LA FOLLE VOLONTÉ
DE TOUT CONTRÔLER

---

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

Utilisation des données et procédures pour leur suppression

Septembre 2018
Version 1

Table des matières

1.1.1 Les différentes catégories de fichiers et leur utilisation

Tout d'abord, 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 parfois seulement pour un objectif précis, pas pour n'importe quoi.

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 le tout dernier 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 2, p.6). Suivent les fichiers de justice (Partie 3, p.9). Ensuite différents types de fichiers de police : les fichiers administratifs (Partie 4, p.19), qui recensent par exemple toutes les personnes ayant un permis pour porter ou détenir une arme ; les fichiers d'antécédents (Partie 5, p.20), qui rassemblent tous les antécédents judiciaires d'une personne ; les fichiers d'identification (Partie 6, p.24), 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 7, p.31), qui servent à analyser des données pour les recouper. Ensuite viennent les fichiers de renseignement, qui sont nombreux (8, p.34). Enfin viennent de nombreux autres fichiers (Partie 9, p.48), 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 10, p.54). 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.

En annexes viennent d'abord quelques schémas récapitulatifs : il s'agit de montrer dans quels fichiers on est susceptible d'être répertorié·e, et quels fichiers sont consultés, dans quelques situations (Annexes 1, p.60).

Enfin, pour rendre encore plus facile les démarches de consultation, de rectification et de suppression des données, un certain nombre de lettres-types sont rassemblées (Annexes 2, p.67).

Caisse de solidarité de Lyon
caissedesolidarite@riseup.net
06.43.08.50.32

2 FICHIERS D'IDENTIFICATION ADMINISTRATIVE

Aujourd'hui, il y a 2 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. 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.

2.1 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.

2.1.1 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.

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 et les actes de terrorisme. De même, les agents français en relation avec INTERPOL et avec N-SIS II (Schengen) peuvent accéder aux données.

Enfin, 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.

Aussi, 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).

2.1.2 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.

2.1.3 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 directement au Ministère : Ministère de l'intérieur, place Beauvau, 75800 PARIS Cedex 08.

2.2 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.

2.2.1 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, 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). C'est pourquoi lorsque quelqu'un·e donne une identité imaginaire et dit qu'il ou elle est titulaire du permis, 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.

2.2.2 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.

2.2.3 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).

2.3 Fichier relatif à la carte d'identité (FNG) et le Fichier relatif aux passeports (ancien TES)

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

2.4 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 la 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.

3 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.

Ensuite, il y a les fichiers qui servent en interne aux magistrats, avec CASSIOPÉE, une grosse machine à gaz qui permet de suivre toutes les procédures, passées et présentes, à l'encontre d'une personne.

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.

Enfin, en cas de condamnation, il y a les fichiers qui suivent les peines et la détention : APPI, FND, GENESIS et DPS.

3.1 Casier judiciaire national automatisé

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

3.1.1 Bulletin n°1

3.1.1.1 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.

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

3.1.1.2 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.

3.1.1.3 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 de Grande Instance 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.

3.1.2 Bulletin n°2

3.1.2.1 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 ».

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.

3.1.2.2 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.

3.1.2.3 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).

3.1.3 Bulletin n°3

3.1.3.1 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. Il 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…

3.1.3.2 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.

3.1.3.3 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://www.cjn.justice.gouv.fr .

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.

3.2 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 de grande instance. 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.

3.2.1 Données concernées

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.

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'aides aux victimes, et l'administration pénitentiaire ont accès à certaines données (Articles R15-33-66-8 et R15-33-66-9).

3.2.2 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).

3.2.3 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).

3.3 Répertoire des expertises (REDEX)

Prévu par les articles 706-56-2 et R53-21-1 et suivants du Code de procédure pénale.

Tenu par le Service du casier judiciaire (Ministère de la justice).

3.3.1 Données concernées

Il concerne toutes les personnes poursuivies ou condamnées pour l'une des infractions dans lesquelles le suivi socio-judiciaire est encouru.

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.

3.3.2 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).

3.3.3 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 JLD (R53-21-13 et suivants).

3.4 Dossier Unique de Personnalité

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 précisé par le Décret n°2014-472 du 9 mai 2014.

Il concerne les personnes mineures qui font l'objet d'une investigation sur leur personnalité (donc dès lors qu'elles sont présentées à un juge des enfants). Il concerne également tout·e mineur·e faisant l'objet d'une liberté surveillée, d'un placement sous contrôle judiciaire, d'une assignation à résidence avec bracelet électronique ou d'une détention provisoire.

3.4.1 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.

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). Le juge des enfants peut autoriser l'avocat à transmettre le dossier au mineur·e lui-même, à ses parents ou à son tuteur.

3.4.2 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.

3.4.3 Droit de communication, de rectification et d'effacement

Il s'agit surtout d'un droit de consultation : Le juge des enfants peut autoriser l'avocat à transmettre le dossier au mineur·e lui-même, à ses parents ou à son tuteur.

3.5 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.

3.5.1 Données concernées

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

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

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

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.

3.5.2 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).

3.5.3 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).

3.6 Fichier national automatisé des personnes incarcérées : Fichier National des Détenus (FND)

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.

3.6.1 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.

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

3.6.2 Conservation des données

On n'a pas trouvé d'informations certaines.

3.6.3 Droit de communication, de rectification et d'effacement

L'Article 2 de l'Arrêté du 28 octobre 1996 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.

3.7 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).

3.7.1 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.

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).

Les données sont accessibles à l'administration pénitentiaire et à certains matons ainsi qu'aux greffiers et juges, les membres de la commission pluridisciplinaire, les membres de la commission d'application des peines, les SPIP, la protection judiciaire de la jeunesse, les agents de l'éducation nationale intervenant en détention, certains personnels privés (intervenants sportifs, personnel d'entretien, personnel de la cantine, ...) ainsi que les personnels des UCSA, SMPR, UHSI, UHSA, mais aussi le préfet, l'avocat, les maires (seulement dans le cadre des modifications d'état civil, et seulement les données relatives à l'identité et au lieu d'incarcération), les flics quand il y a une permission de sortie, les juridictions étrangères et même Pole Emploi et les Missions locales (qui ont accès seulement à l'état civil, le lieu de détention, la date de sortie, de permission ou d'aménagement de peine), les douanes, la CAF (pour certaines informations aussi), les institutions de retraite et les organismes de formation (idem).

3.7.2 Conservation des données

Les données sont conservées 2 ans à compter de la levée d'écrou (Article R57-9-21).

3.7.3 Droit de communication, de rectification et d'effacement

En ce qui concerne le droit d'accès et de rectification des données, il s'exerce (selon l'Article 57-9-24) :

- De manière indirecte, via la CNIL, pour les informations sur les dates prévues de transfert et d'extraction, les prescriptions judiciaires ou pénitentiaires relatives au régime de détention, les désignations des locaux de la taule, les mouvements de la personne détenue.
- Auprès du directeur de la taule pour tout le reste.

3.8 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, etc.

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

Il vise à appliquer un régime spécial à certains détenus considérés comme dangereux. Il s'agit de renforcer la surveillance : contrôle d'œilleton systématique (ce qui entraîne un réveil toutes les 2 heures : bruit de l'œilleton et lumière allumée), consultations médicales menotté·e et sous la surveillance des matons, ceinture abdominale et « chaîne de conduite » pendant les déplacements, etc. L'ensemble est dans une note de la Direction de l'Administration pénitentiaire du 8 novembre 2013, non publiée.

Ce qu'on a, c'est la Circulaire du Ministre de la justice du 15 octobre 2012.

3.8.1 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 aidé·es 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).

3.8.2 Conservation des données

Normalement, les données ne sont pas vraiment collectées : le FND et GENESIS comportent la mention « Détenu Particulièrement Signalé », et cette mention est retirée lorsque le ou la détenu·e sort du DPS.

3.8.3 Droit de communication, de rectification et d'effacement

Il ne s'agit donc pas de l'effacement des données, mais d'une demande de sortir du statut de DPS, à porter devant le tribunal administratif de la taule, avec un·e avocat·e.

3.9 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).

3.10 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.

4 FICHIERS DE POLICE : FICHIERS ADMINISTRATIFS

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.

5 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, …)

5.1 Traitement d'Antécédents Judiciaires (TAJ)

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).

5.1.1 Règles de ce qui est écrit et de ce qui peut ou doit être rectifié

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 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.

5.1.2 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).

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

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

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 en vigueur jusqu'au 1er mai 2018) :

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 dans la loi la fiche est inaccessible lors d'une enquête administrative).

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.

Le problème est que ces règles s'appliquaient jusqu'au 1er mai 2018. Or elles étaient contraires à la Constitution parce que trop restrictives (par exemple, elles ne permettent pas de demander un effacement en cas de condamnation avec dispense de peine), donc le Conseil constitutionnel les a censurées (CC, QPC, 27 octobre 2017, n°2017-670). Il n'en a pas ordonné l'abrogation immédiate, mais seulement avec une prise d'effet au 1er mai 2018, pour que le législateur ait le temps de prendre une nouvelle loi qui soit moins restrictive… et pour ne pas priver tout le monde du droit de demander l'effacement de ses données. Or le législateur n'a pas pris de nouvelle loi avant le 1er mai 2018, donc ces règles n'ont pas été remplacées, et elles ont disparu!

En principe, personne ne peut demander l'effacement de ses données. Oups. Une analyse ici : http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2017670QPC2017670qpc_ccc.pdf

Cependant, c'est quand même possible de s'adresser au Procureur ou à la CNIL : voir le C.

5.1.3 Droit de communication indirecte et demande de rectification ou d'effacement des données

Le droit de communication des données s'effectue de manière indirecte, *via* la CNIL (Article R40-33 du Code de procédure pénale).

En ce qui concerne la demande de rectification ou d'effacement, le problème vu avant (dans le B) est toujours d'actualité : Les règles étaient à l'article 230-8 du Code de procédure pénale, mais une décision du Conseil constitutionnel les a déclarées inconstitutionnelles parce qu'elles ne protégeaient pas assez les particuliers… donc ces règles ont disparu, mais n'ont pas été remplacées. Cependant, ça n'empêche pas de former une demande : peut-être le Procureur la trouvera bien fondée, et fera ce qu'on lui demande.

La demande de rectification ou d'effacement est à adresser à la CNIL (article R40-31) ou au Procureur territorialement compétent (articles 230-8 et R40-31-1) ou au magistrat référent (article 230-9 et R40-31-1). La rectification pour requalification judiciaire est de droit, devant le magistrat spécialisé, qui se prononce alors dans un délai d'1 mois.

Ce magistrat référent était M. Paul MICHEL, Procureur général près la Cour d'appel de Grenoble (Arrêté du 3 août 2012, nommé pour 3 ans). Mais le Décret du 7 juillet 2016 a nommé Jacques DALLEST procureur général près le Cour d'appel de Grenoble… et le mandat de Paul MICHEL s'est terminé le 3 août 2015. Donc c'est difficile de savoir qui est le nouveau magistrat référent ; dans le doute, il vaut mieux s'adresser au Procureur.

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. Pour cela, il vaut mieux avoir l'aide d'un·e avocat·e.

En l'absence de réponse sous 2 mois du Procureur c'est la même chose, on a 1 mois pour faire appel devant le Président de la chambre de l'instruction (si demande a été faite au Procureur). 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 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.

5.2 STIC

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

5.3 JUDEX

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

5.4 ARDOISE et ICARE, remplacés par LRPPN et LRPGN

Ils 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 et ICARE par LRPGN.

Donc ils ne contiennent pas de données en eux-mêmes, ils servent seulement à accéder aux données du TAJ.

6 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).

6.1 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.

6.1.1 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.

6.1.2 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.

6.1.3 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 TGI compétent sur ce domicile, puis envoyer la demande au Procureur de la République de ce TGI (Article 7-1 du Décret n°87-249 du 8 avril 1987). Voir un modèle de lettre en pièce-jointe.

Si le Procureur refuse la suppression, on a 10 jours pour contester ce refus (Article 7-1 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 TGI). 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 TGI. Mais là, il faut vraiment un·e avocat·e.

6.2 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 2015, le fichier rassemblait 3 millions de 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.

6.2.1 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 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.

6.2.2 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).

6.2.3 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 TGI est compétent, et l'envoyer au Procureur de ce TGI 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 TGI). 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 TGI, avec une lettre recommandée avec accusé de réception (Article R53-13-4). Mais là, il faut vraiment un·e avocat·e.

6.3 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.

6.3.1 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 CSI). 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.

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.

6.3.2 Durée de conservation des données

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

6.3.3 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 TGI 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.

6.4 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 articles R53-8-1 et suivants du Code de procédure pénale.

6.4.1 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.

6.4.2 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.

6.4.3 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 TGI 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.

6.5 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).

6.5.1 Règles de ce qui y est écrit

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 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.

6.5.2 Durée de conservation des données

Les règles sont celles de l'article 230-15 du Code de procédure pénale.

Pour SALVAC, la conservation des données dure pendant 40 ans. 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. En cas de non-lieu ou de classement sans suite, les données en font mention, sauf si le Procureur en prescrit l'effacement. 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. En cas de condamnation, la personne concernée peut demander l'effacement, mais le Procureur peut s'y opposer.

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. 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. Aussi, dès que l'auteur a été définitivement condamné, il peut en demander l'effacement, mais le Procureur ou le magistrat spécialisé peut s'y opposer.

6.5.3 Droit de communication et de rectification

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, ou par l'intermédiaire de la CNIL.

Peut-être la décision du Conseil d'État, 11 avril 2014, n°360759, *Ligue des droits de l'homme* est applicable à ces fichiers en plus de l'être au TAJ, donc il y aurait un recours en excès de pouvoir devant le TA contre le refus par le Procureur ou par le magistrat spécialisé d'effacer les données.

7 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.

7.1 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 MERCURE (police nationale). La Circulaire du 18 août 2014 relative aux fichiers d'antécédents judiciaires donne plus d'informations si nécessaire.

7.1.1 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.

7.1.2 Durée de conservation

Elle est définie à l'article 230-22 du Code de procédure pénale : Seulement pour la durée de l'enquête, voire 3 ans maximum (à partir du début de l'enquête, ou de sa clôture?).

7.1.3 Droit d'accès et de rectification indirects

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 via la CNIL ou le Procureur de la République territorialement compétent, ou un magistrat spécialisé (article 230-24). La rectification pour requalification (typiquement : la personne est fichée pour assassinat, mais elle est condamnée pour meurtre) est de droit lorsque la personne concernée la demande.

Ce magistrat référent était M. Paul MICHEL, Procureur général près la Cour d'appel de Grenoble (Arrêté du 3 août 2012, nommé pour 3 ans). Mais le Décret du 7 juillet 2016 a nommé Jacques DALLEST procureur général près le Cour d'appel de Grenoble… et le mandat de Paul MICHEL s'est terminé le 3 août 2015. Donc c'est difficile de savoir qui est le nouveau magistrat référent ; dans le doute, il vaut mieux s'adresser au Procureur ou à la CNIL.

7.2 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.

7.2.1 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).

7.2.2 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).

7.2.3 Droit d'accès indirect

Le droit d'accès aux données s'exerce indirectement, *via* la CNIL (Article 6 II du Décret n°2014-187 du 20 février 2014).

7.3 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.

7.3.1 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.

7.3.2 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).

7.3.3 Droit d'accès indirect

Le droit d'accès aux données s'exerce indirectement, *via* la CNIL (Article 6 de l'Arrêté du 15 octobre 2014).

8 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'un·etel·le 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).

8.1 Fichier des Personnes Recherchées (FPR)

C'est un fichier de police judiciaire (Ministère de l'intérieur), créé en 1996.

8.1.1 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, …). 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.

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	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.*	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)	*Interdiction de porter ou de détenir une arme soumise à autorisation.*	*Interdiction d'exercer une profession, interdiction d'exercer une fonction publique, interdiction d'exercer une profession commerciale ou industrielle, interdiction d'exercer une activité professionnelle ou sociale.*		*Interdiction de paraître dans certains lieux, interdiction de séjour dans certains lieux, interdiction de fréquenter certaines personnes.*	*Interdiction de territoire français prononcée par un juge pénal (Fiche IT : 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.*	*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.

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). Les fiches S sont numérotées de S2 à S15 ou S16 en fonction de la conduite à tenir par les flics, et plus rarement du profil de la personne (par exemple : S14, islamistes revenant de l'Irak ou de la Syrie ; S15, personne à interpeller). 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/secret », dont l'objet même nécessite que la personne ne sait pas qu'elle est fichée. C'est le cas, par exemple, des personnes concernées par une « Fiche S » pour « *prévenir des menaces graves pour la sécurité publique ou la sûreté de l'État* ». Dans ce cas-là, bien sûr, on ne reçoit pas une jolie lettre « *Vous avez une Fiche S au FPR, nous vous souhaitons la bienvenue* » : l'État a tout intérêt à vous cacher le fait que vous êtes fiché·e.

Dans ce dernier cas (le fichage « caché/secret »), il y a néanmoins des indices qui permettent de déduire qu'on est fiché·e. Par exemple, vous attendez 8 mois pour avoir un passeport (effectivement, l'Article 8 du Décret n°2016-1460 du 28 octobre 2016 prévoit la consultation du FPR au moment de la demande de passeport) ; ou alors, à l'aéroport vous faites l'objet d'un contrôle poussé (pas seulement un regard sur le passeport et 5 minutes d'attente, mais plutôt 30 minutes d'attente et un interrogatoire sur les raisons de votre départ, la durée de votre séjour à l'étranger, etc.) ; 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…

8.1.2 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 tout le reste, on ne sait pas.

8.1.3 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 concernent 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). 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).

8.2 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).

8.2.1 Données concernées

Comme le Fichier Enquêtes administratives liées à la sécurité publique : Les enquêtes administratives sur les personnes pour l'embauche et le maintien à leur poste des personnes qui participent aux missions de souveraineté de l'État, de sécurité, de défense, des jeux, paris et courses, de l'utilisation de matériels ou produits dangereux (article L114-1 du Code de la sécurité intérieure) ; pareil pour le recrutement et l'affectation à des emplois en lien direct avec le transport public de personnes, de marchandises dangereuses (L114-2) ; pareil pour toute personne qui participe (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 CSI).

8.2.2 Durée de conservation des données

5 ans à compter de leur enregistrement.

8.2.3 En lien avec

Si, ici, y'a une partie « en lien avec », ça veut pas dire que les autres fichiers sont pas en lien les uns avec les autres…

Le TAJ, le fichier « Enquêtes administratives liées à la sécurité publique » (EASP, Articles R236-1 et suivants du CSI), le fichier « Prévention des atteintes à la sécurité publique » (PASP, Articles R236-11 et suivants du CSI), le fichier « Gestion de l'information et prévention des atteintes à la sécurité publique » (GIPASP, Articles R236-21 et suivants du CSI), le FPR, le FSPRT, le fichier des véhicules volés ou signalés, CRISTINA, GESTEREXT. On n'a que très peu parlé de tous ces fichiers jusqu'ici… ils arrivent tout de suite après ACCReD.

8.2.4 Droit d'accès indirect

Il s'exerce indirectement, *via* la CNIL (Article 8 du Décret n°2017-1224 du 3 août 2017).

8.3 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). Il remplace, avec PASP, EDVIRSP et le projet EDVIGE.

8.3.1 Données concernées

Comme ACCReD, il sert aux enquêtes administratives sur les personnes pour : L'embauche et le maintien à leur poste des personnes qui participent aux missions de souveraineté de l'État, de sécurité, de défense, des jeux, paris et courses, de l'utilisation de matériels ou produits dangereux (article L114-1 du Code de la sécurité intérieure) ; pareil pour le recrutement et l'affectation à des emplois en lien direct avec le transport public de personnes, de marchandises dangereuses (L114-2) ; pareil pour toute personne qui participe (autrement qu'en simple participant/spectateur) à un grand évènement exposé par son ampleur ou par des circonstances particulières à un risque exceptionnel de menace terroriste (article L211-11-1 du CSI).

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).

8.3.2 Durée de conservation

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

8.3.3 Droit d'accès indirect

Il s'exerce auprès de la CNIL (article R236-9 du Code de la sécurité intérieure).

8.4 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).

Le PASP concerne la sûreté de l'État, donc n'est pas soumis à déclaration / autorisation / avis de la CNIL (décret n°2007-914 du 15 mai 2007). Il remplace, avec EASP et GIPASP, le projet EDVIGE abandonné au profit de EDVIRSP.

8.4.1 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.

Le 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.

8.4.2 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.* » (R236-14), 3 ans pour les mineurs.

8.4.3 Droit d'accès

Il est prévu à l'article R236-19 : Droit d'accès indirect via la CNIL.

8.5 Fichier relatif à la 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).

Le système GIPASP-BDSP remplace ATHEN@, qui avait lui-même regroupé ARAMIS et le Fichier alphabétique de renseignement de la gendarmerie (FAR).

8.5.1 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 le 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.

8.5.2 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), 3 ans pour les mineurs.

8.5.3 Droit d'accès

Le droit d'accès s'exerce indirectement, *via* la CNIL (article R236-29).

8.6 Fichier Conservation, gestion et exploitation électroniques des documents des services de 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).

8.6.1 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.

8.6.2 Durée de conservation des données

Les données sont conservées 20 ans.

8.6.3 Droits d'accès et de rectification indirects

L'accès et la rectification se font indirectement, via la CNIL (Article R236-51 du CSI).

8.7 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.

Il concerne la sûreté de l'État, donc n'est pas soumis à déclaration / autorisation / avis de la CNIL (décret n°2007-914 du 15 mai 2007) et est classé secret-défense.

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) créée en 2015 (Loi n°2015-912 du 24 juillet 2015, Article R841-2 du Code de la sécurité intérieure).

8.8 Fichier 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.

GESTEREXT concerne la sûreté de l'État, donc n'est pas soumis à déclaration / autorisation / avis de la CNIL (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, article 6 de la loi du 6 janvier 1978.

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).

8.9 Fichier des 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 le Service Central du Renseignement Territorial (SCRT, dépend de la Direction centrale de la Sécurité Publique, qui dépend de la Direction générale de la police nationale, Ministère de l'intérieur). 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.

Le FSPRT concerne la sûreté de l'État, donc n'est pas soumis à déclaration / autorisation / avis de la CNIL (décret n°2007-914 du 15 mai 2007).

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'Etat mais simplement en raison d'une conduite ou d'un comportement exprimant une conviction politique ou religieuse.* » (Commission Nationale Consultative des Droits de l'Homme, 18 mai 2017, *Avis sur la prévention de la radicalisation*, publié au JORF n°0077 du 1er avril 2018).

Il est alimenté notamment par le numéro de téléphone de la Plateforme anti-radicalisation.

Les données sont conservées pendant 5 ans.

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).

8.10 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 CAR concerne la sûreté de l'État, donc n'est pas soumis à déclaration / autorisation / avis de la CNIL (décret n°2007-914 du 15 mai 2007).

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).

8.11 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.

Concerne la sûreté de l'État, donc n'est pas soumis à déclaration / autorisation / avis de la CNIL (décret n°2007-914 du 15 mai 2007).

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).

8.12 BIOPEX

BIOPEX a été créé en 2017 (Décret n°2017-1231 du 4 août 2017) et dépend du Ministère des Armées. L'avis de la CNIL n°2017-216 du 13 juillet 2017 n'est pas non plus publié.

BIOPEX concerne la sûreté de l'État, donc n'est pas soumis à déclaration / autorisation / avis de la CNIL (décret n°2007-914 du 15 mai 2007).

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).

8.13 Fichier d'informations nominatives de la DGSE

Mis en œuvre par la DGSE (Ministère des Armées).

Concerne la sûreté de l'État, donc n'est pas soumis à déclaration / autorisation / avis de la CNIL (décret n°2007-914 du 15 mai 2007).

Le droit d'accès et de rectification s'exerce de manière indirecte *via* la CNIL. Un recours contre le refus par le Ministre des armées d'accès aux données existe, devant la Formation spécialisée du Conseil d'État.

8.14 Fichier de la DGSE

Mis en œuvre par la DGSE (Ministère des Armées).

Concerne la sûreté de l'État, donc n'est pas soumis à déclaration / autorisation / avis de la CNIL (décret n°2007-914 du 15 mai 2007).

Le droit d'accès et de rectification s'exerce de manière indirecte *via* la CNIL. Un recours contre le refus par le Ministre des armées d'accès aux données existe, devant la Formation spécialisée du Conseil d'État, créée en 2015 (Loi n°2015-912 du 24 juillet 2015, Article L841-2 et Article R841-2 du Code de la sécurité intérieure).

8.15 Fichier de renseignement militaire (DRM)

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

Concerne la sûreté de l'État, donc n'est pas soumis à déclaration / autorisation / avis de la CNIL (décret n°2007-914 du 15 mai 2007).

Le droit d'accès et de rectification s'exerce de manière indirecte *via* la CNIL. Un recours contre le refus par le Ministre des armées d'accès aux données existe, devant la Formation spécialisée du Conseil d'État, créée en 2015 (Loi n°2015-912 du 24 juillet 2015, Article L841-2 et Article R841-2 du Code de la sécurité intérieure).

8.16 Fichier des personnes étrangères de la Direction du renseignement militaire

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

Concerne la sûreté de l'État, donc n'est pas soumis à déclaration / autorisation / avis de la CNIL (décret n°2007-914 du 15 mai 2007).

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).

8.17 SIREX

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

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.

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.

Concerne la sûreté de l'État, donc n'est pas soumis à déclaration / autorisation / avis de la CNIL (décret n°2007-914 du 15 mai 2007).

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.

8.18 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).

Il concerne la sûreté de l'État, donc n'est pas soumis à déclaration / autorisation / avis de la CNIL (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).

8.19 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.

8.20 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.

8.21 Fichier alphabétique de renseignement de la gendarmerie (FAR)

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

8.22 ARAMIS

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

9 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 !

9.1 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.

9.1.1 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 :

- 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.

9.1.2 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).

9.1.3 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 alinéa 1 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).

9.2 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.

9.2.1 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 pubic 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…

9.2.2 Durée de conservation des données

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

Bien sûr, prolongations possibles.

9.2.3 Droits d'accès et de rectification indirect·es

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.

9.3 Système 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.

9.3.1 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, Interpol. Peut être consulté par vraiment plein de monde.

9.3.2 Durée de conservation des données

5 ans (Article L232-7 du CSI).

9.3.3 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 ou son adjoint : 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 : Droit d'accès et de rectification indirect via la CNIL.

9.4 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.

9.4.1 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 fontt l'objet d'une instruction et qui encourent une peine d'au moins 2 ans d'emprisonnement (article 100 CPP), les personnes qui font l'objet d'une enquête pour criminalité organisée (article 706-95 et 706-95-1, 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, etc (Article R40-46 CPP).

9.4.2 Droit d'accès et de rectification indirects

Le droit d'accès et de rectification s'exerce de manière indirecte, via la CNIL (Aeticle R40-55 du Code de procédure pénale).

9.5 Fichier Gestion des sollicitations et des interventions

Articles R236-31 et suivants du CSI.

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

9.5.1 Objectifs et données collectées

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

9.5.2 Durée de conservation des données

2 ans.

9.5.3 Droit d'accès indirect

Via la CNIL (R236-37 du CSI), droit d'accès indirect. Pas de droit de modification.

9.6 Fichier Sécurisation des interventions et demandes particulières de protection

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

Articles R236-38 et suivants du CSI.

9.6.1 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.

9.6.2 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.

9.6.3 Droit d'accès

Droit d'accès indirect via la CNIL (article R236-45 du CSI).

Les personnes qui ont fait une demande de protection ont un droit d'accès direct auprès de la brigade territoriale compétente.

9.7 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.

Le droit d'accès et de rectification s'exerce de manière indirecte via la CNIL (Article 8 de l'Arrêté du 28 août 2007).

9.8 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.

9.8.1 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.

9.8.2 Durée de conservation des données

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

9.8.3 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.

10 RÉCAPITULATIF DU DROIT D'ACCÈS ET DE SUPPRESSION

La loi de 1978 dit qu'on a 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 suppression (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).

10.1 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 34 d'entre eux il faut s'adresser à la CNIL et pour 13 autres il faut s'adresser à d'autres institutions.

10.1.1 Droit d'accès indirect : via *la CNIL*

Pour les fichiers suivants, le droit d'accès s'effectue de manière indirecte : Il faut envoyer un courrier en lettre recommandée avec avis de réception à la CNIL (Commission Nationale Informatique et Libertés, Service du droit d'accès indirect, 3 Place de Fontenoy, TSA 80715, 75334 PARIS CEDEX 07) pour demander un accès aux données, puis pour en demander la rectification ou la suppression. Un modèle de lettre est en pièce-jointe.

Il s'agit de ces 36 fichiers : Traitement d'Antécédents Judiciaires (TAJ) ; Système de Traitement des Infractions Constatées (STIC) ; Système Judiciaire de Documentation et d'Exploitation (JUDEX) ; Gestion nationale des personnes détenues en établissement pénitentiaire (GENESIS) pour les dates prévues de transfert, d'extraction, le régime de détention, les mouvements du détenu ; 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 ; Données exploitées par les logiciels de rapprochement judiciaire prévus par les articles 230-20 à 230-27 du Code de procédure pénale dont ANACRIM et MERCURE ; Automatisation de la consultation centralisée de renseignements et de données (ACCReD) ; Diffusion et Partage de

l'Information Opérationnelle (DPIO) ; Logiciel d'uniformisation des procédures d'identification (LUPIN) ; Fichier des personnes recherchées (FPR) ; Fichier Enquêtes administratives liées à la sécurité publique (EASP) ; Application relative à la prévention des atteintes à la sécurité publique (PASP) ; Fichier relatif à la gestion de l'information et la prévention des atteintes à la sécurité publique (GIPASP) ; Fichier Conservation, gestion et exploitation électroniques des documents des services de renseignement territorial ; Fichier CRISTINA ; Fichier Gestion du terrorisme et des extrémismes à potentialité violente (GESTEREXT) ; Fichier des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT) ; 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) ; ASTREE ; BIOPEX ; Fichier d'informations nominatives de la DGSE ; Fichier de la DGSE ; Fichier de renseignement militaire (DRM) ; Fichier des personnes étrangères de la Direction du renseignement militaire ; Fichier SIREX ; Fichier BCR-DNRED ; Fichier des Objets et Véhicules Signalés (FOVeS) pour les objets et véhicules signalés (et non pour ceux volés ou perdus) ; Fichier du Système d'informations Schengen N-SIS II ; Système API-PNR France ; 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 ; Fichier Gestion des sollicitations et des interventions ; Fichier Sécurisation des interventions et demandes particulières de protection ; Fichier National des Interdits de Stade (FNIS) ; 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) ; Fichier de renseignement des services de l'information générale de la Direction Centrale de la Sécurité Publique et de la Préfecture de Police de Paris.

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

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.

10.1.2 Le droit d'accès, de rectification et de suppression direct

Pour d'autres fichiers, il faut s'adresser directement à l'administration qui gère le fichier pour avoir accès aux informations. Cela concerne les 18 fichiers suivants :

- 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 au Ministère de l'intérieur, Place Beauvau, 75800 PARIS Cedex 08.

- 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).

- 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 de Grande Instance 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.

- 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 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 (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).

- Gestion nationale des personnes détenues en établissement pénitentiaire (GENESIS) : le droit d'accès et de rectification des données, s'exerce auprès du directeur de la taule, et auprès de la CNIL pour certaines informations (Article 57-9-24 du Code de procédure pénale).
- 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.
- Dossier Unique de Personnalité (DUP) : Procédure effectuée par l'avocat·e auprès du Juge des enfants.
- Le Fichier Automatisé des Empreintes Digitales (FAED) : 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. Pour la demande de suppression, il faut une 2e lettre. Voir les procédures ici et des modèles pour la demande d'accès et la demande de suppression des données en pièce-jointe.
- 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.
- Fichier judiciaire national automatisé des auteurs d'infractions terroristes : 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 TGI 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 : Quand on est fiché on le sait. La procédure est la même que pour le Fichier judiciaire national automatisé des auteurs d'infractions terroristes, mais en application des Articles 706-53-9 et 706-53-10 du Code de procédure pénale.
- 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).

- 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).

10.2 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, fichier de la DRM, FSPRT, Fiches S du FPR, N-SIS II (Schengen), TRACFIN, BCR-DNRED, GESTEREXT, BIOPEX.

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

Les membres de la formation spécialisée sont peu nombreux 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).

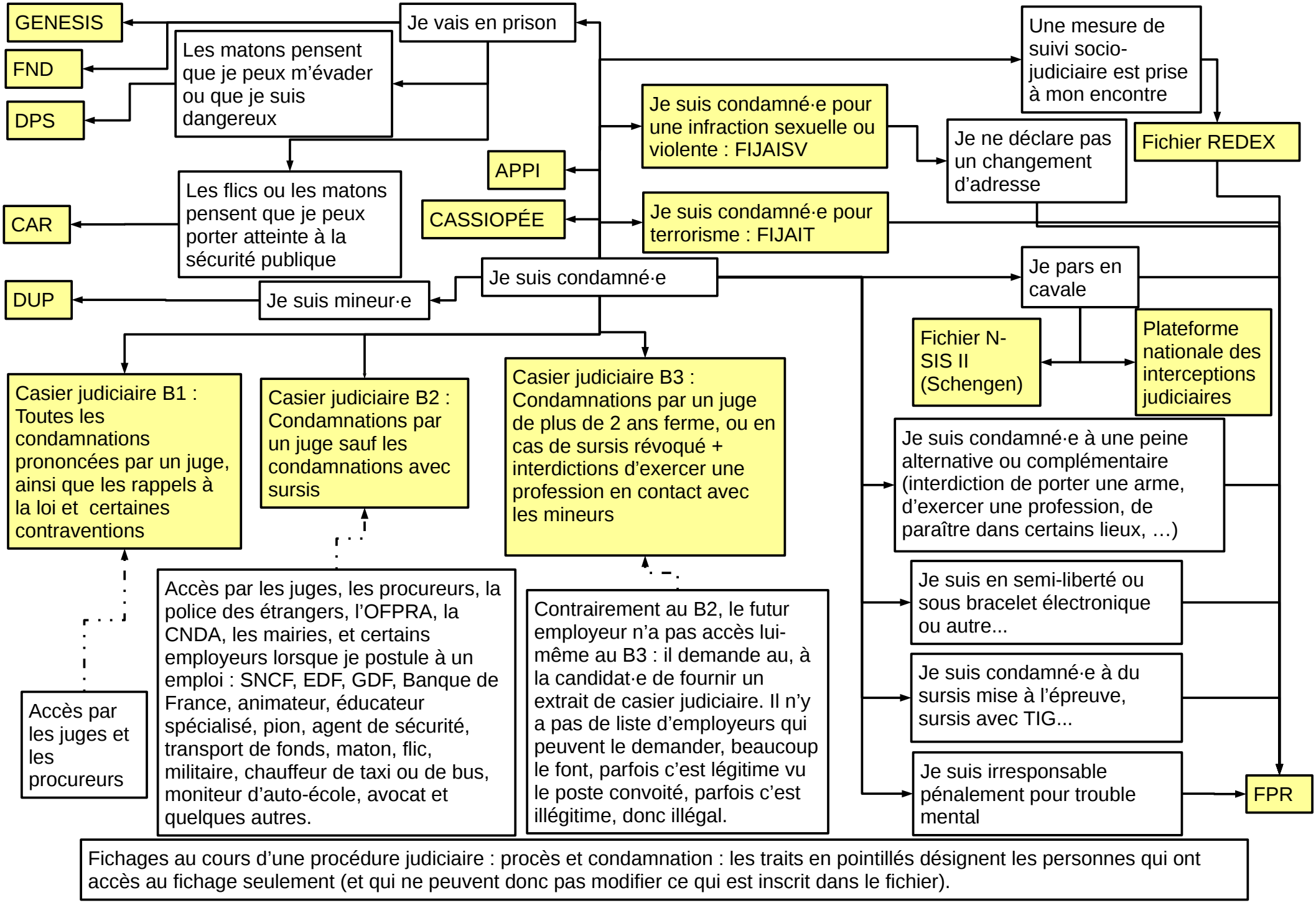
Enfin, pour se donner une idée, le 19 octobre 2016 le Conseil d'État a rendu ses 11 premières décisions relatives à la demande d'effacement de données contenues dans les fichiers de renseignement : 5 portaient sur des fichiers de la DGSE, 5 sur des fichiers de la DPSD (qui est devenue depuis la DRSD, Ministère des armées) et 1 sur des fichiers de la DRM (Direction du renseignement militaire, Ministère des armées aussi). 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).

11 ANNEXES 1 : SCHÉMAS RÉCAPITULATIFS

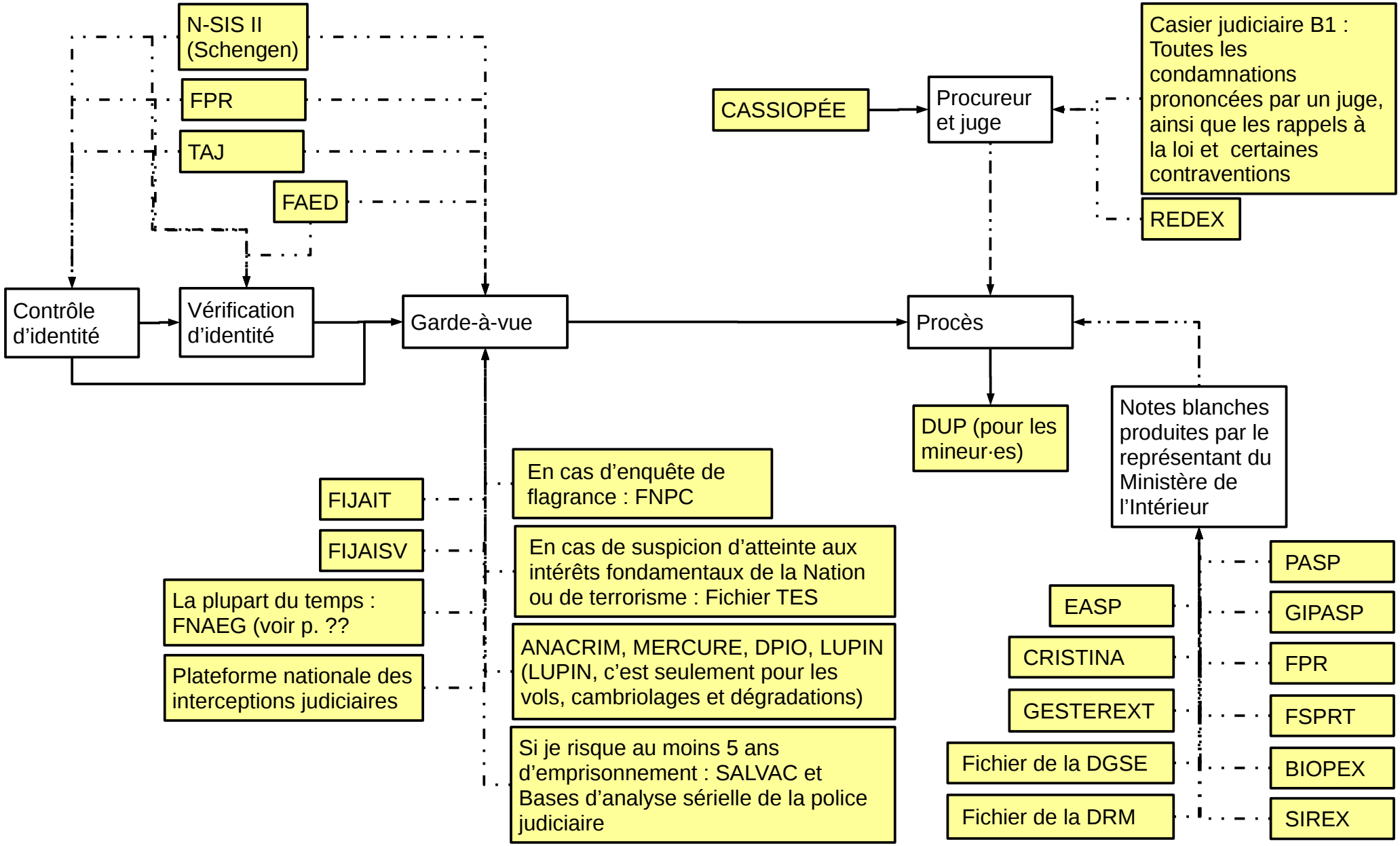
Voilà une liste de situations dans lesquelles les fichages des flics interviennent : Arrestation, enquête, procès, vie militante, vie professionnelle, ainsi que certaines situations de la vie quotidienne.

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-dessus pour avoir plus d'informations sur un fichier en particulier.

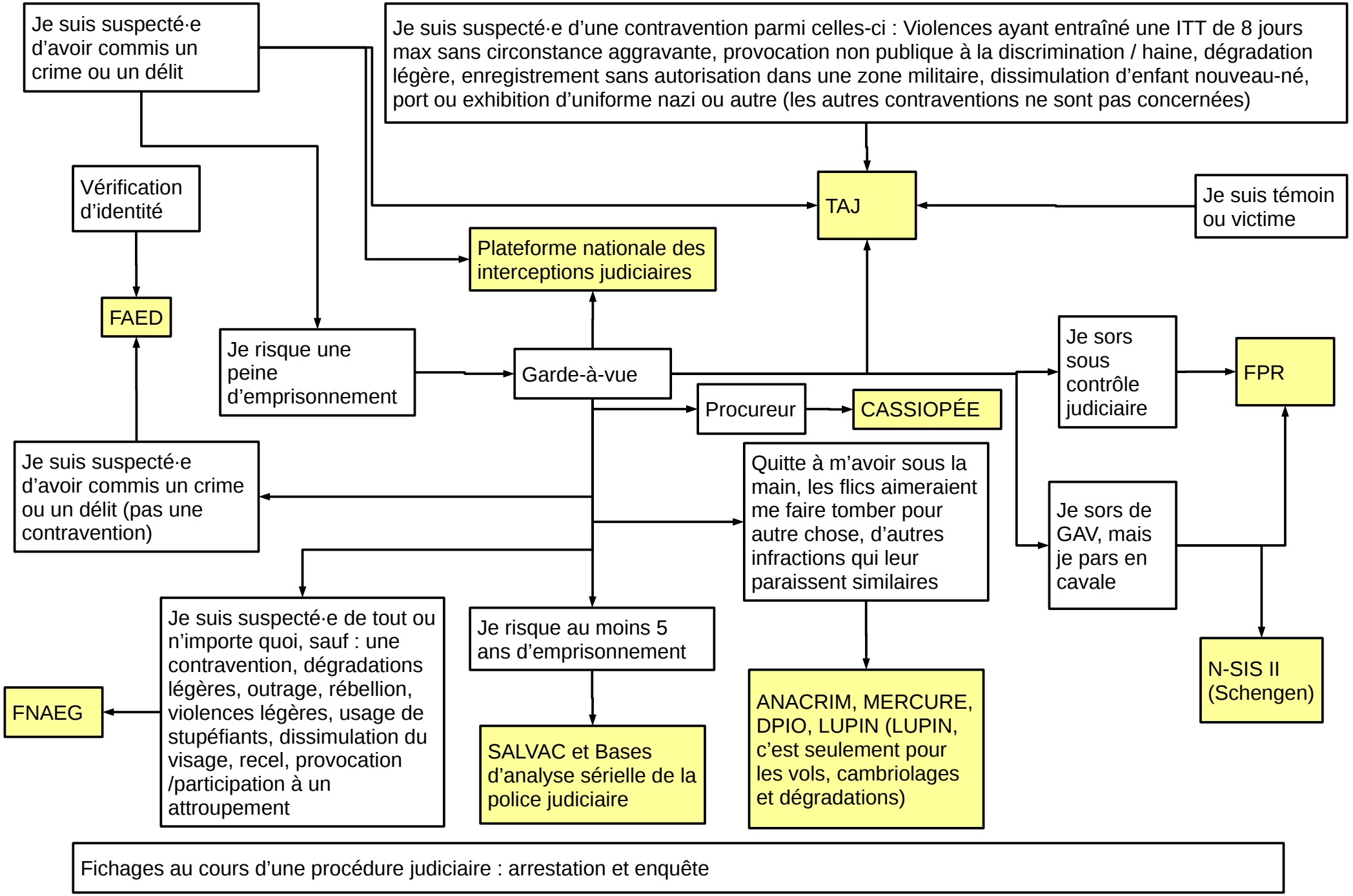
On espère, en tout cas, que ces schémas peuvent donner une vision d'ensemble, et aider à mieux s'y retrouver.

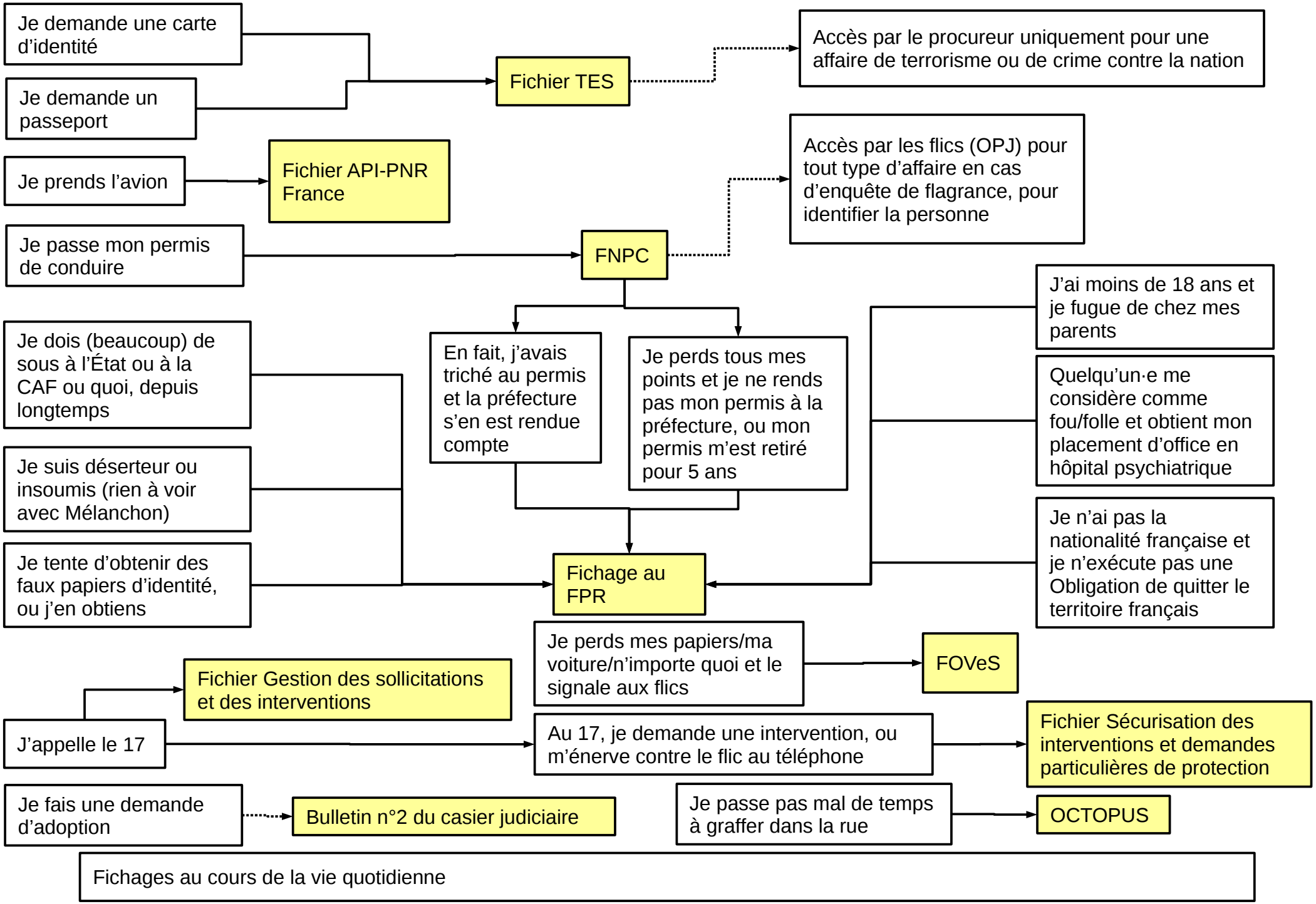


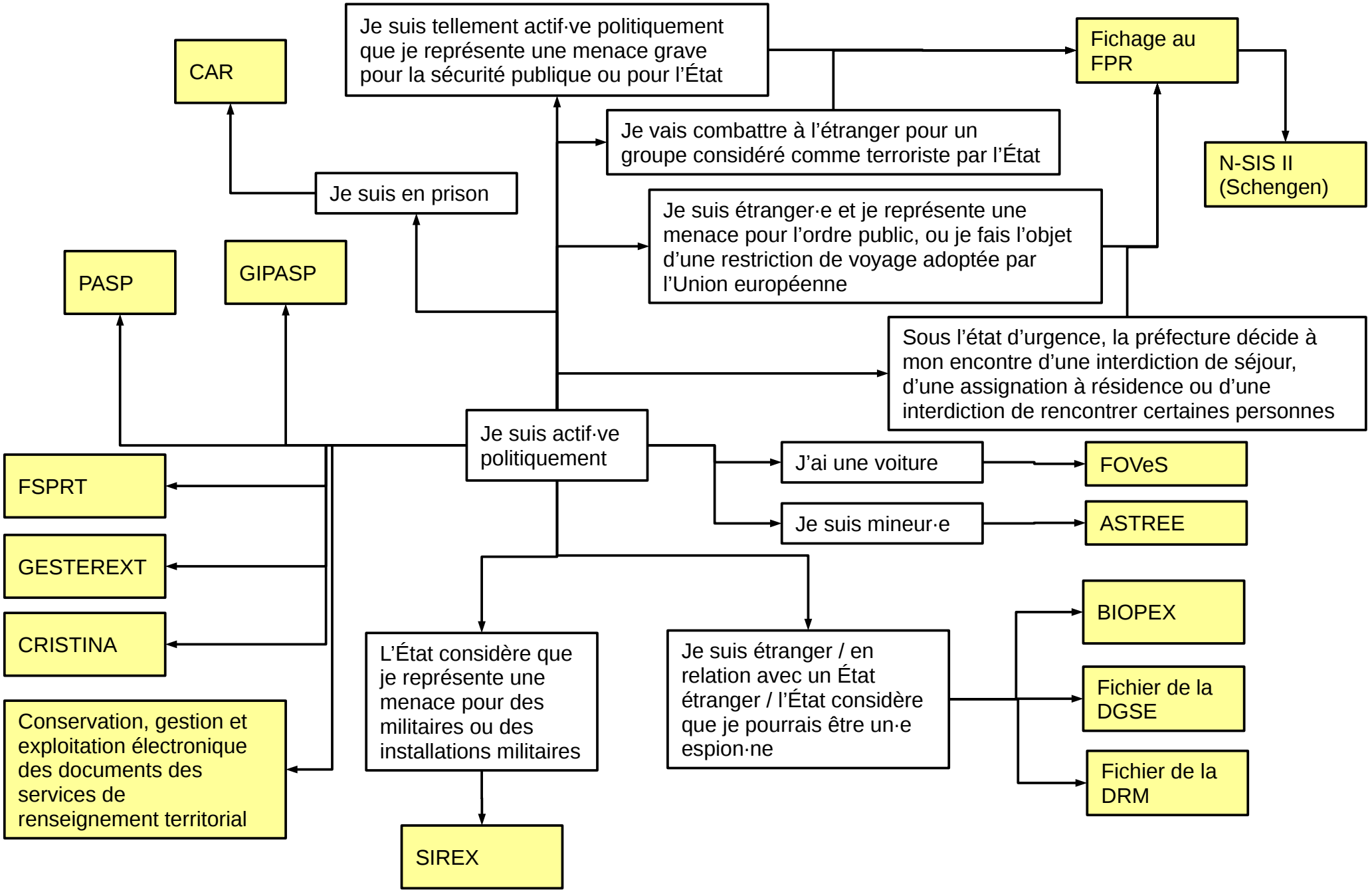
Fichages au cours d'une procédure judiciaire : procès et condamnation : les traits en pointillés désignent les personnes qui ont accès au fichage seulement (et qui ne peuvent donc pas modifier ce qui est inscrit dans le fichier).

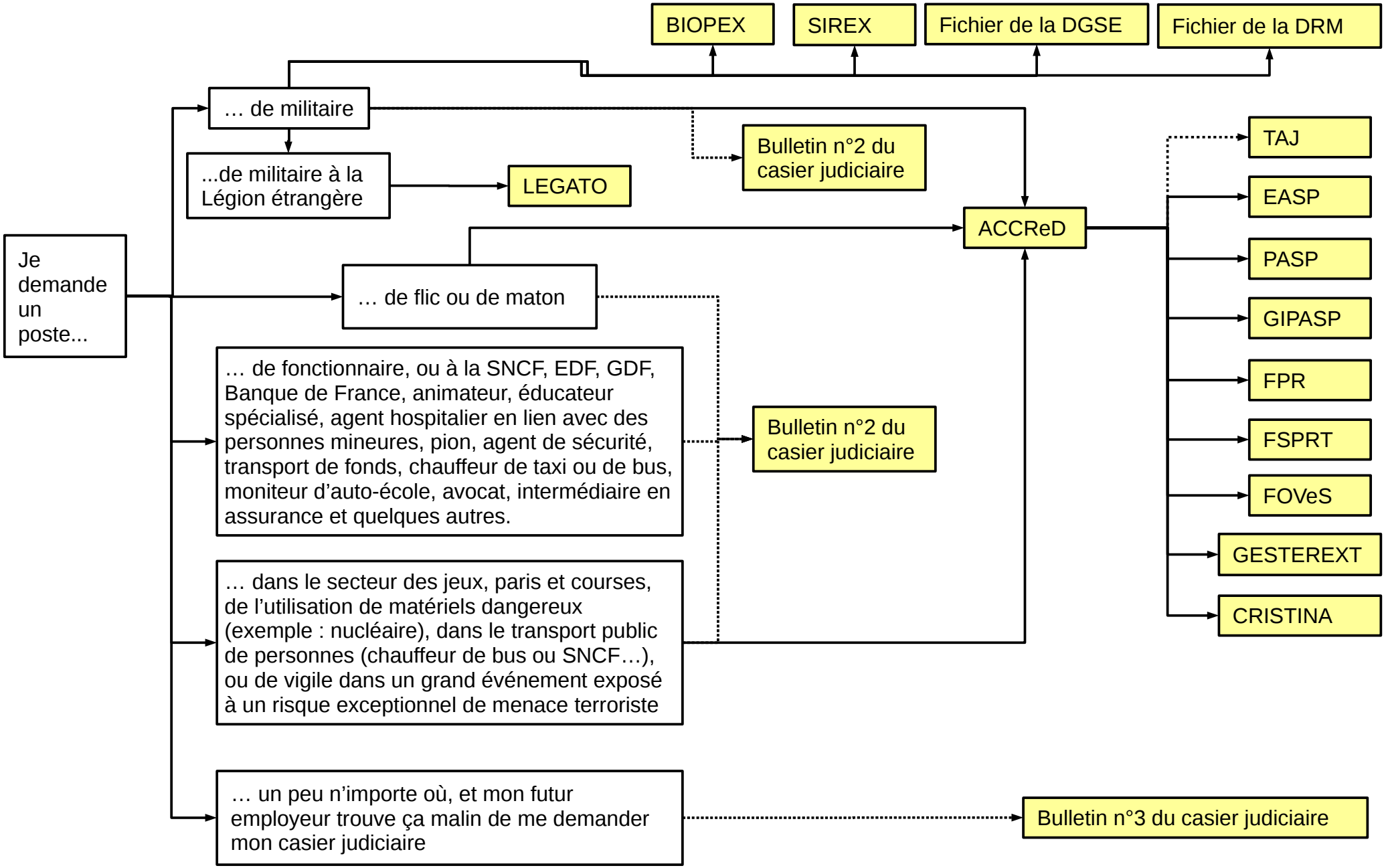


Consultations des fichiers par les flics, les procs, les juges et le Ministère de l'intérieur au cours de la procédure pénale : il y a ici seulement des traits en pointillés, parce qu'il s'agit de la consultation des fichiers et non de leur modification. Attention, pour certains fichiers, leur consultation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


Je suis suspecté·e d'avoir commis un crime ou un délit
Je suis suspecté·e d'une contravention parmi celles-ci : Violences ayant entraîné une ITT de 8 jours max sans circonstance aggravante, provocation non publique à la discrimination / haine, dégradation légère, enregistrement sans autorisation dans une zone militaire, dissimulation d'enfant nouveau-né, port ou exhibition d'uniforme nazi ou autre (les autres contraventions ne sont pas concernées)
Vérification d'identité
TAJ
Je suis témoin ou victime
Plateforme nationale des interceptions judiciaires
FAED
Je risque une peine d'emprisonnement
Garde-à-vue
Je sors sous contrôle judiciaire
FPR
Procureur
CASSIOPÉE
Je suis suspecté·e d'avoir commis un crime ou un délit (pas une contravention)
Quitte à m'avoir sous la main, les flics aimeraient me faire tomber pour autre chose, d'autres infractions qui leur paraissent similaires
Je sors de GAV, mais je pars en cavale
Je suis suspecté·e de tout ou n'importe quoi, sauf : une contravention, dégradations légères, outrage, rébellion, violences légères, usage de stupéfiants, dissimulation du visage, recel, provocation /participation à un attroupement
Je risque au moins 5 ans d'emprisonnement
N-SIS II (Schengen)
FNAEG
SALVAC et Bases d'analyse sérielle de la police judiciaire
ANACRIM, MERCURE, DPIO, LUPIN (LUPIN, c'est seulement pour les vols, cambriolages et dégradations)
Fichages au cours d'une procédure judiciaire : arrestation et enquête


Je demande une carte d'identité
Je demande un passeport
Je prends l'avion
Je passe mon permis de conduire
Je dois (beaucoup) de sous à l'État ou à la CAF ou quoi, depuis longtemps
Je suis déserteur ou insoumis (rien à voir avec Mélanchon)
Je tente d'obtenir des faux papiers d'identité, ou j'en obtiens
J'appelle le 17
Je fais une demande d'adoption
Fichier TES
Fichier API-PNR France
FNPC
En fait, j'avais triché au permis et la préfecture s'en est rendue compte
Je perds tous mes points et je ne rends pas mon permis à la préfecture, ou mon permis m'est retiré pour 5 ans
Fichage au FPR
Fichier Gestion des sollicitations et des interventions
Bulletin n°2 du casier judiciaire
Accès par le procureur uniquement pour une affaire de terrorisme ou de crime contre la nation
Accès par les flics (OPJ) pour tout type d'affaire en cas d'enquête de flagrance, pour identifier la personne
J'ai moins de 18 ans et je fugue de chez mes parents
Quelqu'un·e me considère comme fou/folle et obtient mon placement d'office en hôpital psychiatrique
Je n'ai pas la nationalité française et je n'exécute pas une Obligation de quitter le territoire français
Je perds mes papiers/ma voiture/n'importe quoi et le signale aux flics
FOVeS
Au 17, je demande une intervention, ou m'énerve contre le flic au téléphone
Fichier Sécurisation des interventions et demandes particulières de protection
Je passe pas mal de temps à graffer dans la rue
OCTOPUS
Fichages au cours de la vie quotidienne


Je suis tellement actif·ve politiquement que je représente une menace grave pour la sécurité publique ou pour l'État
Fichage au FPR
CAR
Je vais combattre à l'étranger pour un groupe considéré comme terroriste par l'État
N-SIS II (Schengen)
Je suis en prison
Je suis étranger·e et je représente une menace pour l'ordre public, ou je fais l'objet d'une restriction de voyage adoptée par l'Union européenne
PASP
GIPASP
Sous l'état d'urgence, la préfecture décide à mon encontre d'une interdiction de séjour, d'une assignation à résidence ou d'une interdiction de rencontrer certaines personnes
Je suis actif·ve politiquement
J'ai une voiture
FOVeS
Je suis mineur·e
ASTREE
FSPRT
GESTEREXT
CRISTINA
L'État considère que je représente une menace pour des militaires ou des installations militaires
Je suis étranger / en relation avec un État étranger / l'État considère que je pourrais être un·e espion·ne
BIOPEX
Fichier de la DGSE
Fichier de la DRM
Conservation, gestion et exploitation électronique des documents des services de renseignement territorial
SIREX
Fichages au cours de la vie militante



Fichages et consultations de fichiers au cours de la vie professionnelle : Les traits en pointillés sont ceux pour lesquels c'est certain que le fait que je postule n'augmente pas mon fichage. Les traits pleins sont ceux pour lesquels le fait que je postule est inscrit dans le fichier, voire provoque le fichage (pour ACCReD, EASP et LEGATO au moins, les autres sûrement aussi).

12 ANNEXES 2 : LETTRES-TYPES

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 lettres-types 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 !

Expéditeur :

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

LIEU, le DATE

Objet : Accès indirect à certains fichiers de l'État

Madame la Présidente,

En application de l'article 41 de la Loi du 6 janvier 1978, je soussigné(e) M./Mme XXX, né(e) le XXX à XXX, domicilié(e) au XXX, exerce par la présente mon droit d'accès indirect aux informations me concernant contenues dans les fichiers suivants :

- Traitement d'Antécédents Judiciaires (TAJ), article R40-33 du Code de procédure pénale.
- Système de Traitement des Infractions Constatées (STIC)
- Système Judiciaire de Documentation et d'Exploitation (JUDEX)
- Fichiers d'analyse sérielle prévus aux articles 230-12 à 230-18 du Code de procédure pénale en application de l'article R40-36 du même code, dont SALVAC et les bases d'analyse sérielle de la police judiciaire.
- Données exploitées par les logiciels de rapprochement judiciaire prévus par les articles 230-20 à 230-27 du Code de procédure pénale, en application de l'article 230-23 du même Code et de l'article 5 du Décret n°2012-687 du 7 mai 2012, dont ANACRIM et MERCURE.
- Automatisation de la consultation centralisée de renseignements et de données (ACCReD), article 8 du Décret n°2017-1224 du 3 août 2017.
- Diffusion et Partage de l'Information Opérationnelle (DPIO), article 6 II du Décret n°2014-187 du 20 février 2014.
- Logiciel d'uniformisation des procédures d'identification (LUPIN), article 6 de l'Arrêté du 15 octobre 2014.
- Fichier des personnes recherchées (FPR), article 9 du Décret n°2010-569 du 28 mai 2010.
- Fichier 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.
- Fichier relatif à la gestion de l'information et la prévention des atteintes à la sécurité publique (GIPASP), article R236-29 du Code de la sécurité intérieure.
- Fichier Conservation, gestion et exploitation électroniques des documents des services de renseignement territorial, article R236-51 du Code de la sécurité intérieure.
- Fichier CRISTINA, Décret du 27 juin 2008 et article R841-2 1° du Code de la sécurité intérieure.
- Fichier 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.
- Fichier de renseignement militaire (DRM), 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.
- Fichier SIREX, article R841-2 3° du Code de la sécurité intérieure.
- Fichier BCR-DNRED, article R841-2 9° du Code de la sécurité intérieure.
- 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.
- Système API-PNR France (Advance Passenger Information – Passenger Name Record), article R232-18 du Code de la sécurité intérieure.
- 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, en application de l'article R40-55 du Code de procédure pénale.
- Fichier Gestion des sollicitations et des interventions, article R236-37 du Code de la sécurité intérieure.

- Fichier Sécurisation des interventions et demandes particulières de protection, article R236-45 du Code de la sécurité intérieure.
- Fichier National des Interdits de Stade (FNIS), article 8 de l’Arrêté du 28 août 2007.
- Outil de Centralisation et de Traitement Opérationnel des Procédures et des Utilisateurs de Signatures (OCTOPUS), 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).
- Fichier de renseignement des services de l’information générale de la Direction Centrale de la Sécurité Publique et de la Préfecture de Police de Paris.

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.

Expéditeur :

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

LIEU, le DATE

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

Madame la Présidente,

En application de l'article 41 de la Loi du 6 janvier 1978, je soussigné(e) M./Mme XXX, né(e) le XXX à XXX, domicilié(e) au XXX, exerce par la présente mon droit indirect d'effacement des informations me concernant contenues dans les fichiers suivants :

- Traitement d'Antécédents Judiciaires (TAJ), article R40-31 du Code de procédure pénale.
- Système de Traitement des Infractions Constatées (STIC)
- Système Judiciaire de Documentation et d'Exploitation (JUDEX)
- Fichiers d'analyse sérielle prévus aux articles 230-12 à 230-18 du Code de procédure pénale en application de l'article R40-36 du même code, dont SALVAC et les bases d'analyse sérielle de la police judiciaire.
- Données exploitées par les logiciels de rapprochement judiciaire prévus par les articles 230-20 à 230-27 du Code de procédure pénale, en application de l'article 230-23 du même Code et de l'article 5 du Décret n°2012-687 du 7 mai 2012, dont ANACRIM et MERCURE.
- Automatisation de la consultation centralisée de renseignements et de données (ACCReD), article 8 du Décret n°2017-1224 du 3 août 2017.
- Diffusion et Partage de l'Information Opérationnelle (DPIO), article 6 II du Décret n°2014-187 du 20 février 2014.
- Logiciel d'uniformisation des procédures d'identification (LUPIN), article 6 de l'Arrêté du 15 octobre 2014.
- Fichier des personnes recherchées (FPR), article 9 du Décret n°2010-569 du 28 mai 2010.
- Fichier 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.

- Fichier relatif à la gestion de l'information et la prévention des atteintes à la sécurité publique (GIPASP), article R236-29 du Code de la sécurité intérieure.
- Fichier Conservation, gestion et exploitation électroniques des documents des services de renseignement territorial, article 236-51 du Code de la sécurité intérieure.
- Fichier CRISTINA, Décret du 27 juin 2008 et article R841-2 1° du Code de la sécurité intérieure.
- Fichier 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.
- Fichier de renseignement militaire (DRM), 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.
- Fichier SIREX, article R841-2 3° du Code de la sécurité intérieure.
- Fichier BCR-DNRED, article R841-2 9° du Code de la sécurité intérieure.
- 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.
- Système API-PNR France (Advance Passenger Information – Passenger Name Record), article R232-18 du Code de la sécurité intérieure.
- 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, en application de l'article R40-55 du Code de procédure pénale.
- Fichier Gestion des sollicitations et des interventions, article R236-37 du Code de la sécurité intérieure.
- Fichier Sécurisation des interventions et demandes particulières de protection, article R236-45 du Code de la sécurité intérieure.
- Fichier National des Interdits de Stade (FNIS), article 8 de l'Arrêté du 28 août 2007.

- Outil de Centralisation et de Traitement Opérationnel des Procédures et des Utilisateurs de Signatures (OCTOPUS), 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).
- Fichier de renseignement des services de l'information générale de la Direction Centrale de la Sécurité Publique et de la Préfecture de Police de Paris.

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

Expéditeur :

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

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 de l’article 39 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 de l’article 39 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.

Expéditeur :

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

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 40 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.

77/99 - Annexes : Demande d’accès au fichier des Titres Électroniques Sécurisés

Expéditeur :

Ministre de l’intérieur
Place BEAUVAU
75800 PARIS CEDEX 08

LIEU, le DATE

Objet : Accès aux données du fichier des Titres Électroniques Sécurisés

Madame, 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 d’accès aux informations me concernant contenues dans le fichier des Titres Électroniques Sécurisés.

En conséquence et en application de l’article 39 de la Loi n°78-17 du 6 janvier 1978 et 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.

Expéditeur :

Ministre de l'intérieur
Place BEAUVAU
75800 PARIS CEDEX 08

LIEU, le DATE

Objet : Suppression de données du fichier des Titres Électroniques Sécurisés

Madame, 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 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 40 de la Loi n°78-17 du 6 janvier 1978 et 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

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

79/99 - Annexes : Demande d’accès au Fichier National des Permis de Conduire

Expéditeur :

Préfet du domicile

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 39 de la Loi n°78-17 du 6 janvier 1978 et 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.

Expéditeur :

Préfet du domicile

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 40 de la Loi n°78-17 du 6 janvier 1978 et 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

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

Expéditeur :

Procureur de la République compétent
En fonction du domicile du demandeur

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.

Expéditeur :

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

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 de l’article 41 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.

83/99 - Annexes : Demande de suppression de certaines données du Fichier des personnes recherchées (FPR)

Expéditeur :

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

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 41 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 rectifier/effacer les informations suivantes me concernant contenues dans le Fichier des personnes recherchées :

LISTE DES INFORMATIONS CONCERNÉES

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

Expéditeur :

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

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 de l’article 41 dernier alinéa 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.

Expéditeur :

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

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 41 dernier alinéa 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 rectifier/d'effacer les informations suivantes me concernant contenues dans le Système d'information Schengen (N-SIS II) :

LISTE DES INFORMATIONS CONCERNÉES

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

Expéditeur :

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

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 l’article 41 dernier alinéa de la Loi n°78-17 du 6 janvier 1978 et de l’article R232-18 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.

87/99 - Annexes : Demande de suppression de certaines données du fichier API-PNR France

Expéditeur :

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

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 41 dernier alinéa de la Loi n°78-17 du 6 janvier 1978 et de l'article R232-18 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

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.

Expéditeur :

Procureur de la République compétent
En fonction du domicile du demandeur

LIEU, le DATE

Objet : Accès au Répertoire des expertises (REDEX)

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 Répertoire des expertises (REDEX).

En conséquence et en application de l’article R53-21-10 du Code de procédure pénale, je vous demande de bien vouloir me communiquer les données me concernant contenues dans le Répertoire des expertises (REDEX).

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.

89/99 - Annexes : Demande de suppression du Répertoire d’expertises (REDEX)

Expéditeur :

Procureur de la République compétent
En fonction du domicile du demandeur

LIEU, le DATE

Objet : Rectification/Effacement de données du Répertoire des expertises (REDEX)

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 du Répertoire des expertises (REDEX).

En conséquence et en application de l’article R53-21-11 du Code de procédure pénale, je vous demande de bien vouloir procéder à la rectification/l’effacement des données suivantes me concernant contenues dans le Répertoire des expertises (REDEX) :

LISTE DES INFORMATIONS CONCERNÉES

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

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

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.

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

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

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

Expéditeur :

Procureur de la République compétent
En fonction du domicile du demandeur

LIEU, le DATE

Objet : Accès à la Chaîne Applicative Supportant le Système d'Information Oriente Procédure pénale Et Enfants (CASSIOPÉE)

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 à la Chaîne Applicative Supportant le Système d'Information Oriente Procédure pénale Et Enfants (CASSIOPÉE).

En conséquence et en application de l'article R15-33-66-10 du Code de procédure pénale, je vous demande de bien vouloir me communiquer les données me concernant contenues dans la Chaîne Applicative Supportant le Système d'Information Oriente Procédure pénale Et Enfants (CASSIOPÉE).

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.

Expéditeur :

Procureur de la République compétent
En fonction du domicile du demandeur

LIEU, le DATE

Objet : Effacement/Rectification de données de la Chaîne Applicative Supportant le Système d'Information Oriente Procédure pénale Et Enfants (CASSIOPÉE)

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 la Chaîne Applicative Supportant le Système d'Information Oriente Procédure pénale Et Enfants (CASSIOPÉE).

En conséquence et en application de l'article R15-33-66-10 du Code de procédure pénale, je vous demande de bien vouloir procéder à la rectification/l'effacement des données suivantes me concernant contenues dans la Chaîne Applicative Supportant le Système d'Information Oriente Procédure pénale Et Enfants (CASSIOPÉE) :

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, Monsieur le Procureur, l'expression de ma plus haute considération.

Expéditeur :

Procureur de la République compétent
En fonction du lieu de la procédure ou du SPIP chargé du suivi

LIEU, le DATE

Objet : Accès à Application des Peines, Probation et Insertion (APPI)

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

En conséquence et en application de l’article R57-4-7 du Code de procédure pénale, je vous demande de bien vouloir me communiquer les données me concernant contenues dans Application des Peines, Probation et Insertion (APPI).

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.

Expéditeur :

Procureur de la République compétent
En fonction du lieu de la procédure ou du SPIP chargé du suivi

LIEU, le DATE

Objet : Effacement/Rectification de données d'Application des Peines, Probation et Insertion (APPI)

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 Application des Peines, Probation et Insertion (APPI).

En conséquence et en application de l'article R57-4-7 du Code de procédure pénale, je vous demande de bien vouloir procéder à la rectification/l'effacement des données suivantes me concernant contenues dans Application des Peines, Probation et Insertion (APPI) :

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, Monsieur le Procureur, l'expression de ma plus haute considération.

Expéditeur :

Directeur du lieu de détention si incarcération ;
Procureur de la République compétent
En fonction du domicile si la personne est libre

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 28 octobre 1996, 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.

97/99 - Annexes : Demande de suppression/rectification du FND

Expéditeur :

Directeur du lieu de détention si incarcération ;
Procureur de la République compétent
En fonction du domicile si la personne est libre

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 28 octobre 1996, 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 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.

Expéditeur :

Directeur de l’établissement d’incarcération

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 de l’établissement d’incarcération

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

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.