance à une organisation criminelle, les condamnations pour des faits relevant de la compétence d'Europol, les contacts de l'entourage, les personnes pouvant fournir des informations sur ces infractions, la description physique, **les empreintes digitales, le profil ADN, l'empreinte vocale, le groupe sanguin, le dossier dentaire**, l'emploi et les qualifications professionnelles, la formation, les aptitudes, les données financières et patrimoniales, les liens avec des sociétés, les contacts avec les banques, la situation fiscale, le mode de vie, les habitudes, les déplacements, les lieux fréquentés, les armes, les risques particuliers (par exemple la probabilité de fuite ou les liens avec des services de police), les traits de caractère en lien avec la criminalité, la toxicomanie … les informations sont très nombreuses (annexe II du règlement 2016/794).

5.2 – Échanges avec des États non membres de l'Union européenne

Europol échange des informations personnelles avec le Royaume-Uni (accord de septembre 2021), la Géorgie (accord du 4 avril 2017), le Liechtenstein (accord du 7 juin 2013), Monaco (accord du 6 mai 2011), l'Ukraine (accord du 14 décembre 2016), la Bosnie Herzégovine (accord du 31 août 2016), les États-Unis (accord du 20 décembre 2002), la Serbie (accord du 16 janvier 2014), la Norvège (accord du 28 juin 2001), le Monténégro (accord du 29 septembre 2014), la Moldavie (accord du 18 décembre 2014), la Macédoine (2007), l'Islande, la Colombie, le Canada (accord du 21 novembre 2005), l'Australie (accord du 20 février 2007), l'Albanie (accord du 9 décembre 2013) et la Suisse (accord du 24 septembre 2004).

des actes de terrorisme. L'inscription au FPR sert donc dans le cadre du contrôle du respect de l'assignation à une commune, l'interdiction de paraître à certains endroits ou l'interdiction de relation avec certaines personnes.

- Les personnes de retour d'une zone de guerre ou de terrorisme (« théâtre d'opérations de groupements terroristes »).

- Les étrangers placés sous procédure « Dublin » (dont la demande d'asile doit être étudiée par un autre État européen) et qui sont considérés comme étant « en fuite ».

La loi du 10 avril 2019 visant la répression des manifestations modifie ainsi l'article 230-19 du code de procédure pénale pour y inclure **les interdictions de manifester** prononcées à l'encontre de quelqu'un soit au titre du contrôle judiciaire, soit au titre d'une peine. En conséquence, lors d'un contrôle d'identité, un agent peut très vite se rendre compte si une personne n'a pas le droit d'être présente en manifestation.

De la même manière, les interdictions de paraître dans certains lieux et les interdictions de rencontrer certaines personnes, prononcées par exemple par le procureur de la République avec un avertissement pénal ou lors d'une composition pénale, ou par un juge lors d'un sursis probatoire, d'un suivi socio-judiciaire, d'une libération conditionnelle, etc, apparaissent au FPR.

Au niveau des données qui figurent dans le FPR (l'article 3 du décret n°2010-569 modifié par le décret n°2023-979 est désormais plus prolixe), il y a évidemment l'identité, l'adresse, mais aussi les alias ou surnoms, l'évaluation de la dangerosité, les critères physiques et signes particuliers, photo, motifs de la recherche et autorité qui a décidé de l'inscription, numéros de passeport, carte d'identité, permis de conduire, les véhicules qu'on est susceptible de conduire… Le décret prévoit même désormais que le FPR puisse enregistrer les données les plus sensibles : appartenance ethnique, convictions religieuses, opinions politiques, données génétiques et biométriques, données de santé ou sur l'orientation sexuelle !

Chaque fiche a un volet « conduite à tenir » qui décrit ce que doit faire le flic lorsqu'il a la personne concernée sous la main : interpeller la personne, collecter certains renseignements (documents d'identité, provenance et destination de la personne, véhicule, contrôle des individus accompagnant la personne fichée…) sans attirer l'attention de la personne, informer le service qui a créé la fiche, etc. Il y a 11 conduites à tenir différentes.

4.1 – Données collectées et finalités

Son but : prévenir les actes de terrorisme, les atteintes aux intérêts fondamentaux de la nation et les crimes graves visés par le directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016, soit tous ces crimes et délits s'ils sont passibles d'une peine d'emprisonnement ou d'une mesure de sûreté de minimum 3 ans dans un des États membres de l'UE : participation à une organisation criminelle, traite des êtres humains, exploitation sexuelle des enfants et pédopornographie, trafic de stupéfiants et de substances psychotropes, trafic d'armes, de munitions et d'explosifs, corruption, fraude, y compris la fraude portant atteinte aux intérêts financiers de l'Union, blanchiment du produit du crime et faux monnayage, y compris la contrefaçon de l'euro, cybercriminalité, infractions graves contre l'environnement, y compris le trafic d'espèces animales menacées et le trafic d'espèces et d'essences végétales menacées, aide à l'entrée et au séjour irréguliers, meurtre, coups et blessures graves, trafic d'organes et de tissus humains, vol organisé ou vol à main armée…

Données recueillies par les transporteurs aériens, pour tout vol sauf ceux internes à la France métropolitaine, et transmises à l'UIP.

Fichier en lien avec le FPR, Schengen, le Fichier des objets et véhicules signalés (FoVES), Interpol. Peut être consulté par vraiment plein de monde.

4.2 – Durée de conservation des données

5 ans (article L232-7 IV du code de la sécurité intérieure).

4.3 – Droits d'accès et de rectification

L'exercice de ces droits est régi par l'article R232-22. Pour la plupart des données : S'adresser directement au Directeur de l'Agence nationale des données de voyage, Place Beauvau, 75800 PARIS CEDEX 08.

Pour les données relatives à la mention « connu » ou « inconnu » du FPR, de N-SIS II (Schengen), du Fichier des objets et des véhicules signalés et d'Interpol : s'adresser à la CNIL.

5. Les fichiers Europol

L'office européen de police Europol a été créé par la convention du 26 juillet 1995. Dès l'origine, ses objectifs sont notamment la collecte, l'analyse et l'échange d'informations entre les États européens, et la gestion de données (article 3.1 de la convention du 26 juillet 1995). Europol concerne la lutte contre le terrorisme, contre le trafic de stupéfiants, contre des formes graves de criminalité internationale, les filières d'immigration clandestines, la traite des êtres humains, le trafic de véhicules volés, et le blanchiment d'argent. Donc la convention du 26 juillet 1995 traite principalement des fichiers Europol.

Aujourd'hui Europol est régi par le règlement 2016/794 du 11 mai 2016 modifié par le règlement n°2022/991 du 8 juin 2022.

Type de personne ou de situation	**Événements et personnes inscrites au FPR** : *en italiques, les données dont la consultation et la rectification se fait directement à la DCPJ (ministère de l'intérieur)* ; en caractères romains, celles pour lesquelles il faut passer par la CNIL				
Personne recherchée ou sous le contrôle de la justice en vue de son procès ou de l'exécution d'une peine (Fiches « J »)	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.	*Mesure de contrôle judiciaire (fiche « CJ »).*	N'importe quelle recherche criminelle (donc crime, et non délit ni contravention…) Voir le II 2° de l'article 2 du décret n°2010-569 du 28 mai 2010		Les personnes recherchées dans le cadre d'une enquête préliminaire, d'une enquête de flagrance ou d'une instruction.
Peines prononcées par un juge (alternative ou complémentaire). Ces interdictions sont des fiches « I » (sauf la dernière, « TE »).	*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, de stade Interdiction administrative de sortie du territoire*		*Interdiction de porter ou de détenir une arme soumise à autorisation, interdiction de détenir un animal*	*Interdiction de territoire français prononcée par un juge pénal (fiche « TE » : Interdiction du territoire).*
En cas de certaines condamnations	*Les personnes inscrites au Fichier judiciaire national automatisé des auteurs d'infractions terroristes.*		*Les personnes inscrites au Fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes seulement si elles ne se trouvent plus à l'adresse qu'elles ont indiqué.*		
Peines et aménagements de peine qui incluent l'idée d'aggravation si la personne ne se soumet pas à certaines contraintes	*Interdictions et obligations prononcées dans le cadre d'une contrainte pénale (fiche « I »).*	*Mesures de sursis mise à l'épreuve, sursis assorti de l'obligation d'un TIG.*	*Mesures de suivi socio-judiciaire.*	*Libération conditionnelle, semi-liberté, placement à l'extérieur, bracelet électronique, toutes sortes d'aménagements de peine… (voir le 8e de cet article 230-19).*	
Concernant les personnes mineures	*Interdictions de paraître dans certains lieux, interdictions de circuler la nuit, interdictions de rencontrer la victime ou les coauteurs.*	*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).*		*Mineur·e faisant l'objet d'une opposition à la sortie du territoire.*	*Mineur·e ayant quitté son domicile, en fugue (fiche « M »).*
En cas de trouble mental	*Mesures prononcées en cas d'irresponsabilité pénale prononcée par un juge : entrer en relation avec la victime, interdiction de paraître, de porter une arme… 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 (Fiche « AL » : « Aliénés »).	
Pour les personnes étrangères	Étranger dont l'entrée en France peut être refusée car	Étrangers hors UE faisant l'objet d'une	*Étranger qui n'a pas exécuté une OQTF, ou une*	Étranger de nationalité suisse, islandaise, norvégienne ou d'un État membre de l'Union	

	elle constituerait une menace pour l'ordre public (Fiche « TE » : Opposition à l'entrée en France).	restriction de voyage adoptée par l'UE.	*interdiction de circuler sur le territoire français, ou 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).*	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). Fiche «E»	
En cas de disparition ou de corps non identifié	En cas de disparition dans des conditions inquiétantes ou suspectes.		En cas de découverte de personne décédée ou vivante non identifiée. Fiche «X»		
Exemples de Fiches « S » (« Sûreté de l'État »)	Personne recherchée pour prévenir des menaces graves pour la sécurité publique ou la sûreté de l'État. (Fiche « S »).	« Personne qui a quitté le territoire national et dont il existe des raisons sérieuses de penser que ce déplacement a pour but de rejoindre un théâtre d'opérations de groupements terroristes dans des conditions susceptibles de la conduire à porter atteinte à la sécurité publique lors de son retour sur le territoire français peut faire l'objet d'un contrôle administratif dès son retour sur le territoire national. » (article L225-1 du code de la sécurité intérieure) : Fiche « S14 »			Il y en a beaucoup d'autres, ça va de S2 à S15 ou S16. Certaines sont relatives à des types de personnes, d'autres à des comportements que les flics doivent adopter.
En cas de problème avec le 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.*	
En cas de fraude ou de tentative de fraude relative aux papiers d'identité	*Personne qui a obtenu ou tenté d'obtenir indûment une carte d'identité ou un passeport.*		«TP» : Opposition à la délivrance de document d'identité		
Terrorisme	Français interdit de quitter le territoire parce qu'il est soupçonné de se livrer à des activités terroristes à l'étranger (article L224-1 du code de la sécurité intérieure).				D'autres aussi, voir dans les exemples de Fiches « S ».

Le principe initial, prévu dans Prüm I, était que les services concernés de chaque État de l'Union européenne (et la Suisse) peuvent interroger les autres États afin de savoir s'ils détiennent des informations sur une personne, et lesquelles. Ce principe semble avoir été remplacé, dans le cadre de Prüm II, par la disponibilité directe des données de chaque État à l'ensemble des autres États. Ainsi, en matière de fichage génétique, il est possible pour la police française, par exemple, de comparer l'ADN d'une personne avec l'ensemble des fichiers de données génétiques des États membres de l'Union européenne (articles 5 et suivants du règlement n°2024/982 du 13 mars 2024). Le même système est mis en place pour les empreintes digitales.

Prüm II autorise également la reconnaissance faciale à l'échelle de l'ensemble des fichiers de police de type « TAJ » des pays européens (paragraphe 27 du préambule et articles 24 et suivants du règlement n°2024/982 du 13 mars 2024).

Il permet l'interconnexion de tous les fichiers de police, notamment du type du « TAJ » (articles 25 et suivants du règlement n°2024/982 du 13 mars 2024).

Son application peut prendre un peu de temps compte tenu des outils qui doivent encore être créés pour permettre ces interconnexions.

En application de l'article 31 de la décision 2008/615/JAI du 23 juin 2008, toute personne peut demander à être informée sur « *les données traitées la concernant et sur leur origine, sur les destinataires ou catégories de destinataires, sur la finalité du traitement ainsi que, lorsque le droit national le requiert, sur la base juridique justifiant le traitement.* » Elle peut aussi demander la rectification des données inexactes.

La France ne semble pas avoir mis en place une procédure particulière pour demander ces informations. Il est donc possible de s'adresser à la CNIL, qui fera suivre la demande aux autorités concernées.

4. API-PNR France (Advance Passenger Information – Passenger Name Record)

Il s'agit du volet français du système PNR, et il est encadré par les articles L232-7 et les articles R232-12 et suivants du code de la sécurité intérieure.

Il est mis en œuvre par le ministère de l'intérieur, le ministère de la défense, le ministère des transports et le ministère des douanes, et plus précisément par le Service à compétence nationale Unité Information Passagers (UIP), le rôle d'Unité Information Passagers ayant depuis été transféré à l'Agence nationale des données de voyage (décret n°2022-751 du 29 avril 2022). Cette agence est placée sous l'autorité du ministère de l'Intérieur.

Le PNR actuel ne concerne que les voyages aériens. Cependant, depuis le mois de décembre 2019, le gouvernement affiche sa volonté d'étendre dans le futur le PNR aux voyages en train, en bus et en bateau (arrêté du ministre de l'intérieur du 16 décembre 2019 remplacé par le décret n°2022-752 du 29 avril 2022).

judiciaires des étrangers hors Union européenne (ECRIS-TCN). Il est également interconnecté avec le Portail de recherche européen (ESP, lui-même interconnecté avec les fichiers d'Europol et d'Interpol), le service européen partagé d'établissement de correspondances biométriques (BMS partagé, pour comparer les données biométriques des pays de l'Union européenne), le répertoire commun de données d'identité (CIR, qui permet le croisement des fichiers de cartes nationales d'identité, de passeports et de titres de séjour des États de l'Union européenne), et le détecteur d'identités multiples (MID, qui permet de croiser les données d'identité) (règlement n°2019/817 du 20 mai 2019).

2.2 – Durée de conservation des données

La durée de conservation des données est prévue à l'article 44 de la convention du 19 juin 1990 et à l'article R231-11 du code de la sécurité intérieure. Pour les personnes, les données sont conservées 3 ans par défaut, mais lorsqu'il s'agit de contrôle discret, elles sont conservées un an seulement. Pour les objets, 10 ans par défaut, mais 5 ans lorsqu'il s'agit de contrôle discret.

Bien sûr, des prolongations sont possibles.

2.3 – Droits d'accès et de rectification

Concernant la base de données nationale (N-SIS II), le droit de communication des données est exercé via la CNIL : article R231-12 du code de la sécurité intérieure. Le demandeur doit être informé sous 2 mois des suites de sa demande.

Il y a aussi un droit de communication direct auprès de la Direction nationale de la police judiciaire, ministère de l'intérieur (article R231-12 II), pour : l'état civil, le sexe, la nationalité, les signes physiques particuliers, la photographie, les motifs du signalement, et pour les objets perdus, volés ou détournés.

3. Fichiers européens interconnectés (Bases de données Prüm)

En 2005, les États membres de l'espace Schengen signent le traité de Prüm (Schengen III). À la suite de ce traité, le 23 juin 2008 le Conseil européen prend les décisions 2008/615/JAI et 2008/616/JAI.

Le règlement n°2024/982 du Parlement européen et du Conseil du 13 mars 2024 (règlement Prüm II) a élargi les catégories de données concernées et permis l'automatisation de leur utilisation. Il n'est pas encore totalement appliqué car il semble que certains logiciels doivent être créés.

Ces décisions prévoient une interconnexion de très nombreux fichiers de police de chaque pays membre de l'Union européenne : empreintes génétiques (FNAEG en France, article R53-19-1 du code de procédure pénale), empreintes digitales (FAED en France, article 9-1 du décret n°87-249 du 8 avril 1987), plaques d'immatriculations des véhicules, prévention des infractions pénales en cas de manifestations sportives (FNIS en France) ou de sommets internationaux, prévention du terrorisme (divers fichiers peuvent être concernés en France tels que FIJAIT, FPR, FSPRT, PASP, GIPASP).

	Personnes qui se sont rendues sur un « théâtre d'opération de groupements terroristes » et qui sont surveillées pour cela à leur retour Personnes sous le coup d'une MICAS, et qui ont un régime de restriction de liberté (assignation à une commune) ou d'interdiction de rencontrer d'autres personnes, aux fins de prévention du terrorisme.			
État d'urgence	*Personne qui fait l'objet d'une interdiction de séjour, d'une assignation à résidence ou d'une interdiction de se trouver en relation avec certaines personnes en application de la loi de 1955 sur l'état d'urgence.*			
Autres	*Personne qui n'a pas payé sa dette à l'État, aux collectivités territoriales ou aux établissements publics. (Fiche « T » : Débiteurs envers le Trésor).*	*Insoumis et déserteurs.*	*L'interdiction de sortie du territoire prononcée par le juge lorsqu'il prend une ordonnance de protection de la personne majeure menacée de mariage forcé (article 515-13 du code civil).*	

Tableau 1 : Récapitulatif des personnes concernées par le fichage au FPR. En italiques, les données pour lesquelles le droit de communication et de rectification s'exerce directement auprès de la Direction centrale de la police judiciaire (ministère de l'intérieur) ; en police romaine*, les données pour lesquelles le droit de communication et de rectification s'exerce indirectement, auprès de la CNIL.*

En 2016, **800’000 personnes** étaient inscrites dans N-SIS II[76].

2.1 – Données concernées

Le fichier vise à conserver des informations sur les personnes visées par un mandat d’arrêt européen ou par une extradition, les personnes visées par une non-admission ou une interdiction de séjour à la suite d’une décision administrative ou judiciaire, les personnes disparues, le personnes visées par des mesures de contrôle discret pour la répression d’infractions pénales ou pour la prévention d’atteintes à l’ordre public ou à la sûreté de l’État, et les personnes visées par l’exécution d’une peine. Il conserve aussi des informations sur les personnes témoins de faits revêtant une qualification pénale, les personnes condamnées qui doivent se voir notifier leur condamnation, les personnes recherchées pour exécuter une peine d’emprisonnement.

Le fichier contient également des informations sur les véhicules à moteur, embarcations, avions, remorques, armes à feu, documents officiels volés ou détournés, billets de banque, moyens de paiement volés ou égarés, conteneurs…

N-SIS II est interconnecté avec 12 fichiers français[77]. C’est difficile de déterminer la liste exacte. C’est certain que N-SIS II est alimenté par le FPR, FOVeS et le TES. Les données de N-SIS II sont également versées, ou consultables par LAPI, ACCReD, EASP.

Il est aussi interconnecté avec COVADIS (contrôle et vérification automatiques des documents d’identité sécurisés), PARAFE (passage automatisé aux frontières extérieures, un système de passage rapide aux douanes des aéroports), RMV (Réseau Mondial des Visas), SETRADER (fichier des passagers aériens), API-PNR (comme SETRADER mais plus large), AGDREF (Application de gestion des dossiers des ressortissants étrangers en France), SAT VV (géolocalisation des véhicules) et STCL (système de lecture automatisée des plaques d’immatriculation des véhicules).

N-SIS II peut contenir des **photographies** des personnes, et cela est même automatique quand une personne est inscrite au FPR avec sa photo (articles 20 et 36 du règlement n°1987/2006 du 20 décembre 2006, et R231-9 du code de la sécurité intérieure).

Le règlement européen prévoit également que les **empreintes digitales** peuvent être versées dans N-SIS II (article R231-9 du CSI), mais il semble que l’interconnexion entre le FAED et N-SIS II ne soit pas (encore) opérationnelle.

Concernant ses liens avec les autres fichiers européens et internationaux, N-SIS II est interconnecté avec le fichier européen sur les visa (VIS), le fichier des étrangers hors Union européenne n’ayant pas besoin de visa (ETIAS), le fichier des passages de frontières des étrangers hors Union européenne (EES, système entreé/sortie), le fichier des empreintes digitales des étrangers hors Union européenne (Eurodac), les casiers

76 https://www.cnil.fr/fr/sis-ii-systeme-dinformation-schengen-ii , consulté le 11 mars 2019

77 Clément HAMOIR, *Le renseignement et la gendarmerie nationale : enjeux et perspectives*, thèse de doctorat, Université Côte d’Azur, 2019, p.238 https://core.ac.uk/download/pdf/287474242.pdf

C’est aussi dans le FPR qu’apparaissent les fameuses **Fiches « S »** (Sûreté de l’État). Il y a 21 types différents de fiches « S », en fonction de la conduite à tenir par les flics et du profil de la personne. Par exemple : S14, les personnes considérées comme islamistes revenant de l’Irak ou de la Syrie ; S15, les personnes à interpeller ; S16, les personnes suspectées de radicalisation à propos desquelles il faut collecter des renseignements (domicile, occupation, ressources, manières de vivre, moyens de locomotion, téléphones, vêtements, photo, et les personnes avec qui elle est en relation). Elles existent depuis les années 1960 et ont une durée de deux ans qui peut être renouvelée. En décembre 2018, d'après un rapport d'information au Sénat rédigé par le groupe de travail sur l'amélioration de l'efficacité des fiches S[44], 29.973 personnes faisaient l'objet d'une fiche S, et il y avait environ 30.787 fiches : les personnes pouvant avoir plusieurs fiches.

En octobre 2023, Gérald Darmanin, ministre de l’Intérieur, déclare devant une Commission d’enquête de l’Assemblée nationale[45] que 3.000 personnes seraient fichées en tant que membres de « *l’ultra-gauche* ».

Les fiches S peuvent être inscrites par quatre services : la direction générale de la sécurité intérieure (DGSI), le service central du renseignement territorial (SCRT), la direction du renseignement de la préfecture de police de Paris (DRPP) et la direction générale de la gendarmerie nationale (DGGN). En réalité, c'est la DGSI qui mène la danse : en juin 2018, elle était responsable de l'inscription de 80% des fiches S. Elle s'appuie notamment sur les fichiers CRISTINA et PASP pour le faire. Dans la majorité des fiches S, le comportement à tenir est de ne pas attirer l'attention : seules 4,8 % des fiches indiquent de retenir la personne et d'aviser le service demandeur. Les retenues administratives peuvent durer jusqu'à 4 heures lorsqu'il « existe des raisons sérieuses de penser que leur comportement peut être lié à des activités terroristes» (article 78-3-1 du code de procédure pénale, modifié par l'article 48 de la loi du 3 juin 2016). Si on déclenche un «hit» lors d'un contrôle, il y aura une remontée d'info au service demandeur : un coup de téléphone, associé à l'envoi d'un PV d'observations (une "note de passage" en général envoyée 24 à 48 heures après). La remontée d'infos peut aussi se faire lors de la demande d'un passeport, ou une demande de nationalité. En avril 2018, sur 26.000 fiches, environ 17.000 auraient été délivrées sur la base d'une suspicion de radicalisation islamiste. Des débats semblent animer les parlementaires jusqu'aux services de renseignement sur l'utilité de la fiche S : le grand nombre de personnes inscrites, et la méconnaissance des agents de terrrain sur la conduite à tenir entraîne souvent la révélation de l'existence d'une fiche S, ce qui est contraire à ses objectifs. En mai 2023, lors d'un contrôle routier, les flics décident de fouiller le véhicule d'un conducteur qui apparait comme fiché S. Sous le siège de la voiture, ils découvrent un dispositif artisanal fait de scotch et de fils électriques : panique générale et embarquement de tout le monde pour association de malfaiteurs terroriste. Quelques heures plus tard, le petit paquet noir s'avère être un GPS tracker posé par la

44 https://www.senat.fr/rap/r18-219/r18-2190.html

45 https://www.publicsenat.fr/actualites/institutions/fiche-s-fpr-fsprt-quels-sont-les-differents-fichiers-de-renseignement-utilises-pour-la-lutte-antiterroriste

DSGI[46]... La fiche S s'apparente davantage à un filet de capteurs capables de faire de la remontée d'info qu'à une surveillance continue. Dans le rapport pré-cité, le rapporteur explique que la surveillance continue d'une personne nécessite l'implication de 20 à 25 agents, ce qui représente un coût énorme.

A l'occasion de l'audition de Darmanin en octobre 2023 lors de la commission d'enquête de l'assemblée nationale sur les groupuscules violents, lancée après Sainte-Soline, on apprend qu'il y a d'après le ministre 3000 fichés S d'« ultragauche », 5300 pour « islamisme » et 1300 d' « ultradroite ».

On voit donc qu'il y a 2 types de fichage au FPR : le fichage « ostensible », qui concernent des personnes qui « savent », ou plutôt peuvent facilement savoir qu'elles sont fichées au FPR : par exemple, les personnes condamnées à du sursis avec mise à l'épreuve savent qu'elles sont condamnées, et de cette condamnation découle leur fichage. De la même manière, une personne qui a perdu tous ses points du permis de conduire est censée le savoir, et de là découle son fichage. Parallèlement, il y a le fichage « caché/discret », dont l'objet même nécessite que la personne ne sait pas qu'elle est fichée. C'est le cas, par exemple, des personnes concernées par une « Fiche S » pour « prévenir des menaces graves pour la sécurité publique ou la sûreté de l'État ». Dans ce cas-là, bien sûr, on ne reçoit pas une jolie lettre « Vous avez une Fiche S au FPR, nous vous souhaitons la bienvenue » : l'État a tout intérêt à vous cacher le fait que vous êtes fiché·e.

Dans ce dernier cas (le fichage « caché/secret »), il y a néanmoins des indices qui permettent de déduire qu'on est fiché·e. Par exemple, vous attendez 8 mois pour avoir un passeport (effectivement, l'article 8 du décret n°2016-1460 du 28 octobre 2016 prévoit la consultation du FPR au moment de la demande de passeport) ; ou alors, à l'aéroport vous faites l'objet d'un contrôle poussé (pas seulement un regard sur le passeport et 5 minutes d'attente, mais plutôt 30 minutes d'attente et un interrogatoire sur les raisons de votre départ, la durée de votre séjour à l'étranger, etc, voire la fouille de vos bagages) ; ou alors, au cours d'un banal contrôle routier, les flics vous demandent plus ou moins discrètement d'où vous êtes parti·e, votre destination, voire relèvent l'identité de toutes les personnes voyageant avec vous…

Enfin, le FPR est interconnecté avec de nombreux fichiers : PNR (relatif aux voyages en avion), SETRADER (Système européen de traitement des données d'enregistrement et de réservation), PARAFE (système de contrôle automatique aux frontières, sur volontariat), FIJAISV (Fichier judiciaire automatisé des auteurs d'infractions sexuelles et violentes), AGDREF (Application de gestion des dossiers des ressortissants étrangers en France), ACCRED, N-SIS II (Système d'Informations Schengen II – National), les fichiers d'Europol et d'INTERPOL (article 2 du décret du 28 mai 2010).

46 https://actu.orange.fr/france/joinville-le-pont-l-engin-suspect-decouvert-etait-en-realite-une-balise-gps-de-la-police-magic-CNT0000023OiQq.html

On ne sait pas trop à quoi ça correspond en France. Toutefois, un arrêt du Conseil d'État du 22 décembre 2022 (n°465263, mentionné au recueil Lebon) a un peu clarifié les choses en indiquant que ECRIS est indissociable du casier judiciaire et en déclarant que le juge judiciaire est compétent. Il peut donc être possible de demander au procureur de la République domicile de la personne l'effacement des données de ECRIS (pour les ressortissants européens) et ECRIS-TCN (pour les ressortissants non européens) en même temps que la demande d'effacement du casier.

2. Système d'information Schengen (N-SIS II)

Le système d'information Schengen a été créé par la convention du 19 juin 1990 d'application de l'accord de Schengen du 14 juin 1985. Cette convention a depuis été remplacée par le règlement 1987/2006 du 20 décembre 2006 et par la décision du Conseil n°2007/533 du 12 juin 2007, deux textes remplacés depuis par le règlement n°2018/1860 du 28 novembre 2018 (sur l'utilisation de N-SIS II pour l'expulsion d'étrangers en situation irrégulière), le règlement n°2018/1861 du 28 novembre 2018 (sur l'utilisation de N- SIS II pour les vérifications aux frontières), et le règlement n°2018/1862 du 28 novembre 2018 (sur l'utilisation de N-SIS II pour la coopération policière et judiciaire en matière pénale).

Au niveau européen, le système d'information Schengen est placé sous la responsabilité de l'Agence pour la gestion opérationnelle des systèmes d'information à grande échelle dans le domaine de la liberté, de la sécurité et de la justice.

Au niveau national, le système d'informations Schengen est placé sous la responsabilité du ministère de l'intérieur. Les règles qui l'encadrent au niveau national sont aux articles R231-1 et suivants du code de la sécurité intérieure.

Le système d'information Schengen est composé d'un fichier central (SIS II central) et des fichiers nationaux de chaque État membre (N-SIS II).

La base de données centrale (SIS-II) est alimentée par les bases de données nationales (N-SIS II France, Belgique, Allemagne, Estonie, etc.). Les bases de données nationales sont celles des États membres de l'espace Schengen (tous les pays de l'Union européenne plus la Suisse, la Norvège et l'Islande).

En France, la base de données nationale (N-SIS II) est alimentée par[75] :

- le fichier des personnes recherchées (FPR) (décret du 28 mai 2010)
- le fichier des objets et véhicules signalés (FOVeS) (visas de l'arrêté du 17 mars 2014)
- le fichier des titres électroniques sécurisés (TES) (visas du décret du 28 octobre 2016)

75 Voir l'avis n°2016-371 du 1er décembre 2016 de la CNIL, qui est plutôt clair https://www.legifrance.gouv.fr/jorf/id/JORFARTI000033737083#JORFARTI000033737083

Dans tous les cas, « *si le droit de l'État membre de condamnation autorise la collecte et la conservation des images faciales des personnes condamnées* » (article 5.3 du règlement 2019/816 pour ECRIS-TCN) ou « *si l'autorité centrale y a accès* » (article 11.1 c) de la décision-cadre 2009/315/JAI du 26 février 2009 modifié par l'article 1er de la directive 2019/884 du 17 avril 2019).

En ce qui concerne la France, elle peut donc transmettre aux autres États les empreintes digitales et la photographie, au moins si elle est issue du TAJ ou de GENESIS.

L'utilisation de la **reconnaissance faciale** est déjà prévue, dès que « *la technique requise est disponible et prête à être employée* » (règlement n°2019/816 du Parlement européen et du Conseil du 17 avril 2019).

1.2 – Utilisation de ECRIS et de ECRIS-TCN

Il n'y a pas de fichier centralisé concernant ECRIS. En fait, chaque État conserve les condamnations prononcées contre ses propres ressortissants (article 3 de la décision-cadre 2009/316/JAI du Conseil du 17 avril 2009).

En conséquence, si un juge allemand condamne un·e Français·e, l'État allemand doit transmettre à la France la condamnation, qui la porte au casier judiciaire. Ensuite, si ce·tte même Français·e est arrêté·e en Roumanie, un juge roumain demandera à la France si cette personne a été condamnée auparavant. La France pourra alors transmettre non seulement les éventuelles condamnations prononcées par des juges français, mais aussi celle prononcée par le juge allemand.

ECRIS-TCN (entré en vigueur en juin 2022) sera lui un fichier à part entière, qui rassemblera toutes les condamnations prononcées par un tribunal d'un pays membre de l'Union européenne contre des ressortissants d'États non membres de l'Union (article 4 du règlement 2019/816 du 17 avril 2019).

ECRIS et ECRIS-TCN peuvent être consultés lors du recrutement pour des postes qui nécessitent des contacts avec des enfants (article 10 de la directive 2011/92/UE du 13 décembre 2011 pour ECRIS et article 7 du règlement 2019/816 du 17 avril 2019 pour ECRIS-TCN), pour d'autres procédures de recrutement, de naturalisation, de demandes d'asile, de licence d'arme à feu, d'adoption (article 7 du règlement européen 2019/816 du 17 avril 2019).

1.3 – Durée de conservation des données

C'est les mêmes que pour le casier judiciaire.

1.4 – Accès, rectification, effacement des données

Les règlements européens désignent « *les autorités centrales des États membres* » (article 25 du règlement européen 2019/816 du 17 avril 2019 pour ECRIS-TCN et articles 6.3 et 6.3 bis de la décision-cadre 2009/315/JAI du 26 février 2009 modifiés par l'article 1er de la directive 2019/884 du 17 avril 2019).

1.2 – Durée de conservation des données

Le décret du 23 octobre 2023 a modifié la durée de conservation des données. Auparavant, les données étaient effacées sans délai en cas d'aboutissement de la recherche ou d'extinction du motif de l'inscription, sauf pour les obligations de quitter le territoire notifiées aux étrangers (conservation pendant 3 ans).

Dorénavant la conservation des données est beaucoup plus longue : 6 mois à compter de l'aboutissement de la recherche ou de l'extinction du motif de l'inscription, puis archivées pendant 6 ans !

Selon un Rapport du Sénat du 19 décembre 2018, les fiches « S », sont conservées 2 ans[47], mais elles sont renouvelées aussi longtemps que la fiche apparaît nécessaire aux flics – et ça peut durer plusieurs années.

1.3 – Droit d'accès et de rectification

Le décret du 23 octobre 2023 a (enfin) mis en conformité les procédures de demandes d'accès, de rectification et d'effacement des données inscrites dans le FPR aux modifications apportées par l'ordonnance n°2018-1125 du 12 décembre 2018 à la loi n°78-17 du 6 janvier 1978. L'article 9 du décret n°2010-569 du 28 mai 2010 modifié organise ces procédures, qui sont assez compliquées… mais en fait, pas tant que ça !

Il faut reprendre les 2 catégories précédentes : le fichage « ostensible », qui concerne des personnes qui « savent », ou plutôt peuvent facilement savoir qu'elles sont fichées au FPR (par exemple, une personne qui a perdu tous ses points du permis de conduire est censée le savoir, et de là découle son fichage) et le fichage « caché/secret », dont l'objet même nécessite que la personne ne sait pas qu'elle est fichée.

Pour les premières, celles qui « devraient savoir » qu'elles sont fichées au FPR, le droit de communication, de rectification et d'effacement est direct, auprès du directeur général de la police nationale et du directeur général de la gendarmerie nationale, ministère de l'intérieur, Place Beauvau, 75008 PARIS CEDEX 08. Dans le tableau précédent, ce sont toutes les cases écrites en italiques. Il y a un modèle de lettre en annexe pour faire la demande.

Le directeur général de la police nationale et le directeur général de la gendarmerie nationale peuvent refuser de communiquer, de rectifier et/ou d'effacer ces données. Un recours peut alors être formé devant la CNIL ou devant le Tribunal administratif (plutôt avec l'aide d'un·e avocat·e).

Pour les deuxièmes, celles pour qui le fichage est « caché/secret » (on ne reçoit pas une jolie lettre « Vous avez une Fiche S au FPR, nous vous souhaitons la bienvenue »), le droit de communication et de rectification est indirect, auprès de la CNIL. Dans le tableau précédent, ce sont toutes les cases écrites en caractères romains (ce qui est droit, pas en italiques). Bien sûr, en annexe vous trouverez un modèle de lettre à la CNIL (il s'agit du premier modèle, qui concerne de nombreux fichiers).

47 https://www.senat.fr/rap/r18-219/r18-2190.html

La CNIL peut refuser de transmettre ces données. La personne peut, alors, former un recours juridictionnel devant la formation spécialisée du Conseil d'État (articles L773-1 et suivants du code de justice administrative et article R841-2 du code de la sécurité intérieure) créée en 2015 (loi n°2015-912 du 24 juillet 2015, articles L773-1 et suivants du code de justice administrative). Il vaut mieux avoir l'assistance d'un·e avocat·e. Le Conseil d'État rejette beaucoup de recours, mais ordonne parfois l'effacement des données (par exemple Conseil d'État, 3 juin 2021, n°428892 concernant le FPR et Conseil d'État, 05/05/2017, 396669, Publié, concernant le fichier de la DRSD, SIREX devenu SIRCID).

2. Application relative à la prévention des atteintes à la sécurité publique (PASP)

Elle est dans le code de la sécurité intérieure (articles R236-11 et suivants). Elle est mise en œuvre par la Direction générale de la police nationale (ministère de l'intérieur).

PASP remplace, avec GIPASP (l'équivalent de PASP, mais côté gendarmerie) et EASP (qui sera vu dans la partie 8 sur les fichiers utilisés dans les enquêtes administratives), le projet EDVIGE et EDVIRSP.

En 2016, 68.000 personnes étaient inscrites dans PASP (Réponse à la question parlementaire n° 79731 du député S. Coronado, JO, 17 mai 2016, p. 4241).

PASP apparaît être un fichier qui peut concerner énormément de monde, et contenir énormément de renseignements et de données personnelles, mis en œuvre et à la disposition de la police nationale.

Comme EASP et GIPASP, PASP a été considérablement élargi par le décret n°2020-1511 du 2 décembre 2020, notamment pour pouvoir ficher les opinions politiques.

2.1 – Données concernées

Depuis sa création, les données concernées par PASP sont très vagues. Le plus simple, c'est de citer : « ***Notamment*** *pour finalité de recueillir, de conserver et d'analyser les informations qui concernent les personnes sus*ceptibles d'être impliquées dans des actions de violence collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives » (R236-11 du code de la sécurité intérieure). Dans cette phrase, l'élément étrange c'est le « notamment » : donc il y a ça, mais aussi tout autre chose. Ça ne s'arrête pas là, puisque dès l'origine ce fichier pouvait rassembler beaucoup d'informations, dont, indirectement, les **« motivations » politiques, religieuses, philosophiques ou syndicales.** Il pouvait aussi contenir les motifs de l'enquête administrative, l'état civil, la nationalité, la profession, les adresses physiques et électroniques, le numéro de téléphone, des photographies et les titres d'identité de la personne.

La réforme de 2020 va toujours plus loin, dans toutes les directions.

Côté fichage politique, dorénavant c'est plus cash : PASP contient des informations sur **les opinions politiques, les convictions philosophiques, religieuses et les appartenances syndicales.** En prime, des **données de santé** apparaissent aussi.

tribunal d'un pays membre de l'Union européenne contre une personne ayant la nationalité d'un autre État membre de l'Union. La base de données de ECRIS n'est pas autonome : elle se compose, en fait, des bases de données des casiers judiciaires des États membres de l'Union européenne (article 3.2 de la décision du Conseil 2009/316/JAI du 6 avril 2009). Elle est opérationnelle depuis avril 2012[73].

ECRIS-TCN (entré en vigueur en juin 2022[74]) est lui un fichier à part entière, qui rassemble toutes les condamnations prononcées par un tribunal d'un pays membre de l'Union européenne contre des ressortissants d'États non membres de l'Union (article 4 du règlement 2019/816 du 17 avril 2019).

ECRIS et ECRIS-TCN permettent donc, par exemple, à un procureur ou à un juge français de savoir si une personne a été condamnée en Allemagne.

Ils sont régis par la décision-cadre 2008/675/JAI du Conseil du 24 juillet 2008, par la décision-cadre 2009/315/JAI du Conseil du 26 février 2009, par la décision-cadre 2009/316/JAI du Conseil du 6 avril 2009 (qui met en place de ECRIS, décision-cadre remplacée à compter du 28 juin 2022 par la directive 2019/884 du Parlement européen et du Conseil du 17 avril 2019), par la décision-cadre 2009/315/JAI et par le règlement européen 2019/816 du 17 avril 2019 (pour le fichage des ressortissants de pays non membres de l'Union européenne).

Le règlement n°2019/216 du 30 janvier 2019 et l'ordonnance n°2022-1524 du 7 décembre 2022 permettent que soient versées **les empreintes digitales** (provenant en France du FAED) dans les casiers judiciaires nationaux. Ainsi, un procureur ou un juge français peut savoir, par exemple, à partir des empreintes digitales d'une personne, si elle a été condamnée en Allemagne.

1.1 – Données concernées

Lorsque la justice d'un État membre de l'Union européenne condamne un ressortissant d'un autre État membre de l'Union européenne, il doit informer les autorités de cet État de cette condamnation (article 4.2 de la décision-cadre 2009/315/JAI du 26 février 2009).

Depuis juin 2022, lorsque la justice d'un État membre de l'Union condamne un ressortissant d'un État tiers, cette condamnation est inscrite dans le fichier ECRIS-TCN (article 5 du règlement 2019/816 du 17 avril 2019).

Les données transmises aux autres États membres de l'Union dans le cadre de ECRIS (condamnation d'un ressortissant européen) et ECRIS-TCN (condamnation d'un ressortissant non européen, article 5.1 du règlement 2019/816 du 17 avril 2019) sont les mêmes que celles du casier judiciaire, qui concerne également les empreintes digitales depuis l'ordonnance n°2022-1524 du 7 décembre 2022.

73 https://www.eulisa.europa.eu/Activities/Large-Scale-It-Systems/Ecris-Tcn

74 Communiqué de presse de la société Soprasteria, https://www.soprasteria.com/docs/librariesprovider2/sopra-steria-corporate/cp/080620_cp-fr_eulisa_vdef.pdf?sfvrsn=c71639dc7 et https://what-europe-does-for-me.eu/fr/portal/2/X07_13401

Partie 10 : Fichiers européens et internationaux

Les données des fichiers nationaux sont partagées avec de nombreux États, en premier lieu les États membres de l'Union européenne. Il est difficile de déterminer avec exactitude ces partages de données : tant au niveau de l'Union européenne que du droit national, les textes sont souvent trop généraux. En-dehors de l'Union européenne, c'est encore plus compliqué : les partages de données sont prévus par de nombreuses conventions internationales.

Nous avons essayé de récapituler ici les principaux systèmes de partages de données dans l'Union européenne (ECRIS et ECRIS-TCN sur les partages de casiers judiciaires, le système d'information Schengen, l'interconnexion de fichiers de police sur la base du traité de Prüm, qui est en passe de devenir un véritable hub européen d'échanges de données génétiques, d'empreintes digitales et de reconnaissance faciale, API-PNR sur les voyages en avion, les fichiers de Europol, et ADEP qui concerne les antécédents enregistrés dans les fichiers de police).

Au niveau de l'Union européenne, un projet du groupe de travail sur l'échange et la protection des données (Working party on Information Exchange and Data Protection, DAPIX) porte sur l'échange automatique de données des fichiers de police (Automation of Data Exchange Process, ADEP). Il semble fonctionner entre la France, l'Allemagne, l'Espagne, l'Irlande et la Finlande[71] ainsi que, peut-être, la Hongrie[72].

Enfin, un projet est en cours de partage automatique des fichiers d'antécédents judiciaires au niveau européen. Pour le moment, cet outil, ADEP (Automation of Data Exchange Process, Décision du Conseil européen du 15 octobre 2012) fonctionne avec l'Allemagne, l'Espagne, l'Irlande et la Finlande, mais c'est difficile de savoir quels fichiers sont concernés – le TAJ l'est très sûrement. Il utilise l'infrastructure d'Europol. Ce projet est basé sur la décision-cadre n°2006/960 du 18 décembre 2006, en particulier son article 5.1.

Concernant les partages de données avec les États hors Union européenne, nous n'abordons que ceux organisés par Interpol.

1. ECRIS / ECRIS-TCN

ECRIS (European Criminal Records Information System, Système européen d'information sur les casiers judiciaires) est une base de données qui rassemble les condamnations pénales prononcées par un

71 Conseil européen, 27 mars 2019, EPRIS-ADEP ADEP Pilot Implementation and Evaluation by MS, Evaluation Report https://www.statewatch.org/media/documents/news/2019/apr/eu-council-epris-adep-final-report-7886-19.pdf

72 Question des parlementaires européens Gérard DEPREZ et Louis MICHEL à la Commission européenne, 31 août 2016 https://www.europarl.europa.eu/doceo/document/E-8-2016-006423_EN.html

Ont aussi été ajoutées en 2020 les personnes pouvant porter atteinte à la sûreté de l'État. Avec un effort de définition : les atteintes à la sûreté de l'État sont celles aux intérêts fondamentaux de la nation ou qui constituent une menace terroriste. Alors là, c'est généraliser un fichage qui, pourtant, apparaissait impossible à élargir encore : les atteintes aux intérêts fondamentaux de la nation désignent, par exemple et en vrac, les mouvements insurrectionnels, les intérêts économiques, industriels et scientifiques majeurs, les atteintes à la forme républicaine des institutions, la reconstitution de groupements dissous, les violences collectives de nature à porter gravement atteinte à la paix publique (dont **l'entrave concertée à la liberté du travail** par des menaces ou des violences, **l'attroupement**, la provocation à l'attroupement, l'organisation d'une manifestation interdite, la dissimulation du visage en manifestation), l'aide à l'entrée et au séjour des étrangers en bande organisée (article L811-3 du code de la sécurité intérieure et décision du Conseil constitutionnel n°2015-713 du 23 juillet 2015), les dégradations en bande organisée… voir la liste complète dans la partie sur le fichier TES.

Toujours concernant les ajouts de 2020, ce fichier concerne dorénavant, en plus des personnes physiques, les personnes morales (sociétés, associations, etc) et les groupements (même informels).

Ont été ajoutés par le décret du 2 décembre 2020 de nombreuses autres informations : les signes physiques particuliers, l'origine géographique (lieux de résidence et zones d'activité), les identifiants utilisés sur internet (sans les mots de passe), les adresses et lieux fréquentés, la situation familiale, la formation, les compétences, la profession, les emplois occupés, les moyens de déplacement (y compris les immatriculations des véhicules), la situation au regard du droit au séjour si la personne est étrangère ou même française (par exemple les interdictions de sortie du territoire), le patrimoine.

Ont été ajoutés également « *les activités susceptibles de porter atteinte à la sécurité ou à la sûreté de l'État* », ce qui rassemble les « *activités publiques ou au sein de groupements ou de personnes morales* », donc la seule participation à un parti politique, une association, ou un groupe informel peut apparaître dans EASP. Cela rassemble aussi le comportement et les habitudes de vie (ça va loin), les déplacements, les activités sur les réseaux sociaux, les pratiques sportives (quel lien entre la pratique du canoë-kayak et la sûreté de l'État ? Vous avez 2 heures), et la pratique et le comportement religieux (tout y passe…).

Ont été ajoutés en 2020 (c'est encore long, accrochez-vous) les « *facteurs de dangerosité* », ce qui rassemble les liens avec des groupes extrémistes, les éléments ou signes de radicalisation, le suivi pour radicalisation, les données relatives à la santé psychologique ou psychiatrique, les armes, la détention d'animaux dangereux, les « *agissements susceptibles de recevoir une qualification pénale* » (ça va donc bien au-delà des condamnations), les antécédents judiciaires, les fiches de recherche (d'où un lien étroit avec le FPR), les suites judiciaires, les mesures d'incarcération, et si la personne a accès à des zones ou des informations sensibles.

Il ne s'agit pas seulement d'évaluer la « dangerosité » d'une personne… mais aussi d'évaluer ses fragilités ! Ainsi, **les facteurs de fragilité familiaux, sociaux et économiques,** le régime de protection (tutelle, curatelle), les faits dont la personne a été **victime**, les comportements auto-agressifs, **les addictions,** et les restrictions de droits (par exemple les interdictions de droits civiques, civils et de famille) sont répertoriés.

Ont aussi été ajoutés, pour l'aspect agrégation de données (la liste qui précède ne semblait pas suffire), l'indication de l'inscription de la personne, ou non, au TAJ, dans N-SIS II, dans PASP, dans GIPASP, dans le FPR, dans le FSPRT, et au FOVeS.

PASP contient également des informations relatives **aux enfants, aux parents et aux proches de la personne concernée.**

Enfin, la réforme de 2020 a supprimé l'interdiction de la reconnaissance faciale à partir des photographies contenues dans ce fichier.

Il concerne tout le monde à partir de 13 ans.

De nombreux services de police et de gendarmerie peuvent avoir accès à ce fichier, incluant tous les services de renseignement, y compris ceux des préfectures, ainsi que tous les policiers et les gendarmes (qui doivent formuler une demande motivée pour avoir accès aux renseignements). En 2020 ont été ajoutés les procureurs de la République (article R236-16).

2.2 – Durée de conservation des données

10 ans maximum à partir « du dernier événement de nature à faire apparaître un risque d'atteinte à la sécurité publique ayant donné lieu à un enregistrement » (article R236-14) – les enquêteurs peuvent donc prolonger ce fichage aussi longtemps qu'il leur plaira.

Pour les mineurs, c'est une durée de 3 ans (article R236-15).

2.3 – Droit d'accès

C'est comme pour EASP et GIPASP :

Pour l'accès, la rectification et l'effacement des données relatives à la sûreté de l'État et à la défense, il faut s'adresser à la CNIL (article 118 de la loi du 6 janvier 1978). Le principe de cet article 118 est que lorsque quelqu'un demande à avoir accès à ses données, celles-ci lui sont transmises si cette communication ne met pas en cause les finalités du fichier, la sûreté de l'État, la défense ou la sécurité publique. Autant dire que c'est open bar pour la CNIL pour refuser cette communication. En 2023, la CNIL répond dans un délai de 15 mois environ.

Quand la CNIL refuse de transmettre ces données, la procédure prévue à l'article 118 est tout à fait étonnante : la CNIL indique à la personne « qu'il a été procédé aux vérifications nécessaires et de son droit de

17.3 – Droits d'accès, de rectification et d'effacement

Concernant les données intéressant la sûreté de l'État, il faut s'adresser à la CNIL. Pour les autres données, il faut s'adresser à la direction générale de la gendarmerie nationale.

16. EDVIGE et EDVIRSP

EDVIGE (Exploitation Documentaire et Valorisation de l'Information Générale) a été créé par le décret n°2008-632 du 27 juin 2008 et supprimé par le décret n°2008-1199 du 19 novembre 2008. EDVIGE a été remplacé par EDVIRSP (Exploitation documentaire des valorisation de l'information relative à la sécurité publique), qui a été abandonné au profit des fichiers PASP, EASP, GIPASP.

17. Traitement d'optimisation des données et informations d'intérêt nucléaire

Ce fichier très récent vise à la prévention des atteintes à la sécurité nucléaire. Il a été créé par décret n° 2024-323 du 8 avril 2024, après avis de la CNIL et consultation du Conseil d'État. À côté du contrôle de l'accès aux sites nucléaires et de la délivrance d'habilitations, ce fichier étonne surtout par sa finalité de « collecte et [d']analyse des informations relatives aux personnes impliquées dans des évènements révélant un risque d'atteinte à la sécurité nucléaire », autant dire le fichage de personnes écologistes par exemple.

17.1 – Données concernées

L'ampleur des données enregistrées permet d'établir un portrait précis des personnes représentant un risque potentiel : nom, prénom, surnom, sexe, date et lieu de naissance, nationalité, signes physiques particuliers, photographies, info sur les documents d'identité, origine géographique (lieux de résidence et zone d'activité), coordonnées (téléphoniques, postales, électroniques, identifiants, pseudo en ligne), situation familiale, professionnelle (y compris passée), « formation et compétences », moyens de déplacements, situation de séjour, type d'événements auxquels on a pris part (catégorie, lieu, date, faits, photo) et **facteurs de dangerosité** (« lien avec des groupes extrémistes », « éléments ou signes de radicalisation », données sur la santé mentale, détention d'armes ou d'animaux, formation au maniement d'armes ou d'explosifs). Mais aussi données sur la vie sexuelle ou l'orientation sexuelle (article 5).

En plus, ce fichier recense si on est fiché à PASP, GIPASP, au FPR, FOVES, FSPRT…

Les données enregistrées pour les demandes d'habilitation sont aussi extrêmement extensives (voir article 4 du décret).

Y ont accès : DGSI, direction du renseignement de la sécurité de la défense, DGSE, direction du renseignement de la préfecture de police de Paris, direction du renseignement territorial...

17.2 – Durée de conservation (art.6)

- maximum 5 ans après le dernier événement qui a donné lieu à un enregistrement
- maximum 5 ans pour les demandes d'autorisation d'accès
- un an après la fin de l'habilitation, ou un an après le refus d'habilitation

former un recours juridictionnel ». Donc, la personne qui ne connaît même pas les données contenues dans le fichier, peut dire à la CNIL de les rectifier (comment savoir ce qu'il y aurait à rectifier?) ou de les effacer (comment savoir ce qu'il y aurait à effacer?)… La personne peut, alors, former un recours juridictionnel devant la formation spécialisée du Conseil d'État (article R841-2 du code de la sécurité intérieure) créée en 2015 (loi n°2015-912 du 24 juillet 2015, articles L773-1 et suivants du code de justice administrative). Celle-ci rejette beaucoup de recours, mais il ordonne parfois l'effacement de certaines données (par exemple pour le fichier SIREX, devenu SIRCID, de la DRSD, Conseil d'État, 05/05/2017, 396669, Publié).

3. Gestion de l'information et la prévention des atteintes à la sécurité publique (GIPASP)

Il a été créé en 2011 (décret n°2011-340 du 29 mars 2011) et est aujourd'hui aux articles R236-21 et suivants du code de la sécurité intérieure.

Il est mis en œuvre par la Direction générale de la gendarmerie nationale (ministère de l'intérieur). Il s'agit de l'équivalent gendarmerie du fichier vu juste avant (PASP), donc les informations sont sensiblement les mêmes. Pour y accéder, l'application mise en œuvre est la Base de Données de Sécurité Publique (BDSP).

En 2015, 13.000 personnes étaient fichées dans GIPASP (*Réponse à la question parlementaire n° 79733 du député S. Coronado, JO, 29 mai 2015, p. 7483*).

GIPASP apparaît être un fichier qui peut concerner beaucoup de monde, et contenir énormément de renseignements et de données personnelles, mis en œuvre et à la disposition de la gendarmerie nationale.

Le système GIPASP-BDSP remplace ATHEN@, qui avait lui-même regroupé ARAMIS et le Fichier alphabétique de renseignement de la gendarmerie (FAR).

Comme EASP et PASP, GIPASP a été considérablement élargi par le décret n°2020-1512 du 2 décembre 2020, notamment pour pouvoir ficher les opinions politiques.

3.1 – Données concernées

Ce sont les mêmes que pour PASP. Les modifications ont été les mêmes en 2020, avec en particulier l**e fichage des opinions politiques, des convictions philosophiques et religieuses et l'appartenance syndicale, et l'autorisation de la reconnaissance faciale.**

Comme PASP, GIPASP concerne toute personne à partir de 13 ans.

3.2 – Durée de conservation des données

Les données sont conservées 10 ans maximum à partir « *du dernier événement de nature à faire apparaître un risque d'atteinte à la sécurité publique ayant donné lieu à un enregistrement.* » (article R236-24) – les enquêteurs peuvent donc prolonger ce fichage aussi longtemps qu'il leur plaira.

Lorsque la personne concernée est mineure, cette durée est de 3 ans.

3.3 – Droit d'accès

C'est comme pour EASP et PASP :

Pour l'accès, la rectification et l'effacement des données relatives à la sûreté de l'État et à la défense, il faut s'adresser à la CNIL (article 118 de la loi du 6 janvier 1978). Le principe de cet article 118 est que lorsque quelqu'un demande à avoir accès à ses données, celles-ci lui sont transmises si cette communication ne met pas en cause les finalités du fichier, la sûreté de l'État, la défense ou la sécurité publique. Autant dire que c'est open bar pour la CNIL pour refuser cette communication. En 2023, la CNIL répond dans un délai de 15 mois environ.

Quand la CNIL refuse de transmettre ces données, elle indique « qu'un magistrat a procédé aux vérifications nécessaires. Toutefois, elles ne permettent pas de vous apporter de plus amples informations (…). En effet (…) toute opposition de l'administration gestionnaire d'un fichier relevant de l'exercice des droits indirect fait obstacle à la moindre communication de la CNIL». Donc, la personne qui ne connaît même pas les données contenues dans le fichier, peut dire à la CNIL de les rectifier (comment savoir ce qu'il y aurait à rectifier?) ou de les effacer (comment savoir ce qu'il y aurait à effacer?)… La personne peut, alors, former un recours juridictionnel devant la Formation spécialisée du Conseil d'État (article R841-2 du code de la sécurité intérieure) créée en 2015 (loi n°2015-912 du 24 juillet 2015, articles L773-1 et suivants du code de justice administrative). Celle-ci rejette beaucoup de recours, mais elle ordonne parfois l'effacement de certaines données (par exemple pour le fichier SIREX, devenu SIRCID, de la DRSD : Conseil d'État, 05/05/2017, 396669, Publié).

4. Conservation, gestion et exploitation électroniques des documents du renseignement territorial

Il a été créé en 2016 (décret n°2016-1045 du 29 juillet 2016) et apparaît aux articles R236-46 et suivants du code de la sécurité intérieure. Il est mis en œuvre par la Direction générale de la police nationale et préfecture de police (ministère de l'intérieur).

4.1 – Données concernées

Il concerne toutes les données collectées par la direction centrale de la sécurité publique et par la direction du renseignement de la préfecture de police. : « Les documents élaborés et collectés, dans l'exercice de leurs missions de renseignement territorial, par les services relevant du service central du renseignement

Le droit d'accès et de rectification indirect à SIRCID s'effectue via la CNIL, puis la contestation se fait devant la Formation spécialisée du Conseil d'État (article R841-2 du code de la sécurité intérieure, articles L773-1 et suivants du code de justice administrative).

Quand il s'appelait encore SIREX, ce fichier a fait l'objet de nombreux recours devant cette formation spécialisée du Conseil d'État, notamment 5 décisions rendues le 19 octobre 2016, et surtout une décision du 5 mai 2017 (n°396669, Publié) qui a fait un peu de bruit : pour la première fois, cette formation spéciale du Conseil d'État a ordonné la suppression des données contenues dans un fichier secret – le SIREX donc.

13. BCR-DNRED

BCR-DNRED a été créé en 2016 (décret non publié n°2016-725 du 1er juin 2016), après avis de la CNIL (n°2016-010 du 21 janvier 2016) non publié.

Le fichier est mis en œuvre par la Direction Nationale du Renseignement et des Enquêtes Douanières (ministère des Finances).

La CNIL ne peut pas avoir accès aux locaux dans lesquels ce fichier est mis en œuvre (articles 1 et 3 du décret n°2007-914 du 15 mai 2007).

Il est peut-être utilisé pour les trafics internationaux illicites d'argent et de biens.

Le droit d'accès et de rectification indirect s'effectue via la CNIL, puis la contestation se fait devant la formation spécialisée du Conseil d'État (article R841-2 du code de la sécurité intérieure, articles L773-1 et suivants du code de justice administrative).

14. RINC (Recueil d'informations numériques aux fins de cyber-défense)

Il a été créé par le décret n°2022-1631 du 21 décembre 2022, non publié, après avis de la CNIL du 10 novembre 2022, qui n'a pas été publié non plus.

Le fichier est mis en œuvre par l'état-major des armées.

Le droit d'accès et de rectification indirect s'effectue via la CNIL, puis la contestation se fait devant la Formation spécialisée du Conseil d'État (article R841-2 du code de la sécurité intérieure, articles L773-1 et suivants du code de justice administrative).

15. ATHEN@

Il a été créé en 2002 (arrêté du 17 septembre 2002), il a eu vocation à remplacer ARAMIS et le Fichier alphabétique de renseignement de la gendarmerie (FAR). Finalement, c'est le système GIPASP/BDSP qui a pris la place d'ATHEN@, d'ARAMIS et du FAR.

La CNIL ne peut pas avoir accès aux locaux dans lesquels ce fichier est mis en œuvre (articles 1 et 3 du décret n°2007-914 du 15 mai 2007).

Le droit d'accès et de rectification s'exerce de manière indirecte via la CNIL (article 118 de la loi n°78-17 du 6 janvier 1978), puis la contestation se fait devant la Formation spécialisée du Conseil d'État (article R841-2 du code de la sécurité intérieure, articles L773-1 et suivants du code de justice administrative).

11. Fichier des personnes étrangères de la Direction du renseignement militaire, remplacé par DOREMI

Ce fichier était mis en œuvre par la Direction du renseignement militaire (ministère des armées) et a été remplacé par le fichier DOREMI par le décret n°2018-1287 du 27 décembre 2018.

Le droit d'accès et de rectification indirect s'effectuait via la CNIL, puis la contestation se fait devant la Formation spécialisée du Conseil d'État (article R841-2 du code de la sécurité intérieure, articles L773-1 et suivants du code de justice administrative).

12. SIRCID, qui a remplacé SIREX

Le décret n°2022-1243 du 16 septembre 2022 a remplacé SIREX par SIRCID. Il est mis en œuvre par la direction du renseignement et de la sécurité de la défense (DRSD, ministère des armées). Le 10 avril 2020, le général Eric BUCQUET, patron de la DRSD, déclarait que SIRCID était en cours de développement en partenariat avec AIRBUS et le décrivait comme « *une base de données dédiées à la contre-ingérence* » (le contre-espionnage[70]).

SIREX a été créé en 2014 par un décret non publié, on connaît son existence par le décret n°2014-957 du 20 août 2014 qui ajoute ce fichier à la liste des fichiers qui échappent au contrôle de la CNIL. L'avis de la CNIL (n°2014-142 du 17 avril 2014) n'est pas publié non plus.

La CNIL ne peut pas avoir accès aux locaux dans lesquels ce fichier est mis en œuvre (articles 1 et 3 du décret n°2007-914 du 15 mai 2007).

Tout ce qu'on sait, c'est que la Direction du renseignement et de la sécurité de la défense a pour mission de protéger les militaires et les installations militaires.

Il est consulté lors d'une recherche sur le fichier ACCReD (qui permet de consulter une douzaine de fichiers quand une personne postule à un emploi considéré comme sensible).

70 https://www.challenges.fr/entreprise/defense/le-cyberespionnage-en-progression-constante-est-sans-doute-le-mode-d-action-le-plus-redoutable_705544

territorial de la direction centrale de la sécurité publique et par la direction du renseignement de la préfecture de police » (article R236-46).

Le fichier peut contenir les activités politiques, philosophiques, religieuses et syndicales.

4.2 – Durée de conservation des données

Les données sont conservées 20 ans.

4.3 – Droits d'accès et de rectification indirects

En application des articles 118 et suivants de la loi n°78-17 du 6 janvier 1978 et l'article R236-51 du code de la sécurité intérieure, ces droits s'exercent auprès de la CNIL. Comme pour les données intéressant la sûreté de l'État contenues dans le FPR, dans EASP, PASP et GIPASP, les données ne sont transmises seulement si cette communication ne met pas en cause les finalités du fichier, la sûreté de l'État, la défense ou la sécurité publique. En cas de refus de transmission des données, la CNIL indique à la personne « qu'il a été procédé aux vérifications nécessaires et de son droit de former un recours juridictionnel ». Donc, la personne qui ne connaît même pas les données contenues dans le fichier, peut dire à la CNIL de les rectifier (comment savoir ce qu'il y aurait à rectifier?) ou de les effacer (comment savoir ce qu'il y aurait à effacer?)… La personne peut, alors, former un recours juridictionnel devant la formation spécialisée du Conseil d'État.

5. Fichier alphabétique de renseignement de la gendarmerie (FAR)

Supprimé en 2010, remplacé par ATHEN@ puis par le système GIPASP/BDSP.

6. ARAMIS

Supprimé et remplacé par ATHEN@ puis par le système GIPASP/BDSP.

Partie 6 : Fichiers de police : Images et sons captés sur le terrain

La loi n°2016-731 du 3 juin 2016 contre le crime organisé et le terrorisme, présentée par Jean-Jacques Urvoas, ministre de la justice du gouvernement d'Emmanuel Valls, a été la première à permettre le port par les policiers, les gendarmes et les policiers municipaux de caméras individuelles. La loi « sécurité globale » du 25 mai 2021 a élargi leur utilisation et a permis leur transmission en temps réel au poste de commandement.

Après une censure du Conseil constitutionnel de certaines dispositions de la première loi dite Sécurité globale portant sur les caméras embarquées sur des drones, des hélicoptères et des véhicules[48], la deuxième loi sécurité globale du 24 janvier 2022 a finalement ouvert la voie à ce type de captation d'images.

On observe deux phénomènes d'entrée dans le droit de dispositifs de surveillance vidéo : l'expérimentation sauvage (par exemple par drones policiers ou par hélicoptère[49]) et le lancement de phases d'expérimentation légales (par exemple les caméras piétons pour les contrôleurs). Ces dernières tentatives sont présentées comme une avancée au service des citoyens, alors même qu'ils renforcent les pouvoirs de ceux qui les utilisent. C'est la même rengaine de l'expérimentation qui a été utilisée pour imposer la vidéosurveillance algorithmique dans l'espace public pour les JO 2024[50].

1. Caméras et micros individuels

Les caméras et les micros individuels sont prévus pour les policiers, les gendarmes (article L241-1 du code de la sécurité intérieure), les policiers municipaux (article L241-2) et les agents de la SUGE (SNCF) et de la sécurité de la RATP (article L2251-4-1 du code des transports). Ces derniers n'ont toutefois pas le droit d'enregistrer hors du réseau (stations/gares et transports en commun).

Les derniers à avoir obtenu l'autorisation de porter une caméra et un micro individuel sont les sapeurs-pompiers et les marins-pompiers (loi n°2021-1520 du 25 novembre 2021, article L241-3 du code de la sécurité intérieure), Et puis il y a une série d'expérimentations en cours (ou terminées) pour différents corps de métier :

- les gardes champêtres (article 46 de la loi du 25 mai 2021 et décret n°2022-1235 du 16 septembre 2022). L'expérimentation s'achèvera le 24 novembre 2024. Notons que le maire peut avoir accès aux images (article 6 du décret du 16 septembre 2022).

48 décision 2021-817 du 20 mai 2021, paragraphes 129 et suivants, et 142 et suivants
49 https://www.laquadrature.net/2021/03/05/la-police-en-helicoptere-ou-la-surveillance-militaire-des-citoyens/
50 Voir le combat de la Quadrature du Net à ce sujet : https://www.laquadrature.net/2023/03/23/la-france-premier-pays-deurope-a-legaliser-la-surveillance-biometrique/

7. BIOPEX

BIOPEX a été créé en 2017 (décret n°2017-1231 du 4 août 2017, non publié) et dépend du ministère des armées. L'avis de la CNIL n°2017-216 du 13 juillet 2017 n'est pas non plus publié. Le décret n°2022-769 du 29 avril 2022 précise qu'il est mis en œuvre par la direction du renseignement militaire.

La CNIL ne peut pas avoir accès aux locaux dans lesquels ce fichier est mis en œuvre (articles 1 et 3 du décret n°2007-914 du 15 mai 2007).

Le droit d'accès et de rectification indirect s'effectue via la CNIL (article 118 de la loi n°78-17 du 6 janvier 1978), puis la contestation se fait devant la formation spécialisée du Conseil d'État (article R841-2 du code de la sécurité intérieure, articles L773-1 et suivants du code de justice administrative).

8. TREX (ancien Fichier d'informations nominatives de la DGSE)

Mis en œuvre par la DGSE (ministère des armées), ce fichier est devenu le fichier TREX en application du décret n°2022-769 du 29 avril 2022.

La CNIL ne peut pas avoir accès aux locaux dans lesquels ce fichier est mis en œuvre (articles 1 et 3 du décret n°2007-914 du 15 mai 2007).

Il est consulté lors d'une recherche sur le fichier ACCReD (qui permet de consulter une douzaine de fichiers quand une personne postule à un emploi considéré comme sensible).

Le droit d'accès et de rectification s'exerce de manière indirecte via la CNIL (article 118 de la loi n°78-17 du 6 janvier 1978), puis la contestation se fait devant la Formation spécialisée du Conseil d'État (article R841-2 du code de la sécurité intérieure, articles L773-1 et suivants du code de justice administrative).

9. Fichier du personnel de la DGSE

Mis en œuvre par la DGSE (ministère des armées).

La CNIL ne peut pas avoir accès aux locaux dans lesquels ce fichier est mis en œuvre (articles 1 et 3 du décret n°2007-914 du 15 mai 2007).

Le droit d'accès et de rectification s'exerce de manière indirecte via la CNIL (article 118 de la loi n°78-17 du 6 janvier 1978), puis la contestation se fait devant la Formation spécialisée du Conseil d'État (article R841-2 du code de la sécurité intérieure, articles L773-1 et suivants du code de justice administrative).

10. DOREMI (remplace le fichier de renseignement militaire de la DRM)

Mis en œuvre par la direction du renseignement militaire (ministère des armées).

Les droits d'accès, de rectification et à la limitation des données s'exercent auprès du secrétariat général du comité interministériel de prévention de la délinquance et de la radicalisation, soit par courrier, place Beauvau, 75800 PARIS cedex 08, soit par mail à cipdr-demande-mrzogt@interieur.gouv.fr. L'accès peut être restreint, s'agissant d'un fichier de sécurité publique, et il faut alors se tourner vers la CNIL.

5. Fichier du renseignement pénitentiaire

Le fichier du renseignement pénitentiaire a été créé par le décret n°2023-795 du 18 août 2023, non publié, pris après l'avis n°2023-034 du 6 avril 2023 de la CNIL, non publié. Il remplace le CAR, qui avait été créé par le décret n°2015-1465 du 10 novembre 2015, non publié après l'avis n°2015-128 du 23 avril 2015 de la CNIL non publié. Il est mis en œuvre par la direction de l'administration pénitentiaire et, selon le journal L'ESSOR DE LA GENDARMERIE, il serait géré par le Service national du renseignement pénitentiaire[69].

Le droit d'accès et de rectification indirect s'effectue via la CNIL (article 118 de la loi n°78-17 du 6 janvier 1978), puis la contestation se fait devant la Formation spécialisée du Conseil d'État (article R841-2 du code de la sécurité intérieure, articles L773-1 et suivants du code de justice administrative).

6. ASTREE

ASTREE a été créé en 2017 (décret n°2017-154 du 8 février 2017, non publié tout comme l'avis de la CNIL n°2016-334 du 10 novembre 2016). Il est mis en œuvre par la Direction de la Protection judiciaire de la Jeunesse (PJJ, ministère de la justice). Donc a priori, il ne concerne que des personnes mineures.

Le rapport d'activité de la mission nationale de veille et d'information de la direction de la PJJ pour 2018 indique qu'au 9 mai 2019, 514 mineurs étaient inscrits dans ASTREE. Parmi eux, 115 étaient suivis dans un cadre pénal, 76 suivis dans un cadre civil pour des risques de radicalisation, 114 suivis pour un autre titre par la PJJ en risque de radicalisation, et 215 du fait de la radicalisation de leurs parents (un mineur peut être suivi pour plusieurs motifs différents). Ils étaient 874 en 2016.

Le droit d'accès et de rectification indirect s'effectue via la CNIL (article 118 de la loi n°78-17 du 6 janvier 1978), puis la contestation se fait devant la Formation spécialisée du Conseil d'État (article R841-2 du code de la sécurité intérieure, articles L773-1 et suivants du code de justice administrative).

69 https://lessor.org/societe/comme-une-quinzaine-de-fichiers-mis-en-oeuvre-par

- les surveillants de l'administration pénitentiaire (article 2 de la loi n°2018-697 du 3 août 2018 et décret n°2019-1427 du 23 décembre 2019). L'expérimentation s'est achevée le 5 février 2022. Le dispositif a été pérennisé par l'article L223-20 et suivants du code de l'administration pénitentiaire, mais seulement à partir du 23 novembre 2023. **L'utilisation de caméras piétons par les agents de l'administration pénitentiaire était donc illégale entre le 5 février 2022 et le 23 novembre 2023**. Il n'est toutefois pas certain qu'elle soit devenue légale depuis le 23 novembre 2023 dans la mesure où les décrets d'application n'ont pas été publiés.
- les contrôleurs des transports en commun (article 113 de la loi n° 2019-1428 du 24 décembre 2019 d'orientation des mobilités et article 1er du décret n° 2021-543 du 30 avril 2021) jusqu'au 1er juillet 2024. La loi 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 a repoussé cette date au 1er octobre 2024, et une proposition de loi déposée le 7 février 2024 propose là aussi d'entériner définitivement le dispositif. Cependant, le gouvernement était censé rendre un rapport pour dresser le bilan de l'expérimentation, en l'absence duquel le vote de la loi pourrait capoter.

Les images et les sons captés par les policiers, les gendarmes et les policiers municipaux (pas les gardes champêtres) peuvent être transmis en direct au poste de commandement, et les policiers et gendarmes sur le terrain peuvent avoir accès à leurs propres images (article R241-3 du Code de sécurité intérieure). L'accès aux images captées par les contrôleurs de transports en commun et les agents de la SNCF et la RATP est ouvert aux policiers et gendarmes, aux responsables de sécurité et aux agents individuellement habilités. Pour les contrôleurs, le commandement peut avoir accès aux images en temps réel en cas de danger pour la sécurité.

Les enregistrements captés par les policiers et les gendarmes sont placés sous la responsabilité du ministère de l'intérieur (direction générale de la police nationale, direction générale de la gendarmerie nationale et préfecture de police) ; ceux captés par les policiers municipaux et les garde-champêtres sont placés sous celle du maire.

Côté objectifs de la prise d'images, ce n'est évidemment pas de prouver les violences commises par les forces de l'ordre ou les agents assermentés sur le terrain. Il s'agit plutôt de la « prévention des incidents », le constat des infractions, les preuves, etc. C'est bien sûr pensé pour être au service des forces de l'ordre.

Aucune disposition n'interdisant la reconnaissance faciale, celle-ci peut être utilisée sur ces images.

1.1 – Données concernées

Au-delà des enregistrements audiovisuels, sont enregistrés leur date, leur heure, l'identité de l'agent porteur de la caméra, et le lieu où les données ont été collectées, l'identifiant de la caméra, etc.

1.2 – Durée de conservation des images et des sons

Les données sont conservées un mois depuis la loi n°2022-52 du 24 janvier 2022 (surnommée « sécurité globale II », avant cette durée était de 6 mois). Elles sont conservées plus longtemps dans le cadre d'une procédure judiciaire, administrative ou disciplinaire (articles L241-1, L241-2 du code de la sécurité intérieure, 46 de la loi du 25 mai 2021).

Pour les contrôleurs de transports en commun, la durée de conservation des images et sons est de 6 mois (article 7 du décret n°2021-543 du 30 avril 2021). Idem pour les agents de la SNCF et RATP (article 7 du décret n°2016-1862 du 23 décembre 2016).

Pour les matons, la durée de conservation est de trois mois (L223-20 du code pénitentiaire).

1.3 – Droits d'accès aux images

Concernant les enregistrements captés par les policiers et les gendarmes, l'article R241-6 du code de la sécurité intérieure prévoit qu'il faut s'adresser au responsable du traitement. Il faut donc s'adresser à la Direction générale de la gendarmerie nationale, 4 rue Claude Bernard, CS60003, 92136 ISSY-LES-MOULINEAUX CEDEX, ou à la direction générale de la police nationale, Place Beauvau, 75800 PARIS CEDEX 08, et à la préfecture de police (à Paris et Marseille).

Concernant les enregistrements captés par les policiers municipaux, l'article R241-15 prévoit que les droits d'information, d'accès et d'effacement s'exercent auprès du maire ou de la communauté de communes. En cas de refus, c'est possible d'introduire un recours devant la CNIL.

Concernant les enregistrements captés par les matons, en l'absence de décret d'application, on ne sait pas vraiment, mais on peut tenter d'exercer la même voie de recours que pendant l'expérimentation, c'est à dire s'adresser au directeur de l'établissement pénitentiaire et en cas de refus, à la CNIL (article 8 du décret 2019-1427 du 23 décembre 2019).

2. Images captées par les drones et les hélicoptères

A- En matière de police administrative

En matière de renseignement, il est fréquent que les policiers expérimentent illégalement des dispositifs qui rentrent ensuite dans le droit. Tel est le cas des images captées par les drones qui étaient utilisés illégalement par la police et la gendarmerie durant plusieurs années (par exemple, pour un jugement qui constate l'illégalité : TA Lyon, 30 mars 2022, n°2103092). Deux recours de La Quadrature du Net ont permis de faire constater cette illégalité en mai 2020[51], et à nouveau en décembre 2020[52]. En janvier 2021, la CNIL a forcé le gouvernement à cesser d'utiliser des drones[53]. Le gouvernement a ensuite tenté de légaliser

51 https://www.laquadrature.net/2020/05/18/les-goelands-abattent-leur-premier-drone/
52 https://www.laquadrature.net/2020/12/22/interdiction-des-drones-victoire-totale-contre-le-gouvernement/
53 https://www.cnil.fr/fr/drones-la-cnil-sanctionne-le-ministere-de-linterieur

Les interconnexions avec d'autres fichiers sont très nombreuses. Jusqu'à récemment, il n'y avait pas vraiment d'interconnexions avec les fichiers médicaux : le milieu de la santé tient fort au secret médical. Du coup, le gouvernement a préféré sortir de son chapeau, récemment, un tout nouveau fichier médical, HOPSYWEB : HOPSYWEB a été créé par le décret n°2018-383 du 23 mai 2018 et permet de ficher les personnes faisant l'objet d'une hospitalisation en hôpital psychiatrique sans leur consentement (HO, hospitalisation d'office sur ordre du préfet ou HDT, hospitalisation à la demande d'un tiers, souvent un proche). Le décret n°2019-412 du 6 mai 2019 permet une interconnexion entre HOPSYWEB et le FSPRT. Une habile manière de contourner les blocages autour du secret médical…

Les données sont conservées pendant 5 ans, mais un membre du Conseil de la fonction militaire de la gendarmerie a reconnu que les « *informations ne sont pas perdues ensuite*[66] ».

Le droit d'accès et de rectification indirect s'effectue *via* la CNIL (article 118 de la loi n°78-17 du 6 janvier 1978), puis la contestation se fait devant la formation spécialisée du Conseil d'État (article R841-2 du code de la sécurité intérieure, articles L773-1 et suivants du code de justice administrative).

4. MRZOGT (Mineurs de retour de zones d'opérations de groupements terroristes)

MRZOGT a été créé par le décret n°2023-255 du 6 avril 2023 qui prévoit la surveillance des enfants qui ont, par exemple, été enfermés dans des camps en Syrie (et que la France rechigne à rapatrier concernant les enfants français, raison pour laquelle elle a été condamnée par la CEDH le 14 septembre 2022). Il aurait coûté environ 2 millions d'euros[67].

Les données récoltées sont extrêmement larges : état civil, liens familiaux, situation des parents, prise en charge éducative, sociale, psychologique ou médicale, bilans de santé réalisés, scolarisation, informations et signalements produits par l'autorité scolaire...

Il n'y a pas de limite d'âge pour entrer dans ce fichier : les nouveaux-nés peuvent y figurer. L'effacement se fait d'office à la majorité.

Dix administrations et leurs agents peuvent avoir accès au fichier, et en particulier les ministères de la santé, de l'éducation, de la justice, de l'intérieur, des affaires sociales, de la protection de la jeunesse, et le comité interministériel de prévention de la délinquance et de la radicalisation.

Au cours de l'année 2023, le gouvernement a mis en ligne une jolie brochure, à destination des mineurs fichés, pour leur expliquer ce qu'est MRZOGT[68].

66 Fenech G., Pietrasanta S., 2016, *Rapport d'enquête relative aux moyens mis en œuvre par l'État pour lutter contre le terrorisme depuis le 7 janvier 2015*, Rapport n° 3922, Assemblée nationale, http://www.assemblee-nationale.fr/14/rap-enq/r3922-t1.asp
67 https://www.mediapart.fr/journal/france/180623/fichier-d-enfants-de-retour-de-syrie-meme-le-parquet-antiterroriste-n-en-veut-pas
68 https://www.cipdr.gouv.fr/wp-content/uploads/2024/02/MRZOGT-FALC-BATpdf.pdf

3. Signalements pour la Prévention de la Radicalisation à Caractère Terroriste (FSPRT)

Il a été créé en 2015 (décret n°2015-252 du 4 mars 2015, modifié par le décret du 30 octobre 2015 et par le décret du 2 août 2017, aucun n'a été publié). Les avis de la CNIL ne sont pas publiés non plus (délibération n°2014-499 du 11 décembre 2014, délibération n°2015-342 du 6 octobre 2015, délibération n°2017-155 du 18 mai 2017). Il a été modifié par un décret du 29 novembre 2023, non publié.

Il est mis en œuvre par la Direction Générale de la Sécurité Intérieure (DGSI), qui a repris en décembre 2019 les missions de l'Unité de Coordination de la Lutte Antiterroriste (UCLAT, créé en 1984, qui dépendait de la Direction générale de la police nationale, ministère de l'intérieur), organisme qui gérait initialement le FSPRT. Les personnes fichées considérées comme les plus dangereuses sont suivies directement par la DGSI, les autres par la direction nationale du renseignement territorial.

On ne connaît presque rien du FSPRT. Voilà ce qu'en dit la CNCDH :« *les personnes fichées ne font pas toutes l'objet d'un signalement en raison d'agissements menaçant, directement ou indirectement, la sûreté de l'État mais simplement en raison d'une conduite ou d'un comportement exprimant une conviction politique ou religieuse.* » (Commission Nationale Consultative des Droits de l'Homme, 18 mai 2017, *Avis sur la prévention de la radicalisation*, publié au JORF n°0077 du 1er avril 2018). Le rapport de la commission des lois de l'assemblée nationale du 17 octobre 2018 déclare que plus de 20'000 personnes sont inscrites au FSPRT.

Il est alimenté notamment par le numéro de téléphone de la Plateforme anti-radicalisation (c'est 30 % des personnes fichées), mais aussi par les services de renseignement eux-mêmes (30 à 32 % des personnes fichées) et par d'autres acteurs (Éducation nationale, associations, élus locaux…). Sont aussi systématiquement inscrites au FSPRT les personnes condamnées pour des faits de terrorisme en lien avec l'islam radical[63].

Le rapport du parlement sur l'activité des services de renseignement du 11 avril 2019 annonce que le FSPRT contient 20.867 fiches, dont 11378 « fiches actives » et 9489 « fiches clôturées ».

Au cours de l'automne 2023, Gérald Darmanin, ministre de l'Intérieur, a donné des informations contradictoires sur le nombre de personnes prétendument inscrites au FSPRT : Il disait 8.132 personnes signalées au FSPRT fin août 2023[64], et 20.120 personnes dont à peu près 5.100 faisant l'objet d'un suivi actif le 14 octobre 2023[65]. Des chiffres qui semblent sous-évalués, en particulier concernant les fiches actives.

63 Rapport de la délégation parlementaire au renseignement pour l'année 2019-2020, enregistré à la présidence de l'Assemblée nationale et du Sénat le 11 juin 2020, p, 123

64 https://www.lesechos.fr/politique-societe/societe/cinq-questions-sur-le-fsprt-le-fichier-sur-la-radicalisation-en-france-1243291

65 https://www.publicsenat.fr/actualites/institutions/fiche-s-fpr-fsprt-quels-sont-les-differents-fichiers-de-renseignement-utilises-pour-la-lutte-antiterroriste

l'usage des drones dans la loi sécurité globale, mais ces dispositions ont été censurées par le Conseil constitutionnel le 20 mai 2021[54].

Il n'a pas lâché l'affaire, bien sûr, et a réintroduit les images captées par les drones dans la loi du 24 janvier 2022, surnommée loi sécurité globale II. Il s'agit des articles L242-1 et suivants et R242-1 et suivants du code de la sécurité intérieure.

Sont, depuis, autorisés à procéder à la captation d'images les services de police et de gendarmerie et les militaires opérant sur le territoire national (articles L242-5 I et R242-8).

La captation d'images peut être effectuée pour les objectifs suivants (article L242-5 et R242-8) :

- La prévention des atteintes à la sécurité des personnes et des biens (donc tout et n'importe quoi) dans « *des lieux particulièrement exposés* » en raison des faits qui s'y sont déjà déroulés, ou pour la protection des bâtiments et installations publics,
- La sécurité des rassemblements de personnes sur la voie publique, ou même dans des lieux privés ouverts au public, en vue de permettre de maintenir ou de rétablir l'ordre public lorsque les rassemblements sont susceptibles d'entraîner des troubles graves à l'ordre public (ce qui permet de viser toutes les manifestations par exemple),
- La prévention du terrorisme,
- La régulation des flux de transport pour le maintien de l'ordre et de la sécurité publics,
- La surveillance des frontières,
- Le secours aux personnes.

En principe, le public est informé de l'utilisation des drones ou hélicoptères (article L242-3), et la captation d'images ne peut pas être permanente (article L242-4).

Toujours en principe, il est interdit d'avoir pour objectif de filmer l'intérieur des domiciles et leur entrée… Mais ce qui est interdit c'est l'objectif, donc si l'intérieur des domiciles est filmé « *par hasard* », alors il n'y a pas de problème. Dans ce cas-là, les images doivent être effacées dans un délai de 48 heures (contre 7 jours normalement) (article R242-11).

Le son ne peut pas être enregistré, la **reconnaissance faciale est interdite**, et aucun rapprochement, interconnexion ou mise en relation automatisé avec un autre fichier ne peut être réalisé (article L242-4).

Depuis l'entrée en vigueur, le 19 avril 2023, du décret d'application de la loi donnant la possibilité aux préfets d'autoriser l'utilisation des drones, ceux-ci prennent beaucoup d'arrêtés en ce sens pour surveiller les manifestations. Le Conseil d'État a rejeté en mai 2024 un référé suspension déposé par plusieurs associations contre ce décret.

54 Conseil constitutionnel, décision n°2021-817, 20 mai 2021, paragraphes 129 à 141

De nombreux arrêtés préfectoraux sont contestés auprès des tribunaux, qui donnent parfois raison aux manifestants (voir par exemple : TA Rouen, 30 avril 2023, n°2301728 (restriction du périmètre) ; TA Rouen, 5 mai 2023, n°2301786). Certaines préfectures se font sanctionner pour l'utilisation de drones en l'absence d'arrêté préfectoral le permettant (TA Grenoble, 8 juillet 2023, n°2304323), ou en jugeant que d'autres moyens, moins intrusifs auraient pu être utilisés pour prévenir le franchissement de frontières (TA Pau, 13 juillet 2023, n°2301796). Par contre, le conseil d'État a jugé en décembre 2023 que le survol par drone du marché de Noël de Strasbourg n'était pas disproportionné (12 décembre 2023, n°489923).

2.1 – Durée de conservation des données

Les données sont conservées 7 jours, mais seulement 48 heures si elles ont filmé l'intérieur d'un domicile ou son entrée (sauf transmission dans ce délai d'un signalement à l'autorité judiciaire, voir l'article L242-5 III). Elles sont conservées plus longtemps dans le cadre d'une procédure judiciaire, administrative ou disciplinaire (article L242-4 du CSI).

2.2 – Demandes de consultation et d'effacement des données

Les demandes sont à adresser aux responsables du traitement (article R242-13 IV) donc, suivant les cas, à la direction générale de la police nationale ou à la direction générale de la gendarmerie nationale.

B. En matière de police judiciaire

La captation vidéo par drone avait été autorisée au printemps 2023 en police administrative, c'est-à-dire aux fins de prévention des troubles et de maintien de l'ordre public. Désormais, un décret du 30 décembre 2023 a élargi ces captations à l'usage de la police judiciaire (c'est-à-dire la constatation d'infractions et la poursuite de leurs auteurs). Les articles R40-57 à R40-63 ont été insérés dans le code de procédure pénale.

Les données enregistrées sont les mêmes que pour les captations par drones en police administrative.

Qui y a accès ? Les magistrats, OPJ et sous leur contrôle, les APJ. Mais aussi, accessoirement, les personnes qui ont accès au dossier pénal numérique (greffiers, avocats, parquetiers…) et les experts si besoin.

2.3 – Durée de conservation des données

Les données sont conservées un mois (R40-61) après la captation. En cas d'ouverture d'investigation, les données sont placées sous scellé au maximum un mois après la captation, et leur conservation dure alors jusqu'à la prescription des faits (six ans pour les délits et 10 ans pour les crimes, art. 8 CPP).

1. Fichier de renseignement CRISTINA

Il s'appelle Centralisation du Renseignement Intérieur pour la Sécurité du Territoire et des Intérêts Nationaux et a été créé en 2008 (décret du 27 juin 2008, modifié par le décret du 2 août 2017, non publiés). Il est mis en œuvre par la DGSI (ministère de l'Intérieur), et est issu d'une fusion du fichier de la DST et de données des RG. On ne sait pas grand-chose dessus.

Par l'arrêt n°5149/21 de la Cour européenne des droits de l'Homme du 7 mars 2024, on apprend qu'un agent de la DGSI a perdu son habilitation « secret défense » pour avoir consulté CRISTINA à des fins personnelles – comme quoi la consultation illégale des fichiers par des flics, c'est à tous les étages.

La CNIL ne peut pas contrôler ce fichier (articles 1 et 3 du décret n°2007-914 du 15 mai 2007).

Il est consulté lors d'une recherche sur le fichier ACCReD (qui permet de consulter une douzaine de fichiers quand une personne postule à un emploi considéré comme sensible).

Le droit d'accès et de rectification s'effectue auprès de la CNIL (article 118 de la loi n°78-17 du 6 janvier 1978), puis la contestation se fait devant la formation spécialisée du Conseil d'État (article R841-2 du code de la sécurité intérieure) créée en 2015 (loi n°2015-912 du 24 juillet 2015, articles L773-1 et suivants du code de justice administrative).

2. GESTEREXT (GEStion du TERrorisme et des EXTrémismes à potentialité violente)

Il a été créé en 2008 (arrêté du 27 juin 2008 du Ministre de l'intérieur), et est resté illégal a priori jusqu'en 2017. En 2017, après avis de la CNIL tenu secret (délibération n°2017-157 du 18 mai 2017), un décret, tenu secret aussi (n°2017-1218 du 2 août 2017) « recrée » GESTEREXT.

Il semble que GESTEREXT soit mis en œuvre par la préfecture de police de Paris, selon les déclarations du 6 novembre 2019 de M. Michel DELPUECH, alors préfet de police de Paris, devant la Commission d'enquête de l'Assemblée nationale créée suite à l'attaque dans les locaux de cette préfecture le 3 octobre 2019.

La CNIL ne peut pas avoir accès aux locaux dans lesquels ce fichier est mis en œuvre (articles 1 et 3 du décret n°2007-914 du 15 mai 2007).

Il est consulté lors d'une recherche sur le fichier ACCReD (qui permet de consulter une douzaine de fichiers quand une personne postule à un emploi considéré comme sensible).

Aucune durée de conservation des données n'est prévue, donc les données peuvent être conservées aussi longtemps qu'elle est nécessaire eu égard aux finalités du fichier – on peut difficilement faire plus flou.

Le droit d'accès et de rectification indirect s'effectue via la CNIL (article 118 de la loi n°78-17 du 6 janvier 1978), puis la contestation se fait devant la formation spécialisée du Conseil d'État (article R841-2 du code de la sécurité intérieure, articles L773-1 et suivants du code de justice administrative).

Partie 9 : Fichiers des services de renseignement

Ici, il y a plus de choses, et plus ça va plus les choses sont gardées confidentielles. Ces fichiers sont ceux de la police judiciaire, mais aussi du ministère des armées, de la DGSE, de la DGSI… Ils sont peu voire très peu transparents. Pour certains, on sait à peu près ce qu'il y a dedans et à quoi ils servent, parce que les textes (décrets, arrêtés) qui les ont créés sont publics. Mais même ceux-là, quand on demande à savoir ce qu'il y a dedans qui nous concerne directement, on a rarement une réponse (ça n'empêche pas de demander…). Pour d'autres, on ne sait rien ou presque, tous les textes sont confidentiels, on sait juste qu'ils existent. Dans tous les cas, c'est pas interdit de demander à la CNIL quelles infos ces fichiers ont sur nous.

Ces fichiers servent donc aux services de renseignement. Normalement, ils ne peuvent pas être utilisés en justice, contre des personnes : en principe donc, ils peuvent servir à savoir qu'untel ou unetelle a fait ça, mais ne peuvent pas servir à le prouver face à un juge – les flics devront donc trouver d'autres preuves. Sauf que, pas de chance, les juges ont tendance à être plus conciliants envers les flics et à accepter les preuves venues de ces fichiers : ce sont les « notes blanches ». Donc, des notes qui viennent de fichiers dont on sait à peine qu'ils existent, en tout cas pas lesquels, ni à quoi ils servent, ni ce qu'ils ont sur nous. Bienvenue dans le joyeux monde de la paranoïa. Sauf, quand même, que c'est pas souvent qu'ils sont utilisés.

Et les services de renseignement, ce sont d'une part ceux du ministère des Armées (avec notamment la DGSE), d'autre part ceux du ministère de l'Intérieur. Côté ministère de l'Intérieur, il s'agit de la DGSI et de la direction nationale du renseignement territorial (créée en 2023, dans le cadre de la réorganisation de la police nationale[62]). Avant, c'était le SCRT (ex-RG-DST, qui sont devenus en 2008 les DCRI et SDIG, qui sont devenus en 2014 la DGSI et le SCRT).

La DNRT (direction nationale du renseignement territorial) exerce nationalement, sauf à Paris, en Seine-Saint-Denis, dans le Val-de-Marne et dans les Hauts-de-Seine (pré carré de la Préfecture de police de Paris). La DNRT est rattachée à la direction générale de la police nationale (DGPN). La DNRT se voit désignée comme tête de file de la prévention des extrémismes violents, avec environ 3100 agents. Elle fait partie des agences de deuxième cercle du renseignement et travaille sur les questions relatives à l'indépendance nationale, la prévention du terrorisme, la prévention des atteintes à la forme républicaine des institutions, la prévention des actions tendant au maintien ou à la reconstitution de groupements violents, la prévention des violences collectives de nature à porter gravement atteinte à la paix publique, la prévention de la criminalité et de la délinquance organisées.

62 Voir le décret n° 2023-530 du 29 juin 2023 relatif à l'organisation de l'administration centrale de la police nationale et modifiant diverses dispositions relatives à la police nationale

2.4 – Demandes de consultation et d'effacement des données

Il peut être intéressant de savoir que toute opération de consultation, transfert, ou modification est enregistrée, avec identification de l'auteur, pendant 3 ans (R40-62).

Après le délai d'un mois de conservation, les règles pour demander l'effacement ou la consultation de données nous concernant sont les mêmes que pour un dossier pénal.

3. Images captées par les caméras embarquées sur les véhicules de police et de gendarmerie

L'enregistrement d'images au moyen de caméras embarquées a été légalisé par la loi sécurité globale II (n°2022-52 du 24 janvier 2022) pour les agents de la police nationale, de la gendarmerie, des douanes, des sapeurs-pompiers et les missions de sécurité civile, dans leurs missions de prévention d'atteinte à l'ordre public et de protection des personnes (le cadre est donc très large), lorsqu'un incident est susceptible de se produire. Les dispositions permettant l'enregistrement de ces images sont aujourd'hui aux articles L243-1 et suivants du code de la sécurité intérieure.

L'enregistrement ne peut être permanent, et les véhicules sont censés porter une signalétique informant de ce dispositif, sauf... pour les voitures banalisées. Le commandement et les agents sur le terrain peuvent avoir accès en temps réel aux images.

La reconnaissance faciale et la connexion avec d'autres traitements de données sont interdits (article L243-3 du code de la sécurité intérieure).

L'article L243-4 du même code prévoit que le délai de conservation est de 7 jours après l'intervention, sous la responsabilité du chef de service, et plus en cas de procédure judiciaire, administrative ou disciplinaire. Ce délai est ramené à 48 H lorsqu'il s'agit d'images d'entrées ou d'intérieur de domicile (sauf transmission à l'autorité judiciaire pour signalement).

Toutefois, le décret précisant les modalités d'application de cette loi n'est pas paru, ainsi il semble que, si des véhicules sont déjà équipés et les caméras utilisées, les enregistrements sont illégaux.

4. Images captées par les Cellules image ordre public de la gendarmerie mobile (CIOP)

Il est très courant de voir, notamment en manifestation, des gendarmes mobiles équipés de petits caméscopes en train de filmer ostensiblement ce qu'il se passe, y compris les contrôles d'identité. Nous n'avons pas trouvé le fondement légal qui permet cette prise d'images et la conservation de ces images mais plusieurs sources, et en particulier la circulaire n°200000/GEND/DOE/S2DOP/BOP du 22 juillet 2011 *relative à l'organisation et à l'emploi des unités de la gendarmerie mobile* et l'instruction n°200000/GEND/DOE/SDEF/BSOP du 26 juillet 2022 *relative à la gestion de l'ordre public par les unités de la gendarmerie nationale* indiquent qu'elles sont prises par les « Cellules image ordre public ».

Le but de la prise d'images est leur utilisation à des fins judiciaires (rassemblement de preuves, identification des auteurs), de défendre les militaires en cas de plainte contre eux, et de dissuader en faisant en sorte que cet enregistrement soit ostensible, à la vue de tou·tes.

Toutefois, en l'absence de texte autorisant la captation des images et leur conservation et organisant les personnes y ayant accès et les conditions dans lesquelles elles peuvent être transmises dans des procédures ainsi que celles dans lesquelles les personnes concernées peuvent exercer leurs droits, il apparaît qu'elles sont illégales (à part si, comme cela est théoriquement le cas pour la CNOEIL, l'utilisation des CIOP est, à chaque fois, autorisée par le préfet en amont de la manifestation, et que celui-ci organise le traitement des images).

5. Images captées par la Cellule nationale d'observation et d'exploitation de l'imagerie légale (CNOEIL) de la gendarmerie mobile

La gendarmerie mobile comporte aussi, au niveau national, une cellule chargée de la captation et de l'exploitation d'images, la CNOEIL (voir en particulier l'instruction n°200000/GEND/DOE/SDEF/BSOP du 26 juillet 2022 *relative à la gestion de l'ordre public par les unités de la gendarmerie nationale*).

Elle est intervenue, par exemple, pendant les manifestations des Gilets jaunes, à Notre-Dame-des-Landes ou pendant le Grand prix de France de Formule 1 le 23 juin 2019.

Elle est équipée de deux camionnettes Renault Master équipées de mâts télescopiques pouvant atteindre 6,50 mètres de haut et d'un drone, et peut installer un mini-réseau de caméras fixes, en filaire ou en wifi[55].

Il ne semble pas exister de texte autorisant, de manière générale, l'utilisation de ces moyens. Elle semble toutefois permise au coup par coup par les préfets (voir par exemple l'arrêté du préfet du Var du 19 juin 2019), ce qui signifie qu'en l'absence d'une telle autorisation, les images captées le seraient illégalement.

6. Système SARISE (Système autonome de retranscription d'images pour la sécurisation d'événements) de la gendarmerie nationale

Il s'agit ici d'un système de vidéosurveillance que le gendarmerie nationale peut installer pour surveiller une manifestation ou un événement particulier.

Encore une fois, nous n'avons pas trouvé de base légale pour la captation et l'enregistrement des images, ce qui signifie que ce système est potentiellement illégal.

55 https://www.gendarmerie.interieur.gouv.fr/gendinfo/dossiers/la-gm-d-hier-et-de-demain/gbgm-des-cellules-et-des-moyens-speciaux-au-service-du-maintien-de-l-ordre

Pour l'accès, la rectification et l'effacement des données relatives à la sûreté de l'État et à la défense, il faut s'adresser à la CNIL (article 118 de la loi du 6 janvier 1978). Le principe de cet article 118 est que lorsque quelqu'un demande à avoir accès à ses données, celles-ci lui sont transmises si cette communication ne met pas en cause les finalités du fichier, la sûreté de l'État, la défense ou la sécurité publique. Autant dire que c'est open bar pour la CNIL pour refuser cette communication. En 2023, le délai de réponse de la CNIL est de… 15 mois environ !!

Quand la CNIL refuse de transmettre ces données (quasi systématiquement en réalité), la procédure prévue à l'article 118 est tout à fait étonnante : la CNIL indique à la personne « *qu'il a été procédé aux vérifications nécessaires et de son droit de former un recours juridictionnel* ». Donc, la personne qui ne connaît même pas les données contenues dans le fichier, peut dire à la CNIL de les rectifier (comment savoir ce qu'il y aurait à rectifier?) ou de les effacer (comment savoir ce qu'il y aurait à effacer?)… La personne peut, alors, former un recours juridictionnel devant la Formation spécialisée du Conseil d'État (article R841-2 du code de la sécurité intérieure) créée en 2015 (loi n°2015-912 du 24 juillet 2015, articles L773-1 et suivants du code de justice administrative). Celle-ci rejette beaucoup de recours, mais il ordonne parfois l'effacement de certaines données (par exemple pour le fichier SIREX, devenu SIRCID, de la DRSD : Conseil d'État, 05/05/2017, 396669, Publié).

curatelle), les faits dont la personne a été victime, les comportements auto-agressifs, les addictions, et les restrictions de droits (par exemple les interdictions de droits civiques, civils et de famille) sont répertoriés.

Ont aussi été ajoutés, pour l'aspect agrégation de données (la liste qui précède ne semblait pas suffire), l'indication de l'inscription de la personne, ou non, au TAJ, dans N-SIS II, dans PASP, dans GIPASP, dans le FPR, dans le FSPRT, et au FOVeS.

Ah, après toute cette liste, l'article R236-2 du code de la sécurité intérieure précise, tout à la fin, que « *le traitement ne comporte pas de dispositif de reconnaissance faciale à partir de la photographie* ». On dirait que c'est pour rassurer. Mais on remarque ce petit complément : « ***à partir de la photographie*** », et on peut légitimement se demander à partir de quoi d'autre ils pourraient faire tourner un logiciel de reconnaissance faciale, si ce n'est la photographie… et oui ! Bien sûr ! Les papiers d'identité… A priori, donc, la reconnaissance faciale serait possible, non à partir de la photographie contenue dans le fichier, mais à partir de la photographie qui est sur un papier d'identité qui est contenu dans le fichier. C'est tordu, on ne sait pas vraiment ce qu'il en est en réalité.

Il concerne toute personne qui a postulé, âgée d'au moins 16 ans.

Jusqu'à la réforme de 2020, la personne était censée être informée que les informations qu'elle donne entrent dans le fichier (article R236-9 du code de la sécurité intérieure issu du décret n°2013-1113 du 4 décembre 2013). **Cette information a été supprimée par le décret n°2020-1510 du 2 décembre 2020.** Le fait de ne pas donner cette information semble avoir été adopté en application de l'article 116 de la loi n°78-17 du 6 janvier 1978 pour ce qui concerne les données intéressant la sûreté de l'État et de la défense nationale. Pour ce qui concerne les autres données (relatives à la prévention et à la détection des infractions pénales, aux enquêtes, aux poursuites, et à l'exécution des sanctions pénales), il semble que les articles 104 et suivants de la loi du 6 janvier 1978 ne prévoient pas, de toute manière, une information de la personne lorsque ses données font l'objet d'un traitement automatique.

2.2 – Durée de conservation

Les données sont conservées 5 ans (article R236-4).

2.3 – Droit d'accès, de rectification et d'effacement

L'article R236-9 du code de la sécurité intérieure organise le droit d'accès, de rectification et d'effacement des données contenues dans EASP. Comme pour le FPR et ACCReD (par exemple), deux types de données sont présentes dans EASP, des données relatives à la prévention et à la détection des infractions pénales, et des données relatives à la sûreté de l'État et à la défense. Par conséquent, deux procédures doivent être menées en même temps pour l'exercice des droits d'accès, de rectification et d'effacement.

Il pourrait être autorisé au coup par coup par les préfets, mais nous n'avons pas trouvé de traces d'arrêtés préfectoraux en ce sens (par exemple pour son utilisation à Nantes pendant une manifestation des Gilets jaunes le 14 septembre 2019[56] ou pendant la feria de Dax le 20 août 2015).

7. Caméras et micros fixés sur les Taser et LBD

Depuis que les Taser ont été introduits dans l'armement des forces de l'ordre en 2006, ils sont équipés d'une caméra et d'un micro. Ils se déclenchent lorsque l'arme est allumée (avant le tir donc)[57].

Nous n'avons pas trouvé de dispositions faisant état de l'existence de ces enregistrements dans la réglementation relative aux armes portées par la police nationale et par la gendarmerie. Pour accéder aux enregistrements (ou demander à ce qu'ils soient versés dans une procédure pénale), ça devrait être possible de s'adresser à la direction générale de la police nationale, à la direction générale de la gendarmerie nationale et à la CNIL.

Le décret n°2022-1409 du 7 novembre 2022 modifie les modalités de prise d'images pour la police municipale : l'enregistrement visuel et sonore est effectué soit par déclenchement automatique intégré à l'arme soit par la caméra individuelle dont est porteur le tireur.

Concernant la police municipale, l'article R511-12 du code de la sécurité intérieure et l'arrêté du 26 mai 2010 autorisent ses membres à utiliser le Taser. L'article R511-28 du code de la sécurité intérieure mentionne l'existence des enregistrements sonores et vidéos et, depuis sa modification par le décret n°2022-1409 du 7 novembre 2022, l'enregistrement est obligatoire en cas d'usage d'un taser ou d'un LBD par la police municipale. Nous n'avons pas trouvé de dispositions relatives au traitement de ces images. Pour accéder à l'enregistrement, il semble nécessaire de s'adresser au maire de la commune, et à la CNIL dans le même temps.

Concernant le LBD, il est parfois fait mention de caméras fixées sur l'arme[58], mais nous n'avons pas trouvé de dispositions encadrant l'enregistrement et la conservation des données.

56 https://nantes.sous-surveillance.net/spip.php?article5

57 Guillaume BIET, *Taser : l'arrestation a été filmée*, EUROPE 1, 1er décembre 2010 et JT FRANCE 2, 22 novembre 2006

58 https://www.lemonde.fr/societe/article/2023/02/14/non-lieu-infirme-pour-une-policiere-accusee-d-avoir-eborgne-avec-un-lbd-un-gilet-jaune_6161761_3224.html

Partie 7 : Fichiers de police : Analyse de données

Ici, on trouve des fichiers et des logiciels. Ils servent à faire des liens entre différentes enquêtes, qu'elles soient encore en cours ou terminées. ANACRIM et MERCURE sont des fichiers de rapprochement automatique mis en œuvre au niveau local. DPIO, lui, permet de l'analyse de données au niveau national. Quant à LUPIN, il ne sert qu'aux cambriolages.

1. Fichiers d'analyse sérielle

Ils sont créés en application de l'article 230-12 du code de procédure pénale. Ce sont des fichiers de police judiciaire (ministère de l'intérieur).

Ces fichiers sont très nombreux, par exemple : BABCO (base atteintes aux biens et criminalité organisée de la direction générale de la gendarmerie nationale), base de l'office central de lutte contre la délinquance itinérante, base escroqueries, base HARPIE en Guyane (contre l'orpaillage illégal), CALIOPE (base de comparaison et analyse logicielles des images d'origine pédopornographique), PITEH (base des personnes impliquées dans la traite des êtres humains), SERAFIM (système d'exploitation, de recherche et d'analyse sur les filières d'immigration).

Parmi eux il y a le fichier Analyse et liens de la violence associée aux crimes créé en 2009 (SALVAC, décret n°2009-786 du 23 juin 2009) et les Bases d'analyse sérielle de la police judiciaire créées en 2013 (décret n°2013-1054 du 22 novembre 2013).

Ces fichiers peuvent être interconnectés avec les fichiers d'Europol et d'INTERPOL (article 4 du décret du 22 novembre 2013).

1.1 – Données concernées

Ces fichiers concernent les personnes visées comme auteurs et complices par des enquêtes de flagrance, des enquêtes préliminaires ou des commissions rogatoires (instruction). Elles sont fichées pendant l'enquête ou après condamnation. Ils concernent aussi les personnes susceptibles de fournir des informations et les victimes. Attention, tout cela seulement pour les infractions punies d'au moins 5 ans d'emprisonnement.

Ces fichiers concernent aussi les personnes disparues, ou dont on recherche les causes de la mort.

En ce qui concerne SALVAC : Ça concerne toute enquête concernant les infractions de meurtre, d'assassinat, d'empoisonnement, d'actes de torture et de barbarie, d'enlèvement et séquestration, de viol, d'agression sexuelle, d'atteinte sexuelle sur mineur et de corruption de mineur lorsqu'elles constituent un crime ou un délit puni de plus de cinq ans d'emprisonnement, et leurs tentatives lorsqu'elles sont punissables.

sécurité, de la défense, les jeux, paris, courses, ou qui utilisent des produits dangereux, ou qui induisent l'accès à des zones protégées (par exemple un site nucléaire). La liste complète est dans l'article sur ACCReD.

Il est également utilisé, depuis la loi n°2018-778 du 10 septembre 2018, lorsqu'un·e étranger·e demande un premier titre de séjour, un renouvellement de titre de séjour ou la nationalité française !

Comme PASP et GIPASP, ce fichier a été modifié par le décret n°2020-1510 du 2 décembre 2020 afin d'élargir considérablement les données collectées.

2.1 – Données concernées

En 2020, le nombre d'informations contenues dans EASP a été très élargi.

Auparavant, il pouvait déjà contenir beaucoup d'informations, dont, indirectement, les **« motivations » politiques, religieuses, philosophiques ou syndicales.** Il pouvait aussi contenir les motifs de l'enquête administrative, l'état civil, la nationalité, la profession, les adresses physiques et électronique, le numéro de téléphone, des photographies et les titres d'identité de la personne.

Ont été ajoutés par le décret du 2 décembre 2020 les signes physiques particuliers, l'origine géographique (lieux de résidence et zones d'activité), les identifiants utilisés sur internet (sans les mots de passe), les adresses et lieux fréquentés, la situation familiale, la formation, les compétences, la profession, les emplois occupés, les moyens de déplacement (y compris les immatriculations des véhicules), la situation au regard du droit au séjour si la personne est étrangère ou même française (par exemple les interdictions de sortie du territoire), le patrimoine.

Ont été ajoutés également « *les activités susceptibles de porter atteinte à la sécurité ou à la sûreté de l'État* », ce qui rassemble les « *activités publiques ou au sein de groupements ou de personnes morales* », donc la seule participation à un parti politique, une association, ou un groupe informel peut apparaître dans EASP. Cela rassemble aussi le comportement et les habitudes de vie (ça va loin), les déplacements, les activités sur les réseaux sociaux, les pratiques sportives (quel lien entre la pratique du canoë-kayak et la sûreté de l'État ? Vous avez 2 heures), et la pratique et le comportement religieux (tout y passe…).

Ont été ajoutés en 2020 (c'est encore long, accrochez-vous) les « *facteurs de dangerosité* », ce qui rassemble les liens avec des groupes extrémistes, les éléments ou signes de radicalisation, le suivi pour radicalisation, les données relatives à la santé psychologique ou psychiatrique, les armes, la détention d'animaux dangereux, les « *agissements susceptibles de recevoir une qualification pénale* » (ça va donc bien au-delà des condamnations), les antécédents judiciaires, les fiches de recherche (d'où un lien étroit avec le FPR), les suites judiciaires, les mesures d'incarcération, et si la personne a accès à des zones ou des informations sensibles.

Il ne s'agit pas seulement d'évaluer la « dangerosité » d'une personne… mais aussi d'évaluer ses fragilités ! Ainsi, les facteurs de fragilité familiaux, sociaux et économiques, le régime de protection (tutelle,

1.4 – Droit d'accès, de rectification et d'effacement des données

Il y a 2 types de données dans ACCReD, qui obéissent chacun à une procédure différentes :

Concernant les données de fichiers « classiques » (types fichiers de police) : L'article 8 II du décret n°2017-1224 prévoit qu'on peut demander l'accès, la rectification et l'effacement des données contenues dans ACCReD directement auprès du Ministre de l'intérieur, Place Beauvau, 75008 PARIS cedex 08. Cependant, cet article renvoie à l'article 107 de la loi du 6 janvier 1978. En conséquence, le ministre peut refuser la rectification et l'effacement, et même s'abstenir de dire à la personne concernée qu'il a refusé cette rectification ou cet effacement !

Sur ce premier groupe de données, en cas de refus par le ministre, on peut faire un recours devant la CNIL ou un recours juridictionnel (article 107 de la loi du 6 janvier 1978).

Pour l'accès, la rectification et l'effacement des données relatives à la sûreté de l'État et à la défense, il faut s'adresser à la CNIL (article 118 de la loi du 6 janvier 1978). Le principe de cet article 118 est que lorsque quelqu'un demande à avoir accès à ses données, celles-ci lui sont transmises si cette communication ne met pas en cause les finalités du fichier, la sûreté de l'État, la défense ou la sécurité publique. Autant dire que c'est open bar pour la CNIL pour refuser cette communication. Quand la CNIL refuse de transmettre ces données, la procédure prévue à l'article 118 est tout à fait étonnante : la CNIL indique à la personne « *qu'il a été procédé aux vérifications nécessaires et de son droit de former un recours juridictionnel* ». Donc, la personne qui ne connaît même pas les données contenues dans le fichier, peut dire à la CNIL de les rectifier (comment savoir ce qu'il y aurait à rectifier?) ou de les effacer (comment savoir ce qu'il y aurait à effacer?)…

La personne peut former un recours juridictionnel devant la Formation spécialisée du Conseil d'État (article R841-2 du code de la sécurité intérieure) créée en 2015 (loi n°2015-912 du 24 juillet 2015, articles L773-1 et suivants du code de justice administrative). Celle-ci rejette beaucoup de recours, mais il ordonne parfois l'effacement de certaines données (par exemple pour le fichier SIREX, devenu SIRCID, de la DRSD : Conseil d'État, 05/05/2017, 396669, Publié).

2. <u>Fichier Enquêtes administratives liées à la sécurité publique (EASP)</u>

Il est prévu aux articles R236-1 et suivants du code de la sécurité intérieure. Il est mis en œuvre par la Direction centrale de la sécurité publique et par la Préfecture de police (ministère de l'intérieur). Avec PASP, EASP remplace EDVIRSP et le projet EDVIGE.

Initialement accessible par la police nationale et les services de renseignement, sa consultation a été élargie aux douaniers par la loi n°2023-22 du 24 janvier 2023.

Il sert aux mêmes enquêtes administratives que celles pour lesquelles ACCReD est utilisé : pour vérifier si une personne peut être admise lorsqu'elle postule à tout un tas d'emplois dans le domaine de la

Ça concerne aussi les données collectées au cours des procédures de recherche de cause de la mort ou d'une disparition. Ça comprend les données transmises par des États étrangers.

En ce qui concerne les bases d'analyse sérielle de la police judiciaire : Ça concerne toute enquête ou instruction sur une infraction punie d'au moins 5 ans d'emprisonnement, et aussi les recherches pour cause de mort ou de disparition.

Attention, ces fichiers peuvent contenir « *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.* » (article 6 de la loi du 6 janvier 1978 et article 230-12 du code de procédure pénale).

1.2 – Durée de conservation des données

Pour SALVAC, la conservation des données dure pendant 40 ans (article 6 du décret n°2011-1308).

Pour les bases d'analyse sérielle de la police judiciaire, la conservation des données dure 15 ans à compter de la clôture de l'enquête pour les délits, 20 ans à compter de la clôture de l'enquête pour les crimes.

Pour SALVAC et les bases d'analyse sérielle, en cas de personne disparue, il y a effacement dès qu'elle est retrouvée ; en cas de mort, dès que les suspicions de crime ou de délit sont écartées ; en tout cas maximum 25 ans dans ces 2 derniers cas.

Lorsque la personne disparue est retrouvée, il y a effacement des données. Lorsqu'il y a relaxe ou acquittement, les données sont effacées sauf si le procureur en prescrit le maintien (article 230-14 renvoyant à l'article 230-8). En cas de non-lieu ou de classement sans suite, les données en font mention, sauf si le procureur en prescrit l'effacement (idem).

1.3 – Droit de communication, de rectification et d'effacement

Il faut distinguer deux situations : l'enquête est en cours ou elle est terminée.

Lorsque l'enquête est en cours, les règles sont celles de l'article R40-36 du code de procédure pénale tant pour SALVAC que pour les bases d'analyse sérielle de la police judiciaire : Les demandes de rectification ou d'effacement peuvent être portées devant le procureur de la République territorialement compétent, ou devant le magistrat spécialisé.

Lorsque l'enquête est terminée, en plus des règles précédentes, celles-ci s'appliquent :

Si la personne a été définitivement condamnée, elle peut en demander l'effacement, mais le procureur ou le magistrat spécialisé peut s'y opposer (article 230-15).

En cas de requalification (la personne a été enregistrée dans le fichier pour assassinat, et finalement elle est condamnée pour meurtre), la rectification est de droit lorsque la personne concernée le demande (article 230-14 qui renvoie à l'article 230-8).

Pour cela, il faut s'adresser au procureur de la République compétent ou au magistrat spécialisé.

2. ANACRIM et MERCURE

Leur création a été permise par une loi de 2011, qui autorise l'exploitation de données par les logiciels de rapprochement judiciaire (articles 230-20 à 230-27 du code de procédure pénale). Ensuite, le décret n°2012-687 du 7 mai 2012 a permis la création d'ANACRIM (gendarmerie nationale) et de MERCURE (police nationale). La circulaire du 18 août 2014 relative aux fichiers d'antécédents judiciaires donne plus d'informations si nécessaire.

Contrairement aux bases d'analyse sérielle, ANACRIM et MERCURE traitent des données relatives à toutes les catégories d'infractions pour créer des relations entre elles.

Ces outils sont capables de mettre en lien des données très diverses recueillies au cours d'enquêtes (photographies, fadettes de téléphonie, exploitation de matériel informatique, données de balises GPS, etc.) et de les analyser pour effectuer des rapprochements (relations entre les personnes, lieux fréquentés, présence d'une personne dans un lieu à un moment précis, etc).

2.1 – Données concernées

Tout ce qui concerne une enquête préliminaire, une enquête de flagrance ou une commission rogatoire (instruction) sur des crimes ou des délits punis d'une peine d'emprisonnement.

Il permet de traiter des données bancaires, téléphoniques, de cartographier des réseaux de connaissance, de recouper des indices.

2.2 – Durée de conservation

Elle est définie à l'article 230-22 du code de procédure pénale : seulement pour la durée de l'enquête et pour un maximum de 3 ans.

2.3 – Droit d'accès et de rectification

Ils obéissent aux règles de l'article 230-23 et à l'article 5 du décret n°2012-687 du 7 mai 2012 : Le droit d'accès et de rectification s'exerce auprès du procureur de la République territorialement compétent (celui du tribunal judiciaire du lieu où est ouverte l'enquête ou du lieu du domicile de la personne concernée), ou un magistrat spécialisé (article 230-24).

La rectification pour requalification (par exemple : la personne est fichée pour assassinat, mais elle est condamnée pour meurtre) est de droit lorsque la personne concernée la demande.

Attention, depuis la loi n°2018-778 du 10 septembre 2018 et le décret du 21 octobre 2019, ce fichier est aussi consulté lorsqu'un·e étranger·e demande un premier titre de séjour, un renouvellement de titre de séjour ou la nationalité française !

En vue des Jeux Olympiques de 2024, le Service National des Enquêtes Administratives de Sécurité (SNEAS) a été créé, qui a effectué 520'000 enquêtes en 2021 et prévoit d'en effectuer 1'000'000 en lien avec les Jeux Olympiques afin de contrôler toutes les personnes amenées à intervenir (y compris les bénévoles), en-dehors des participants et des spectateurs… Ces contrôles peuvent même concerner les personnes qui résident dans les zones concernées par les Jeux Olympiques (article R211-33 du code de la sécurité intérieure).

1.2 – Données concernées

ACCReD est un véritable agglomérateur de fichiers. Quand on lance une recherche ACCReD, le logiciel va chercher les informations dans une dizaine de fichiers environ : le TAJ, EASP, PASP, GIPASP, FPR, N-SIS II, le FSPRT, le fichier des véhicules volés ou signalés (FoVES), CRISTINA, GESTEREXT, SIRCID (qui a remplacé SIREX en septembre 2022) et le fichier de la DGSE. On n'a que très peu parlé de tous ces fichiers jusqu'ici… ils arrivent tout de suite après ACCReD.

Le décret n°2023-1388 du 29 décembre 2023 a ajouté à cette liste le bulletin n°2 du casier judiciaire et deux fichiers d'Interpol : SLTD (sur les passeports et cartes d'identité volés, perdus, révoqués, invalides) et ICIS (qui contient des informations sur les personnes recherchées par Interpol).

L'ajout du bulletin n°2 du casier judiciaire permet, par ricochet, une consultation du Répertoire national des personnes physiques et un fort soupçon d'une fausse identité. En effet, un retour du service du casier judiciaire selon lequel la personne est inconnue de lui signifie que cette identité ne lui est absente du Répertoire national des personnes physiques, qui comporte les identités de l'ensemble des personnes nées en France et qui peut également comporter les identité de personnes nées à l'étranger.

En plus, **ACCReD contient des informations sur les opinions philosophiques, politiques ou religieuses des personnes** (alors même qu'il est consulté lorsqu'une personne étrangère demande un titre de séjour!).

Attention : en 2020, ACCReD n'a pas été modifié, mais les données contenues dans EASP ont été très largement étendues. Or, les données de ACCReD contiennent automatiquement toutes les données de EASP… donc c'est utile de voir ce que contient EASP (ci-dessous, prochain fichier) pour savoir à quoi s'en tenir avec ACCReD.

1.3 – Durée de conservation des données

6 ans à compter de leur enregistrement (article 6 du décret n°2017-1224, le décret du 21 octobre 2019 ayant ajouté 1 an à la conservation des données : quitte à ficher, autant conserver plus longtemps encore).

Partie 8 : Fichiers de renseignement utilisés principalement pour les enquêtes administratives

Cette partie regroupe les deux fichiers de renseignement utilisés pour les enquêtes administratives, par exemple quand une personne demande un poste d'agent de sécurité, ou est amenée à travailler sur un site utilisant des produits dangereux.

Ils sont aussi consultés quand un étranger demande un titre de séjour.

1. ACCReD

ACCReD signifie « Automatisation de la consultation centralisée de renseignements et de données ». Il a été créé en 2017 (décret n°2017-1224 du 3 août 2017) et dépend de la Direction générale de la police nationale et Direction générale de la gendarmerie nationale (ministère de l'intérieur).

Il a été modifié par le décret n°2023-1388 du 29 décembre 2023 par la création de nouvelles interconnexions d'ACCReD avec d'autres fichiers.

1.1 – Utilisation du fichier

Comme le Fichier Enquêtes administratives liées à la sécurité publique : Le fichier est consulté pour les enquêtes administratives pour l'embauche et le maintien à leur poste des personnes travaillant dans les secteurs suivants (articles L114-1, L114-2, L211-11-1, R114-2, R114-3 du code de la sécurité intérieure) :

- aux missions de souveraineté de l'État, de sécurité, de défense
- aux jeux, paris et courses
- à l'utilisation de matériels ou produits dangereux (article L114-1 du code de la sécurité intérieure) ;
- aux emplois en lien direct avec le transport public de personnes, de marchandises dangereuses
- à la participation (autrement qu'en simple participant/spectateur) à un grand événement exposé par son ampleur ou par des circonstances particulières à un risque exceptionnel de menace terroriste (article L211-11-1 du code de la sécurité intérieure). Re-coucou les JO 2024 !
- la magistrature et les juges administratifs
- les policiers, gendarmes, douaniers, militaires, matons, policiers municipaux
- les agents de sécurité
- et de nombreux hauts fonctionnaires

Il est aussi consulté quand une personne demande une autorisation de port d'arme.

3. Diffusion et Partage de l'Information Opérationnelle (DPIO)

Il a été créé en 2014 (décret n°2014-187 du 20 février 2014, avec auparavant l'avis de la CNIL n°2013-039 du 14 février 2013), et profondément modifié par le décret n° 2024-354 du 16 avril 2024.

Au départ, la police nationale a créé, en 2006, la Cellule opérationnelle de rapprochement et d'analyse des infractions liées (CORAIL). Côté gendarmerie, le groupe Partage de l'Information Opérationnelle (PIO) fait la même chose : Ce sont des groupes de gendarmes spécialisés dans l'analyse des informations, leur comparaison et leur rapprochement. Pour travailler, CORAIL et PIO utilisent DPIO, logiciel créé (recréé pour lui donner une existence légale?) en 2014. Contrairement aux logiciels vus précédemment (fichiers d'analyse sérielle et fichiers de rapprochement judiciaire), DPIO collecte les données de l'ensemble des enquêtes des services de police et de gendarmerie. Des algorithmes traitent ces informations pour créer des bases de données, avec des velléités d'analyse prédictive de la délinquance.

DPIO a permis à la gendarmerie de créer l'application de traitement du renseignement criminel (ATRC) qui fonctionne comme un moteur de recherche à partir de l'ensemble des informations collectées par DPIO.

3.1 – Données concernées

Il traite des données recueillies au cours d'enquêtes préliminaires, d'enquêtes de flagrance et de commissions rogatoires (instructions) à propos de crime et de délit, dont les photographies naturellement (mais avec interdiction de la reconnaissance faciale, art. 2). Il concerne aussi les recherches de personnes disparues, les morts suspectes et les personnes en fuite.

Il concerne tout le monde à partir de 10 ans ; pour les victimes, il n'y a pas d'âge minimum (article 3 du décret n°2014-187 du 20 février 2014).

Y ont accès : policiers, gendarmes, services des douanes, magistrats, et depuis avril 2024 les agents de police municipale, sur initiative des flics ou gendarmes.

3.2 – Durée de conservation des données

Les données relatives à un délit sont conservées 6 ans, celles relatives à un crime sont conservées 10 ans (article 4 du décret n°2014-187 du 20 février 2014, modifié par le décret n° 2024-354 du 16 avril 2024).

3.3 – Droit d'accès

L'article 6 du décret n°2014-187 du 20 février 2014 prévoit que ces droits s'exercent auprès de la CNIL. Cependant, cela est en contradiction avec les articles 104 à 106 de la loi n°78-17 du 6 janvier 1978 tels que modifiés par l'ordonnance n°2018-1125 du 12 décembre 2018, qui prévoient qu'il faut s'adresser au responsable du traitement. Il faut appliquer les dispositions de la loi et non celles du décret.

En conséquence, il faut s'adresser au ministère de l'intérieur, Place Beauvau, 75800 PARIS CEDEX 08.

4. Logiciel d'Uniformisation des Procédures d'IdeNtification (LUPIN)

Il a été créé en 2014 (arrêté du 15 octobre 2014). Il a surtout été vendu comme un outil pour permettre de faire des liens entre les cambriolages pour retrouver plus facilement les coupables : l'idée c'est qu'une même personne ou un même groupe utilise un même mode opératoire dans des endroits différents, plus ou moins proches, et donc que l'analyse de tout ça permettrait d'arrêter les voleurs et les voleuses.

4.1 – Données concernées

Il concerne toutes les données relatives à des infractions de vol, y compris vols aggravés (articles 311-1 à 311-15 du code pénal), ainsi que des infractions de dégradation, destruction de biens (articles 322-5 à 322-11-1 du même code). Cela va de l'identité de la victime aux biens volés, en passant par le mode opératoire et les empreintes digitales et génétiques laissées sur place. Le but est l'identification des auteurs de ces infractions.

4.2 – Durée de conservation des données

Les données sont conservées 3 ans à compter de leur enregistrement (article 4 de l'arrêté du 15 octobre 2014).

4.3 – Droit d'accès

L'article 6 de l'arrêté du 15 octobre 2014 prévoit que ces droits s'exercent auprès de la CNIL. Cependant, cela est en contradiction avec les articles 104 à 106 de la loi n°78-17 du 6 janvier 1978 tels que modifiés par l'ordonnance n°2018-1125 du 12 décembre 2018, qui prévoient qu'il faut s'adresser au responsable du traitement. Il faut appliquer les dispositions de la loi et non celles de l'arrêté.

En conséquence, il faut s'adresser au ministère de l'intérieur, Place Beauvau, 75800 PARIS CEDEX 08.

5. Fichier central de la criminalité organisée (F2CO) et Fichier des brigades spécialisées (FBS)

À l'origine il existe le Fichier des brigades spécialisées (FBS). Il a fait l'objet d'un avis de la CNIL (avis n°90-090 du 8 octobre 1991), mais le décret qui crée ce fichier n'a jamais été publié. Il n'a sûrement jamais été signé. Ça ne veut pas dire que le fichier n'a pas existé, au contraire. Il a été mis en œuvre en toute illégalité, au moins jusqu'en 2019.

Cette existence illégale est confirmée par un rapport du Sénat relatif au projet de loi de finances pour 2010[59]. Un rapport d'Alain Bauer indique qu'en 2005, 174.593 personnes étaient fichées au FBS[60]. En 2007, 191.647 personnes apparaissaient au FBS[61].

Le rapport de la commission des lois de l'assemblée nationale du 17 octobre 2018 annonce que, au cours de 2019, le Fichier des brigades spécialisées serait remplacé par le Fichier central de la criminalité organisée.

Toutefois, on a l'impression que le secret et l'illégalité perdurent dans ce domaine : on n'a pas trouvé la trace d'une création officiel de ce Fichier central de la criminalité organisée. Il semble donc que si le FBS a été remplacé, c'est par un autre fichier tout aussi illégal.

Ce qui est probable, c'est que le FBS a été intégré dans le fichier d'analyse sérielle BABCO (gendarmerie nationale) et/ou dans son équivalent côté police nationale.

59 Projet de loi de finances pour 2010: Sécurité – Immigration, asile et intégration, https://www.senat.fr/rap/a09-106-11/a09-106-114.html

60 Alain Bauer et a., Fichiers de police et de gendarmerie, comment améliorer leur contrôle et leur gestion?, 2007, https://www.vie-publique.fr/sites/default/files/rapport/pdf/064000885.pdf

61 Groupe de contrôle des fichiers de police et de gendarmerie, décembre 2008, https://referentiel.nouvelobs.com/file/438/610438.pdf