EXPÉDITEUR

Madame la Ministre de la justice
13 Place Vendôme
75042 PARIS CEDEX 01

Par lettre recommandée avec avis de réception

LIEU, le DATE

Objet : Rectification/Effacement des données me concernant détenues par l'Agence nationale des techniques d'enquête numérique et dans DataJust

Madame la 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 suivantes :

- 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) :

LISTE DES INFORMATIONS CONCERNÉES

- DataJust (décret n°2020-356 du 27 mars 2020) :

LISTE DES INFORMATIONS CONCERNÉES

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

Je vous prie d'agréer, Madame la Ministre, 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 et procédures pour leur suppression

Version longue : 60 fichiers actifs

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

Juin 2020
Version 2 (Longue)

Table des matières

EXPÉDITEUR

Madame la Ministre de la justice
13 Place Vendôme
75042 PARIS CEDEX 01

Par lettre recommandée avec avis de réception

LIEU, le DATE

Objet : Consultation des données me concernant détenues par l'Agence nationale des techniques d'enquête numérique et dans DataJust

Madame la 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 suivantes :

- 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 (décret n°2020-356 du 27 mars 2020).

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

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

Pièce-jointe : copie de ma pièce d'identité

EXPÉDITEUR

Greffe du Tribunal de police saisi de la contestation de la contravention

Par lettre recommandée avec avis de réception

LIEU, le DATE

Objet : Rectification/Effacement des données me concernant dans Minos

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/effacement des informations me concernant contenues dans Minos.

En conséquence et en application de l'arrêté du 22 février 2008, je vous demande de bien vouloir procéder à la rectification/l'effacement des données suivantes me concernant contenues dans Minos :

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

Utilisation du dossier

Ceci est la 2e version (2020) du dossier sur les fichiers de police, de renseignement et de justice.

Pour cette 2e version, nous avons décidé d'en éditer une version courte, plus maniable et qui comprend les fichiers les plus importants, c'est-à-dire ceux qui sont le plus utilisés et qui ont un impact fort en termes de surveillance policière et de conséquences sur la vie quotidienne et militante. Nous éditons également la version longue, qui comprend le plus de fichiers possible, sachant qu'il ne s'agit pas de l'intégralité de ceux utilisés par la police, les services de renseignement et la justice.

Ceci est la version longue.

Pour une utilisation plus facile, nous avons ramené les schémas au début du dossier. Ça permet de montrer dans quels fichiers on est susceptible d'être répertorié·e, et quels fichiers sont consultés, dans quelques situations. Ainsi, c'est plus facile d'aller voir dans le reste du dossier les fichiers qui nous intéressent plus particulièrement.

Chaque schéma correspond à une situation dans laquelle la police, la gendarmerie, les services de renseignement 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-là parce qu'elles sont relativement critiques ou courantes… Aussi, il s'agit de schémas : ils ne sont pas très précis, un certain nombres d'informations sont perdues. Ça vaut toujours le coup de se reporter au texte ci-dessous pour avoir plus d'informations sur un fichier en particulier.

On espère, en tout cas, que ces schémas peuvent donner une vision d'ensemble, et aider à mieux s'y retrouver.

EXPÉDITEUR

Greffe du Tribunal de police saisi de la contestation de la contravention

Par lettre recommandée avec avis de réception

LIEU, le DATE

Objet : Consultation des données me concernant dans Minos

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 consultation des informations me concernant contenues dans Minos.

En conséquence et en application de l'arrêté du 22 février 2008, je vous demande de bien vouloir me communiquer les données me concernant contenues contenues dans Minos.

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

EXPÉDITEUR

Direction générale de la santé
14 avenue DUQUESNE
75350 PARIS SP 07

Par lettre recommandée avec avis de réception

LIEU, le DATE

Objet : Rectification/Effacement des données me concernant dans SI-VIC

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 des informations dans le Système d'information pour le suivi des victimes (SI-VIC).

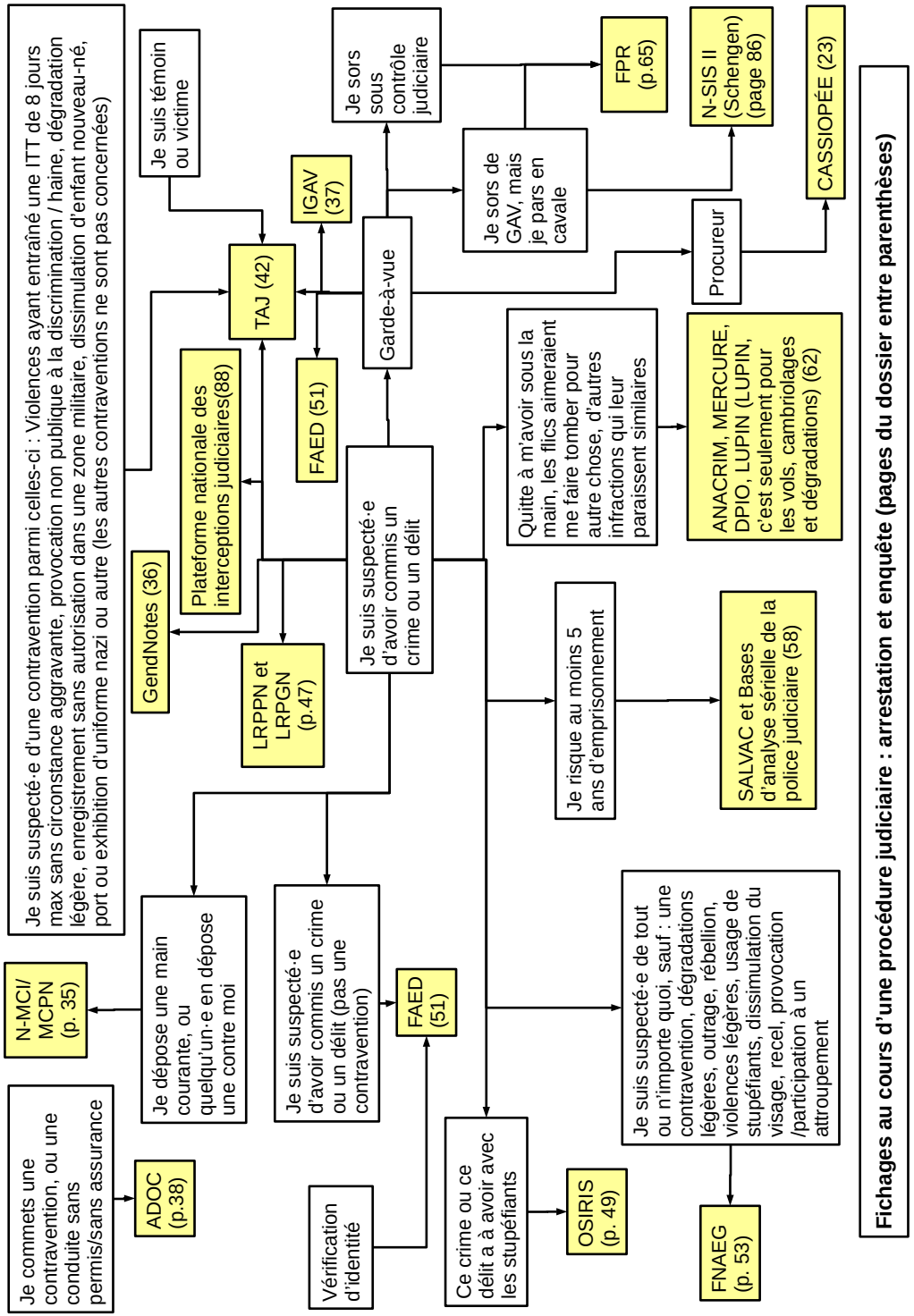
En conséquence et en application de l'article R3131-10-2 du code de la santé publique, je vous demande de bien vouloir procéder à la rectification/l'effacement des données suivantes me concernant contenues dans SI-VIC :

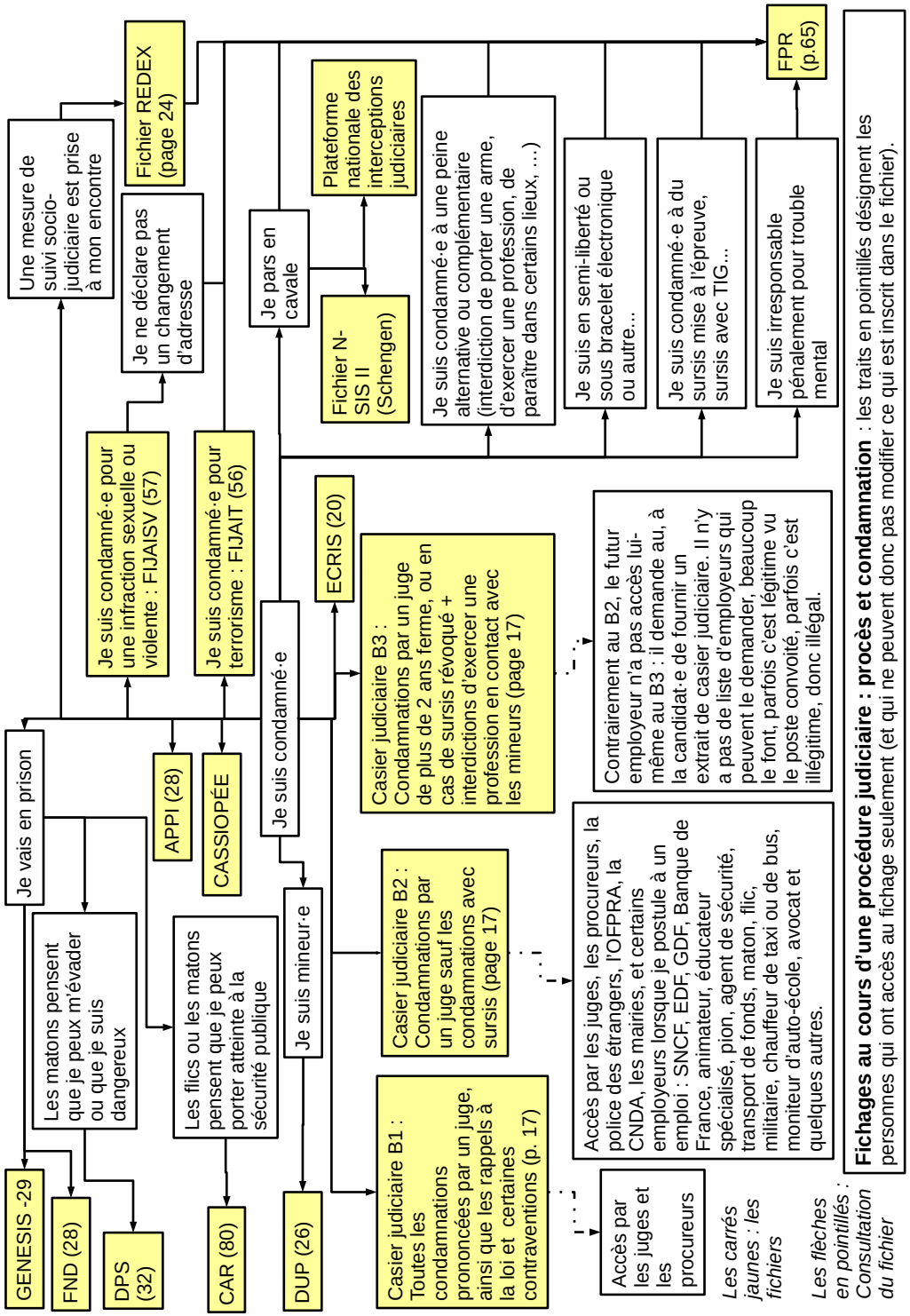
LISTE DES INFORMATIONS CONCERNÉES

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 santé
14 avenue DUQUESNE
75350 PARIS SP 07

Par lettre recommandée avec avis de réception

LIEU, le DATE

Objet : Consultation des données me concernant dans SI-VIC

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 consultation des informations me concernant contenues dans le Système d'information pour le suivi des victimes (SI-VIC).

En conséquence et en application de l'article R3131-10-2 du code de la santé publique, je vous demande de bien vouloir me communiquer les données me concernant contenues contenues dans SI-VIC.

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

EXPÉDITEUR

Centre national de traitement automatisé
CS 41101
35911 RENNES

Par lettre recommandée avec avis de réception

LIEU, le DATE

Objet : Rectification/Effacement des données me concernant dans ADOC

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 Accès aux Dossiers des Contraventions (ADOC).

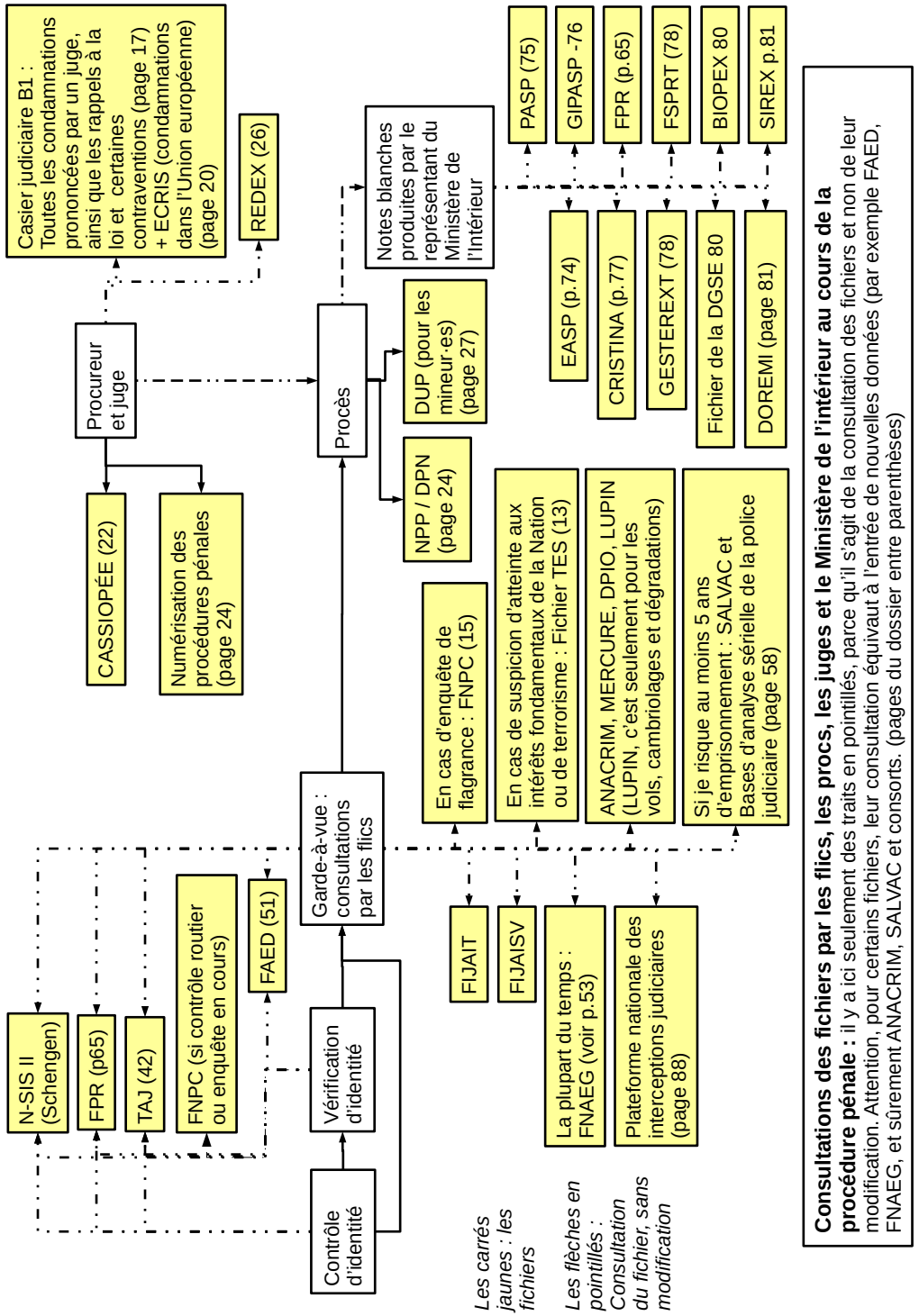
En conséquence et en application de l'article 6 de l'arrêté du 13 octobre 2004, je vous demande de bien vouloir procéder à la rectification/l'effacement des données suivantes me concernant contenues dans ADOC :

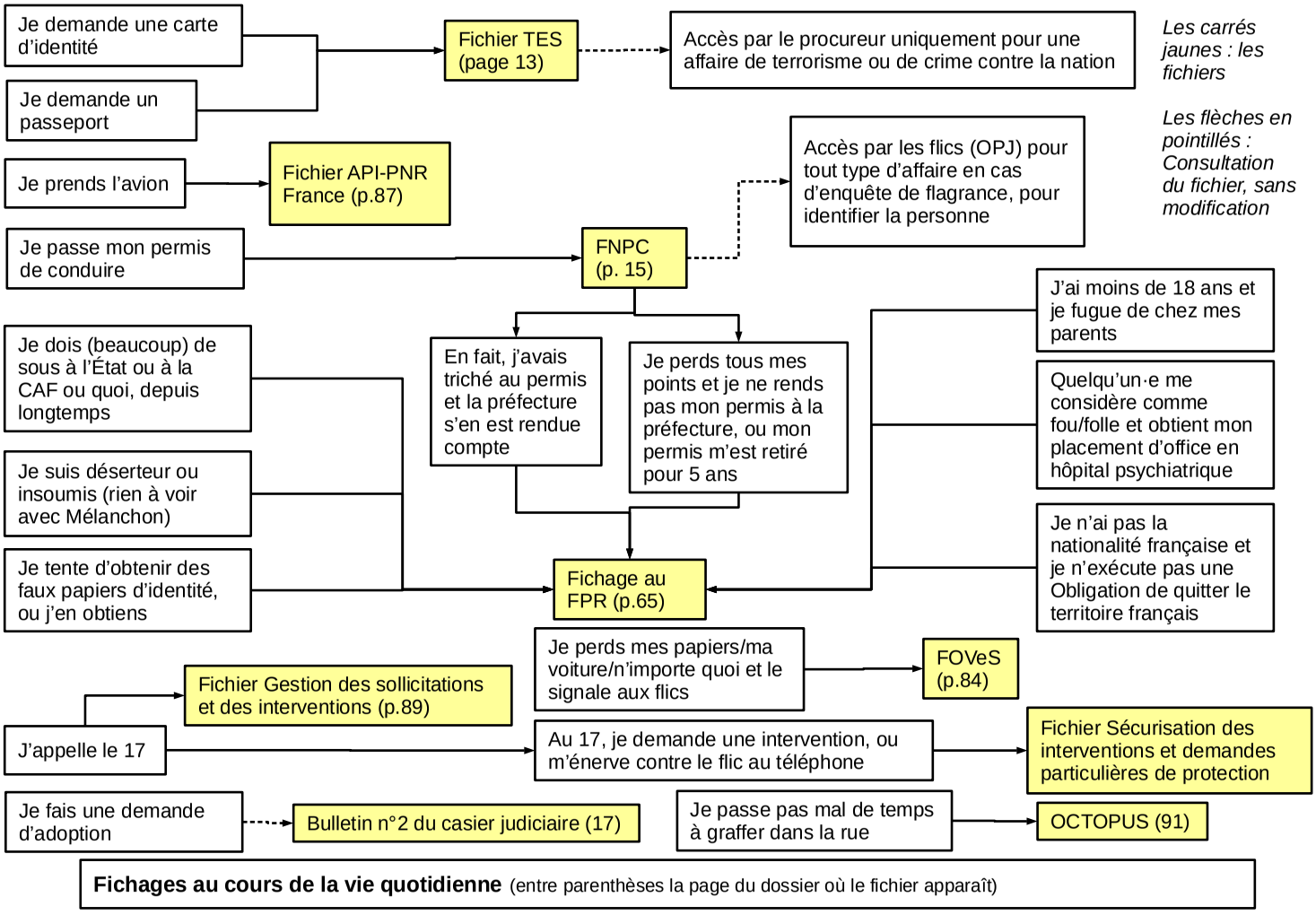
LISTE DES INFORMATIONS CONCERNÉES

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

Centre national de traitement automatisé
CS 41101
35911 RENNES

Par lettre recommandée avec avis de réception

LIEU, le DATE

Objet : Consultation des données me concernant dans ADOC

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 consultation des informations me concernant contenues dans le fichier Accès aux Dossiers des Contraventions (ADOC).

En conséquence et en application de l'article 6 de l'arrêté du 13 octobre 2004, je vous demande de bien vouloir me communiquer les données me concernant contenues contenues dans ADOC.

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

Expéditeur :

Directeur de l'établissement d'incarcération

Par le greffe de l'établissement

LIEU, le DATE

Objet : Effacement/Rectification de Gestion nationale des personnes détenues en établissement pénitentiaire (GENESIS)

Madame, Monsieur le Directeur,

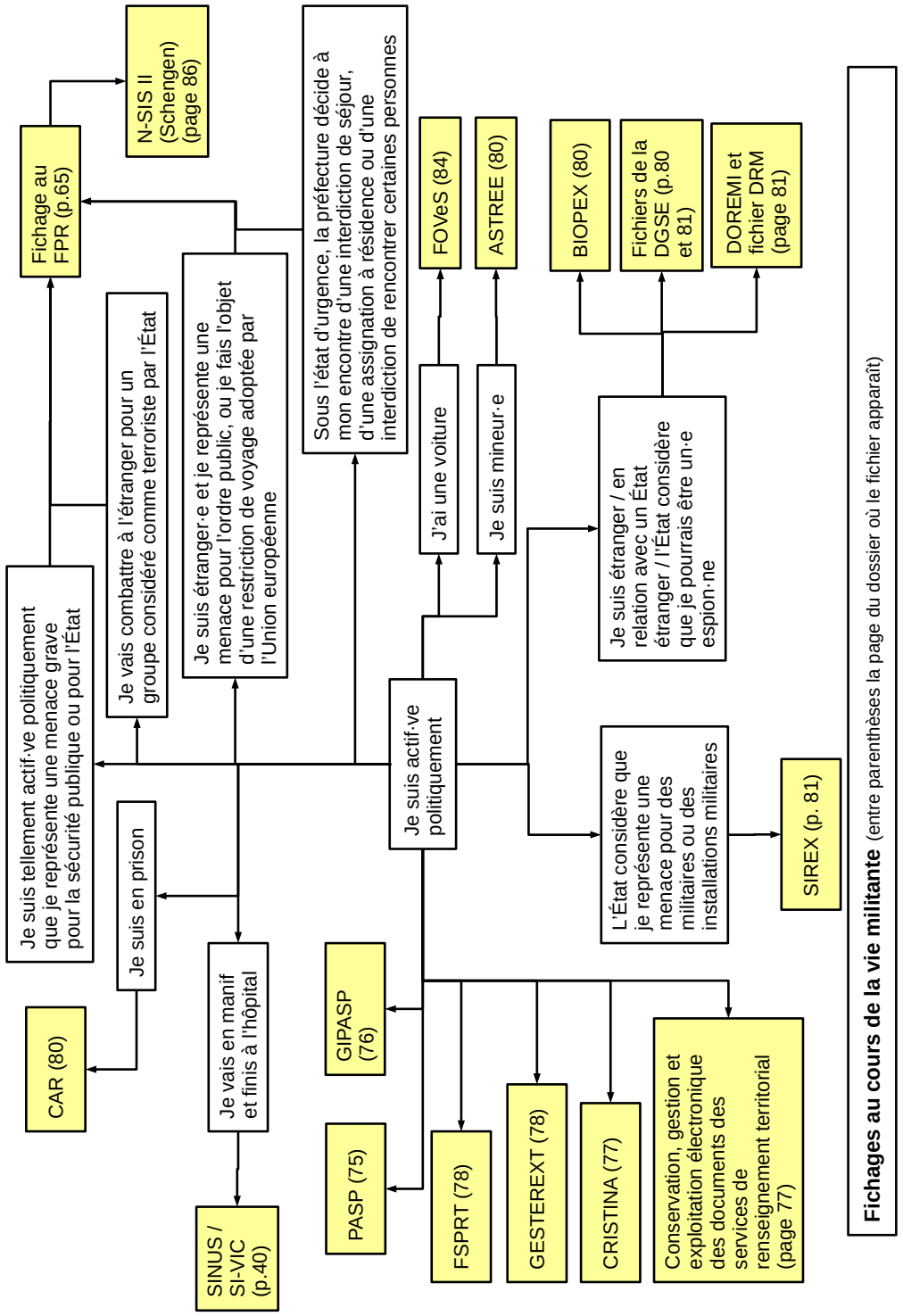
Je soussigné(e) M./Mme XXX, né(e) le XXX à XXX, domicilié(e) au XXX, exerce par la présente mon droit d'effacement/de rectification d'informations me concernant contenues dans Gestion nationale des personnes détenues en établissement pénitentiaire (GENESIS).

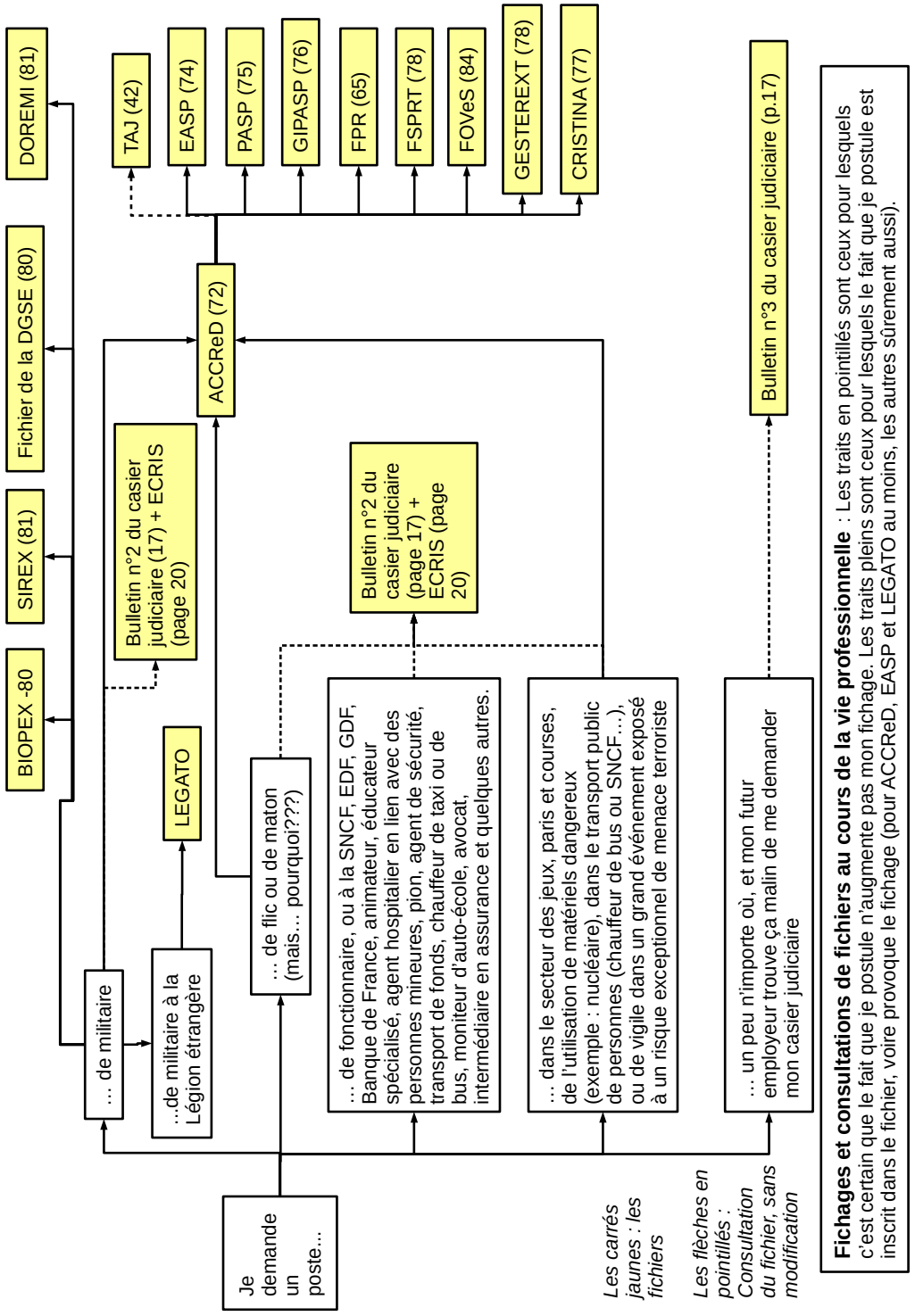
En conséquence et en application de l'article 57-9-24 du code de procédure pénale, je vous demande de bien vouloir procéder à la rectification/l'effacement des données suivantes me concernant contenues dans Gestion nationale des personnes détenues en établissement pénitentiaire (GENESIS) :

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 Directeur, l'expression de ma plus haute considération.





Expéditeur :

Directeur de l'établissement d'incarcération

Par le greffe de l'établissement

LIEU, le DATE

Objet : Accès à Gestion nationale des personnes détenues en établissement pénitentiaire (GENESIS)

Madame, Monsieur le Directeur

Je soussigné(e) M./Mme XXX, né(e) le XXX à XXX, domicilié(e) au XXX, exerce par la présente mon droit d'accès à Gestion nationale des personnes détenues en établissement pénitentiaire (GENESIS).

En conséquence et en application de l'article 57-9-24 du code de procédure pénale, je vous demande de bien vouloir me communiquer les données me concernant contenues dans Gestion nationale des personnes détenues en établissement pénitentiaire (GENESIS).

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

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

Expéditeur :

Directeur interrégional des services pénitentiaires si incarcération ;
Procureur de la République compétent
En fonction du domicile si la personne est libre

Par lettre recommandée avec accusé de réception

LIEU, le DATE

Objet : Effacement/Rectification du Fichier national automatisé des personnes incarcérées (FND)

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'effacement/de rectification d'informations me concernant contenues dans Fichier national automatisé des personnes incarcérées (FND).

En conséquence et en application de l'article 2 de l'arrêté du 20 février 2003, je vous demande de bien vouloir procéder à la rectification/l'effacement des données suivantes me concernant contenues dans le Fichier national automatisé des personnes incarcérées (FND) :

LISTE DES INFORMATIONS CONCERNÉES

Je vous demande de bien vouloir m'informer de l'issue donnée à cette demande.

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

Pièce-jointe : copie de ma pièce d'identité

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 (n° 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, qui sont simplement tenus par l'administration), qui comportent le plus grand nombre de personnes (Partie 1, p.13). Suivent les fichiers de justice (Partie 2, p.17). Ensuite différents types de fichiers de police : les fichiers administratifs (Partie 3, p.35), qui recensent par exemple toutes les personnes ayant un permis pour porter ou détenir une arme ; les

fichiers d'antécédents (Partie 4, p.42), qui rassemblent tous les antécédents judiciaires d'une personne ; les fichiers d'identification (Partie 5, p.51), qui servent à retrouver l'identité d'une personne (par exemple le fameux FNAEG, qui contient l'ADN de plus de 3 millions de personnes) ; les fichiers de rapprochement automatique et manuel (Partie 6, p.62), qui servent à analyser des données pour les recouper. Ensuite viennent les fichiers de renseignement, qui sont nombreux (Partie 7, p.65). Enfin viennent de nombreux autres fichiers (Partie 8, p.84), qu'il est difficile de classer dans les catégories précédentes (par exemple le volet français du fichier de l'espace Schengen, OCTOPUS pour les tags et le Fichier national des interdits de stade).

Après cette longue liste, une partie est consacrée au récapitulatif du droit d'accès et de suppression (Partie 9, p.92). Il s'agit de rassembler les informations utiles pour comprendre un peu 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, p.102).

Expéditeur :

Directeur interrégional des services pénitentiaires si incarcération ;
Procureur de la République compétent
En fonction du domicile si la personne est libre

Par lettre recommandée avec accusé de réception

LIEU, le DATE

Objet : Accès au Fichier national automatisé des personnes incarcérées (FND)

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 Fichier national automatisé des personnes incarcérées (FND).

En conséquence et en application de l'article 2 de l'arrêté du 20 février 2003, je vous demande de bien vouloir me communiquer les données me concernant contenues dans le Fichier national automatisé des personnes incarcérées (FND).

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

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

Pièce-jointe : copie de ma pièce d'identité

EXPÉDITEUR

Direction générale de la gendarmerie nationale
4 rue Claude-Bernard
CS60003
92136 ISSY-LES-MOULINEAUX CEDEX

Par lettre recommandée avec avis de réception

LIEU, le DATE

Objet : Rectification/Effacement des données me concernant dans certains fichiers de la DGGN

Madame, Monsieur le Directeur,

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 les fichiers suivants mis en œuvre par la Direction générale de la gendarmerie nationale :

- 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 (articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) ;

LISTE DES INFORMATIONS CONCERNÉES

- Fichier Gestion des sollicitations et des interventions (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) ;

LISTE DES INFORMATIONS CONCERNÉES

- Fichier Sécurisation des interventions et demandes particulières de protection (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) ;

LISTE DES INFORMATIONS CONCERNÉES

- GendNotes (décret n°2020-151 du 20 février 2020).

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 procureur/Directeur, l'expression de ma plus haute considération.

Pièce-jointe : copie de ma pièce d'identité

Partie 1 : Fichiers d'identification administrative

Voici deux fichiers d'identification administrative : L'un concerne les passeports et les cartes d'identité, l'autre les permis de conduire.

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 flics 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. Cela n'empêche bien sûr pas les flics d'avoir accès à ces fichiers. Par exemple, lorsqu'ils vérifient l'identité d'une personne, ils accèdent à ces fichiers 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 flics peuvent accéder à ces fichiers aussi.

1. 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 le ministère de l'intérieur.

Au moment de la demande d'une carte d'identité ou d'un passeport, le Fichier des Personnes Recherchées (FPR) est consulté pour vérifier qu'aucun élément ne s'oppose à la délivrance du titre (article 8 du décret n°2016-1460 du 28 octobre 2016).

1.1 – Données concernées

Ces données sont listées à l'article 2 du décret n°2016-1460 du 28 octobre 2016, et les personnes qui y ont accès aux articles 3 à 5.

Quiconque demande une carte d'identité ou un passeport voit ses données déposées dans le TES. C'est tout un tas de données : 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 et de la signature, l'email ou le téléphone si la personne l'a donnée.

Cependant, **c'est possible d'obtenir une carte d'identité (mais pas un passeport) en refusant la numérisation de ses empreintes digitales** (attention, on les donne quand même, mais « à l'ancienne », avec de l'encre, article 4-3 II du décret n°55-1397 du 22 octobre 1955). Le formulaire est disponible ici :

http://www.dordogne.gouv.fr/content/download/23497/171854/file/formulaire%20empreintes.pdf et en annexe de cet article.

1.2 – Utilisation du fichier TES

Les personnes qui peuvent avoir accès à ce fichier sont les agents du ministère de l'intérieur qui sont affectés au service des passeports et de la carte d'identité, les agents de la préfecture et agents consulaires chargés de la délivrance des passeports et des cartes d'identité, ainsi que les agents des communes habilités pour recueillir les demandes et délivrer les titres. 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 flics 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 (trahison, espionnage, complot, mouvement insurrectionnel, atteinte au secret de la défense nationale…) et les actes de terrorisme. De même, les agents français en relation avec INTERPOL et avec N-SIS II (Schengen) peuvent accéder aux données.

De plus, les flics 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.

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 ALICEM. 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 ALICEM est seulement volontaire : si on ne crée pas un compte ALICEM sur l'application (ou, peut-être, sur FranceConnect), on ne rentre pas dans le fichier.

1.3 – Durée de conservation des données

Les données sont conservées 15 ans s'il s'agit d'un passeport et 20 ans s'il s'agit d'une carte d'identité, à compter de la délivrance du titre. Ces durées sont réduites à 10 et 15 ans lorsque la personne est mineure.

EXPÉDITEUR

Direction générale de la gendarmerie nationale
4 rue Claude-Bernard
CS60003
92136 ISSY-LES-MOULINEAUX CEDEX

Par lettre recommandée avec avis de réception

LIEU, le DATE

Objet : Consultation des données me concernant dans certains fichiers de la DGGN

Madame, Monsieur le Directeur,

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 mis en œuvre par la Direction générale de la gendarmerie nationale :

- 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 (articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) ;
- Fichier Gestion des sollicitations et des interventions (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 (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) ;
- GendNotes (décret n°2020-151 du 20 février 2020).

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

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

Pièce-jointe : copie de ma pièce d'identité

EXPÉDITEUR

Direction générale de la police nationale
Place Beauvau
75800 PARIS CEDEX 08

Par lettre recommandée avec avis de réception

LIEU, le DATE

Objet : Rectification/Effacement des données me concernant dans certains fichiers de la DGPN

Madame, Monsieur le Directeur,

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 les fichiers suivants mis en œuvre par la Direction générale de la police nationale :

- Nouvelle Main Courante Informatisée (N-MCI, 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) :

  LISTE DES INFORMATIONS CONCERNÉES

- 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 (articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) :

  LISTE DES INFORMATIONS CONCERNÉES

- Fichier National des Interdits de Stade (FNIS, arrêté du 28 août 2007 et articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) :

  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 procureur/Directeur, l'expression de ma plus haute considération.

Pièce-jointe : copie de ma pièce d'identité

1.4 – Droits d'accès et de rectification directs

L'article 11 du décret n°2016-1460 du 28 octobre 2016 prévoit que les droits d'accès et de rectification s'exercent auprès de l'autorité de délivrance, c'est-à-dire la préfecture qu a délivré le passeport ou la carte nationale d'identité.

2. Fichier National des Permis de Conduire (FNPC)

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.

2.1 – 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.

Enfin, comme pour le TES, certains flics 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 (trahison, espionnage, complot, mouvement insurrectionnel, atteinte au secret de la défense nationale…) et les actes de terrorisme.

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

2.2 – 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.

2.3 – Droits d'accès et de rectification

L'article L225-3 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).

3. 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).

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

Au début il y avait le fichier MENS (Minorités Ethniques Non Sédentarisées), qui a existé illégalement pendant longtemps. Ensuite, ou plutôt 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 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.

Ça ne veut pas dire que d'autres fichiers ne continuent pas d'exister illégalement.

EXPÉDITEUR

Direction générale de la police nationale
Place Beauvau
75800 PARIS CEDEX 08

Par lettre recommandée avec avis de réception

LIEU, le DATE

Objet : Consultation des données me concernant dans certains fichiers de la DGPN

Madame, Monsieur le Directeur,

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 mis en œuvre par la Direction générale de la police nationale :

- Nouvelle Main Courante Informatisée (N-MCI, 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) ;
- 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 (articles 104 à 106 de la loi n°78-17 du 6 janvier 1978) ;
- Fichier National des Interdits de Stade (FNIS, arrêté du 28 août 2007 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, Madame, Monsieur le Directeur, l'expression de ma plus haute considération.

Pièce-jointe : copie de ma pièce d'identité

Expéditeur :

Procureur de la République compétent
En fonction du lieu de la procédure

Par lettre recommandée avec accusé de réception

LIEU, le DATE

Objet : Effacement/Rectification de données personnelles de certains fichiers de justice

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'effacement/de rectification d'informations me concernant contenues dans les fichiers suivants :

- Numérisation des procédures pénales (arrêté du 16 janvier 2008) :

  LISTE DES INFORMATIONS CONCERNÉES

- Dossier pénal numérique (DPN, article R249-14 du code de procédure pénale) :

  LISTE DES INFORMATIONS CONCERNÉES

- Application des Peines, Probation et Insertion (APPI, article R57-4-7 du code de procédure pénale) :

  LISTE DES INFORMATIONS CONCERNÉES

Je vous demande de bien vouloir m'informer de l'issue donnée à cette demande.

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

Pièce-jointe : copie de ma pièce d'identité

Partie 2 : Fichiers de justice

Ici, on trouve 4 types de fichiers :

Les fichiers d'antécédents, avec surtout le casier judiciaire. Il permet aux juges et aux procureurs de savoir si une personne a été condamné·e auparavant, donc si elle est en état de récidive. Ils permettent aussi d'interdire certaines professions lorsqu'on a été condamné·e par le passé. Le casier judiciaire est en lien avec le système ECRIS / ECRIS-TCN qui permet l'échange d'informations sur les condamnations entre États membres de l'Union européenne.

Ensuite, il y a les fichiers qui servent en interne aux magistrats, avec CASSIOPÉE et « Numérisation des procédures pénales » (NPP), une grosse machine à gaz qui permet de suivre toutes les procédures, passées et présentes, à l'encontre d'une personne (qui va être progressivement remplacé par le Dossier Pénal Numérique (DPN), ainsi que MINOS, pour le tribunal de police seulement.

Puis viennent les fichiers qui permettent de mieux connaître une personne, pour permettre aux juges de mieux la condamner : REDEX pour tout le monde, DUP pour les mineur·es.

En cas de condamnation, il y a les fichiers qui suivent les peines et la détention : APPI, FND, GENESIS et DPS. Enfin, il y a DataJust, qui ne doit servir qu'à produire des statistiques.

1. <u>Casier judiciaire national automatisé</u>

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, B3.

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.

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 sanctions 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 condamnations prononcées contre les mineurs de moins de 2 mois d'emprisonnement, 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. Il peut être consulté par les administrations (préfectures, ministère des armées, …).

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

Expéditeur :

Procureur de la République compétent
En fonction du lieu de la procédure

Par lettre recommandée avec accusé de réception

LIEU, le DATE

Objet : Accès à certains fichiers de justice

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 aux informations personnelles me concernant contenues dans les traitements suivants :

- Numérisation des procédures pénales (arrêté du 16 janvier 2008) ;
- Dossier pénal numérique (DPN, article R249-14 du code de procédure pénale) ;
- Application des Peines, Probation et Insertion (APPI, article R57-4-7 du code de procédure pénale).

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

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 :

Direction générale de la police nationale
Place Beauvau
75800 PARIS CEDEX 08

OU Direction générale de la gendarmerie nationale
4 Rue Claude-Bernard
CS 60003
92136 ISSY-LES-MOULINEAUX CEDEX

Par lettre recommandée avec accusé de réception

LIEU, le DATE

Objet : Effacement/Rectification de données du Fichier des Objets et Véhicules Signalés (FOVeS)

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'effacement/de rectification de données me concernant contenues dans le Fichier des Objets et Véhicules Signalés (FOVeS).

En conséquence et en application de l'article 8 de l'arrêté du 7 juillet 2017, je vous demande de bien vouloir procéder à la rectification/l'effacement des données suivantes me concernant contenues dans le Fichier des Objets et Véhicules Signalés (FOVeS) :

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 procureur, l'expression de ma plus haute considération.

Pièce-jointe : copie de ma pièce d'identité

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.

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 .

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. 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 tribunal d'un pays membre de l'Union européenne contre une personne.

Il permet donc, par exemple, à un procureur ou à un juge français de savoir si une personne a été condamnée en Allemagne.

Il est régi 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 (mise en place de ECRIS), par la directive 2011/93/UE du 13 décembre

Expéditeur :

Direction générale de la police nationale
Place Beauvau
75800 PARIS CEDEX 08

OU Direction générale de la gendarmerie nationale
4 Rue Claude-Bernard
CS 60003
92136 ISSY-LES-MOULINEAUX CEDEX

Par lettre recommandée avec accusé de réception

LIEU, le DATE

Objet : Accès au Fichier des Objets et Véhicules Signalés (FOVeS)

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 Fichier des Objets et Véhicules Signalés (FOVeS).

En conséquence et en application de l'article 8 de l'arrêté du 7 juillet 2017, je vous demande de bien vouloir me communiquer les données me concernant contenues dans le Fichier des Objets et Véhicules Signalés (FOVeS).

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

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 :

Procureur de la République compétent
En fonction du domicile du demandeur
Par lettre recommandée avec accusé de réception

LIEU, le DATE

Objet : Rectification/Effacement de données de certains fichiers de justice

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 rectification/d'effacement des données me concernant contenues dans les traitements automatique de données suivants :

- Répertoire des expertises (REDEX, article R53-21-11) :

  DONNÉES CONCERNÉES

- Chaîne Applicative Supportant le Système d'Information Oriente Procédure pénale Et Enfants (CASSIOPÉE, article R15-33-66-10 du code de procédure pénale) :

  DONNÉES CONCERNÉES

- Fichier judiciaire national automatisé des auteurs d'infractions terroristes (FIJAIT, article 706-25-12 du code de procédure pénale) :

  DONNÉES CONCERNÉES

- Fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes (FIJAISV, article 706-53-10 du code de procédure pénale) :

  DONNÉES CONCERNÉES

- ANACRIM (article 230-23 du code de procédure pénale) : DONNÉES CONCERNÉES
- MERCURE (article 230-23 du code de procédure pénale) : DONNÉES CONCERNÉES

Je vous demande de bien vouloir m'informer de l'issue donnée à cette demande.

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

Pièce-jointe : copie de ma pièce d'identité

2011 et par le règlement européen 2019/816 du 17 avril 2019 (pour le fichage des ressortissants de pays non membres de l'Union européenne).

ECRIS existe déjà. ECRIS-TCN, qui concerne le fichage des ressortissants de pays non membres de l'Union européenne, ne semble pas être encore opérationnel au 8 juin 2020[1].

2.1 – Données concernées

ECRIS rassemble l'ensemble des données conservées dans le casier judiciaire, et en plus, les empreintes digitales et la photographie de la personne. 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).

2.2 – Utilisation de ECRIS

Il n'y a pas de fichier centralisé. 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.

Pour les ressortissants de pays non membres de l'Union européenne, l'État dont le juge a condamné la personne conserve les données dans son casier judiciaire. Ensuite, si cet·te Canadien·ne (par exemple) se fait arrêter en Italie, l'Italie pourra demander à tous les États membres de l'Union si ils ont des informations sur cet·te Canadien·ne.

Enfin, ECRIS peut être consulté 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 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).

2.3 – Durée de conservation des données

C'est les mêmes que pour le casier judiciaire.

1 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

2.4 – 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). On ne sait pas trop à quoi ça correspond en France. Dans le doute, on peut donc s'adresser à la CNIL, qui devrait transmettre aux autorités compétentes.

3. 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).

3.1 – 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, 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.

Expéditeur :

Procureur de la République compétent
En fonction du domicile du demandeur

Par lettre recommandée avec accusé de réception

LIEU, le DATE

Objet : Accès aux données personnelles contenues dans certains fichiers de justice

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 aux données me concernant contenues dans les fichiers suivants :

- Répertoire des expertises (REDEX, article R53-21-10 du code de procédure pénale) ;
- Chaîne Applicative Supportant le Système d'Information Oriente Procédure pénale Et Enfants (CASSIOPÉE, article R15-33-66-10 du code de procédure pénale) ;
- Fichier judiciaire national automatisé des auteurs d'infractions terroristes (FIJAIT, article 706-25-11 du code de procédure pénale) ;
- Fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes (FIJAISV, articles 706-53-9 du code de procédure pénale) ;
- ANACRIM (article 230-23 du code de procédure pénale) ;
- MERCURE (article 230-23 du code de procédure pénale).

En conséquence, je vous demande de bien vouloir me communiquer les données me concernant contenues dans ces traitements de données personnelles.

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

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 :

Directeur de l'Unité Information Passagers
11 Rue des Deux-Communes
93558 MONTREUIL CEDEX

Par lettre recommandée avec accusé de réception

LIEU, le DATE

Objet : Rectification/Effacement de données du système Advance Passenger Information – Passenger Name Record (API-PNR France)

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 Advance Passenger Information – Passenger Name Record (API-PNR France).

En conséquence et en application de l'article R232-22 du Code de la sécurité intérieure, je vous demande de rectifier/d'effacer les informations suivantes me concernant contenues dans le système Advance Passenger Information – Passenger Name Record (API-PNR France) :

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 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

3.2 – 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).

3.3 – 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).

3.4 – 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).

4. 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.

4.1 – 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.

4.2 – Utilisation de Minos

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

4.3 – 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.

4.4 – 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).

5. Numérisation des procédures pénales (NPP)

Ce fichier a été créé par l'arrêté du 16 janvier 2008. Il est géré par le ministère de la justice et sert au suivi des procédures pénales dans les tribunaux. À compter du 24 juin 2020, il est progressivement remplacé par le fichier « Dossier pénal numérique » (DPN), en commençant par Blois et Amiens.

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

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

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

On peut 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).

6. Dossier pénal numérique (DPN)

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. Il est mis en œuvre par chaque tribunal et cour d'appel par à la cour de cassation, et apparaît aux articles R249-9 et suivants du code de procédure pénale.

Expéditeur :

Directeur de l'Unité Information Passagers
11 Rue des Deux-Communes
93558 MONTREUIL CEDEX

Par lettre recommandée avec accusé de réception

LIEU, le DATE

Objet : Accès aux données du système Advance Passenger Information – Passenger Name Record (API-PNR France)

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 Advance Passenger Information – Passenger Name Record (API-PNR France).

En conséquence et en application de de l'article R232-22 du code de la sécurité intérieure, je vous demande de me communiquer les informations me concernant contenues dans le système Advance Passenger Information – Passenger Name Record (API-PNR France).

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

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

6.1 – Données concernées

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). 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.

6.2 – 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.

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

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

6.3 – 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).

6.4 – 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. Dans le doute, on peut appliquer la procédure qui était prévue pour Numérisation des procédures pénales : On peut 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).

Sinon, on peut toujours s'adresser à la CNIL, en lui citant cet article R249-14, et en lui demandant de transmettre aux autorités compétentes en application de cette formule.

7. 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).

7.1 – 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, pédopornographie, trafic d'armes, 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.

7.2 – Utilisation de REDEX

Les juges et procureurs peuvent avoir accès au REDEX.

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

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

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

7.3 – 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).

7.4 – 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).

8. 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.

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

8.1 – 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

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

8.2 – Utilisation du DUP

Ont accès au fichier : les avocat·es, la protection judiciaire de la jeunesse, les juges d'instruction et les juges des enfants (pas les flics), ainsi que le mineur·e lui-même 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.

8.3 – 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.

8.4 – 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 conditiion 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 entrera en vigueur 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.

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

Il est régi par les articles R57-4-1 à R57-4-10 du Code de procédure pénale et 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, GIDE et le casier judiciaire.

9.1 – 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.

LEXPÉDITEUR

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) :

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

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.

9.2 – 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 taule, la protection judiciaire de la jeunesse, les greffe, et même certains matons.

9.3 – Durée de conservation des données

Les données sont conservées 5 ans à compter de la fin de la peine (article R57-4-4 du Code de procédure pénale).

9.4 – 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 R57-4-7).

10. 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.

10.1 – 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 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.

10.2 – Utilisation du FND

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

10.3 – 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.

10.4 – 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.

11. GENESIS

Gestion nationale des personnes détenues en établissement pénitentiaire (GENESIS) a été créé par le décret n°2014-558 du 30 mai 2014, il apparaît aux articles R57-9-18 et suivants du Code de procédure pénale. Il remplace GIDE (Gestion Informatisée des Détenus en Établissement) depuis le 1er janvier 2017. Il devrait aussi remplacer le Fichier National des Détenus (FND, Fichier national automatisé des personnes incarcérées).

11.1 – 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 « *recueillir 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* ». Donc toute personne qui serait soupçonnée de porter atteinte à la sécurité des taules est susceptible d'être fichée dans GENESIS.

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 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 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 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

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 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).

11.2 – 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, aux juridictions étrangères 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), aux institutions de retraite et aux organismes de formation (idem).

11.3 – Conservation des données

Les données sont conservées 2 ans à compter de la levée d'écrou (article R57-9-21 du Code de procédure pénale).

11.4 – 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 R57-9-24) directement auprès du directeur de la taule.

Par contre, ce même directeur a des pouvoirs importants (article R57-9-24 II). 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 I 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 107 III de la loi du 6 janvier 1978 et article R57-9-24 du code de procédure pénale). Cependant la loi a tout prévu : le directeur de la taule peut même refuser d'informer la personne de son refus de rectification ou d'effacement des données (article 107 II 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…

12. 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, et la dernière est une circulaire du 15 octobre 2012.

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

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

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. L'ensemble est dans une note de la Direction de l'Administration pénitentiaire du 8 novembre 2013, non publiée.

Selon l'OIP, en 2014, il y avait environ 300 personnes concernées par ce régime d'exception en prison.

12.1 – Données concernées

Le Répertoire des Détenus Particulièrement Signalés concerne les détenu·es qui sont susceptibles de s'évader et dont l'évasion constituerait une atteinte importante à l'ordre public, ainsi qu'aux détenus ayant un comportement violent en détention. Il vise les personnes appartenant à la criminalité organisée, ou ayant un projet d'évasion, ou susceptibles d'être aidées par des organisations criminelles ou terroristes, ou dont l'évasion pourrait avoir un impact important sur l'ordre public, ou étant susceptibles d'actes de grande violence en détention. C'est le ministre de la justice qui décide qui est inscrit·e, après avis du personnel de la taule, et après que le ou la détenu·e concerné·e ait pu se défendre (sauf urgence bien sûr, il ne faudrait quand même pas que les détenu·es puissent se défendre convenablement).

12.2 – 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.

12.3 – 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, à porter devant le tribunal administratif dont dépend la taule, avec un·e avocat·e.

13. 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).

14. 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 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.

15. DataJust

Il a été créé par décret le 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.

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

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

Expéditeur :

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

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

Partie 3 : Fichiers de police : fichiers administratifs et fichiers généraux

Ils ne sont pas abordés ici. Il s'agit par exemple des fichiers suivants :

- AGRIPPA (Application de gestion du répertoire informatisé des propriétaires et possesseurs d'armes) qui recense tous les détenteurs d'armes ;
- FINIADA (Fichier national des personnes interdites d'acquisition d'armes) ;
- Fichier de suivi des personnes faisant l'objet d'une rétention administrative ;
- Fichier des personnes nées à l'étranger de la Gendarmerie nationale ;
- Fichier de la batellerie… Il y en a beaucoup.

Par contre, on va faire un point sur le système des mains-courantes informatisées (N-MCI / MCPN), qui n'est pas seulement un fichier administratif, mais aussi un fichier judiciaire et de renseignement.

On va voir aussi GendNotes et iGAV, qui concernent beaucoup de monde, ainsi que ADOC et SINUS/SI-VIC.

1. 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 flics. Il est régi par l'arrêté du 22 juin 2011 modifié par l'arrêté du 9 août 2016.

Tous les flics 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 formées aux violences conjugales).

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

1.1 – 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 champs libre pour décrire les détails qu'ils veulent sur l'événement enregistré dans la fiche.

1.2 – 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.

1.3 – 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.

2. 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.

2.1 – Données concernées

C'est extrêmement large : les gendarmes peuvent recueillir « *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*

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 : I__I__I__I__I__I__I__I__I à _____

Votre adresse : _____

_____

Code postal I__I__I__I__I__I Commune : _____

Pays: _____

Adresse courriel : _____@_____

Numéro de téléphone: I__I__I__I__I__I__I__I__I__I__I

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)* :

_____

_____

_____

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).

2.2 – 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 !

2.3 – 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.

2.4 – 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.

3. 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.

Il a pour objet la gestion et le suivi des gardes à vue.

3.1 – 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. »

3.2 – 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.

3.3 – 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 dernières années, 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.

3.4 – Droit de consultation, de rectification et d'effacement des données

L'article R15-33-82 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 prévoit qu'il faut s'adresser au responsable du traitement. Même si le décret (qui crée l'article R…) n'a pas été mis à jour depuis l'adoption de la loi, cette dernière, plus récente et plus « forte » juridiquement, doit s'appliquer.

En conséquence, il faut s'adresser au ministère de l'intérieur, Place Beauvau, 75800 PARIS CEDEX 08.

4. 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.

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

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 importants : conduite sans permis, conduite sans assurance, violation du confinement, et surtout consommation de stupéfiants.

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

4.1 – Données concernées

Le fichier ADOC concerne maintenant presque toutes les contraventions, et même certains délits (conduite sans permis, sans assurance, usage de stupéfiants, et quelques autres délits).

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.

4.2 – 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.

4.3 – 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.

4.4 – 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.

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) – ainsi, si la procédure est classée sans suite, on n'a pas la possibilité de faire effacer ses données, sauf à l'obtenir en justice… et là encore c'est compliqué, 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.

5. 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 fait un mouchard des flics à l'intérieur des hôpitaux[2].

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).

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[3]). 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

2 https://rebellyon.info/Fichier-SIVIC-et-fichage-des-manifestant-20576
3 Le Canard Enchaîné, 24 avril 2019

- Gestion de l'information et la prévention des atteintes à la sécurité publique (GIPASP article R236-29 du Code de la sécurité intérieure) ;
- 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) ;
- 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 ;
- 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 du Règlement n°2016/679 (RGPD), 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 :

- Fichier des personnes recherchées (FPR, article 9 du décret n°2010-569 du 28 mai 2010).
- Automatisation de la consultation centralisée de renseignements et de données (ACCReD, article 8 du décret n°2017-1224 du 3 août 2017) ;
- Fichier des Objets et Véhicules Signalés (FOVeS, article 8 de l’arrêté du 7 juillet 2017).
- Fichier du Système d’informations Schengen N-SIS II, article R231-12 du code de la sécurité intérieure.
- 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) ;
- Fichier Central de la Criminalité Organisée (F2CO) et Fichier des Brigades Spécialisées ;
- Enquêtes administratives liées à la sécurité publique (EASP, article R236-9 du code de la sécurité intérieure) ;
- Application relative à la prévention des atteintes à la sécurité publique (PASP, article R236-19 du code de la sécurité intérieure) ;

(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, les données sont 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).

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.

Partie 4 : Fichiers de police : fichiers d'antécédents

Les fichiers d'antécédents servent à connaître les précédentes mises en examen, condamnations et suspicions autour d'une personne. Il s'agit du casier judiciaire (qui est un fichier de justice, donc on l'a vu dans la partie précédente, qui sert notamment pour déterminer si une personne est en état de récidive ou pas) et du Traitement d'antécédents judiciaires (TAJ, qui permet de dire si une personne est « *connue des services de police* »). Dans le TAJ, il n'y a pas seulement les condamnations, mais aussi les victimes. Il est connu parce qu'il est truffé d'erreurs… ainsi, un·e auteur·e peut être enregistré·e comme victime et vice-versa.

Ces fichiers servent principalement à 2 choses :

- Savoir si une personne est « *connue des services de police* » : si on est inscrit·e au TAJ, on est connu·e des services de police.
- Ces fichiers sont aussi consultés lors des enquêtes administratives, qui ont lieu pour donner l'accès à une personne à certaines professions, certains emplois ou certains lieux (prison, nucléaire, …)

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.

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.

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.

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

- 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) ;
- 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 ;
- 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 du Règlement n°2016/679 (RGPD), 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 :

- Fichier des personnes recherchées (FPR, article 9 du décret n°2010-569 du 28 mai 2010).
- Automatisation de la consultation centralisée de renseignements et de données (ACCReD, article 8 du décret n°2017-1224 du 3 août 2017) ;
- Fichier des Objets et Véhicules Signalés (FOVeS, article 8 de l'arrêté du 7 juillet 2017).
- Fichier du Système d'informations Schengen N-SIS II, article R231-12 du code de la sécurité intérieure.
- 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) ;
- Fichier Central de la Criminalité Organisée (F2CO) et Fichier des Brigades Spécialisées ;
- Enquêtes administratives liées à la sécurité publique (EASP, article R236-9 du code de la sécurité intérieure) ;
- Application relative à la prévention des atteintes à la sécurité publique (PASP, article R236-19 du code de la sécurité intérieure) ;
- Gestion de l'information et la prévention des atteintes à la sécurité publique (GIPASP article R236-29 du Code de la sécurité intérieure) ;
- Conservation, gestion et exploitation électroniques des documents des services de renseignement territorial, article R236-51 du code de la sécurité intérieure ;

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

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).

Attention, la reconnaissance faciale dans le TAJ est autorisée (article R40-26 1° et 3° du code de procédure pénale). 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. Ça ne veut pas dire qu'elle le fera systématiquement. Pour l'instant, il est rare que la reconnaissance faciale soit utilisée au tribunal, mais ça arrive, par exemple à Lyon le 17 septembre 2019[4].

Le TAJ, c'est énormément de fiches, 15,6 millions en 2016. Selon la CNIL, il y avait environ 9,5 millions de personnes fichées dans le TAJ en 2015.

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,

4 https://rebellyon.info/A-Lyon-la-gendarmerie-utilise-la-21118

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, 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.

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 au acquittement : 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).

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'INTÉRIEUR

Recueil des empreintes

POUR LES DEMANDES DE CARTE NATIONALE D'IDENTITE UNIQUEMENT

AVERTISSEMENT : La numérisation des empreintes digitales et leur enregistrement dans la base « Titres électroniques sécurisés » (TES) protège contre l'usurpation d'identité, notamment en cas de perte ou de vol du titre. En l'absence de numérisation des empreintes, la transmission dématérialisée de ces données au service instructeur est impossible, conduisant ainsi à l'allongement du délai de délivrance de la carte nationale d'identité.

☐ **Je refuse qu'il soit procédé à la numérisation de mes empreintes digitales lors du dépôt de ma demande de carte nationale d'identité et à leur enregistrement dans la base TES.**

Je suis informé(e) qu'en conséquence, conformément à l'article 4-3 du décret n° 55-1397 du 22 octobre 1955, mes deux empreintes digitales seront recueillies sur le présent formulaire et conservées de manière sécurisée par le service instructeur de ma demande pendant la durée prévue aux dispositions du cinquième alinéa du même article (20 ans pour un majeur et 15 ans pour un mineur).

Nom : ……

Prénom(s) :……

Né le …… **A**……

Partie complétée par l'administration :

Numéro de la demande :……

Lieu de dépôt de la demande :……

Date de dépôt de la demande :……

Empreinte de la main gauche (index)

Empreinte de la main droite (index)

Si une autre empreinte a été prise, précisez, pour chaque main, s'il s'agit :

☐ du majeur ☐ du majeur

☐ de l'annulaire ☐ de l'annulaire

Signature du demandeur : **Date :**

(ou du représentant légal)

- S’il y a eu ordonnance de non-lieu ou classement sans suite (par exemple, rappel à la loi) : 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).

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.

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 de rappel à la loi. Cependant, le rappel à la loi peut être assimilé à un classement sans suite. A priori, c'est donc 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

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, 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, 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 concerne peut provoquer la création d'une fiche à notre nom !

Page suivante, vous trouverez le formulaire qui permet de demander une carte nationale d'identité sans que ses empreintes digitales soient numérisées et versées dans le fichier TES (sans intérêt si vous avez déjà un passeport numérique) :

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) c'est la même chose, 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. STIC

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

3. JUDEX

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

4. 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 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).

LRPPN doit être remplacé au cours de l'année 2021 par SCRIBE.

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

4.1 – 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.

4.2 – 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, acquisition de la nationalité française).

4.3 – Conservation des données

Les textes ne prévoient pas de durée maximale de conservation des données.

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

L'article 6 du décret n°2011-110 du 27 janvier 2011 (LRPPN) et l'article 7 du décret n°2011-111 du 27 janvier 2011 (LRPGN) prévoient 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 prévoit qu'il faut s'adresser au responsable du traitement. Même si le décret n'a pas été mis à jour depuis l'adoption de la loi, cette dernière, plus récente et plus « forte » juridiquement, doit s'appliquer.

En conséquence, la loi s'applique et il faut s'adresser au ministre 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°).

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 est 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 spéciale 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).

- 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).

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 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

En cas de refus du ministre, ou de son silence pendant 2 mois à compter de sa réception de la demande, on peut former un recours devant la CNIL (3 place de Fontenoy, TSA 80715, 75334 PARIS CEDEX 07).

Pour la rectification et l'effacement, il faut aussi s'adresser au ministre de l'intérieur (article 106 de la loi n°78-17 du 6 janvier 1978). En cas de refus ou de silence pendant 2 mois du ministre, le recours s'effectue également devant la CNIL.

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

5. 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 présente lui-même comme un fichier d'antécédents judiciaires, nominatif.

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.

5.1 – 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).

5.2 – Utilisation des données

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

5.3 – 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.

5.4 – Accès, rectification, effacement des données

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

On peut seulement en demander l'accès et la rectification, l'article 6 de l'arrêté du 12 janvier 2016 prévoit qu'il faut s'adresser à 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 prévoit 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, plus récente et plus « forte » juridiquement, doit s'appliquer.

En conséquence, la loi s'applique et il faut s'adresser au ministère de l'intérieur, Place Beauvau, 75800 PARIS CEDEX 08.

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 ;
- 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).

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

Attention, pour 4 fichiers (FPR, API-PNR, N-SIS II, FoVES), 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 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).

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)

e – Fichiers à demander à la préfecture

2 fichiers 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 7 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

Partie 5 : Fichiers de police : fichiers d'identification

Ces fichiers-là servent à identifier une personne. Le plus simple pour comprendre le fonctionnement, c'est : Les flics relèvent une empreinte digitale sur une voiture volée, puis ils cherchent dans leur fichier une empreinte digitale similaire. Ils ne cherchent alors que dans leurs fichiers de flics, pas dans tous les fichiers, donc pour que les flics retrouvent à qui appartient l'empreinte, il faut que la personne ait déjà, dans le passé, au cours de n'importe quelle enquête, donné son empreinte aux flics. Donc, si la personne a seulement un passeport biométrique et est fichée au TES, les flics ne la retrouveront pas de cette manière-là ; en effet ils ne recherchent pas dans le fichier des passeports biométriques, qui n'est pas un fichier de police.

Bien sûr, il y a une exception : En cas d'atteinte aux intérêts fondamentaux de la nation ou en cas de terrorisme, les flics peuvent consulter le TES (fichier des passeports et des cartes d'identité, article L222-1 du code de la sécurité intérieure).

Enfin, c'est possible d'obtenir une carte d'identité (mais pas un passeport) en refusant la numérisation de ses empreintes digitales (attention, on les donne quand même, mais « à l'ancienne », avec de l'encre, article 4-3 II du décret n°55-1397 du 22 octobre 1955). Le formulaire est disponible ici : http://www.dordogne.gouv.fr/content/download/23497/171854/file/formulaire%20empreintes.pdf et en annexe de cet article.

1. Fichier automatisé des empreintes digitales (FAED)

C'est un fichier ancien, ancien, 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.

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 76-1 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 L611-1-1, L611-3, L611-4 du Code de l'entrée et du séjour des étrangers et des demandeurs d'asile). Les empreintes peuvent aussi être prises sur une personne décédée, pour l'identifier.

Quand on rentre en garde-à-vue pour une enquête de flagrance ou pour une enquête préliminaire (c'est le cas dans la plupart des garde-à-vue), les flics prennent systématiquement nos empreintes et notre photo. 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 qu'on va prendre systématiquement cette peine, mais la peine prononcée varie beaucoup, de presque rien lorsqu'on est relaxé pour le délit pour lequel on est rentré en garde-à-vue, à quelques centaines d'euros d'amende et quelques mois de prison, le plus souvent avec sursis, lorsqu'on est condamné pour le délit principal.

1.2 – 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).

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).

1.3 – Droit d'accès et de rectification

Le droit d'accès et de rectification s'exerce de manière directe (article 6 du décret n°87-249 du 8 avril 1987).

Pour exercer son droit d'accès aux données, il faut envoyer une lettre recommandée avec accusé de réception au Chef du service central de la police technique et scientifique, ministère de l'intérieur, place Beauvau, 75800 PARIS Cedex 08. Voir un modèle de lettre en annexes.

Pour demander la rectification ou la suppression des données, il faut envoyer une 2e 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 pièce-jointe.

- Numérisation des procédures pénales (NPP) : il faut s'adresser au procureur de la République en charge de la procédure (arrêté du 16 janvier 2008).
- 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

c – Fichiers à demander au ministère de la justice

Pour 3 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).

d – Fichiers à demander au procureur de la République

Pour 12 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.

Si le procureur refuse la suppression, on 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 »), on a 10 jours à compter de la date de ce refus. Si 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 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.

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.

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 6 fois) et aujourd'hui les flics peuvent faire un prélèvement d'ADN presque pour un oui ou pour un non.

Aujourd'hui, les règles qui l'organisent sont aux articles 706-54 et suivants et R53-9 et suivants du code de procédure pénale.

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, même à l'encontre d'un flic (article 433-5 du code pénal) ou au drapeau (433-5-1) ;
- Rébellion, même à l'encontre d'un flic (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) ;
- 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 ;
- La dissimulation du visage dans l'espace public ;
- Le recel (articles 321-1 et suivants du code pénal) ;
- Provocation et participation délictueuse à un attroupement avec ou sans arme (articles 431-3 et suivants du code pénal).

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 qu'on va prendre systématiquement cette peine, mais la peine prononcée varie beaucoup, de presque rien lorsqu'on est relaxé pour le délit pour lequel on est rentré en garde-à-vue, à quelques centaines d'euros d'amende et quelques mois de prison, le plus souvent avec sursis, lorsqu'on est condamné pour le délit principal. Aussi, si on refuse le prélèvement ADN alors qu'on est déjà condamné·e, cela enlève tout droit à des réductions de peine (mais on peut encore bénéficier d'aménagements de peine) (article 706-55 III du code de procédure pénale).

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

- 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) ;
- 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).

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

Les 6 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, 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).

- 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).

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

- Le Fichier Automatisé des Empreintes Digitales (FAED) : Le droit d'accès et de rectification s'exerce auprès du Chef du service central de la police technique et scientifique, ministère de l'intérieur, Place Beauvau, 75800 PARIS Cedex 08 (article 6 du décret n°87-249 du 8 avril 1987) ;
- Le Fichier National Automatisé des Empreintes Génétiques (FNAEG) : Comme pour le FAED, mais pour la demande de suppression il faut utiliser le Cerfa n°12411*02 ;
- 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) ;

2.2 – Durée de conservation des données

Les données sont conservées pendant 40 ans (article R53-14 du code de procédure pénale). Cependant, si l'ADN a été prélevé sur une personne suspectée d'un crime ou d'un délit susceptible d'entraîner ce prélèvement, et que cette personne n'a pas été condamnée ensuite, les données sont conservées 25 ans (même article).

2.3 – Droit d'accès et de rectification

Pour l'accès aux données, il faut envoyer une lettre recommandée avec accusé de réception au Chef du service central de la police technique et scientifique, ministère de l'intérieur, place Beauvau, 75800 PARIS Cedex 08 (article R53-15 du code de procédure pénale). Voir un modèle de lettre en pièce-jointe.

Pour la rectification et la demande d'effacement des données, il faut remplir le Cerfa n°12411*02 et l'envoyer au procureur de la République compétent, c'est-à-dire regarder où l'ADN a été prélevé, regarder quel Tribunal judiciaire est compétent, et l'envoyer au procureur de ce Tribunal judiciaire en lettre recommandée avec accusé de réception (article R53-13-1 du code de procédure pénale).

Si le procureur refuse la suppression, on a 10 jours pour contester ce refus (article R53-13-2 du code de procédure pénale). Donc s'il y a refus expresse (réponse du procureur qui dit « non »), on a 10 jours à compter de la date de ce refus. Si 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 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·e avocat·e. 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.

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, avec une lettre recommandée avec accusé de réception (article R53-13-4). Mais là, il faut vraiment un·e avocat·e.

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 la décision 2008/615/JAI.

Cette décision prévoit une interconnexion de très nombreux fichiers de police de chaque pays membre de l'Union européenne : empreintes génétiques (FNAEG en France), empreintes digitales (FAED en France), 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).

Le principe est que les services concernés de chaque État peut interroger les autres États afin de savoir s'ils détiennent des informations sur une personne, et lesquelles.

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. On peut donc s'adresser à la CNIL.

4. 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.

4.1 – Données contenues dans 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). 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 si le juge d'instruction le demande. Il ne concerne pas les personnes condamnées pour apologie d'actes de terrorisme, ni pour transmission d'apologie d'actes de terrorisme.

- 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 ;
- Enquêtes administratives liées à la sécurité publique (EASP, article R236-9 du code de la sécurité intérieure) ;
- Application relative à la prévention des atteintes à la sécurité publique (PASP, article R236-19 du code de la sécurité intérieure) ;
- Gestion de l'information et la prévention des atteintes à la sécurité publique (GIPASP article R236-29 du Code de la sécurité intérieure) ;
- 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) ;
- 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 ;
- SIREX, article R841-2 3° du code de la sécurité intérieure ;

Partie 9 : Récapitulatif du droit d'accès, de rectification et d'effacement

La loi de 1978 et le RGPD prévoient qu'on a un droit d'accès aux informations nous concernant. Pour certaines informations, on y a à peu près accès – encore faut-il savoir qu'une institution a rassemblé ces informations et les conserve. On peut aussi demander leur rectification et leur effacement (ce qui est toujours un peu plus compliqué). Pour d'autres informations, notamment tous les fichiers classés « secret-défense », il y a des procédures qui existent… 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 l'intéressé, 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 de 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 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) ;

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.

4.2 – Durée de conservation des données

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

4.3 – Droit de communication, de rectification et de suppression des données

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.

5. 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.

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

5.2 – 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.

5.3 – Droit de communication, de rectification et de suppression des données

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 706-53-9 et 706-53-10 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.

6. 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).

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).

6.1 – 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. 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*

7. Fichier National des Interdits de Stade (FNIS)

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 prévoit qu'il faut s'adresser au responsable du traitement. Même si le décret (qui crée l'article R…) n'a pas été mis à jour depuis l'adoption de la loi, cette dernière, plus récente et plus « forte » juridiquement, doit s'appliquer.

En conséquence, la loi s'applique et il faut s'adresser à la Direction générale de la police nationale, Place Beauvau, 75800 PARIS CEDEX 08.

8. 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.

8.1 – 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.

8.2 – Durée de conservation des données

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

8.3 – 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.

janvier 1978 tels que modifiés par l'ordonnance n°2018-1125 du 12 décembre 2018, qui prévoit qu'il faut s'adresser au responsable du traitement. Même si le décret (qui crée l'article R…) n'a pas été mis à jour depuis l'adoption de la loi, cette dernière, plus récente et plus « forte » juridiquement, doit s'appliquer.

En conséquence, la loi s'applique et il faut s'adresser à la Direction générale de la gendarmerie nationale, 4 rue Claude Bernard, CS60003, 92136 ISSY-LES-MOULINEAUX CEDEX.

6. Sécurisation des interventions et demandes particulières de protection

Direction générale de la gendarmerie nationale (ministère de l'intérieur).

articles R236-38 et suivants du code de la sécurité intérieure.

6.1 – Objectifs et données collectées

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, et personnes demandant une intervention, et personnes se trouvant dans une situation de vulnérabilité particulière.

Concerne tout le monde à partir de 13 ans.

6.2 – Durée de conservation des données

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.

6.3 – 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 prévoit qu'il faut s'adresser au responsable du traitement. Même si le décret (qui crée l'article R…) n'a pas été mis à jour depuis l'adoption de la loi, cette dernière, plus récente et plus « forte » juridiquement, doit s'appliquer.

En conséquence, la loi s'applique et il faut s'adresser à la Direction générale de la gendarmerie nationale, 4 rue Claude Bernard, CS60003, 92136 ISSY-LES-MOULINEAUX CEDEX.

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).

6.2 – 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 ùprocureur en prescrit l'effacement (idem).

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

Il faut distinguer que l'enquête soit en cours ou qu'elle soit 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.

L'article R40-36 prévoit que ces droits s'exercent également auprès de la CNIL qui transmettra au responsable du traitement. 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 prévoit qu'il faut s'adresser au responsable du traitement. Même si le décret (qui crée l'article R…) n'a pas été mis à jour depuis l'adoption de la loi, cette dernière, plus récente et plus « forte » juridiquement, doit s'appliquer. En conséquence, la loi s'applique et il faut s'adresser à la Direction générale de la police nationale et à la Direction générale de la gendarmerie nationale (articles 230-12 et R40-36 du code de procédure pénale et 104 à 106 de la loi du 6 janvier 1978).

Lorsque l'enquête est terminée, en plus des règles précédentes, celles-ci s'appliquent :

Si l'auteur a été définitivement condamné, il 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 soit au procureur de la République compétent, soit au magistrat spécialisé, mais on peut aussi s'adresser à la DGPN et à la DGGN.

7. 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).

Le fichier est interconnecté avec le FoVES et N-SIS II.

Cependant, LAPI ne permet pas une consultation et une gestion centralisées des données. Assez rapidement, LAPI sera 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, le STCL devrait donc arriver sous peu.

7.1 – Règles relatives à ce qui est écrit dans le fichier

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.

7.2 – Durée de conservation des données

Les données sont conservées 8 jours.

4.1 – Ce qui peut être intercepté

L'article R40-43 du code de procédure pénale définit les données qui peuvent être interceptées. Ce sont celles relatives à toute personne en fuite (article 74-2 CPP), c'est large, les personnes disparues (article 80-4 CPP), les personnes qui font l'objet d'une instruction et qui encourent une peine d'au moins 3 ans d'emprisonnement (article 100 CPP), les personnes qui font l'objet d'une enquête pour criminalité organisée (articles 706-95, 706-95-1, 706-73, 706-73-1, c'est large), et même toutes les personnes qui font l'objet d'une enquête de flagrance ou d'une enquête préliminaire.

Les données recueillies sont vraiment très nombreuses, jusqu'aux écoutes téléphoniques et à la géolocalisation (article R40-46 CPP).

4.2 – Droit d'accès et de rectification

Cependant, l'article R40-55 du code de procédure pénale 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 prévoit qu'il faut s'adresser au responsable du traitement. Même si le décret (qui crée l'article R…) n'a pas été mis à jour depuis l'adoption de la loi, cette dernière, plus récente et plus « forte » juridiquement, doit s'appliquer.

En conséquence, la loi s'applique et il faut s'adresser au ministère de la justice, 13 Place Vendôme, 75042 PARIS CEDEX 01.

5. Gestion des sollicitations et des interventions

articles R236-31 et suivants du code de la sécurité intérieure.

Mis en œuvre par la Direction générale de la gendarmerie nationale (ministère de l'intérieur).

5.1 – Objectifs et données collectées

Enregistrement des appels vers les centres d'appel de la gendarmerie.

5.2 – Durée de conservation des données

2 ans.

5.3 – Droit d'accès

L'article R236-37 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

3.1 – Données collectées et finalités

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.

3.2 – Durée de conservation des données

5 ans (article L232-7 IV du code de la sécurité intérieure).

3.3 – Droits d'accès et de rectification

L'exercice de ces droits est régi par l'article R232-18. Pour la plupart des données : S'adresser directement au Directeur de l'Unité Information Passagers, 11 Rue des Deux-Communes, 93558 MONTREUIL CEDEX.

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.

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

Cette agence est sous la tutelle du ministère de la justice. Le texte qui la crée est à l'article 230-45 du code de procédure pénale.

En cas de rapprochement avec le FoVES ou N-SIS II, elles sont conservées 1 mois.

7.3 – 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 prévoit qu'il faut s'adresser au responsable du traitement. Même si le décret (qui crée l'article R…) n'a pas été mis à jour depuis l'adoption de la loi, cette dernière, plus récente et plus « forte » juridiquement, doit s'appliquer.

En conséquence, la loi s'applique et il faut s'adresser au ministère de l'intérieur, Place Beauvau, 75800 PARIS CEDEX 08.

8. Fichier central de la criminalité organisée (F2CO) et Fichier des brigades spécialisées

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.

Cependant, on n'a trouvé nulle part une trace de la réglementation relative à ces deux fichiers.

Partie 6 : Fichiers de police : rapprochement automatique et manuel

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. DPIO, lui, est un fichier de rapprochement manuel : c'est la même chose mais en moins performant (ce n'est pas la machine qui détecte des similitudes, mais le flic). Quant à LUPIN on ne sait pas trop.

1. 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.

1.1 – 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.

1.2 – 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.

1.3 – 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.

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.

2.2 – Durée de conservation des données

article R231-11 CSI : Pour les personnes, 3 ans par défaut, mais lorsqu'il s'agit de contrôle discret, 1 an seulement. Pour les objets, 10 ans par défaut, mais 5 ans lorsqu'il s'agit de contrôle discret.

Bien sûr, prolongations possibles.

2.3 – Droits d'accès et de rectification

Droit de communication indirecte 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.

Et attention : Il y a un droit de communication direct auprès de la Direction centrale 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 et les motifs du signalement pour personnes concernées par ça au FPR aussi, et pour les objets perdus, volés ou détournés.

3. API-PNR France (Advance Passenger Information – Passenger Name Record)

Volet français du système PNR.

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) sous la tutelle du ministère des douanes.

Le PNR actuel ne concerne que les voyages aériens. Cependant, le gouvernement a, en décembre 2019, créé le Service national des données de voyage (SNDV), rattaché au directeur général de la police national, afin 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).

***1.3* – 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).

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).

2. Système d'information Schengen (N-SIS II)

Au niveau européen, 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, sous la responsabilité du ministère de l'intérieur. Les règles qui l'encadrent au niveau national sont aux articles R231-5 et suivants du code de la sécurité intérieure.

2.1 – Données concernées

Personnes visées par un mandat d'arrêt européen ou par une extradition, personnes visées par une non-admission ou une interdiction de séjour à la suite d'une décision administrative ou judiciaire, personnes disparues, 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, personnes visées par l'exécution d'une peine.

Et aussi : Véhicules à moteur, embarcations, avions, remorques, armes à feu, documents officiels volés ou détournés, billets de banque, moyens de paiement volés ou égarés, conteneurs…

Attention, N-SIS II permet de consulter et d'alimenter le FOVeS et le FPR.

Il permet en outre d'alimenter (et non de consulter) le TES et DOCVERIF (fichier ayant pour but la vérification de la validité des titres d'identité et des cartes de séjour).

N-SIS II permet de consulter (et non d'alimenter) COVADIS (contrôle et vérification automatiques des documents d'identité sécurisés), PARAFE (passage automatisé aux frontières extérieures, un système auquel chacun·e peut s'inscrire et qui permet de passer plus vite la douane aux aéroports), RMV (Réseau Mondial des Visas), SETRADER (fichier des passagers aériens), API-PNR (comme SETRADER mais plus large), AGDREF (Application de gestion des dossiers

2. 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).

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 flics 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 ne rapproche pas automatiquement les données et les affaires ; ce sont des flics et des gendarmes (donc des humain·es, quoi qu'on en pense) qui analysent les données manuellement.

2.1 – Données concernées

Il traite des données recueillies au cours d'enquêtes préliminaires, d'enquêtes de flagrances et de commissions rogatoires (instructions) à propos de crime et de délit. 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).

2.2 – Durée de conservation des données

Les données relatives à un délit sont conservées 3 ans, celles relatives à un crime sont conservées 10 ans (article 4 du décret n°2014-187 du 20 février 2014).

2.3 – 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 prévoit qu'il faut s'adresser au responsable du traitement. Même si le décret (qui crée l'article R…) n'a pas été mis à jour depuis l'adoption de la loi, cette dernière, plus récente et plus « forte » juridiquement, doit s'appliquer.

En conséquence, la loi s'applique et il faut s'adresser au ministère de l'intérieur, Place Beauvau, 75800 PARIS CEDEX 08.

3. 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.

3.1 – 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.

3.2 – 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).

3.3 – 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 prévoit qu'il faut s'adresser au responsable du traitement. Même si le décret (qui crée l'article R…) n'a pas été mis à jour depuis l'adoption de la loi, cette dernière, plus récente et plus « forte » juridiquement, doit s'appliquer.

En conséquence, la loi s'applique et il faut s'adresser au ministère de l'intérieur, Place Beauvau, 75800 PARIS CEDEX 08.

- 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.

1.2 – 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).

Partie 8 : Autres fichiers et données recueillies

Cette partie concerne de nombreux fichiers qui n'ont rien à voir entre eux. Peut-être certains appartiennent aux catégories précédentes, mais nous n'avons pas pu l'établir avec certitude. Certains fichiers n'apparaissent pas dans cette partie, et sont pourtant très semblables à ceux qui y figurent. Par exemple, il est question ici du système API-PNR France (qui recense tous les passagers des avions atterrissant ou décollant du territoire français), mais pas du système PARAFE, qui permet de passer le contrôle des passeports automatiquement, sans file d'attente. Eh bien, si vous avez fait les démarches pour vous inscrire sur PARAFE et leur donner toutes vos données personnelles et biométriques pour éviter la queue à l'aéroport, vous pouvez aller voir aux articles R232-6 et suivants du code de la sécurité intérieure pour essayer de faire effacer vos données !

1. 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 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, transport public de personnes, jeux, paris, utilisation de matières dangereuses, grand événement exposé à un risque terroriste…)… 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.

1.1 – 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 :

Partie 7 : Fichiers 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, ces derniers temps 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 du SCRT (c'est les ex-RG-DST, qui sont devenus en 2008 les DCRI et SDIG, qui sont devenus en 2014 la DGSI et le SCRT). Le SCRT dépend de la Direction générale de la police nationale, et a 63 antennes locales. À Paris, en Seine-Saint-Denis, dans le Val-de-Marne et dans les Hauts-de-Seine, le SCRT n'opère pas, ses missions sont remplies par la direction du renseignement de la préfecture de police de Paris. En zone gendarmerie, la sous-direction de l'anticipation opérationnelle (SDAO) participe au SCRT.

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). Aujourd'hui, 580'000 personnes sont inscrites au FPR.

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 données 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.

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.

Le FPR peut aussi contenir des photographies, des documents type « mandat d'arrêt » et autres.

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, 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.

19. 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.

20. 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.

21. Fichier alphabétique de renseignement de la gendarmerie (FAR)

Supprimé en 2010, remplacé par ATHEN@ puis par le système GIPASP/BDSP.

22. ARAMIS

Supprimé et remplacé par ATHEN@ puis par le système GIPASP/BDSP.

Il est 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.

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).

Ce fichier SIREX 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 1 décision du 5 mai 2017 (n°396669) 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.

18. 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).

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 décidée par un juge d'instruction (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.*	*Interdiction de porter ou de détenir une arme soumise à autorisation.*
			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 elle constituerait une menace pour l'ordre public (Fiche « TE » : Opposition à l'entrée en France).	Étrangers hors UE faisant l'objet d'une restriction de voyage adoptée par l'UE.	*Étranger qui n'a pas exécuté une OQTF, ou une 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).*	Étranger de nationalité suisse, islandaise, norvégienne ou d'un État membre de l'Union européenne ne résidant pas habituellement en France et qui fait l'objet d'une interdiction administrative du territoire français car il constituerait une menace réelle pour un intérêt fondamental de la société (articles L214-1 du CESEDA). Personne de nationalité autre qui ne réside pas habituellement en France et qui ne se trouve pas sur le territoire national dans la même situation (article L214-2 du CESEDA).
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.	
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.

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).

14. Fichier 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).

15. DOREMI (remplace le fichier de renseignement militaire de la DRM)

Mis en œuvre par la Direction du renseignement militaire (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).

16. Fichier des personnes étrangères de la Direction du renseignement militaire

Mis en œuvre par la Direction du renseignement militaire (ministère 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).

17. SIREX

Mis en œuvre par la Direction du renseignement et de la sécurité de la défense (DRSD, ministère des armées).

10. 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)

Le CAR a été créé par le décret n°2015-1465 du 10 novembre 2015, non publié. L'avis n°2015-128 du 23 avril 2015 de la CNIL n'est pas publié non plus. Il est mis en œuvre par la Direction de l'administration pénitentiaire.

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).

11. 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 (ministère de la justice). Donc a priori, il ne concerne que des personnes mineures.

Selon une rumeur sur le net, environ 30 personnes y étaient fichées en 2017.

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).

12. 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.

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).

13. Fichier d'informations nominatives de la DGSE

Mis en œuvre par la DGSE (ministère des armées).

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.*			
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 ».
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).*	*Interdiction de stade.*

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.*

Ce qui peut être important, c'est de savoir ce qui normalement n'apparaît plus dans le FPR, ces les données qui ont été supprimées du fichier, donc ce n'est pas normal si on se rend compte qu'elles y sont toujours :

- Depuis le 1er octobre 2014, le suivi socio-judiciaire dans le cadre du sursis mise à l'épreuve (interdiction de certaines activités, de paraître en certains lieux, d'entrer en relation avec certaines personnes) (article 230-19 7° ancien).
- Depuis la même date, interdictions de paraître dans certains lieux, de rencontrer certaines personnes ou de quitter le territoire, en cas de libération conditionnelle (article 230-19 11° ancien).
- La peine d'interdiction d'entrer dans certaines infrastructures aéroportuaires etc. prononcée pour exercice illégal de l'activité de taxi (article 230-19 13° ancien).

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 d'1 an qui peut être renouvelée.

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

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…).

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 ».

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* » (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).

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).

(article R841-2 du code de la sécurité intérieure) créée en 2015 (loi n°2015-912 du 24 juillet 2015, article R841-2 du code de la sécurité intérieure).

8. 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.

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).

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 (article 4 de la loi du 6 janvier 1978).

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).

9. 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 publiées 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 est mis en œuvre par l'Unité de Coordination de la Lutte Antiterroriste (UCLA, qui dépend de la Direction générale de la police nationale, ministère de l'intérieur), et les personnes fichées considérées comme les plus dangereuses sont suivies par la Direction Générale de la Sécurité Intérieure (DGSI), les autres par le Service Central du Renseignement Territorial (SCRT). Le SCRT, c'est les ex-RG-DST, qui sont devenus en 2008 les DCRI et SDIG, qui sont devenus en 2014 la DGSI et… le SCRT. L'UCLA, c'est un service de renseignement issu des RG, créé en… 1984.

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*

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.) ; 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, plutôt pensé pour les hommes d'affaire), FIJAISV (Fichier judiciaire automatisé des auteurs d'infractions sexuelles et violentes), AGDREF (Application de gestion des dossiers des ressortissants étrangers en France), N-SIS II (Système d'Informations Schengen II – National).

1.2 – Durée de conservation des données

L'article 7 du décret n°2010-569 prévoit l'effacement sans délai en cas d'aboutissement de la recherche ou extinction du motif d'inscription. Pour les OQTF des étrangers : effacement au plus tard 3 ans après la signature de l'OQTF.

Pour les fiches « S », elles sont conservées 2 ans, mais elles sont renouvelées aussi longtemps que la fiche apparaît nécessaire aux flics – et ça peut durer plusieurs années.

Pour tout le reste, on ne sait pas.

1.3 – Droit d'accès et de rectification

L'article 9 du décret n°2010-569 du 28 mai 2010 organise les règles pour le droit d'accès et de rectification, 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 et de rectification est direct, auprès de la Direction centrale de la police judiciaire, ministère de l'intérieur, Place Bauveau, 75008 PARIS CEDEX 08. Dans le tableau précédent, ce

sont toutes les cases écrites en *italiques*. Il y a un modèle de lettre en annexes pour faire la demande.

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 annexes vous trouverez un modèle de lettre à la CNIL (il s'agit du premier modèle, qui concerne de nombreux fichiers).

2. ACCReD

« 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).

2.1 – 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)
- la magistrature et les juges administratifs
- les flics, gendarmes, douaniers, militaires, matons, policiers municipaux
- les agents de sécurité

5.3 – Droit d'accès

En application des articles 118 et suivants de la loi n°78-17 du 6 janvier 1978 et l'article R236-29 du code de la sécurité intérieure, ces droits s'exercent auprès de la CNIL.

6. 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).

6.1 – 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 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.

6.2 – Durée de conservation des données

Les données sont conservées 20 ans.

6.3 – 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.

7. 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.

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'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

5. 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).

5.1 – Données concernées

Concerne « ***les personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique.*** *Le traitement a* ***notamment*** *pour finalité de recueillir, conserver et d’analyser les informations qui concernent les personnes susceptibles d’être impliquées dans des actions de violence collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives.* » (article R236-21 du code de la sécurité intérieure). Même remarque que pour PASP en ce qui concerne ce « *notamment* » : ça peut donc être ça, mais tout autre chose.

Les données peuvent concerner les **activités politiques, philosophiques, religieuses ou syndicales.**

Concerne toute personne à partir de 13 ans.

5.2 – 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.

- et de nombreux hauts fonctionnaires

Il est aussi consulté quand une personne demande une autorisation de port d’arme.

Attention, depuis 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 !

2.2 – 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, SIREX 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.

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!).

2.3 – 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).

2.4 – Droit d’accès aux 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 à avoir accès aux 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 communication des données.
- Concernant les données de fichiers de renseignement : L’article 8 III du même décret prévoit qu’il faut demander l’accès à ces données à la CNIL.

2.5 – Droit de rectification et d’effacement

Idem, le droit de rectification et d’effacement s’exerce selon 2 procédures 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 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 à la CNIL.

- Concernant les données de fichiers de renseignement : L'article 8 III du même décret prévoit qu'il faut demander l'accès à ces données à la CNIL.

  En cas de refus, on peut faire un recours devant le Conseil d'État, qui statue en sa formation spécialisée aux fichiers de renseignement.

3. Fichier Enquêtes administratives liées à la sécurité publique (EASP)

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.

3.1 – Données concernées

Il sert aux mêmes enquêtes administratives que celles pour lesquelles ACCReD est utilisé.

Il peut contenir beaucoup d'informations, et notamment, indirectement, les motivations politiques, religieuses, philosophiques ou syndicales.

Il concerne toute personne qui a postulé, âgée d'au moins 16 ans.

La personne est censée être informée que les informations qu'elle donne entrent dans le fichier (article R236-9 du code de la sécurité intérieure).

3.2 – Durée de conservation

Les données sont conservées 5 ans (article R236-4).

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

En application des articles 118 et suivants de la loi n°78-17 du 6 janvier 1978 et l'article R236-9 du code de la sécurité intérieure, ces droits s'exercent auprès de la CNIL.

4. 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 EASP et GIPASP, 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.

4.1 – Données concernées

Le plus simple, c'est de citer : « ***Notamment*** *pour finalité de recueillir, de conserver et d'analyser les informations qui concernent les personnes susceptibles d'être impliquées dans des actions de violence collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives* » (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 aussi.

PASP contient les **activités publiques de la personne**, son comportement, ses déplacements, **les personnes avec qui elle est en relation, ses activités politiques, philosophiques, religieuses ou syndicales.**

Il concerne tout le monde à partir de 13 ans.

4.2 – 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.

4.3 – Droit d'accès

En application des articles 118 et suivants de la loi n°78-17 du 6 janvier 1978 et l'article R236-19 du code de la sécurité intérieure, ces droits s'exercent auprès de la CNIL.