N° 1335

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUINZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 17 octobre 2018

RAPPORT D'INFORMATION

DÉPOSÉ
en application de l'article 145 du Règlement

PAR LA COMMISSION DES LOIS CONSTITUTIONNELLES, DE LA LÉGISLATION ET DE L'ADMINISTRATION GÉNÉRALE DE LA RÉPUBLIQUE,

En conclusion des travaux d'une mission d'information [(1)]

*sur les **fichiers** mis à la **disposition** des **forces de sécurité***

ET PRÉSENTÉ PAR

MM. DIDIER PARIS ET PIERRE MOREL-À-L'HUISSIER,

Députés

(1) La composition de cette mission figure au verso de la présente page.

La mission d'information sur les fichiers mis à la disposition des forces de sécurité est composée de : M. Didier Paris, *président-rapporteur* ; M. Pierre Morel-À-L'Huissier, *vice-président, co-rapporteur* ; MM. Ugo Bernalicis, Éric Diard, Mme Élise Fajgeles, MM. Jean-Michel Fauvergue, David Habib, Sébastien Huyghe, Mme Alexandra Louis, MM. Jean-Louis Masson, Jean-Michel Mis, Stéphane Peu, Éric Poulliat, Jean Terlier, Mmes Alice Thourot, Laurence Vichnievsky, M. Guillaume Vuilletet et Mme Hélène Zannier.

SOMMAIRE

___

Pages

MESDAMES, MESSIEURS,

La mission d'information sur les fichiers mis à la disposition des forces de sécurité a été créée par la commission des Lois de l'Assemblée nationale le 31 janvier 2018. Les dix-huit membres qui la composaient représentaient l'ensemble des groupes politiques constitués à l'Assemblée nationale. Un peu moins de dix ans après le rapport de Mme Delphine Batho et de M. Jacques Alain Bénisti consacré aux fichiers de police [(1)], cette mission d'information s'est fixé un triple objectif : dresser un état des lieux du recours par les forces de sécurité aux traitements automatisés de données personnelles ; mettre en lumière les problèmes existants ; formuler des recommandations pour y répondre. En une décennie, en effet, le contexte politique, juridique et technologique a profondément changé. La menace terroriste a pris une ampleur considérable. Le cadre législatif, reposant sur la loi fondatrice du 6 janvier 1978, a beaucoup évolué, en particulier sous l'influence du droit européen. Les évolutions techniques, enfin, offrent des possibilités inédites.

La mission d'information a choisi d'intégrer dans le périmètre de son étude l'ensemble des services de police et de gendarmerie, en y incluant ceux accomplissant des missions de renseignement ainsi que la Direction générale de la sécurité intérieure (DGSI), rattachée au ministre de l'intérieur. Elle a par ailleurs pris le parti de s'intéresser non seulement aux fichiers dont ces services ont la responsabilité, mais également à ceux auxquels ils ont ou souhaiteraient avoir accès, y compris lorsque leurs finalités sont purement administratives (comme les fichiers de sécurité sociale, par exemple).

Le champ de leurs travaux ayant ainsi été défini, les rapporteurs ont mené vingt-et-une auditions et organisé trois tables rondes, rencontrant des magistrats et des avocats aussi bien que des fonctionnaires de police et des militaires de la gendarmerie, ou des directeurs d'administration centrale tout comme des représentants associatifs et des experts indépendants. Ils ont également effectué deux journées de déplacement en région parisienne et à Lyon. Tous ces échanges leur ont fourni l'occasion d'aborder les problématiques multiples de la fiabilité et

(1) Rapport d'information sur les fichiers de police, n° 1548, commission des Lois, 24 mars 2009. Ce premier rapport a été suivi d'un second déposé par les mêmes parlementaires : rapport d'information sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police, n° 4113, commission des Lois, 21 décembre 2011.

de la durée de conservation des données, des besoins d'interconnexions ou d'accès nouveaux, des garanties en termes d'habilitation et de traçabilité des consultations, *etc*.

Au terme de leur mission, les rapporteurs saluent la diffusion au sein de la police comme de la gendarmerie d'une véritable culture des libertés individuelles. En revanche, le très grand nombre des fichiers, la complexité de leur encadrement juridique et les difficultés de leur mise à jour nuisent malheureusement à leur efficacité. Les nouvelles menaces pesant sur la sécurité publique engendrent par ailleurs pour les services de nouveaux besoins en termes d'accès aux fichiers, d'interconnexions et de fiabilisation des identités des personnes inscrites. Il convient d'y répondre, tout comme à la montée en puissance des enquêtes administratives préalables à l'exercice de certains emplois sensibles. L'ensemble de ces constats dressés par les rapporteurs les amènent à formuler vingt-et-une recommandations.

Les rapporteurs forment le vœu que leurs conclusions seront utiles à la fois au Gouvernement et à leurs collègues, sur quelque banc qu'ils siègent, pour apporter au droit encadrant les fichiers tout comme à la pratique des services de police et de gendarmerie les évolutions nécessaires. Ils n'ont été guidés dans leurs travaux que par le souci de faciliter l'exercice de leur mission par les forces de sécurité, tout en veillant à ce que les libertés individuelles soient parfaitement respectées.

I. UNE VÉRITABLE CULTURE DES LIBERTÉS INDIVIDUELLES CONTREBALANCÉE PAR DES DIFFICULTÉS JURIDIQUES ET PRATIQUES

A. LA DIFFUSION RÉUSSIE D'UNE BONNE CULTURE DES LIBERTÉS INDIVIDUELLES

1. L'ensemble des fichiers disposent aujourd'hui d'une base juridique solide

Dans leur premier rapport d'information de 2009, Mme Delphine Batho et M. Jacques Alain Bénisti avaient dressé un constat alarmant : sur les 58 fichiers de police qu'ils avaient recensés, 27 % n'avaient fait l'objet ni d'une autorisation légale ou réglementaire ni d'une déclaration à la Commission nationale de l'informatique et des libertés (CNIL). En 2011, dans leur second rapport, ils notaient qu'un mouvement de régularisation s'était amorcé à la suite de leurs recommandations mais que, compte tenu des délais de préparation des textes et de l'augmentation du nombre de fichiers (80 recensés), 45 % d'entre eux restaient dépourvus de base juridique.

Ce mouvement de régularisation s'est poursuivi depuis 2011 par l'adoption de nombreux textes réglementaires, si bien que **la CNIL estime aujourd'hui qu'il n'y a plus de mise en œuvre irrégulière d'importants traitements nationaux**.

Des initiatives ont été prises afin de procéder à un recensement des **fichiers locaux** qui s'étaient développés hors de tout cadre juridique et de sensibiliser les acteurs aux obligations de la loi du 6 janvier 1978. Grâce à la constitution d'un réseau de référents « Informatique et Libertés », des actes-cadres permettant la régularisation de ces traitements ont été adoptés.

Le choix a également pu être fait de détruire des fichiers locaux irréguliers, à l'image du fichier alphabétique de renseignements (FAR) tenu par chaque brigade de gendarmerie sous forme de fiches cartonnées. Celui-ci a été remplacé en 2011 par la base de données de sécurité publique (BDSP), qui inclut le fichier GIPASP (Gestion de l'information et prévention des atteintes à la sécurité publique).

Désormais, **l'enjeu est donc davantage la prise en compte de la protection des données personnelles dès la conception d'un projet de traitement** (1) que celui de la régularisation des fichiers existants.

---

(1) La notion de protection des données personnelles dès la conception, ou privacy by design *en anglais, a été introduite par le règlement (UE) 2016/679 du 27 avril 2016, dit règlement général sur la protection des données personnelles (RGPD). Elle s'applique également aux responsables de traitement mis en œuvre en matière policière et judiciaire, conformément à la directive (UE) 2016/680 du 27 avril 2016.*

À cet égard, le général Bruno Poirier-Coutansais, chef du service des technologies et des systèmes d'information de la sécurité intérieure du ministère de l'intérieur, a indiqué aux rapporteurs qu'une évaluation juridique initiale était systématiquement effectuée dès le premier stade d'un projet, au cours de la phase de l'étude d'opportunité. Cette évaluation fournit au responsable du traitement (direction générale de la police nationale et/ou direction générale de la gendarmerie nationale) une analyse précise du cadre juridique au regard de la finalité du traitement et du type de données collectées. Les équilibres entre les différents paramètres (finalité, nature de données, durées de conservation, périmètre des accédants, mesures de sécurité) sont ensuite recherchés au cours de la phase d'étude de faisabilité, parallèlement à la démarche d'intégration de la sécurité des systèmes d'information dans les projets.

Si cette volonté d'intégrer les impératifs de la protection des données personnelles à un stade précoce du développement d'un projet est positive, il serait néanmoins souhaitable que les services de la CNIL, qui ne sont pas systématiquement consultés à ce stade par le ministère, soient davantage associés en amont du dépôt officiel des demandes d'avis sur les actes réglementaires de création des fichiers, afin de résoudre les difficultés juridiques ou techniques susceptibles de se poser.

Proposition n° 1 : Mieux associer les services de la CNIL en amont du dépôt officiel des demandes d'avis sur les actes réglementaires de création des fichiers, de façon à résoudre les difficultés juridiques ou techniques susceptibles de se poser.

2. Les fichiers sont soumis à différents contrôles

a. Le rôle central de la CNIL

La CNIL exerce un double contrôle sur les traitements mis en œuvre par les forces de sécurité.

Il s'agit en premier lieu d'un **contrôle *a priori***. En application du I de l'article 26 de la loi du 6 janvier 1978, les traitements « *qui intéressent la sûreté de l'État, la défense ou la sécurité publique* » ou qui « *ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté* » sont **autorisés par arrêté ministériel pris après avis motivé et publié de la CNIL**.

Le II du même article prévoit que, lorsque ces traitements portent sur des données sensibles, au sens du I de l'article 8 [(1)], ils doivent être **autorisés par décret en Conseil d'État pris après avis motivé et publié de la CNIL**.

(1) Les données sensibles au sens du I de l'article 8 de la loi du 6 janvier 1978 incluent les données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou les données génétiques, biométriques traitées aux fins d'identifier une personne physique de manière unique, ainsi que les données concernant la santé ou la vie sexuelle ou l'orientation sexuelle d'une personne physique.

La récente loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, transposant la directive UE 2016/680 du 27 avril 2016 relative aux traitements en matière judiciaire et policière, a maintenu le régime d'autorisation des fichiers mis en œuvre pour le compte de l'État, en raison des garanties qu'il présente à l'égard des libertés individuelles.

La CNIL exerce, en second lieu, un **contrôle *a posteriori*** sur les traitements, en application de l'article 44 de la loi du 6 janvier 1978. Elle peut dans ce cadre diligenter des missions de contrôle de sa propre initiative ou à la suite de plaintes. Ces contrôles peuvent s'effectuer sur place, sur pièces, sur convocation et en ligne. Ils peuvent donner lieu, en application des articles 45 à 47 de la loi du 6 janvier 1978, à des mises en demeure ou à des sanctions. S'agissant des traitements relevant de l'article 26, les sanctions financières sont exclues et seuls des rappels à l'ordre ou des injonctions peuvent être prononcés.

La CNIL a, depuis 2015, diligenté 29 contrôles sur les traitements mis en œuvre par la direction générale de la police nationale, la direction générale de la gendarmerie nationale et la préfecture de police de Paris. À la suite de ces contrôles, elle n'a prononcé que deux mises en demeure et aucune sanction.

b. Le contrôle des fichiers d'antécédents et d'identification judiciaires par les procureurs de la République et les magistrats-référents

Le fichier de traitement des antécédents judiciaires (TAJ), le fichier national des empreintes génétiques (FNAEG) et le fichier automatisé des empreintes digitales (FAED) sont soumis au contrôle de la CNIL mais ils sont également **contrôlés par des magistrats du parquet, en application de dispositions spécifiques** [(1)].

(1) Les dispositions détaillées relatives au contrôle de ces fichiers par l'autorité judiciaire sont présentées infra.

Le traitement d'antécédents judiciaires (TAJ)

Le traitement d'antécédents judiciaires (TAJ) est utilisé, en application des articles 230-6 à 230-11 du code de procédure pénale, dans le cadre des enquêtes judiciaires afin de faciliter la constatation des infractions, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs.

Il est également utilisé dans le cadre d'enquêtes administratives (comme les enquêtes préalables à certains emplois relevant du domaine de la sécurité ou de la défense). Il est alimenté par la police et la gendarmerie.

Le TAJ est géré par la direction centrale de la police judiciaire.

Sont enregistrées dans le TAJ les informations relatives :

– aux personnes mises en cause, c'est-à-dire à l'encontre desquelles il y a des indices graves et concordants d'avoir participé soit à un crime, soit à un délit, soit à certaines contraventions limitativement énumérées par la loi ;

– aux victimes de ces infractions ;

– aux personnes faisant l'objet d'une enquête pour recherche des causes de la mort ou de la disparition.

En application de l'article R. 40-26 du code de procédure pénale, les données concernant l'état civil des personnes mises en cause, leur signalement et leur photographie, ainsi que les données relatives aux faits qui font l'objet de l'enquête, sont enregistrés dans le traitement.

Il existe 18,9 millions de fiches de personnes mises en cause [(1)] et plus de 87 millions d'affaires répertoriées dans le TAJ.

(1) La direction centrale de la police judiciaire a précisé que ce nombre était supérieur à celui des personnes mises en cause car une même personne peut être enregistrée sous plusieurs identités, d'une part, et certaines données ont fait l'objet d'une "anonymisation" suite à la purge mensuelle basée sur les durées maximales de conservation des infractions, ou sur décision de justice, sans que la fiche elle-même soit effacée, d'autre part.

Le fichier automatisé des empreintes digitales (FAED)

Créé par le décret n° 87-249 du 8 avril 1987, le fichier automatisé des empreintes digitales (FAED) a pour finalité principale de faciliter la recherche et l'identification des auteurs de crimes et de délits, ainsi que la poursuite, l'instruction et le jugement des procédures criminelles et délictuelles dont l'autorité judiciaire est saisie.

Le FAED peut également être utilisé pour faciliter la recherche de personnes disparues et l'identification de personnes décédées ou grièvement blessées.

Le FAED est géré par le service central de la police technique et scientifique (SCPTS).

Sont notamment enregistrées dans le FAED :

– les traces relevées dans le cadre d'une enquête ;

– les empreintes digitales et palmaires des personnes mises en cause en matière criminelle ou délictuelle ;

– les données relatives à l'état civil des personnes dont les empreintes sont enregistrées ;

– la nature de l'affaire et la référence de la procédure.

Actuellement, 6,2 millions de personnes et 220 000 traces non résolues sont enregistrées dans le FAED.

Le fichier national automatisé des empreintes génétiques (FNAEG)

Le fichier national automatisé des empreintes génétiques (FNAEG) est utilisé, en application de l'article 706-54 du code de procédure pénale, pour effectuer des rapprochements entre les empreintes génétiques prélevées sur des personnes mises en cause ou condamnées ou issues de traces biologiques prélevées sur des scènes d'infractions, et les profils déjà enregistrés dans la base de données.

Le FAED est géré par le service central de la police technique et scientifique (SCPTS).

Sont notamment enregistrées dans le FNAEG (article R. 53-11 du code de procédure pénale) :

– les empreintes génétiques de personnes non identifiées relevées sur les lieux d'une infraction ;

– les empreintes génétiques des personnes mises en cause ou condamnées pour l'une des infractions énumérées à l'article 706-55 du code de procédure pénale ;

– les données d'état civil des personnes identifiées ;

– la nature de l'affaire et la référence de la procédure.

Actuellement, environ 2,9 millions de profils génétiques et 480 000 traces non identifiées sont enregistrés dans le FNAEG.

Ces trois fichiers sont placés sous le contrôle des **procureurs de la République territorialement compétents**, dans le ressort desquels les procédures ont été ouvertes. Les procureurs de la République peuvent être saisis de requêtes

en effacement des données contenues dans les fichiers sur lesquels s'opère leur contrôle. Les conditions de cet effacement diffèrent selon les fichiers [(1)].

Les trois fichiers sont également placés sous le contrôle de magistrats du parquet dits **magistrats référents.** S'agissant du TAJ et du FNAEG, ces magistrats sont désignés pour trois ans par arrêté du ministre de la justice et sont assistés de comités composés de trois personnes nommées dans les mêmes conditions. S'agissant du FAED, le magistrat référent est le procureur général près la cour d'appel de Lyon, dans le ressort de laquelle est situé le service central de la police technique et scientifique, gestionnaire du fichier.

Les compétences des magistrats référents sont différentes selon les fichiers concernés :

– le magistrat référent chargé du contrôle du TAJ est compétent pour les demandes d'effacement ou de rectification portant sur des données issues de procédures diligentées sur plusieurs ressorts de TGI ;

– le magistrat référent chargé du contrôle du FAED peut d'office ordonner l'effacement des informations dont la conservation ne paraîtrait manifestement plus utile compte tenu de la finalité du traitement ;

– le magistrat référent chargé du contrôle du FNAEG contrôle les informations enregistrées dans le fichier et peut solliciter l'effacement de toute inscription illicite.

c. Le régime dérogatoire des fichiers intéressant la sécurité de l'État, la défense ou la sécurité publique

La loi du 6 janvier 1978 prévoit que différentes dérogations peuvent s'appliquer aux fichiers intéressant la sécurité de l'État, la défense ou la sécurité publique.

● Le **décret n° 2007-914 du 15 mai 2007** [(2)] énumère les dix-sept fichiers pour lesquels, en application de l'article 30 de la loi du 6 janvier 1978, **les demandes d'avis adressées à la CNIL peuvent ne pas comporter tous les éléments d'information exigés pour les autres traitements**. Il s'agit des fichiers mis en œuvre par les services spécialisés de renseignement [(3)] mais aussi de certains fichiers gérés par la DGPN ou la DGGN, comme le fichier « Prévention des atteintes à la sécurité publique » (PASP) et le fichier « Gestion de l'information et prévention des atteintes à la sécurité publique » (GIPASP), ou

---

(1) Cf. infra.

(2) Décret n°2007-914 du 15 mai 2007 pris pour l'application du I de l'article 30 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

(3) Direction générale de la sécurité extérieure, direction du renseignement et de la sécurité de la défense, direction du renseignement militaire, direction générale de la sécurité intérieure, direction nationale du renseignement et des enquêtes douanières et service « traitement du renseignement et action contre les circuits financiers clandestins » (TRACFIN).

relevant d'autres ministères comme le ministère de la justice ou le ministère de la défense.

● Les actes réglementaires autorisant ces fichiers (à l'exception des fichiers PASP et GIPASP) bénéficient d'une **dispense de publication**, comme l'autorise le III de l'article 26 de la loi du 6 janvier 1978, et seul le sens de l'avis adopté par la CNIL est publié.

● Enfin, onze de ces fichiers ne sont **pas soumis au contrôle *a posteriori* exercé par la CNIL**, en application du IV de l'article 44 de la loi du 6 janvier 1978. La CNIL peut uniquement contrôler les fiches individuelles contenues dans ces traitements, dans le cadre du droit d'accès indirect obligatoire pour ces fichiers, aux termes de l'article 41 de la loi.

Le droit d'accès indirect

L'article 41 de la loi du 6 janvier 1978 prévoit que, par exception aux articles 39 et 40, le droit d'accès s'exerce de manière indirecte lorsqu'un traitement intéresse la sûreté de l'État, la défense ou la sécurité publique.

La demande est adressée à la CNIL « *qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires* ». Si, en accord avec le responsable du traitement, elle estime que la communication des données ne met pas en cause ses finalités, la sûreté de l'État, la défense ou la sécurité publique, elle communique les éléments au requérant. En cas de désaccord, elle informe simplement le requérant qu'elle a procédé aux vérifications nécessaires.

L'acte réglementaire portant création du fichier peut néanmoins autoriser le responsable du traitement directement saisi à communiquer ces informations « *lorsque le traitement est susceptible de comprendre des informations dont la communication ne mettrait pas en cause les fins qui lui sont assignées* ».

Le champ des traitements auxquels s'applique le droit d'accès indirect a été réduit par la loi du 20 juin 2018 relative à la protection des données personnelles assurant la transposition de la directive (UE) 2016/680 sur les traitements en matière judiciaire ou policière. L'article 29 de cette loi supprime en effet l'application du droit d'accès indirect aux traitements de police judiciaire, auparavant prévu par l'article 42 de la loi du 6 janvier 1978. Le nouvel article 70-19 de la loi du 6 janvier 1978 prévoit un droit d'accès direct à ces traitements, qui peut cependant faire l'objet de restrictions pour certains motifs (par exemple, pour éviter de gêner des enquêtes, des recherches ou des procédures administratives ou judiciaires), en application de l'article 70-21. Les actes réglementaires relatifs aux différents traitements devront être modifiés pour prendre en compte ces nouvelles dispositions. S'agissant du TAJ, le décret n° 2018-687 du 1er août 2018 (1) a déjà prévu un droit d'accès direct s'exerçant auprès du ministère de l'intérieur (article R. 40-33 du code de procédure pénale).

(1) Décret n° 2018-687 du 1er août 2018 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

Le tableau ci-dessous fait état des fichiers concernés par les différentes dérogations.

LES FICHIERS RELEVANT DU DÉCRET N° 2007-914 DU 15 MAI 2007

Nom du fichier	**Gestionnaire**	**Dispense de publication de l'acte réglementaire**	**Exclusion du contrôle *a posteriori* de la CNIL**
Centralisation du renseignement intérieur pour la sécurité du territoire et les intérêts nationaux (CRISTINA)	Direction générale de la sécurité intérieure (DGSI)	X	X
Fichiers d'informations nominatives	Direction générale de la sécurité extérieure (DGSE)	X	X
Système d'information de la recherche et de l'exploitation du renseignement de contre-ingérence (SIREX)	Direction du renseignement et de la sécurité de la défense (DRSD)	X	X
Fichier d'informations nominatives	Direction du renseignement militaire (DRM)	X	X
BCR (Base centrale de renseignement) - DNRED	Direction nationale du renseignement et des enquêtes douanières (DNRED)	X	X
Fichier de la DGSE	DGSE	X	X
Fichier du personnel de la DGSE	DGSE	X	X
Traitement automatisé d'informations nominatives de personnes étrangères	DRM	X	X
Prévention des atteintes à la sécurité publique (PASP)	DGPN		
Système de traitement et analyse du renseignement de TRACFIN (STARTRAC)	TRACFIN	X	
Gestion de l'information et la prévention des atteintes à la sécurité publique (GIPASP)	DGGN		
Fichier des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT)	UCLAT	X	
CAR (suivi des personnes placées sous main de justice et destiné à la prévention des atteintes à la sécurité pénitentiaire et à la sécurité publique)	Administration pénitentiaire	X	
Fichier relatif à l'assistance au suivi du traitement de la radicalisation en services éducatifs (ASTREE)	Protection judiciaire de la jeunesse	X	
Gestion du terrorisme et des extrémismes violents (GESTEREXT)	Préfecture de police de Paris	X	X
BIOPEX	DRM	X	X
LEGATO	Commandement de la légion étrangère	X	X

Par ailleurs, les traitements relevant de la sécurité nationale et du renseignement sont exclus du champ d'application du droit de l'Union européenne en matière de protection des données personnelles, qu'il s'agisse du règlement

général sur la protection des données ou de la directive (UE) 2016/680 sur les traitements en matière judiciaire ou policière.

Cette situation paraît satisfaisante aux rapporteurs au regard des finalités de ces fichiers.

d. Le contrôle des juridictions nationales et européennes

Les fichiers mis en œuvre par les forces de sécurité font également l'objet d'un contrôle juridictionnel au regard des différentes normes qui les régissent, au plan national, par le Conseil constitutionnel, le Conseil d'État et la Cour de cassation, et au plan européen, par la Cour européenne des droits de l'homme (CEDH) et la Cour de justice de l'Union européenne (CJUE). Ce contrôle donne lieu à une jurisprudence abondante, qui a fait évoluer le cadre juridique des fichiers sur plusieurs points importants (1).

3. Des systèmes d'habilitation, d'authentification et de traçabilité sont mis en œuvre pour garantir la protection et la sécurité des données personnelles

Le code de déontologie de la police et de la gendarmerie nationales énonce clairement l'obligation pour les agents de se conformer aux dispositions législatives et réglementaires relatives à la création et à l'utilisation des fichiers et d'alimenter et consulter ces fichiers dans le strict respect de leurs finalités et règles propres (2).

L'habilitation, l'authentification et la traçabilité sont les trois volets du contrôle de l'accès aux fichiers, élément essentiel de la protection des libertés individuelles et de la sécurité des données.

La définition et la mise en œuvre des règles d'habilitation, au niveau central dans la gendarmerie nationale et au niveau des chefs de service dans la police nationale, sont jugées satisfaisantes par la CNIL.

L'authentification repose sur un logiciel commun à la gendarmerie et à la police nationales, nommé Proxyma pour la gendarmerie, et CHEOPS-NG pour la police. L'accès aux applications se fait soit à partir d'une carte professionnelle à puce, soit par identifiant et mot de passe.

Comme le recommande la CNIL dans ses réponses écrites aux rapporteurs, il conviendrait de supprimer définitivement l'utilisation des identifiants et mots de passe, et de **généraliser à l'ensemble des fichiers l'authentification par la carte professionnelle** qui offre plus de garanties en matière de sécurité et de confidentialité.

---

(1) Cf. infra.

(2) Article R. 434-21 du code de la sécurité intérieure.

Proposition n° 2 : Supprimer l'authentification par identifiants et mots de passe, et généraliser l'authentification par la carte professionnelle.

Les fichiers mis en œuvre au cours des dernières années par la DGPN et la DGGN prévoient systématiquement **la traçabilité des consultations**. Cette obligation de traçabilité, ainsi que la durée de conservation des traces, sont mentionnées dans l'acte réglementaire autorisant le traitement. L'article 70-15 de la loi du 6 janvier 1978, qui transpose la directive du 27 avril 2016, prévoit un **renforcement des obligations de traçabilité**. Les responsables de traitement auront l'obligation d'établir « *un journal des opérations de collecte, de modification, de consultation et de communication, y compris les transferts, l'interconnexion et l'effacement, portant sur de telles données* ». Des évolutions techniques vont devoir être engagées pour se conformer à ces nouvelles obligations.

La recherche en traçabilité peut être ordonnée dans le cadre d'enquêtes judiciaires [(1)] ou administratives conduites par les directions d'emploi du ministère de l'intérieur ou par les inspections générales de la police et de la gendarmerie nationales (IGPN et IGGN).

Ces inspections procèdent également à des contrôles d'initiative. Les contrôles portent essentiellement sur le fichier TAJ et visent à déceler les consultations irrégulières, portant par exemple sur les agents ou leur famille, ou relatives à des personnalités connues.

Mme Marie-France Moneger-Guyomarc'h, cheffe de l'IGPN, a indiqué aux rapporteurs qu'au vu de ces différents contrôles, il demeurait quelques cas de consultations personnelles, donnant systématiquement lieu à des suites, mais que les cas de consultations par intérêt personnel avaient beaucoup diminué. Ces faits isolés ne caractérisent pas un dysfonctionnement du système.

Ainsi que l'a souligné le général Michel Labbé, chef de l'IGGN, il faut désormais **développer l'analyse massive des données pour détecter plus largement les comportements irréguliers**. En effet, les traces collectées pourraient être davantage exploitées grâce à la puissance de calcul, au recours aux algorithmes et à la collecte de données de masse. Cette évolution paraît d'autant plus nécessaire que le programme NEO d'équipement des policiers et gendarmes de terminaux mobiles (*smartphones* et tablettes) conduit à une augmentation significative des consultations de fichiers, et donc des traces de connexions.

Proposition n° 3 : Développer, notamment par des procédés algorithmiques, l'analyse massive des données recueillies grâce à la traçabilité pour détecter plus largement les comportements irréguliers d'utilisation des fichiers.

(1) L'article 226-21 du code pénal prévoit que le détournement de données à caractère personnel de leur finalité est puni d'une peine de cinq ans d'emprisonnement et 300 000 euros d'amende.

B. DES LIMITES JURIDIQUES ET PRATIQUES

1. Un nombre trop élevé de fichiers

a. Un champ très vaste

La notion de « fichiers mis à la disposition des forces de sécurité » retenue par la mission d'information vise à couvrir la grande diversité des fichiers utilisés.

D'un point de vue juridique, elle ne correspond pas au champ des fichiers régis par l'article 26 de la loi du 6 janvier 1978, qui vise les fichiers ayant pour finalité la sûreté de l'État, la défense ou la sécurité publique et ceux relatifs à la prévention, la recherche, la constatation ou la poursuite des infractions pénales. Les services de police et de gendarmerie ont en effet recours, pour l'accomplissement de leurs missions, à différents fichiers administratifs, qui se distinguent par leur finalité des fichiers régis par l'article 26. Il s'agit le plus souvent de fichiers dépendant d'autres directions du ministère de l'intérieur, comme le fichier national des permis de conduire (FNPC) ou l'application de gestion du répertoire informatisé des propriétaires et possesseurs d'armes (AGRIPPA), mais qui peuvent aussi relever d'autres ministères. Dans cette dernière hypothèse, les agents doivent recourir à des réquisitions judiciaires pour pouvoir accéder aux données des traitements concernés, sauf s'ils disposent d'une habilitation spécifique [(1)].

À l'inverse, des fichiers répondant à la définition de l'article 26 peuvent être administrés et utilisés par d'autres acteurs que les forces de sécurité (douanes, services du ministère de la justice...).

En 2009, la mission d'information sur les fichiers de police conduite par Mme Delphine Batho et M. Jacques Alain Bénisti avait distingué, en fonction de leurs finalités, plusieurs catégories de fichiers, qui sont encore aujourd'hui parfaitement valables [(2)] :

– **les fichiers à caractère administratif**, destinés à enregistrer des données administratives sur des personnes, des objets ou des moyens de transport ;

– **les fichiers judiciaires**, qui incluent les **fichiers à vocation judiciaire**, ayant pour objet la collecte et la centralisation de renseignements destinés à lutter contre des infractions bien déterminées, par exemple le fichier des objets et véhicules volés (FOVeS), le fichier national du faux monnayage (FNFM) ou le fichier des brigades spécialisées (FBS), le fichier **d'antécédents judiciaires** (TAJ) ayant pour finalité de faciliter la constatation des infractions pénales, le

---

(1) Les officiers de police judiciaire peuvent par exemple consulter directement le fichier national des comptes bancaires (FICOBA) et le fichier des contrats de capitalisation et d'assurance-vie (FICOVIE) du ministère de l'économie et des finances.

(2) Cette classification est proche de celle établie en 2008 par le groupe de contrôle des fichiers de police et de gendarmerie présidé par M. Alain Bauer dans son rapport remis au ministre de l'intérieur, Mieux contrôler la mise en œuvre des dispositifs pour mieux protéger les libertés.

rassemblement des preuves des infractions et la recherche de leurs auteurs et les **fichiers d'identification judiciaire**, comme le fichier automatisé des empreintes digitales (FAED) et le fichier national des empreintes génétiques (FNAEG) ;

– **les fichiers de renseignement**, qui peuvent désigner les fichiers mis en œuvre par les services spécialisés de renseignement ainsi que ceux mis en œuvre par l'ensemble des services du ministère de l'intérieur chargés du renseignement de sécurité intérieur et territorial, ce qui inclut les fichiers mis en œuvre par la DGPN et la DGGN, par exemple le fichier « Prévention des atteintes à la sécurité publique » (PASP) mis en œuvre par la DGPN et le fichier « Gestion de l'information et prévention des atteintes à la sécurité publique » (GIPASP) mis en œuvre par la DGGN ;

– **les fichiers de rapprochement destinés à lutter contre la délinquance sérielle**, comme le fichier SALVAC (système d'analyse des liens de la violence associée aux crimes) **et les fichiers ou logiciels de rapprochement et d'analyse criminelle utilisés dans le cadre d'une même enquête**, comme ANACRIM.

b. Une multiplication des fichiers qui nuit à leur bonne utilisation

Le tableau publié en annexe fait état de 106 fichiers mis à la disposition des forces de sécurité [(1)].

Ayant fait le constat du manque de transparence de ces informations, les rapporteurs ont souhaité rendre publique la liste de ces fichiers [(2)].

L'article 30 du règlement général sur la protection des données et l'article 30 de la loi du 20 juin 2018, pour les traitements relevant de la directive 2016/680 du 27 avril 2016, rendent obligatoire la tenue d'un **registre des fichiers** par les responsables de traitement. Ce document est destiné à être mis à disposition de la CNIL en cas de contrôle. Les rapporteurs espèrent que l'élaboration de ce registre au sein du ministère de l'intérieur, qui est en cours, permettra de disposer d'une cartographie exacte des traitements mis en œuvre.

Le texte est encore trop récent pour en vérifier l'application mais les rapporteurs relèvent l'intérêt qui s'y attache, notamment au regard de la nécessité d'une cartographie à jour.

Sur la base du recensement qu'ils ont établi, les rapporteurs estiment que **les fichiers mis à la disposition des forces de sécurité sont trop nombreux et forment un ensemble trop complexe.**

---

(1) La liste des fichiers utilisés ou gérés par la préfecture de police de Paris n'a pas été communiquée en dépit de la demande des rapporteurs.

(2) Cf. annexe n° 4.

Cette situation peut s'expliquer par différents facteurs :

– la nécessité légale de définir précisément les finalités de chaque traitement et les personnes habilitées à y accéder impose un certain cloisonnement des fichiers ;

– l'évolution des besoins opérationnels des forces de sécurité a conduit à une multiplication des fichiers, sans réflexion sur la cohérence de l'architecture globale ;

– l'organisation institutionnelle du ministère de l'intérieur – caractérisée par la dualité entre police nationale et gendarmerie nationale, l'organisation de la police nationale en directions centrales exerçant des missions spécialisées, les compétences de la préfecture de police de Paris – a favorisé le développement de fichiers spécifiques sans tenir suffisamment compte des besoins communs. Des efforts de rationalisation ont certes été entrepris, puisque les grands fichiers (TAJ, FPR, FOVeS...) sont aujourd'hui communs à la police et à la gendarmerie et que la DGPN s'efforce d'adopter depuis quelques années une approche plus transversale du développement des fichiers, mais ils restent insuffisants.

Le trop grand nombre de fichiers et la complexité de leur architecture nuisent à leur utilisation optimale, comme le révèlent de nombreuses auditions, dont celle de Mme Mireille Ballestrazzi, directrice centrale de la police judiciaire. La multiplication des fichiers conduit les enquêteurs à hésiter à y recourir ou bien à consacrer un temps de travail croissant à l'interrogation des différentes bases disponibles (une trentaine de fichiers ont vocation à être interrogés par les enquêteurs de la police judiciaire dans le cadre de leurs missions). Les conditions d'urgence dans lesquelles se trouvent les enquêteurs (garde à vue, opérations sur la voie publique…) rendent en outre plus compliquée la consultation de multiples fichiers.

Les rapporteurs souhaitent donc que soit menée au sein du ministère de l'intérieur **une réflexion globale sur la rationalisation des fichiers existants**. Cette réflexion devra s'appuyer sur une analyse de la finalité des différents fichiers et de leur utilisation par les forces de sécurité.

Se pose par ailleurs la question de l'interconnexion des fichiers ou d'une interface pour y accéder (*cf. infra*).

Proposition n° 4 : Mener, au sein du ministère de l'intérieur, une réflexion globale sur la rationalisation des fichiers existants, s'appuyant sur une analyse de leur finalité et de leur utilisation par les forces de sécurité.

2. Un encadrement complexe et instable

Les fichiers mis à la disposition des forces de sécurité font l'objet d'un encadrement juridique particulièrement complexe, qui entremêle des normes d'origines et de niveaux différents dont l'harmonisation se révèle parfois difficile.

La maîtrise de la réglementation par les services de police et de gendarmerie en est rendue moins aisée, de même que l'exercice de leurs droits par les citoyens. Cette complexité est aussi source de fragilité juridique non seulement parce qu'il est difficile de connaître l'état du droit applicable mais aussi parce que certaines poursuites courent le risque d'être privées de base légale.

a. Un cadre législatif et réglementaire foisonnant

i. Des dispositions législatives éparses et fréquemment modifiées

Le cadre juridique des fichiers mis à la disposition des forces de sécurité est constitué tout d'abord de dispositions législatives multiples et en perpétuelle évolution, au premier rang desquelles figure la loi fondatrice du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Comme cela a été rappelé plus haut, l'article 26 de cette loi pose le cadre applicable aux fichiers mis à la disposition des forces de sécurité, autorisés par arrêté ministériel, pris après avis motivé et publié de la CNIL. Ceux de ces traitements qui portent sur des données « sensibles » au sens du I de l'article 8 de la même loi, dont la collecte est en principe interdite, ne peuvent être autorisés que par décret en Conseil d'État, pris après avis motivé et publié de la CNIL. Aux termes de l'article 27, les traitements mis en œuvre pour le compte de l'État, agissant dans l'exercice de ses prérogatives de puissance publique, qui portent sur des données génétiques ou biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes, ne peuvent également être autorisés que par décret en Conseil d'État, pris après avis motivé et publié de la CNIL.

Les fichiers mis à la disposition des forces de sécurité sont par ailleurs soumis aux principes généraux suivants posés par l'article 6 de la loi de 1978 :

— les données doivent être collectées et traitées de manière loyale et licite (principe de légalité) ;

— elles sont collectées « *pour des finalités déterminées, explicites et légitimes* » (principe de finalité) ;

— elles sont « *adéquates, pertinentes et non excessives* » au regard des finalités poursuivies (principe de proportionnalité) ;

— elles sont exactes, complètes et mises à jour et « *les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées* » ;

— elles « *sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées* ».

La loi du 6 janvier 1978 a été modifiée à de nombreuses reprises, et encore de façon très récente par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles [(1)]. L'article 30 de cette dernière crée ainsi au sein de la loi de 1978 un nouveau chapitre XIII, consacré aux dispositions applicables aux traitements relevant de la directive du Parlement européen et du Conseil du 27 avril 2016.

Outre la loi fondatrice de 1978, maintes fois retouchée, de nombreux textes législatifs se sont succédé pour encadrer le droit applicable aux fichiers mis à la disposition des forces de sécurité, souvent en complétant le code de procédure pénale ou le code de la sécurité intérieure.

La loi n° 80-2 du 4 janvier 1980 relative à l'automatisation du casier judiciaire a ainsi inséré dans le code de procédure pénale un article 777-3 aux termes duquel aucun fichier ou traitement de données à caractère personnel détenu par une personne quelconque ou par un service de l'État ne dépendant pas du ministère de la justice ne peut mentionner, hors les cas et dans les conditions prévus par la loi, des jugements ou arrêts de condamnation.

La loi n° 2010-242 du 10 mars 2010 tendant à amoindrir le risque de récidive criminelle a modifié les articles 706-53-5 et suivants du même code afin de prévoir notamment que le gestionnaire du FPR (Fichier des personnes recherchées) soit directement informé des effacements opérés au sein du Fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes (FIJAISV).

La loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, dite « LOPPSI 2 », a fixé dans le même code [(2)] les règles applicables aux fichiers d'antécédents, d'analyse sérielle et des personnes recherchées, en précisant notamment les modalités de contrôle des données inscrites dans ces fichiers par l'autorité judiciaire.

La loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale a créé, toujours au sein du même code, un article 706-56-1-1 consacrant l'existence des recherches en parentalité dans le Fichier national automatisé des empreintes génétiques (FNAEG) [(3)].

---

(1) L'article 8 de cette loi a par ailleurs élargi, conformément au RGPD, le champ des données dites « sensibles », prévues à l'article 8 de la loi du 6 janvier 1978, aux « données génétiques », aux « données biométriques » ainsi qu'aux « données concernant (...) l'orientation sexuelle d'une personne physique ». Son article 11 a supprimé le régime simplement déclaratif dont bénéficiaient certains fichiers.

(2) Articles 230-6 et suivants.

(3) Ces recherches consistent à comparer les résultats des analyses génétiques d'une trace issue d'une personne inconnue recueillie sur une scène d'infraction avec les profils génétiques des personnes suspectes ou déclarées coupables enregistrés au FNAEG, dans le but d'identifier une ou des personnes pouvant être apparentées en ligne directe à cette personne inconnue.

La loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme (dite loi « SILT ») a autorisé, pour la prévention des actes de terrorisme et des atteintes aux intérêts fondamentaux de la nation, la mise en œuvre de deux traitements automatisés de données à caractère personnel. Son article 13 a modifié le code de la sécurité intérieure afin de pérenniser le régime permettant la consultation des données du fichier des passagers du transport aérien (*Passenger Name Record* ou PNR). Son article 14 a modifié le même code pour créer, selon des modalités appropriées à ses spécificités, un système national de collecte des données des dossiers passagers du transport maritime à destination ou au départ de la France, distinct du système PNR.

La loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles a notamment [(1)] réécrit l'article 230-8 du code de procédure pénale relatif au contrôle du fichier TAJ par le procureur de la République.

Des dispositions régissant les fichiers mis à la disposition des forces de sécurité figurent également dans le code civil, par exemple à son article 16-11 [(2)] qui traite notamment de l'identification d'une personne par ses empreintes génétiques dans le cadre de mesures d'enquête ou d'instruction ou aux fins d'établir l'identité de personnes décédées.

Divers textes de nature législative sont aussi intervenus pour créer directement un certain nombre de fichiers, tels que le FNAEG (Fichier national automatisé des empreintes génétiques) [(3)], le FIJAIS (Fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes) [(4)] ou encore le FIJAIT (Fichier judiciaire national automatisé des auteurs d'infractions terroristes) [(5)].

ii. De multiples dispositions réglementaires

À cet éparpillement législatif s'ajoute une multiplicité de dispositions réglementaires, dont les rapporteurs ne donneront que quelques exemples. On y trouve bien entendu un certain nombre de textes créant directement des fichiers, tels que le décret n° 87-249 du 8 avril 1987 créant le FAED, le décret n° 2010-569 du 28 mai 2010 créant le FPR (Fichier des personnes recherchées), le décret n° 2012-652 du 4 mai 2012 créant le TAJ (Traitement des antécédents judiciaires) ou encore l'arrêté du 28 août 2007 créant le FNIS (Fichier national des interdits de stade). À titre d'illustration également, les fichiers EASP (Enquêtes administratives liées à la sécurité publique), PASP (Prévention des atteintes à la sécurité publique) et GIPASP (Gestion de l'information et prévention des atteintes

(1) Article 36.

(2) Modifié en dernier lieu par la loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure et par la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.

(3) Loi n° 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs.

(4) Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.

(5) Loi n° 2015-912 du 24 juillet 2015 relative au renseignement.

à la sécurité publique) sont régis par les articles R. 236-1 et suivants du code de la sécurité intérieure.

On peut citer ensuite tous les décrets d'application des textes de loi mentionnés plus haut. Un décret n° 2018-687 du 1er août 2018 précise par exemple les conditions d'application de la loi du 20 juin 2018. Son article 32 prévoit, compte tenu du droit d'accès et de rectification direct en particulier au fichier TAJ désormais reconnu à toute personne (de sorte qu'il n'est plus nécessaire de demander à la CNIL d'intervenir), que la CNIL transmet aux responsables de traitement l'ensemble des demandes tendant à la mise en œuvre des droits d'accès indirect, de rectification et d'effacement prévus par le chapitre XIII de la loi du 6 janvier 1978 qui lui ont été adressées avant le 4 août 2018.

Un certain nombre de décrets spécifiques viennent enfin compléter le droit applicable aux fichiers mis à la disposition des forces de sécurité, comme le décret précité du 15 mai 2007 énumérant les fichiers de renseignement (1) qui se trouvent dispensés de l'obligation de publication des actes qui les autorisent (CRISTINA, GESTEREXT, FSPRT, *etc.*).

iii. Les durées de conservation et les conditions d'effacement, caractéristiques de l'hétérogénéité des régimes applicables

Les durées de conservation et les conditions d'effacement constituent un exemple emblématique de l'hétérogénéité, d'un fichier à l'autre, des régimes juridiques applicables, comme le montre le tableau ci-dessous relatif au FNAEG, au FAED (2) et au TAJ (3).

(1) Chaque service de renseignement dispose d'un fichier principal.

(2) Articles 7,7-1 et 7-2 du décret n° 87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur.

(3) Articles 230-8 et 230-9 du code de procédure pénale.

PRINCIPALES RÈGLES RELATIVES AUX DURÉES DE CONSERVATION ET AUX CONDITIONS D'EFFACEMENT DES DONNÉES DANS LE FNAEG, LE FAED ET LE TAJ

	DURÉES DE CONSERVATION DES DONNÉES	CONDITIONS D'EFFACEMENT ANTICIPÉ DES DONNÉES
FNAEG	- 40 ans (pour les personnes définitivement condamnées et pour celles ayant bénéficié d'un classement sans suite, d'un non-lieu, d'une relaxe ou d'un acquittement exclusivement fondés sur l'existence d'un trouble mental - 25 ans (pour les personnes mises en cause et pour les empreintes génétiques des ascendants ou descendants)	Personnes soupçonnées (« *à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient commis une infraction mentionnée à l'article 706-55* » du CPP) : effacement des empreintes sur instruction du procureur de la République agissant soit d'office, soit à la demande de l'intéressé, lorsque leur conservation n'apparaît plus nécessaire compte tenu de la finalité du fichier. Recours possible devant le juge des libertés et de la détention (JLD), puis devant le président de la chambre de l'instruction.
		Personnes condamnées : pas de possibilité d'effacement.
FAED	10 ans, 15 ans ou 25 ans (en fonction de la gravité de l'infraction, de la qualité de mineur ou de majeur de la personne concernée et du caractère national ou international de la procédure)	En cas de décision de relaxe ou d'acquittement devenue définitive : effacement des empreintes dès réception de l'avis qui en informe le service gestionnaire.
		En cas de décision de non-lieu ou de classement sans suite pour absence d'infraction ou insuffisance de charges ou pour auteur inconnu : effacement des empreintes, sauf si le procureur de la République estime que la conservation est nécessaire pour des raisons liées à la finalité du fichier au regard de la nature ou des circonstances de commission de l'infraction ou de la personnalité de la personne concernée (il ne peut s'opposer à l'effacement lorsque la prescription de l'action publique est acquise). Recours possible devant le JLD, puis le président de la chambre de l'instruction.
		Autres motifs de classement sans suite (pour motifs de droit ou inopportunité des poursuites) : pas de possibilité d'effacement.
		Le procureur général près la cour d'appel de Lyon peut d'office ordonner l'effacement des informations dont la conservation ne paraîtrait manifestement plus utile compte tenu de la finalité du traitement.
TAJ	- 5 ans, 10 ans, 20 ans ou 40 ans pour les personnes mises en cause (en fonction de la gravité de l'infraction et de la qualité de mineur ou de majeur de la personne concernée) - 15 ans au maximum pour les victimes	Le procureur de la République territorialement compétent (ou le magistrat référent en cas d'inscriptions relevant de plusieurs ressorts de TGI) peut, d'office ou à la demande de la personne concernée, ordonner que les données soient effacées, complétées ou rectifiées.
		En cas de requalification judiciaire : rectification de droit.
		En cas de décision de relaxe ou d'acquittement devenue définitive : effacement des données, sauf si le procureur de la République en prescrit le maintien, auquel cas elles font l'objet d'une mention (elles ne peuvent plus alors être consultées dans le cadre des enquêtes administratives).
		En cas de décision de non-lieu ou de classement sans suite : mention, sauf si le procureur de la République ordonne l'effacement.
		Recours possible devant le président de la chambre de l'instruction.

b. Des précisions et des réserves apportées par la jurisprudence constitutionnelle

Le Conseil constitutionnel est intervenu à plusieurs reprises en matière de droit des fichiers pour formuler des réserves d'interprétation ou pour constater une inconstitutionnalité dont l'effet a toutefois été repoussé dans le temps.

Saisi de la conformité à la Constitution des articles 706-54 à 706-55 du code de procédure pénale, le Conseil constitutionnel a formulé, dans sa décision n° 2010-25 QPC du 16 septembre 2010, une réserve d'interprétation portant sur la fixation de la durée de conservation des empreintes au fichier national automatisé des empreintes génétiques (FNAEG). Il a jugé qu'il appartenait au pouvoir réglementaire, compte tenu de l'objet du fichier, de proportionner la durée de conservation de ces données personnelles à la nature ou à la gravité des infractions concernées tout en adaptant ces modalités aux spécificités de la délinquance des mineurs. Des durées excessives seraient sanctionnées par le juge administratif. Le décret supposé moduler ainsi la durée de conservation au FNAEG n'a pas vu le jour pour l'instant.

Les rapporteurs relèvent aussi que le Conseil constitutionnel a jugé, dans une décision n° 2017-670 QPC du 27 octobre 2017, qu'en privant les personnes mises en cause dans une procédure pénale, autres que celles ayant fait l'objet d'une décision d'acquittement, de relaxe, de non-lieu ou de classement sans suite, de toute possibilité d'obtenir l'effacement de leurs données personnelles inscrites dans le fichier des antécédents judiciaires (TAJ), les dispositions de l'article 230-8 du code de procédure pénale portaient une atteinte disproportionnée au droit au respect de la vie privée. La loi du 20 juin 2018 relative à la protection des données personnelles a modifié l'article 230-8 afin de tenir compte de cette jurisprudence.

c. La prise en compte du droit européen

Dans un arrêt *Brunet* du 18 septembre 2014 [(1)], la Cour européenne des droits de l'homme a jugé que le régime de conservation des données inscrites au Système de traitement des infractions constatées (STIC) qui, pour une personne ayant bénéficié d'un classement sans suite, prévoyait une durée de conservation de la fiche de vingt ans et n'offrait pas de possibilité réelle de demander l'effacement des données, violait l'article 8 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales, relatif au droit au respect de la vie privée.

De même, dans un arrêt *Aycaguer* du 22 juin 2017 [(2)], la Cour européenne des droits de l'homme a jugé que le régime français de conservation des profils ADN dans le FNAEG n'offrait pas, en raison tant de sa durée (quarante ans maximum en cas de condamnation) que de l'absence de possibilité d'effacement pour les personnes condamnées (l'effacement n'étant prévu que pour les personnes soupçonnées), une protection suffisante à la personne concernée et

(1) Cour européenne des droits de l'homme, 5ème section, Affaire Brunet c. France*, requête n° 21010/10.*

(2) Cour européenne des droits de l'homme, 5ème section, Affaire Aycaguer c. France*, requête n° 8806/12.*

violait ainsi l'article 8 de la convention. Le requérant à l'origine de l'affaire avait refusé de se prêter à un prélèvement biologique destiné à un enregistrement dans le FNAEG.

Au regard de ce dernier arrêt, il est permis de se demander s'il existe encore une base légale pour sanctionner aujourd'hui le refus de se soumettre à un prélèvement d'empreintes génétiques. Il importe dans ces conditions de mettre en conformité notre droit dans les plus brefs délais pour garantir aux poursuites la sécurité juridique nécessaire.

Un projet de décret en Conseil d'État est en préparation en vue de répondre aux griefs de l'arrêt *Aycaguer*, et donc de modifier les articles 53-9 et suivants du code de procédure pénale

En ce qui concerne les infractions les moins graves, la durée de conservation au FNAEG devrait être réduite à 15 ans pour les majeurs et à 10 ans pour les mineurs, alors que pour les infractions les plus graves, cette durée devrait être de 25 ans pour les majeurs et de 15 ans pour les mineurs. Par exception, pour les délits et les crimes les plus graves et limitativement énumérés par le décret, les durées de conservation pourraient être portées jusqu'à 40 ans. La modification de la durée de conservation au FNAEG devra toutefois s'harmoniser avec les récentes dispositions de la loi n° 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes, qui portent le délai de prescription pour les crimes sexuels commis sur mineurs de 20 à 30 ans après leur majorité (les victimes, mineures au moment des faits, ayant donc désormais jusqu'à leurs 48 ans pour porter plainte).

Proposition n° 5 : Publier dans les plus brefs délais un décret prévoyant une modulation de la durée de conservation des données enregistrées dans le FNAEG au regard de la nature et de la gravité de l'infraction en cause tout en tenant compte des spécificités de la délinquance des mineurs.

S'agissant des conditions d'effacement, elles relèvent de la loi, contrairement aux durées de conservation qui sont du domaine du règlement. La Cour européenne des droits de l'homme estime que les personnes condamnées doivent, tout comme les personnes simplement soupçonnées [(1)], se voir offrir une possibilité concrète de présenter une requête en effacement de leurs empreintes génétiques au FNAEG, afin que leur durée de conservation soit proportionnée à la nature des infractions.

Prévoir cette possibilité d'effacement pour les personnes condamnées suppose une base législative définissant le principe, les critères de la demande et les modalités procédurales. Une telle disposition pourrait être introduite à l'article 706-54 du code de procédure pénale. Le projet de loi de programmation 2018-2022 et de réforme pour la justice constituerait un vecteur législatif approprié pour introduire une telle mesure.

(1) Cf. deuxième alinéa de l'article 706-54 du code de procédure pénale.

Proposition n° 6 : Légiférer dans de brefs délais sur les conditions d'effacement des données enregistrées dans le FNAEG pour les personnes condamnées.

À cette jurisprudence de la Cour européenne des droits de l'homme se sont ajoutés deux textes communautaires de grande portée. Le choix fait par le législateur européen d'adopter un règlement général et une directive « police et pénal » n'a fait qu'accroître la complexité du cadre juridique.

Le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD) renforce les droits des personnes physiques dont les données sont utilisées et responsabilise les acteurs traitant des données en privilégiant le recours à des outils de « droit souple » en contrepartie de l'allégement des formalités administratives préalables (la loi relative à la protection des données personnelles, adoptée par le Parlement, a néanmoins fait le choix de maintenir l'obligation de publication d'un acte réglementaire, donc pris après avis de la CNIL, pour tous les traitements mis en œuvre pour le compte de l'État et intéressant la sûreté de l'État, la défense ou la sécurité publique ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté).

Quant à la directive 2016/680 du 27 avril 2016 relative aux traitements de données à caractère personnel en matière pénale, elle crée un droit à l'information des personnes dont les données sont conservées en matière pénale. Un certain nombre d'obligations prévues par la directive étaient souvent déjà mises en œuvre par la France (traçabilité, distinction des faits et de leur appréciation, distinction entre victimes et mis en cause).

*

* *

En résumé, un service de police ou de gendarmerie, tout comme un citoyen, désireux de connaître l'état du droit encadrant les fichiers utilisés par les forces de sécurité, devra prendre en compte des textes communautaires, d'application directe ou non, la loi de 1978 modifiée, d'autres textes législatifs, le code de procédure pénale, le code de la sécurité intérieure et le code civil, ainsi que de nombreux décrets et arrêtés, le tout au prisme de la jurisprudence européenne et constitutionnelle. Ainsi éclaté, cet encadrement juridique est en outre particulièrement instable puisque les modifications et les compléments qui lui sont apportés se succèdent à un rythme particulièrement élevé.

3. De réelles marges de progrès dans l'alimentation des fichiers et la saisie des données

a. D'importants progrès vers l'automatisation

De nets progrès sont intervenus en matière d'alimentation des fichiers. Le service des technologies et des systèmes d'information de la sécurité intérieure [(1)] (ST(SI)²) a engagé la mutualisation des fichiers en doublons de la police et de la gendarmerie nationales qui reposaient sur des briques techniques hétérogènes et obsolètes. Tel a été le cas pour le Fichier des objets et des véhicules signalés (FOVeS) en 2011 (intégration des objets), puis en 2014 (intégration des véhicules volés), pour le TAJ en 2013 et enfin pour le FPR, le FAED et l'application AGEC [(2)] en 2017.

Dans un souci de cohérence des données, ces travaux ont favorisé l'alimentation automatique des fichiers depuis les logiciels de rédaction de procédure de la gendarmerie et de la police nationales. Le développement des logiciels de rédaction de procédures LRPPN [(3)] et LRPGN a ainsi permis une amélioration de la qualité des données transmises au fichier TAJ, dont police nationale et gendarmerie nationale sont co-responsables. Le TAJ est nourri automatiquement, à l'issue des comptes rendus d'enquêtes après identification (CREI), par les éléments de procédure relatifs tant aux victimes qu'aux mis en cause.

Le LRPPN et le LRPGN transmettent également des données à l'application du ministère de la justice dite « CASSIOPEE [(4)] ». L'alimentation de CASSIOPEE par ces logiciels a permis de raccourcir le délai de traitement des procédures judiciaires et d'assurer une bonne information des victimes. Lors de son audition, M. Paul Michel, ancien magistrat chargé du contrôle des fichiers de police judiciaire, a estimé de l'ordre de 30 à 40 % le gain en temps (et donc en moyens humains) permis par la connexion TAJ-CASSIOPEE dans l'enregistrement des procédures au bureau d'ordre du parquet, sans compter les garanties apportées en termes de fiabilité.

Autre point positif, les parquets ont théoriquement accès directement au TAJ depuis le mois d'aout 2018 alors qu'auparavant ils devaient demander aux services de police et de gendarmerie de tirer un « relevé TAJ » et de le leur envoyer par transmission papier.

---

(1) Créé par l'arrêté du 27 août 2010 modifiant l'arrêté du 23 décembre 2009 portant organisation de la direction générale de la gendarmerie nationale (NOR: IOCJ1020161A).

(2) Acheminement, Gestion, Exploitation et Conservation documentaire au sein du Renseignement Territorial.

(3) Le logiciel de rédaction des procédures de la police nationale (LRPPN) prend place au sein du nouveau système d'information dédié à l'investigation (NS2i) de la police nationale.

(4) Chaîne applicative supportant le système d'information orienté procédure pénale et enfants. Ce traitement, mis en place au début des années 2000 (au prix de beaucoup d'efforts de la part des juridictions), est destiné à la rédaction des actes de procédure et à l'échange d'informations entre parquets.

Cet accès direct a un intérêt notamment dans le cadre des requêtes en effacement mais aussi pour la permanence assurée par les magistrats du parquet, en permettant une meilleure orientation des procédures par les substituts de permanence. Il est encore aujourd'hui trop peu pratiqué et il convient de veiller à son effectivité.

La mise en place de processus de contrôle interne relatifs à l'alimentation des fichiers et impliquant plusieurs niveaux hiérarchiques a également été un facteur de fiabilisation des données. Il existe ainsi dans le TAJ un système de purge automatique effectuée en fonction du croisement des durées de conservation des infractions et de l'état de la personne (majeur, mineur, mis en cause, victime), comme cela a été confirmé aux rapporteurs lors de leur déplacement au Service central de renseignement criminel (SCRC) de la gendarmerie nationale à Pontoise.

b. Des progrès qui rencontrent toutefois des limites

Ces avancées indéniables ne sauraient masquer le caractère daté, par bien des côtés, de la gestion des fichiers mis à la disposition des forces de sécurité. Le TAJ, par exemple, est encore souvent alimenté manuellement par l'administrateur national et les administrateurs régionaux, notamment lorsque les données d'une procédure n'ont pas été remontées dans le traitement par les « procéduriers » et pour les opérations de mise à jour des données.

Quant aux logiciels de rédaction de procédures de la police et de la gendarmerie nationales, s'ils envoient bien à CASSIOPEE un certain nombre d'éléments d'information, ils ne lui transmettent pas en revanche les pièces de procédure. Une telle transmission fera en principe l'objet, sous le vocable de *« procédure pénale numérique »* (PPN), d'une prochaine étape, prévue pour l'année 2019. Le Service central de la police technique et scientifique, situé à Écully, près de Lyon, a fait savoir aux rapporteurs qu'il travaillait à un procédé de signature numérique qui permettrait d'authentifier les procès-verbaux.

Un certain nombre d'inexactitudes subsistent notamment dans le TAJ. Celui-ci est parfois rempli dans la précipitation par les fonctionnaires de police ou les militaires de la gendarmerie. Il arrive ainsi que des victimes soient enregistrées par erreur en qualité d'auteurs. La saisie incomplète ou imprécise des informations ou le défaut d'enrichissement des données peuvent être source d'alimentation de données de mauvaise qualité. À titre d'exemple, lorsqu'un fonctionnaire omet de remplir le champ « *mode opératoire* », l'alimentation du TAJ est imparfaite et cela limite ensuite les capacités de recoupements offertes par ce fichier. De même, il peut arriver que, pour décrire la nature de l'infraction concernée, il soit fait usage d'un terme usuel, tel que « *cambriolage* », qui ne correspond pas à une qualification juridique précise. Ce type d'erreurs est susceptible d'entraîner en particulier dans le TAJ, le FAED ou le FNAEG un dépassement des délais réglementaires de conservation des données.

Mme Sylvie Moisson, procureure générale près la cour d'appel de Lyon, en charge du contrôle du FAED et du FNAEG, a attiré l'attention des rapporteurs sur un phénomène du même ordre. Le raccourcissement des délais de conservation prévus dans les textes réglementaires (1) a nécessité une actualisation des fichiers. Cette actualisation ne peut pas être faite de façon automatisée, mais seulement manuelle, lorsque le champ relatif à l'infraction a été rempli de façon libre et non pas uniformisée. Mme Sylvie Moisson évalue à 533 000 le nombre de fiches au FAED qui ne peuvent pas faire l'objet d'une qualification précise et auxquelles, par conséquent, on ne sait pas quelle durée de conservation appliquer. Compte tenu de cette indétermination, c'est logiquement la règle plus favorable, et donc la durée de conservation la plus courte, qui doit recevoir application. Le problème se posera de manière identique pour le FNAEG lorsque le décret modulant les durées de conservation de ses données aura été publié.

c. Une mise à jour des fichiers effectuée de façon manuelle

La mise à jour des fichiers recouvre les opérations de rectification, d'enrichissement ou d'effacement des données. Elle est effectuée par les services gestionnaires de façon encore manuelle, ce qui nécessite un investissement lourd en termes de ressources humaines.

Ainsi, l'inscription au TAJ des suites judiciaires favorables s'effectue toujours manuellement sur la base des informations transmises par les parquets par fiches navettes (imprimées à partir de CASSIOPEE et mises sous enveloppe), ou dans certains cas par messagerie électronique, aux vingt services régionaux de documentation criminelle (SRDC) de la direction centrale de la police judiciaire et de la direction régionale de la police judiciaire de la préfecture de police de Paris (pour ce qui est des procédures établies par la police nationale).

Le délai de renvoi des suites judiciaires est très variable d'une juridiction à l'autre. En outre, il peut arriver que, lors de l'envoi de la « fiche retour » relative à la suite judiciaire, le parquet se trompe de destinataire (l'erreur portant soit sur le service régional de documentation criminelle, soit même sur l'institution, police ou gendarmerie). De même, le responsable du traitement ne peut intervenir dans le TAJ que s'il dispose, pour s'assurer qu'il s'agit bien des faits visés dans la bonne procédure, de l'exemplaire papier de la procédure (transmise par le service rédacteur), ce qui n'est pas toujours le cas. Pour ces différentes raisons, la mise à jour des suites judiciaires favorables dans le TAJ prend parfois du retard.

Le procureur de la République territorialement compétent (ou, le cas échéant, le magistrat référent (2)) peut également solliciter le service gestionnaire

---

(1) Le décret n° 2015-1580 du 2 décembre 2015 a ainsi modifié le décret n° 87-249 du 8 avril 1987 relatif au FAED afin de moduler les durées de conservation des traces et empreintes au regard de la gravité de l'infraction et de la qualité de la personne, selon notamment qu'elle est majeure ou mineure.

(2) S'agissant du TAJ, s'il y a pour une même personne plusieurs inscriptions relevant des ressorts de plusieurs tribunaux de grande instance, les requêtes en effacement sont traitées par un magistrat référent. Cette fonction a été assumée de 2012 à 2108 par M. Paul Michel, procureur général honoraire près la cour d'appel de Grenoble. Au cours de ses deux mandats, M. Paul Michel a reçu un peu plus de 2 500 requêtes,

pour obtenir l'effacement de données dans l'application. Dans ce cas, les corrections prescrites sont également effectuées de façon manuelle et réalisées aussi bien par la police nationale que par la gendarmerie nationale, chaque institution se chargeant de ses propres procédures. Pour la police nationale, cette mission est dévolue aux SRDC et à la « *cellule d'administration fonctionnelle unique* ».

La difficulté matérielle à laquelle sont confrontés certains parquets, aussi bien dans la transmission des suites judiciaires que dans le traitement des requêtes en effacement, pose évidemment la question centrale des moyens dont ils sont dotés. La Conférence nationale des procureurs de la République (CNPR), tout comme les magistrats rencontrés à Lyon, ont insisté auprès des rapporteurs sur la nécessité de doter les parquets de moyens suffisants en effectifs (magistrats, greffiers, fonctionnaires de catégorie C) et en équipement informatique pour leur permettre d'exercer leur contrôle sur la fiabilité des données personnelles figurant sur les fichiers et de répondre rapidement aux requêtes en rectification et en effacement.

Les parquets ne semblent guère à ce jour en capacité de satisfaire aux prescriptions posées par l'article 230-8 du code de procédure pénale (tel qu'il a été modifié par l'article 36 de la loi du 20 juin 2018 relative à la protection des données personnelles) pour ce qui concerne le TAJ, et en particulier à l'obligation de se prononcer dans un délai de deux mois sur les demandes d'effacement et de rectification qui leur sont adressées ainsi qu'à l'obligation d'informer les responsables de tous les traitements automatisés pour lesquels ces mesures ont des conséquences sur la durée de conservation des données personnelles. Pour M. Jérôme Bourrier, procureur de la République près le tribunal de grande instance de Vienne, « *en l'état de leurs moyens humains, il est également parfaitement illusoire d'exiger du greffe la vérification effective des mises à jour opérées dans le TAJ* ». Faute de moyens adéquats, la transmission des suites judiciaires, le traitement des requêtes en effacement et la vérification des modifications effectuées ne constituent manifestement pas une priorité pour les parquets.

Proposition n° 7 : Accentuer l'informatisation des parquets et les doter de moyens suffisants.

On remarque par ailleurs que les procureurs tendent, peut-être du fait d'une maîtrise insuffisamment précise des dispositions de l'article 230-8, à demander systématiquement l'effacement et à faire peu usage de la faculté qui leur est offerte d'ordonner simplement l'inscription d'une mention au TAJ.

---

soit environ 600 par an (alors que les prévisions tablaient sur 80 par an). En ce qui concerne le FAED, il est placé sous le contrôle du procureur général près la cour d'appel dans le ressort de laquelle est situé le service gestionnaire (c'est-à-dire celle de Lyon) qui peut d'office ordonner l'effacement des informations dont la conservation ne paraîtrait manifestement plus utile compte tenu de la finalité du traitement.

Au demeurant, ils ne cachent pas un certain scepticisme quant au dispositif complexe prévu par la loi en matière d'effacement, qui les amène à remplir quasiment le rôle de magistrats du siège. En effet, hors le cas de la rectification pour requalification judiciaire (qui est de droit), il leur faut porter une appréciation au cas par cas sur l'opportunité ou non de maintenir, d'effacer ou d'apposer une mention sur des données personnelles figurant au TAJ, leur décision étant susceptible de recours. La loi leur laisse de ce point de vue une large marge d'appréciation. Lors de son audition, M. Paul Michel a expliqué que, lorsque des requêtes en effacement souffraient d'un défaut de motivation et ne le mettaient pas en mesure de prendre une décision en connaissance de cause, il était enclin à ne pas faire droit à la demande. Compte tenu de la complexité de ce dispositif, les rapporteurs suggèrent de dresser un bilan de son application dans un délai de deux ans afin de dégager, le cas échéant, des pistes tendant à sa simplification.

Proposition n° 8 : Rappeler aux parquets, par la voie d'une circulaire, la faculté offerte par l'article 230-8 du code de procédure de pénale d'ordonner l'inscription d'une mention au TAJ.

La réponse aux difficultés de mise à jour du TAJ passera en partie, outre par une augmentation des moyens des parquets, par la mise en relation automatisée de CASSIOPEE vers TAJ, c'est-à-dire par la circulation de flux informatiques depuis CASSIOPEE vers TAJ, que ce soit en cours d'affaire ou à la clôture de celle-ci. Une telle mise en relation est expérimentée, depuis octobre 2014, dans sept juridictions pilotes, dont le tribunal de grande instance de Vienne [(1)]. Le procureur de la République de ce tribunal a fait savoir aux rapporteurs que le système fonctionnait bien « *à condition de disposer de fonctionnaires du bureau d'ordre performants* ». Il est aujourd'hui impératif et urgent de généraliser cette relation automatisée de CASSIOPEE vers TAJ.

Le procureur de la République près le tribunal de grande instance de Vienne a souligné que, dans le cadre de l'expérimentation actuelle, la Chancellerie avait souhaité que soit maintenue en parallèle la transmission aux services de police et de gendarmerie des fiches papier en retour, afin de vérifier la corrélation entre l'alimentation via Cassiopée et l'exploitation des fiches, ce qui représente donc un double travail. Il est évident que, dans le cadre d'une extension de l'interconnexion CASSIOPEE-TAJ, cette transmission des fiches-navettes devrait être supprimée, sous peine de priver cette interconnexion de toute utilité.

Comme l'a souligné encore le procureur de la République près le tribunal de grande instance de Vienne, il faudra prendre garde à ce que l'accès désormais direct des procureurs au TAJ conserve une vocation purement consultative, destinée à permettre la vérification des modifications apportées au traitement, et ne fournisse pas un prétexte pour leur transférer dans un second temps la charge de la mise à jour elle-même.

---

(1) La mise à jour automatisée du TAJ grâce à l'interconnexion avec CASSIOPEE est également expérimentée au sein des juridictions de Grenoble, Bourgoin-Jallieu, Avignon, Carpentras, Nancy et Briey.

Proposition n° 9 : Généraliser dans de brefs délais l'interconnexion de CASSIOPEE vers TAJ, en remplacement des fiches-navettes, actuellement expérimentée dans sept juridictions.

En résumé, si des efforts ont incontestablement été faits, il reste que des dizaines de milliers de fiches demeurent à mettre à jour en particulier dans le TAJ, le FAED et le FNAEG. Les insuffisances de cette mise à jour ne sont pas acceptables au regard des libertés publiques, eu égard notamment aux conséquences qu'elles peuvent avoir sur l'accès à certains emplois faisant l'objet d'enquêtes administratives.

II. DES FICHIERS CONFRONTÉS À LA VAGUE TERRORISTE ET À LA MONTÉE EN PUISSANCE DES ENQUÊTES ADMINISTRATIVES QU'ELLE GÉNÈRE

A. DANS LEUR LUTTE CONTRE LA CRIMINALITÉ, LES FORCES DE SÉCURITÉ ONT UN BESOIN FORT DE FIABILISATION DES IDENTITÉS ET D'INTERCONNEXIONS

1. Un manque réel de sécurisation des fichiers autour d'un pivot central des identités ou d'un identifiant commun

a. Un problème aigu d'établissement de l'identité des personnes mises en cause

L'ensemble des forces de sécurité auditionnées par les rapporteurs ont fait part d'un problème majeur de fiabilisation de l'identité des personnes inscrites dans les fichiers mis à la disposition des forces de sécurité. Ce problème ne résulte pas seulement des erreurs de saisie et des insuffisances dans la mise à jour mais aussi et surtout de la déclaration par les personnes mises en cause de multiples identités successives (qui peuvent être parfois des usurpations d'identité). On sait, à titre d'illustration, qu'Ahmed Hanachi, auteur de l'attentat perpétré à la gare Saint-Charles à Marseille le 1er octobre 2017, avait « *été signalisé pour des faits commis sous six identités différentes* [(1)] », étant précisé que « *son casier judiciaire ainsi que les casiers de ses alias étaient vierges* ».

Il est très difficile aux forces de sécurité de lier de manière certaine les alias utilisés par un même individu et de déterminer le véritable état civil de la personne parmi les différentes identités déclarées. Lorsqu'une personne mise en cause dans une procédure judiciaire n'a pu être authentifiée par un document d'identité, les bases de données (en particulier le TAJ et le FAED) sont alors alimentées sur la seule foi de ses déclarations. Faute d'interopérabilité avec les fichiers administratifs de titres (de séjour ou d'identité), les erreurs ainsi introduites ne peuvent être corrigées. Tout au plus peut-on, s'agissant du FAED,

(1) Traitement administratif de la situation de M. Ahmed Hanachi par la préfecture du Rhône, *Inspection générale de l'administration, n° 17095-R, octobre 2017.*

relier différentes identités grâce à la comparaison des empreintes digitales, mais le lien ainsi établi n'apparaît pas dans le TAJ, compte tenu de l'étanchéité juridique et technique de ces deux bases. Des fichiers distincts, comme le TAJ et le FAED, peuvent donc donner des informations parcellaires ou partiellement différentes sur un même individu mis en cause.

Les gendarmes rencontrés par les rapporteurs au Service central de renseignement criminel (SCRC) à Pontoise ont souligné à quel point la fiabilisation des identités devenait un enjeu crucial en un temps marqué par la mobilité des populations et les flux migratoires. On peut aussi remarquer que de nombreux pays étrangers ont un casier judiciaire avec empreintes digitales, ce qui n'est pas le cas de la France.

b. De timides progrès déjà accomplis

Quelques avancées ont certes eu lieu en matière de sécurisation des identités. La mise en œuvre en octobre 2017 de l'outil « GASPARD NG [(1)] », dédié à la gestion des signalisations, a marqué une étape importante. Désormais, dès qu'une personne est interpellée, elle est signalisée [(2)] avec ce logiciel qui permet d'intégrer le signalement, les photographies et les empreintes digitales. GASPARD NG transmet des références communes au TAJ et au FAED, ce qui est un facteur de fiabilisation des données contenues dans ces deux applications.

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

c. La fausse piste d'une interconnexion avec le fichier TES

Il a parfois été suggéré aux rapporteurs, pour aller plus loin dans la fiabilisation de l'état civil des personnes mises en cause, de créer une application centrale biométrique qui serait interconnectée avec les données d'identité du fichier TES (Titres électroniques sécurisés). Ce fichier contient les images numérisées des empreintes digitales et de la photographie de l'ensemble des demandeurs de cartes nationales d'identité et de passeports. Le gendarme ou le

---

(1) Application de gestion automatisée des signalements et des photographies anthropométriques répertoriées et distribuables (Nouvelle Génération). L'outil Gaspard NG, intégré à LRPPN, est l'un des fichiers qui composent le nouveau système d'information dédié à l'investigation (NS2i), qui remplace depuis 2011 l'ancien système d'information (composé du LRP, STIC, STIC-FCE, CANONGE et FVV), celui-ci ayant trouvé des limites à son utilisation avec le temps et n'ayant pu échapper à une certaine obsolescence tant technique que fonctionnelle.

(2) C'est le rôle de l'« ijiste » (policier de l'identité judiciaire et de la police scientifique).

policier pourrait rentrer une identité ou une empreinte digitale dans cette application et aller y chercher une vérification.

Le fichier des titres électroniques sécurisés (TES)

Le fichier TES résulte du décret en Conseil d'État n° 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité.

Mis en place par le ministère de l'intérieur, ce fichier administratif vise à permettre de procéder à l'établissement, à la délivrance, au renouvellement ou à l'invalidation des cartes nationales d'identité et des passeports ainsi qu'à prévenir et à détecter leur falsification.

Il contient notamment des données d'état civil (nom, prénoms, date et lieu de naissance, sexe, données relatives à la filiation, *etc*.), des renseignements sur l'apparence physique (couleur des yeux, taille), l'image numérisée du visage et celle des empreintes digitales qui peuvent être légalement recueillies, l'image numérisée de la signature du demandeur de la carte nationale d'identité, *etc*.

Le décret précise expressément que « *le traitement ne comporte pas de dispositif de recherche permettant l'identification à partir de l'image numérisée du visage ou de l'image numérisée des empreintes digitales enregistrées* ».

Cette idée se heurte tout d'abord à des difficultés techniques. L'architecture technique du fichier TES exclut en effet la possibilité d'interroger ce fichier par les empreintes digitales. Cette architecture est fondée sur un lien unidirectionnel, qui impose d'entrer l'état civil pour appeler l'empreinte digitale correspondante.

Une interconnexion avec le traitement TES rencontrerait ensuite des obstacles de nature constitutionnelle. Le Conseil constitutionnel, dans sa décision n° 2012-652 DC du 22 mars 2012 [(1)], a en effet censuré des dispositions législatives qui autorisaient l'interrogation d'un traitement destiné à recueillir les données biométriques à des fins de délivrance ou de renouvellement des titres d'identité et de voyage et de vérification de l'identité du possesseur d'un tel titre, mais aussi à d'autres fins de police administrative ou judiciaire.

Enfin, le traitement TES, dont la mise en place en 2016 avait suscité beaucoup de craintes et de débats, présente une extrême sensibilité politique. On ne saurait le faire évoluer sans dommages vers un registre de la population. Une telle finalité mettrait en danger la finalité première du traitement, qui est la délivrance de titres sécurisés. Au demeurant, la tradition politique et culturelle française est réticente envers toute idée de registre de la population ou de contrôle de l'habitant, plus facilement admise dans des pays comme la Suisse ou l'Allemagne.

(1) Décision n° 2012-652 DC du 22 mars 2012, Loi relative à la protection de l'identité.

Pour ces différents motifs, l'interconnexion avec le fichier TES ne constitue pas une solution adéquate pour lutter contre le phénomène des alias.

d. La création d'une base centrale commune reliant FAED, FNAEG et TAJ ou d'un identifiant commun à ces trois applications

La sécurisation des identités (et accessoirement du domicile) passe par la mise en relation du FAED, du FNAEG et du TAJ. Cette mise en relation pourrait se traduire par la création d'une base-pivot faisant le lien entre ces trois applications. La Cour des comptes a formulé des recommandations allant en ce sens. Dans un rapport de décembre 2016 sur *La police technique et scientifique* (1), elle propose de connecter le FAED et le FNAEG à une base commune d'identité des personnes signalisées. Elle suggère plus précisément d'« *engager des travaux en vue de connecter le fichier automatisé des empreintes digitales (FAED) et le fichier national automatisé des empreintes génétiques (FNAEG) à une base commune d'identité des personnes signalisées* ». Selon elle, « *une interconnexion des deux fichiers sur une base commune contenant l'identité des personnes signalisées (précisant l'état civil, les alias, le nom phonétique) permettrait d'améliorer la fiabilité des identités et de repérer plus systématiquement les individus signalisés déjà présents dans l'une des bases. Ceci suppose que les deux bases actuelles soient auparavant nettoyées de leurs nombreux doublons. En retour, l'inspection générale de la police nationale recommande la création d'un système commun aux deux fichiers en réponse notamment à ce problème de doublons* ».

La création d'une telle base commune suscite toutefois des réticences, notamment de la part de la direction des libertés publiques et des affaires juridiques. La mise en place d'une base unique comportant des données biométriques mise en œuvre par le ministère de l'intérieur poserait, selon elle, des difficultés en termes d'acceptabilité politique mais également en termes de proportionnalité au regard de la protection des données personnelles. Elle conduirait à une base de données particulièrement sensibles issues de différents traitements de données à caractère personnel poursuivant des finalités distinctes.

De façon alternative, la mise en relation du FAED, du FNAEG et du TAJ pourrait, de manière plus réaliste et certainement moins coûteuse, prendre la forme d'un identifiant commun pour l'inscription dans ces trois bases de données. Comme l'a indiqué la direction centrale de la police judiciaire (2), « *le PPMEC (personne physique mise en cause) pourrait remplir cette fonction. Généré par LRPPN, ce numéro est déjà enregistré dans TAJ puis dans le FAED depuis octobre 2017. Des évolutions techniques seraient nécessaires pour le rendre exploitable depuis cette dernière application et étendre cette transmission aux procédures de la gendarmerie nationale (LRPGN). Cet identifiant devrait*

---

(1) Cour des comptes, La police technique et scientifique, *décembre 2016, Communication à la Commission des finances, de l'économie générale et du contrôle budgétaire de l'Assemblée nationale.*

(2) Dont on peut rappeler qu'elle est saisie de l'enquête sur l'attentat de la gare Saint-Charles.

également être enregistré dans le FNAEG. La présence du PPMEC permettrait d'établir une correspondance certaine entre les fiches présentes dans chaque application ». En consultant l'une des trois bases, soit à partir de l'état-civil, soit à partir des empreintes (génétiques ou papillaires) s'agissant du FNAEG et du FAED, on aurait accès aux informations contenues dans les deux autres. La performance du TAJ comme des deux grands fichiers criminalistiques en sortirait renforcée.

La direction des libertés publiques et des affaires juridiques a indiqué aux rapporteurs que des réflexions étaient en cours pour mettre en place des passerelles entre les fichiers, notamment par la création d'un identifiant unique lié à un numéro d'empreinte digitale. Cela nécessitera de modifier les actes réglementaires de chacun des traitements concernés afin, d'une part, de lever l'interdiction de toute interconnexion, mise en relation ou rapprochement et, d'autre part, de prévoir une mise en relation aux seules fins de fiabilisation des données contenues dans chacun des fichiers.

Quoi qu'il en soit, la nécessaire mise en relation du FAED, du FNAEG et du TAJ en vue de sécuriser les identités suscite un large consensus. Dans ses éléments de réponse écrits adressés aux rapporteurs, la direction centrale de la police judiciaire se déclare « *favorable à ce que soient interconnectés (ou reliés par une base-pivot) le TAJ, le FAED et le FNAEG afin de garantir la cohérence des informations entre des fichiers aujourd'hui discordants et améliorer l'efficacité des policiers dans l'exercice de leurs missions* ». M. Éric Morvan, directeur général de la police nationale, comme M. Pascal Lalle, directeur central de la sécurité publique, partagent cette recommandation d'interconnecter ces trois fichiers.

Les textes européens [(1)] prennent en compte la même préoccupation. Ils imposent que le système d'information Schengen (SIS) soit alimenté par des empreintes digitales des personnes signalées, ce qui implique une interconnexion avec le FAED. Les futurs règlements SIS, en cours de négociation, prévoient de leur côté la possibilité d'associer des profils ADN à des signalements de personnes.

La sécurisation des identités grâce à la création d'une base-pivot reliant le TAJ et les deux grands fichiers d'identification criminelle, ou grâce à la mise en place d'un identifiant commun, présenterait en outre un intérêt financier. Elle permettrait en effet de réduire le nombre de prélèvements d'empreintes génétiques (particulièrement coûteux), qu'il faut aujourd'hui réitérer lorsqu'une personne figurant déjà au FNAEG donne une nouvelle identité.

---

(1) Règlement (CE) n° 1987/2006 du 20 décembre 2006 du Parlement européen ; décision 2007/533/JAI du Conseil de l'Europe du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du SIS-II.

Proposition n° 10 : Relier le TAJ, le FAED et le FNAEG par une base-pivot, ou créer un identifiant commun (lié à un numéro d'empreinte digitale) à ces différentes applications, afin de garantir la cohérence des informations entre les fichiers et de fiabiliser les identités des personnes mises en cause.

La mise en place de cette base commune nécessitera une modification des textes réglementaires relatifs au FAED et au FNAEG qui interdisent aujourd'hui toute interconnexion, compte tenu de la sensibilité des données qu'ils contiennent. L'article 9 du décret n° 87-249 du 8 avril 1987 relatif au FAED dispose en effet que celui-ci « *ne peut faire l'objet d'aucune interconnexion, rapprochement ou d'aucune autre forme de mise en relation avec un autre traitement automatisé de données à caractère personnel, à l'exception du traitement visé à l'article 48-1 du code de procédure pénale* [(1)] *aux seules fins d'alimentation et de mise à jour du fichier prévu par le présent décret* ». Quant à l'article R. 53-19 du code de procédure pénale, il précise de son côté que « l*e fichier national automatisé des empreintes génétiques ne peut faire l'objet d'aucune interconnexion ni de rapprochement ou de mise en relation avec un autre traitement automatisé d'informations nominatives, sous réserve des dispositions du troisième alinéa de l'article R. 53-20*. »

2. Un développement souhaité des accès et des interconnexions

Un élargissement des accès et le développement d'interconnexions pourraient utilement remédier au cloisonnement des fichiers constaté par les forces de sécurité.

a. Le développement des accès aux fichiers

Les demandes exprimées au cours des auditions concernent les accès aux **fichiers relevant du ministère de l'intérieur** mais aussi aux **fichiers relevant d'autres ministères**.

● S'agissant des fichiers relevant du ministère de l'intérieur, les demandes concernent principalement **les accès des services de renseignement**.

Il semble ainsi tout à fait légitime d'ouvrir à ces services l'accès aux **fichiers de renseignement territorial PASP et GIPASP** qui, de façon surprenante, n'est pas prévu par les textes relatifs à ces traitements.

Par ailleurs, les services de renseignement spécialisés, ainsi que les services concourant à la mission de renseignement peuvent, dans le cadre des besoins liés à la protection de certains intérêts [(2)], consulter **le fichier TAJ**. Cette

---

(1) La référence à l'article 48-1 du code de procédure pénale vise le bureau d'ordre national automatisé des procédures judiciaires.

(2) L'article L. 234-4 du code de la sécurité intérieure, introduit par la loi n° 2015-912 du 24 juillet 2015 relative au renseignement autorise la consultation par ces services du fichier TAJ dans le cadre des besoins liés à la protection de l'indépendance nationale, l'intégrité du territoire et de la défense nationale, la

consultation s'opère selon un profil spécifique permettant d'accéder à toutes les données des procédures judiciaires, y compris celles concernant des procédures en cours. **Elle exclut en revanche les données relatives aux victimes**. Les rapporteurs sont favorables à une évolution de la loi sur ce point. Les données concernées pourraient en effet être une source d'informations utile aux services de renseignement, les personnes faisant l'objet d'un suivi ou d'une surveillance par ces services, notamment en matière de prévention du terrorisme, n'étant pas toujours connues en tant que mises en cause.

Proposition n° 11 : Autoriser l'accès des services de renseignement spécialisés :

– aux fichiers « prévention des atteintes à la sécurité publique » (PASP) et « Gestion de l'information et prévention des atteintes à la sécurité publique » (GIPASP) ;

– à la partie « victimes » du TAJ.

● S'agissant de l'accès à des fichiers relevant d'autres ministères que le ministère de l'intérieur, les demandes concernent d'une part la consultation des fichiers **dans le cadre d'enquêtes judiciaires** et, d'autre part, **l'accès des services de renseignement**.

Les enquêteurs judiciaires ont fréquemment besoin d'informations contenues dans des fichiers relevant d'autres administrations. Ils peuvent pour cela recourir à des réquisitions judiciaires. Cependant, ainsi que l'ont souligné de nombreuses personnes entendues par la mission, ce système, très chronophage et fastidieux, n'est pas adapté aux délais souvent très courts s'imposant aux enquêteurs. Les rapporteurs estiment donc nécessaire de **substituer aux réquisitions judiciaires un accès direct aux fichiers les plus utilisés**.

Les droits d'accès devraient être définis **dans le cadre d'habilitations précises**, correspondant à des fonctions d'enquêtes spécialisées.

Un tel accès a d'ores et déjà été ouvert aux officiers de police judiciaire pour certains fichiers, par exemple le fichier national des comptes bancaires (FICOBA) et le fichier des contrats de capitalisation et d'assurance-vie (FICOVIE), qui relèvent du ministère de l'économie et des finances [(1)].

Il convient de poursuivre ce mouvement s'agissant de l'accès des agents et officiers de police judiciaire à d'autres fichiers :

– le **répertoire national commun de la protection sociale (RNCPS)** [(2)] géré par la direction de la sécurité sociale, qui répertorie les informations d'organismes privés et publics (caisse nationale d'assurance vieillesse, caisse

prévention du terrorisme ainsi que la prévention des atteintes à la forme républicaine des institutions, des actions tendant au maintien ou à la reconstitution de groupements dissous et des violences collectives de nature à porter gravement atteinte à la paix publique.

(1) Article L. 135 ZC du livre des procédures fiscales, issu de l'article 126 de la loi n° 2015-1785 du 29 décembre 2015 de finances pour 2016.

(2) Article L. 114-12-1 du code de la sécurité sociale.

nationale d'allocations familiales, mutuelles, Pôle emploi, URSSAF, *etc.*), utiles dans le cadre de la lutte contre le travail illégal et la fraude sociale ;

– **les bases de l'administration fiscale « Base nationale de données patrimoniales » (BNDP)**, qui contient les données relatives aux mutations à titre onéreux ou gratuit **et PATRIM**, service à destination principalement des particuliers, qui permet d'estimer la valeur d'un bien, qui compléteraient les informations issues de la consultation des fichiers FICOBA et FICOVIE.

Les rapporteurs se félicitent donc que le projet de loi relatif à la lutte contre la fraude, adopté définitivement par l'Assemblée nationale le 10 octobre 2018, autorise ces accès [(1)].

Les **services de renseignement** ont également besoin de disposer d'un accès à des fichiers relevant d'autres ministères. Un tel accès pourrait être ouvert à la DGSI s'agissant du **fichier national des personnes incarcérées**, géré par le ministère de la justice (auquel ont accès seulement les officiers de police judiciaire), qui enregistre les entrées et sorties des détenus ainsi que l'historique de leurs incarcérations [(2)]. Ces informations permettraient en effet d'organiser le suivi des personnes justifiant une surveillance et de connaître les liens qu'elles ont pu nouer lors de leur détention.

Proposition n° 12 : Autoriser l'accès de la DGSI au fichier national des personnes incarcérées.

b. Le développement des interconnexions

La notion d'interconnexion entre deux fichiers désigne une modalité technique de transmission d'informations d'un fichier vers un autre fichier.

D'un point de vue juridique, la CNIL définit l'interconnexion comme **la mise en relation automatisée de deux traitements de données à caractère personnel distincts et ayant des finalités différentes**.

Avant l'application du RGPD, l'interconnexion de fichiers était soumise à l'autorisation de la CNIL. Elle reste mentionnée par l'article 30 de la loi du 6 janvier 1978 aux côtés des notions de « *rapprochement* » et de « *mise en relation* », parmi les éléments devant être précisés dans les demandes d'autorisations et les demandes d'avis adressées à la CNIL.

Les objectifs des interconnexions sont multiples :

– l'**échange d'informations automatique entre différents services** ;

(1) Article 3 du texte de la commission mixte paritaire .

(2) Arrêté du 20 février 2003 modifiant l'arrêté du 28 octobre 1996 portant création d'un fichier national automatisé des personnes incarcérées.

– la **mutualisation de l'alimentation** de différents fichiers, ce qui permet des gains d'efficacité et renforce la fiabilité des données ;

– la **mise à jour automatique des données** ;

– la **consultation simultanée** de plusieurs fichiers, avec un champ plus ou moins large des informations consultées ;

– le **recoupement des informations** sur une même personne issues de différents fichiers.

Le développement des interconnexions est une demande forte des services pour renforcer la cohérence des fichiers et remédier à leur cloisonnement.

De nombreux fichiers sont d'ores et déjà interconnectés, par exemple :

– les fichiers constituant **le système d'information dédié à l'investigation (NS2i)** mis en œuvre depuis 2011 : le LRPPN alimente de manière automatique les fichiers TAJ et FOVeS ; il échange des informations avec GASPARD NG (outil de gestion des signalisations) ; LRPPN alimente également CASSIOPEE ;

– conformément à la réglementation européenne, **le système d'information Schengen (SIS)** est interconnecté pour alimentation et/ou consultation à 12 fichiers nationaux (dont FOVeS, FPR, et, pour alimentation uniquement, TES et DOCVERIF) [(1)].

Néanmoins, **les textes relatifs à certains fichiers interdisent toute interconnexion en raison de la sensibilité des données** : c'est le cas par exemple des fichiers FAED et FNAEG. La mise en œuvre d'une base commune d'identité à partir de ces fichiers ou leur interconnexion dans un objectif de fiabilisation des données relatives à l'identité, déjà évoquées par les rapporteurs, supposerait donc une modification des textes applicables à ces traitements.

Interrogée par les rapporteurs sur le développement des interconnexions, la CNIL a indiqué n'être nullement défavorable par principe à leur mise en œuvre, dès lors qu'elles intervenaient dans des conditions de nature à assurer une protection des données à caractère personnel.

M. Thomas Campeaux, directeur des libertés publiques et des affaires juridiques au ministère de l'intérieur, a pour sa part souligné que des interconnexions pouvaient être légitimes mais qu'elles devaient être analysées en fonction des missions exercées par les agents et des finalités de chacun des traitements concernés.

(1) Cf. infra.

Sous réserve d'une telle analyse, qui ne peut être menée qu'au cas par cas, **les rapporteurs soulignent l'intérêt du développement des interconnexions et retiennent, à titre d'exemple, les pistes suivantes** :

– l'interconnexion des traitements **SIS, FPR et FAED** pour se conformer aux obligations du règlement Schengen, qui impose d'insérer les empreintes dactyloscopiques des personnes signalées dès lors qu'elles sont disponibles et que les législations nationales le permettent ;

– l'interconnexion des logiciels LRPPN et LRGGN et du système d'immatriculation des véhicules (SIV) pour permettre l'alimentation automatisée de la partie « véhicules » du FOVeS.

Proposition n° 13 : Développer les interconnexions entre fichiers et étudier en particulier la possibilité d'interconnexions :

– entre les traitements SIS, FPR et FAED pour se conformer aux obligations du règlement Schengen ;

– entre les logiciels de rédaction des procédures LRPPN et LRGGN et le système d'immatriculation des véhicules pour permettre l'alimentation automatisée de la partie « véhicules » du FOVeS.

Les rapporteurs rappellent également la nécessité d'une mise en œuvre effective de l'interconnexion entre **TAJ et CASSIOPEE**. Cette mise en œuvre suppose la modification l'article R. 15-33-66-12 du code de procédure pénale, qui cite les traitements avec lesquels CASSIOPEE peut être mis en relation, au nombre desquels le TAJ ne figure pas, ainsi que le déploiement technique national de cette interconnexion [(1)].

c. L'enjeu d'une interconnexion entre le TAJ et le casier judiciaire national

Compte tenu du manque de fiabilité des données du fichier TAJ, déjà évoqué, qu'il s'agisse des données d'état civil ou de celles relatives aux suites judiciaires, les rapporteurs souhaitent que **la possibilité de mettre en œuvre une interconnexion entre le TAJ et le casier judiciaire national soit envisagée**.

(1) Cf. supra.

Le casier judiciaire national (CJN)

Mis en œuvre depuis 1980 sous forme automatisée, le casier judiciaire national est régi par les articles 768 à 781 du code de procédure pénale.

Sont notamment enregistrées dans le CJN toutes les condamnations pénales pour crime, délit et contravention de cinquième classe. L'identité des personnes concernées est contrôlée au moyen du répertoire national d'identification des personnes physiques (RNIPP).

Le CJN est tenu sous l'autorité du ministère de la justice.

La communication des informations du CJN prend la forme d'extraits appelés bulletins du casier judiciaire :

– le bulletin n° 1 : réservé aux autorités judiciaires, il comprend l'ensemble des condamnations enregistrées dans le CJN ;

– le bulletin n° 2 : réservé aux administrations, aux autorités militaires et à des organismes privés pour l'accès à certaines professions, il comprend les informations du bulletin n° 1, à l'exception de certaines condamnations prononcées à l'encontre de mineurs, des condamnations de nature contraventionnelle, de certaines condamnations avec sursis, des condamnations faisant l'objet d'une dispense de peine, des condamnations prononcées à l'étranger et des compositions pénales exécutées.

– le bulletin n° 3 : il ne fait apparaître que les sanctions les plus graves (condamnations à une peine d'emprisonnement ferme de plus de deux ans ou d'une durée inférieure si le juge en a ordonné l'inscription, ainsi que les condamnations à des interdictions, déchéances ou incapacités prononcées sans sursis).

L'interconnexion du TAJ et du CNJ permettrait d'alimenter automatiquement le TAJ afin qu'il intègre les suites judiciaires défavorables. Une telle évolution impliquerait une modification de l'article 777-3 du code de procédure pénale selon lequel : « *Aucun fichier ou traitement de données à caractère personnel détenu par une personne quelconque ou par un service de l'État ne dépendant pas du ministère de la justice ne pourra mentionner, hors les cas et dans les conditions prévus par la loi, des jugements ou arrêts de condamnation*. », à moins de considérer qu'elle peut s'inscrire dans la possibilité de dérogation prévue par cet article (« *hors les cas et dans les conditions prévus par la loi* »). Elle nécessiterait dans tous les cas une disposition législative.

La mention des condamnations pénales dans le TAJ présenterait plusieurs avantages :

– dans le cadre des **enquêtes administratives**, elle permettrait une meilleure compréhension de la situation de la personne concernée et éviterait le risque de décisions injustifiées se fondant uniquement sur les antécédents judiciaires [(1)] ;

(1) Cf. infra.

– s'agissant de la **mise en œuvre des amendes forfaitaires délictuelles** pour les infractions de conduite sans permis et de conduite sans assurance [(1)], la mention des condamnations pénales dans le TAJ permettrait aux policiers et aux gendarmes de déterminer avec certitude si le délit a été commis en état de récidive légale, et donc d'exclure le cas échéant le recours à l'amende forfaitaire ; les rapporteurs soulignent à cet égard que la question de l'accès des services de police et des unités de gendarmerie au casier judiciaire national a été évoquée à plusieurs reprises au cours des auditions.

Si l'interconnexion du TAJ et du CNJ n'était pas mise en œuvre, les rapporteurs souhaitent au moins que l'accès au bulletin n° 1 soit autorisé aux policiers et aux gendarmes ainsi qu'aux agents des services chargés des enquêtes administratives.

Proposition n° 14 : Mettre en œuvre une interconnexion entre le TAJ et le casier judiciaire national pour permettre l'inscription dans le TAJ des condamnations pénales.

À défaut d'une telle interconnexion, autoriser l'accès des policiers et des gendarmes ainsi que des agents des services chargés des enquêtes administratives au bulletin n° 1 du casier judiciaire.

d. La mise en œuvre d'une interface permettant la consultation simultanée des fichiers

Les auditions menées ont mises ont évidence l'utilité d'une **interface permettant l'interrogation simultanée de différents fichiers, qui fonctionnerait comme un moteur de recherche à partir de la saisie d'une identité ou d'un identifiant technique commun**. Une telle interface permettrait en effet d'importants gains de temps et d'efficacité. Elle permettrait de remédier à la dispersion des fichiers et de mettre fin au risque d'oubli de consultation de certains fichiers.

A minima, cette interface relierait les fichiers auxquels l'agent est autorisé à accéder. **Une étape supplémentaire pourrait être proposée avec la mise en œuvre d'un système d'alerte de présence au sein d'autres fichiers (système dit « *hit/no hit* »)**. À partir de la saisie de l'identité ou de l'identifiant technique d'une personne, cette interface permettrait de savoir si celle-ci est inscrite dans un certain nombre de fichiers, sans pour autant donner accès aux informations contenues dans ces fichiers. Le cas échéant, des fichiers relevant d'autres ministères que le ministère de l'intérieur pourraient être intégrés, ce qui permettrait de ne recourir aux réquisitions judiciaires que si la personne concernée figure dans le fichier visé.

(1) Articles L. 221-2 et L. 324-2 du code de la route.

Un tel système pourrait néanmoins soulever des difficultés juridiques, la CNIL considérant que la connaissance de l'inscription d'une personne dans un fichier est en soi une donnée personnelle sensible.

Compte tenu de la plus-value opérationnelle et de la simplification quelle pourrait apporter, les rapporteurs souhaitent qu'une telle solution puisse être étudiée. L'architecture de l'interface, qui reposerait sur des interconnexions entre fichiers, devrait, en tout état de cause, être définie de manière très précise en fonction des missions des agents et dans le respect du principe de proportionnalité.

Proposition n° 15 :

– Mettre en œuvre une interface entre les différents fichiers auxquels un agent a accès, permettant leur consultation simultanée à partir de la saisie d'une identité ou d'un identifiant technique ;

– Étudier la possibilité de mettre en œuvre, dans le cadre de cette interface, un système d'alerte de présence, indiquant uniquement si une personne est inscrite au sein d'autres fichiers auxquels l'agent n'a pas accès.

B. LE FSPRT ET LE FPR : DES OUTILS EFFICACES DANS LA LUTTE ANTI-TERRORISTE MAIS QUI PEUVENT ENCORE ÊTRE AMÉLIORÉS

1. FSPRT et FPR : des outils performants

a. Le fichier des personnes recherchées (FPR)

Initialement créé sous une première forme en 1969, le FPR (Fichier des personnes recherchées) constitue un fichier de police non spécialisé, de type alphanumérique. Dans sa version actuelle (FPR2, en vigueur depuis le 18 mai 2017), il est commun à la police nationale et à la gendarmerie nationale. Ses fiches peuvent, le cas échéant, être consultées sur tablette ou sur terminal embarqué.

Le fichier des personnes recherchées (FPR)

Régi actuellement par le décret en Conseil d'État n° 2010-569 du 28 mai 2010, le fichier des personnes recherchées (FPR) a pour finalité principale de faciliter les recherches effectuées par les services de police et de gendarmerie à la demande des autorités judiciaires ou administratives et de faciliter les recherches, surveillances et contrôles effectués, dans le cadre de leurs attributions respectives, par les services de la police nationale, les unités de la gendarmerie nationale et les agents des douanes exerçant des missions de police judiciaire ou des missions administratives ainsi que par les agents du service mentionné à l'article L. 561-23 du code monétaire et financier (TRACFIN).

La direction centrale de la police judiciaire est en charge, par l'intermédiaire de sa Division nationale de la documentation criminelle et de la coordination de la police technique et scientifique (DND2CPT) [(1)], de la direction d'application et de la maîtrise d'œuvre du fichier.

Le FPR est alimenté manuellement par le service gestionnaire (DCPJ), s'agissant de l'inscription des personnes faisant l'objet de mesures de surveillance sollicitées par les services opérationnels (une alimentation semi-automatique est envisagée pour l'avenir) et de décisions émises par l'autorité judiciaire (mandats, interdictions judiciaires, mesures de contrôles judiciaire). Les services centraux du ministère de l'intérieur et les préfectures et sous-préfectures alimentent manuellement le FPR des mesures émises par les autorités administratives.

La mise à jour est effectuée manuellement par le service gestionnaire sur indication des services demandeurs qui sont les uniques prescripteurs en la matière.

Le FPR contient environ 620 000 fiches actives.

Le FPR vise les personnes faisant l'objet d'une mesure de recherche administrative ou judiciaire et permet l'affichage des critères de dangerosité, notamment celui lié à une personne en fuite. Une inscription peut intervenir pour des motifs :

— judiciaires (exécution de mandats, de condamnation, d'un contrôle judiciaire, enquête de police judiciaire, *etc.*) ;

— administratifs (application de réglementations spécifiques de police administrative, en matière par exemple de droit des étrangers, d'infractions à la législation fiscale ou de recherche de personnes disparues, *etc*.) ;

— d'ordre public (prévention des menaces contre la sécurité publique ou la sûreté de l'État).

Le FPR est subdivisé en différentes catégories (« *contrôle judiciaire* », « *sûreté de l'État* », *etc*.). À chaque catégorie correspond un type de fiche particulier, par exemple CJ (contrôles judiciaires), E (police des étrangers), I (interdictions judiciaires, interdictions de sortie du territoire), J (recherches de

(1) Sise à Écully.

Justice), M (Mineurs fugueurs), T (débiteurs envers le Trésor), TE (opposition à l'entrée en France) ou S (sûreté de l'État).

Lorsqu'il complète le FPR, l'« *inscripteur* » insère des informations sur l'identité de la personne recherchée et mentionne son signalement, le motif de la recherche, le service qui a demandé l'inscription (par exemple, pour une fiche « *contrôle judiciaire* », un juge d'instruction) ainsi que la conduite à tenir (CAT) ou la mesure immédiate à prendre (par exemple, « *CJ 01 : interdiction de sortie du territoire* » ou bien « *appréhender* » ou encore « *informer le service demandeur* »). Il peut aussi insérer dans le FPR 2 une photographie ou un document, tel qu'un mandat d'arrêt.

Les fiches S concernent les personnes qui peuvent, en raison de leur activité individuelle ou collective, porter atteinte à la sûreté de l'État et à la sécurité publique par le recours ou le soutien actif apporté à la violence, ainsi que celles entretenant ou ayant des relations directes et non fortuites avec ces personnes. Elles sont demandées par la DGSI, le Service central du renseignement territorial (SCRT) et la Direction du renseignement de la Préfecture de police (DRPP). Si depuis quelques années le terrorisme islamiste constitue le vivier le plus important des fichés S, il existe d'autres motifs d'inscription qui restent significatifs (ultra-gauche, ultra-droite, « animalistes », terrorisme autonomiste, espionnage, *etc*.).

Onze conduites à tenir sont possibles lors du contrôle d'une personne fichée S. Il s'agit généralement de collecter certains types de renseignements (documents d'identité, provenance et destination de l'individu, véhicules, individus accompagnant l'individu fiché, *etc.*) sans attirer l'attention de l'intéressé. Le contrôle d'un individu surveillé doit être signalé au service demandeur dans les meilleurs délais.

Les approximations de certains médias ont, à la suite des attentats qui ont endeuillé notre pays, fait naître une certaine confusion sur la finalité de la fiche S. Celle-ci est un outil de suivi des personnes et de collecte du renseignement. Elle ne préjuge pas nécessairement de la dangerosité de l'individu concerné mais signifie seulement qu'un service souhaite obtenir une remontée d'information en cas de contrôle de l'intéressé à l'occasion d'un déplacement. Des individus non dangereux peuvent donc faire l'objet d'une fiche S, de même que des individus dangereux peuvent ne pas être inscrits au FPR, notamment lorsque leur surveillance s'opère par d'autres moyens.

Plusieurs personnes auditionnées ont signalé aux rapporteurs que les fiches S souffraient d'un manque de visibilité concernant la « *conduite à tenir* ». Il faut parfois prendre le temps de lire deux ou trois pages pour connaître celle-ci. Cela ne peut qu'être de nature à éveiller les soupçons d'un individu alors qu'il importe au plus haut point au contraire que l'intéressé ignore la surveillance dont il fait l'objet. Mis en alerte, il se montrera méfiant et prendra davantage de précautions pour dissimuler ses activités. Les rapporteurs préconisent donc

d'apporter une amélioration à la fiche S en y faisant ressortir visuellement, de manière immédiate, l'attitude à adopter.

Proposition n° 16 : Faire ressortir visuellement sur la fiche S, de manière immédiate, la « *conduite à tenir* » face à la personne contrôlée.

Le FPR est interconnecté avec de nombreux fichiers tels que le PNR, PARAFE [1], FIJAISV, SETRADER [2], AGDREF [3], *etc*. Ces systèmes, lorsqu'ils sont consultés, permettent d'interroger de manière automatisée le FPR afin de déterminer si une personne fait l'objet de recherches ou d'une surveillance. Par ailleurs, les manquements aux obligations incombant aux personnes inscrites au FIJAISV engendrent des alertes au sein du FPR.

Le FPR alimente aussi le Système d'information Schengen (SIS). Le FPR ne permettait pas à ses utilisateurs, jusqu'à une date récente, d'accéder à l'ensemble des données mises à disposition par les États étrangers connectés au SIS, c'est-à-dire aux photographies, aux liens, aux descriptions de personnes, aux extensions liées aux identités usurpées ainsi qu'aux éventuels empreintes digitales et mandats d'arrêt européens disponibles. Ce problème est toutefois en voie d'être réglé.

Dans leur rapport du 11 septembre 2018 [4], Mme Alice Thourot et M. Jean-Michel Fauvergue recommandent de « *travailler à un dispositif d'accès aux fichiers FPR (dans des conditions très limitées) pour les policiers municipaux* ». Selon eux, « *un policier municipal doit être en situation de savoir rapidement si une personne dont il relève l'identité est ou non signalée comme une personne recherchée, sans avoir à transiter par un de ses partenaires des forces de l'État. Il s'agit d'un gain en opérationnalité et en efficacité. Le cas échéant, l'accès pourrait se limiter à un dispositif « hit / no hit », et ne porter que sur une partie des informations figurant dans ces fichiers* ». Les rapporteurs incitent à la plus grande prudence sur ce point. D'une part, le FPR n'a pas pour but de signaler la dangerosité d'un individu mais de permettre avant tout le suivi d'un certain nombre de personnes et le recueil de renseignements les concernant. L'accès des policiers municipaux au FPR pourrait se révéler contre-productif en multipliant les risques de révéler à une personne la surveillance dont elle fait l'objet. D'autre part, l'élargissement de l'accès au FPR paraît également délicat au regard de la protection des libertés individuelles, compte tenu de la sensibilité des données qu'il renferme. Enfin, d'un point de vue technique, cet accès supposerait que ces policiers soient dotés d'équipements informatiques mobiles adéquats, de type « Néo », ce qui ne paraît pas à l'ordre du jour. Aussi la direction des libertés

(1) Passage rapide aux frontières extérieures. Il s'agit d'un traitement de données relevant du ministère de l'intérieur et créé par un décret n° 2010-1274 du 25 octobre 2010.

(2) Système Européen de Traitement des Données d'enregistrement et de Réservation.

(3) Application de gestion des dossiers des ressortissants étrangers en France.

(4) Mme Alice Thourot, M. Jean Michel Fauvergue, D'un continuum de sécurité vers une sécurité globale*, septembre 2018.*

publiques et des affaires juridiques a-t-elle fait part aux rapporteurs de ses plus vives réserves quant à cette proposition.

b. Le fichier des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT)

Le Fichier des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT) est une base de données spécialisée dans le domaine de la lutte anti-terroriste. Géré par l'UCLAT (Unité de coordination de la lutte antiterroriste), il recense et centralise les informations relatives aux personnes qui, engagées dans un processus de radicalisation, sont susceptibles de vouloir se rendre à l'étranger sur un théâtre d'opérations de groupements terroristes ou de vouloir prendre part à des activités à caractère terroriste.

Le fichier des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT)

Créé par décret en Conseil d'État (non publié) du 5 mars 2015 (modifié par décret en Conseil d'État non publié du 2 août 2017), le fichier des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT) a pour finalité principale de recenser et de centraliser les informations relatives aux personnes qui, engagées dans un processus de radicalisation, sont susceptibles de vouloir se rendre à l'étranger sur un théâtre d'opérations de groupements terroristes ou de vouloir prendre part à des activités à caractère terroriste, en vue de l'information des autorités compétentes et de leur exploitation par les services et du suivi des personnes concernées.

Son gestionnaire est l'Unité de coordination de la lutte antiterroriste (UCLAT), rattachée à la direction générale de la police nationale (DGPN).

Le centre national d'assistance et de prévention de la radicalisation (CNAPR), les états-majors de sécurité placés sous l'autorité du préfet de département (EMS) et les services de renseignement peuvent alimenter directement le fichier.

Le FSPRT recense aujourd'hui plus de 20 000 individus signalés (dont 6 000 « *en sommeil* », c'est-à-dire moins prioritaires, ce qui ne signifie pas pour autant qu'ils ne sont plus observés).

Le FSPRT permet d'assurer le suivi de tous les signalements qui remontent du centre national d'assistance et de prévention de la radicalisation (CNAPR) ou des préfectures. La surveillance des personnes concernées est ensuite assurée par différents services ayant des ministères de tutelle différents (ministère des armées, ministère de l'intérieur, ministère de la justice [(1)]) et des niveaux de compétence géographique variés (services nationaux, zonaux ou locaux).

Les services de renseignement estiment que ce fichier a prouvé sa pertinence en matière de suivi des individus radicalisés susceptibles de basculer dans l'action violente. Le FSPRT a démontré son utilité en termes de partage de l'information. Il permet d'appréhender le phénomène de la radicalisation sur le

(1) Ministère de tutelle de l'administration pénitentiaire. Le Bureau central du renseignement pénitentiaire (BCRP), service du deuxième cercle du renseignement, a accès au FSPRT et alimente celui-ci.

territoire français dans sa globalité. Des études sont ainsi réalisées par l'UCLAT à partir du FSPRT. Les différentes statistiques extraites du fichier contribuent ainsi à l'élaboration des politiques publiques de lutte contre la radicalisation.

Les accédants à ce fichier sont essentiellement les fonctionnaires de police et les militaires de la gendarmerie chargés de missions de lutte contre le terrorisme ainsi que les préfets et les agents spécialement désignés par ceux-ci. On sait ainsi précisément quel service est en charge du suivi de l'individu concerné.

Les services auditionnés par les rapporteurs sont extrêmement réservés à l'encontre de toute ouverture plus large de l'accès au FSPRT, même limitée au « haut du spectre », notamment au bénéfice des élus locaux. Les maires sont parfois demandeurs d'un tel accès afin de pouvoir être informés de la présence sur le territoire de leur commune d'un individu potentiellement « dangereux ». Toutefois, une trop large diffusion de ce type d'information risquerait de lui faire perdre de son efficacité comme outil de renseignement. L'inscription au FSPRT, pour être utile, doit en effet demeurer inconnue de l'intéressé. Ainsi, si l'on peut évidemment faire confiance à l'immense majorité des maires, on ne peut exclure l'hypothèse d'une initiative malencontreuse ou maladroite de la part de l'un ou l'autre en présence d'un individu « fiché ».

Quant aux autorités judiciaires, elles ne semblent pas réclamer d'avoir accès de manière générale aux fichiers de police, lesquels sont sous la responsabilité des autorités administratives, sous peine d'être noyées. Toutefois, les rapporteurs jugent utile de ménager une exception en ce qui concerne le FSPRT et de donner aux procureurs de la République accès à ce dernier. Dès lors en effet qu'ils prennent part aux groupes d'évaluation départementaux (GED) [(1)], ils devraient pouvoir, à l'instar des autres participants, consulter ce fichier. La demande en a été faite notamment par les membres du parquet du tribunal de grande instance de Lyon rencontrés par les rapporteurs.

Proposition n° 17 : Donner accès au FSPRT aux procureurs de la République.

2. La nécessaire prise en compte de l'aspect psychiatrique

Les services de sécurité auditionnés par les rapporteurs ont souligné à plusieurs reprises la présence de plus en plus fréquente d'une dimension psychiatrique dans la criminalité, notamment terroriste. On évalue à 30 % la part de la population carcérale souffrant de troubles mentaux. Les services médico-psychologiques régionaux (SMPR) et les unités hospitalières spécialement aménagées (UHSA), qui prennent en charge les détenus les plus atteints sont pleins. Les services territoriaux de la police judiciaire indiquent de leur côté être saisis de beaucoup d'enquêtes périphériques au terrorisme (pour apologie du

(1) Le groupe d'évaluation départemental (GED) rassemble autour du préfet des représentants des services de renseignement, des services de police et de gendarmerie, du parquet et de l'administration pénitentiaire. Il évalue l'ensemble des signalements pour radicalisation et décide des mesures de suivi policier.

terrorisme, menaces de mort, *etc.*) dans lesquelles les mis en cause apparaissent perturbés mentalement. Dans une vague d'attentats, telle que celle ayant débuté en France en 2015, les actes commandités par des organisations structurées sont souvent suivis par des passages à l'acte individuels de la part de déséquilibrés (schizophrènes, psychotiques, délirants, *etc.*).

Ces passages à l'acte individuels, qui émanent souvent du « bas du spectre » (c'est-à-dire de personnes qui n'ont envoyé que des « signaux faibles » de radicalisation) sont difficiles à prévenir. Pour les détecter, il pourrait être intéressant de croiser le FSPRT avec un fichier faisant état d'antécédents psychiatriques d'une certaine gravité.

Deux fichiers sont envisageables de ce point de vue.

Le premier est le répertoire des données à caractère personnel collectées dans le cadre des procédures judiciaires, dit « *Répertoire des Expertises* » (REDEX) [(1)]. Prévu à l'article 706-56-2 du code de procédure pénale, il centralise les expertises, évaluations et examens psychiatriques, médico-psychologiques, psychologiques et pluridisciplinaires réalisés notamment au cours de l'enquête, de l'instruction et de l'exécution de la peine. Ce fichier a toutefois un objet spécifique, consistant à répertorier les expertises réalisées dans le cadre d'une procédure pénale.

Le second est le fichier relatif au suivi des personnes hospitalisées sans leur consentement en raison de troubles mentaux, dit « HOPSY », qui relève du ministère de la santé. Le croisement avec ce fichier ne semble pas pertinent. Le milieu psychiatrique hospitalier se montre très réticent envers cette idée, eu égard au principe du secret médical. Un croisement entre FSPRT et HOPSY pourrait peut-être néanmoins se concevoir, mais de manière très encadrée, en étant réservé par exemple à quelques acteurs comme la sous-direction anti-terroriste (SDAT) de la police judiciaire.

Le Gouvernement ne semble pas exclure de progresser en ce sens si l'on se réfère à la mesure n° 39 du Plan national de prévention de la radicalisation présenté par le Premier ministre le 23 février 2018. Celle-ci invite en effet à « *actualiser les dispositions existantes relatives à l'accès et la conservation des données sensibles contenues dans l'application de gestion des personnes faisant l'objet d'une mesure de soins psychiatriques sans consentement* ». Un pas semble avoir été accompli en ce sens avec la publication du décret n° 2018-383 du 23 mai 2018 autorisant les traitements de données à caractère personnel relatifs au suivi des personnes en soins psychiatriques sans consentement. Celui-ci autorise les agences régionales de santé (ARS) à collecter des données qui pourront être consultées nationalement via un dispositif appelé Hopsyweb et fixe à trois ans la durée de conservation des données.

(1) Cf. Circulaire du 11 avril 2018 de la direction des affaires criminelles et des grâces.

Le fichier HOPSY donne par ailleurs lieu à des vérifications par les services de santé à la demande des préfectures dans le cadre du dispositif encadrant les demandes d'acquisition ou de détention d'armes. L'article R. 312-8 du code de la sécurité intérieure prévoit en effet que « *le préfet peut* (…), *avant de statuer, s'il l'estime nécessaire, demander à l'agence régionale de santé de l'informer, dans le respect des règles du secret médical, de l'éventuelle admission en soins psychiatriques sans consentement dans un établissement de santé mentionné à l'article L. 3222-1 du code de la santé publique ou de l'éventuel traitement dans un service ou secteur de psychiatrie d'un demandeur qui n'a pas produit le certificat médical* » attestant que son état de santé physique et psychique n'est pas incompatible avec la détention de ces matériels, armes ou munitions.

Dans le même ordre d'idées, un certain nombre de conventions ont été conclues entre des agences régionales de santé et des préfectures en vue de renforcer leur coopération en matière de prévention de la radicalisation, conformément à la mesure n° 38 du Plan national de prévention de la radicalisation. C'est, selon l'UCLAT, le signe que le monde de la santé et celui de la sécurité publique ont commencé à engager un véritable dialogue.

C. RÉPONDRE À LA MONTÉE EN PUISSANCE DES ENQUÊTES ADMINISTRATIVES

a. L'extension du champ des enquêtes administratives

Des enquêtes administratives sont réalisées pour vérifier que le comportement d'une personne n'est pas incompatible avec l'exercice de certaines fonctions, l'accès à certains lieux ou l'utilisation de certains produits dangereux. **Dans le contexte de l'aggravation de la menace terroriste, le champ de ces enquêtes a été élargi**. Il existe à présent une grande diversité d'enquêtes relevant de bases juridiques différentes.

Les différentes catégories d'enquêtes administratives

● L'article L. 114-1 du code de la sécurité intérieure prévoit que des enquêtes administratives peuvent précéder les décisions administratives de recrutement, d'affectation, de titularisation, d'autorisation, d'agrément ou d'habilitation concernant :

– **les emplois publics participant à l'exercice des missions de souveraineté de l'État** ;

– les **emplois publics ou privés relevant du domaine de la sécurité ou de la défense** ;

– les emplois privés ou activités privées réglementées relevant des domaines des jeux, paris et courses ;

– **l'accès à des zones protégées** en raison de l'activité qui s'y exerce ;

– l'utilisation de matériels ou produits présentant un caractère dangereux.

Si le résultat de l'enquête conclut à une incompatibilité, l'administration peut procéder au retrait ou à l'abrogation de la décision administrative précédemment délivrée ou à la mutation, voire la radiation des cadres, du fonctionnaire en cause.

La loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme a étendu le champ des enquêtes en prévoyant que celles-ci peuvent être réalisées postérieurement aux décisions administratives pour s'assurer que le comportement d'une personne n'est pas devenu incompatible avec l'exercice de ses fonctions, l'accès à des lieux sensibles ou l'utilisation de produits dangereux.

● Des enquêtes administratives peuvent également être réalisées en application de l'article L. 114-2 du code de la sécurité intérieure, créé par la loi n° 2016-339 du 22 mars 2016 dite loi « Savary » [(1)]. Elles concernent les décisions de recrutement et d'affectation relatives aux **emplois en lien direct avec la sécurité des personnes et des biens au sein d'une entreprise de transport public de personnes** ou d'une entreprise de transport de marchandises dangereuses.

● La loi n° 2016-731 du 3 juin 2016 a créé un **dispositif dit « grands événements »**, relevant de l'article L. 211-11-1 du code de la sécurité intérieure. Dans ce cadre, les organisateurs de grands événements, désignés par décret, exposés à un risque exceptionnel de menace terroriste, doivent recueillir l'avis préalable de l'autorité administrative rendu à la suite d'une enquête pour l'accès de toute personne, à un autre titre que celui de spectateur ou de participant, à tout ou partie des lieux désignés par le décret.

● L'article 17-1 de la loi n° 95-73 du 21 janvier 1995 prévoit la réalisation d'enquêtes administratives pour **l'instruction des demandes d'acquisition de la nationalité française et de délivrance et de renouvellement des titres relatifs à l'entrée et au séjour des étrangers** ainsi que pour la nomination et la promotion dans les ordres nationaux.

(1) Loi n° 2016-339 du 22 mars 2016 relative à la prévention et à la lutte contre les incivilités, contre les atteintes à la sécurité publique et contre les actes terroristes dans les transports collectifs de voyageurs.

b. La nécessaire réorganisation de la conduite des enquêtes administratives

La réalisation d'enquêtes administratives repose en général sur **la saisine du service de police ou de l'unité de gendarmerie territorialement compétent**, afin d'interroger le fichier TAJ et, en fonction de la sensibilité de l'enquête, d'autres fichiers, tels que les fichiers « Enquêtes administratives liées à la sécurité publique » (EASP), PASP, GIPASP ou le FPR. Le fichier EASP, placé sous la responsabilité du ministère de l'intérieur (direction centrale de la sécurité publique et préfecture de police), a pour finalité de faciliter les différentes catégories d'enquêtes administratives [(1)].

D'autres actes d'enquête peuvent compléter la consultation de ces fichiers : contact avec le service ou l'unité du lieu de résidence de la personne, enquête de voisinage, voire entretien administratif avec la personne.

L'intervention des forces de sécurité peut être complémentaire de celle des agents des préfectures ou du Conseil national des activités privées de sécurité (CNAPS). En effet, ces agents peuvent être habilités à accéder aux fichiers TAJ et FPR [(2)] dans le cadre des enquêtes administratives relevant de leur compétence. Ce n'est que dans le cas où la personne concernée est inscrite dans le fichier que les services de police et les unités de gendarmerie seront sollicités pour une enquête complémentaire.

L'extension du champ des enquêtes administratives et la diversité de ces enquêtes font peser des charges très lourdes sur les forces de sécurité, au détriment de leurs autres missions.

Une évolution dans l'organisation des enquêtes administratives a été amorcée avec **la création du service national des enquêtes administratives de sécurité (SNEAS)** [(3)] **et du commandement spécialisé pour la sécurité nucléaire (COSSEN)** [(4)], services à compétence nationale rattachés respectivement au directeur général de la police nationale et au directeur général de la gendarmerie nationale.

Le SNEAS a été chargé des enquêtes administratives en matière de transport public de voyageurs et de marchandises dangereuses (articles L. 114-2 du CSI), de « grands événements » (article L. 211-11-1), ainsi que d'acquisition et

(1) Article R. 236-1 du code de la sécurité intérieure.

(2) Article R. 40-29 du code de procédure pénale et décret n° 2015-648 du 10 juin 2015 relatif à l'accès au traitement d'antécédents judiciaires et au fichier des personnes recherchées.

(3) Décret n° 2017-668 du 27 avril 2017 portant création d'un service à compétence nationale dénommé « service national des enquêtes administratives de sécurité.

(4) Décret n° 2017-588 du 20 avril 2017 portant création d'un service à compétence nationale dénommé « Commandement spécialisé pour la sécurité nucléaire ».

de détention d'armes. Le COSSEN est quant à lui compétent pour les enquêtes administratives dans le domaine de la sécurité nucléaire.

La création du SNEAS et du COSSEN vise en particulier à permettre **l'utilisation, dans le cadre d'enquêtes administratives, d'informations issues des fichiers de renseignement** (FSPRT, CRISTINA et GESTEREXT) auxquelles les services de police et les unités de gendarmerie n'ont pas accès.

Le SNEAS et le COSSEN utilisent **l'application « ACCReD »** (« Automatisation de la consultation centralisée de renseignements et de données ») permettant le « criblage » d'une personne grâce à la consultation simultanée des fichiers TAJ, FPR, FOVeS, PASP, EASP, GIPASP et FSPRT et la consultation indirecte des fichiers CRISTINA et GESTEREXT. En cas d'inscription de la personne concernée dans l'un de ces fichiers, le SNEAS et le COSSEN procèdent aux vérifications complémentaires auprès des services gestionnaires des fichiers auxquels ils n'ont pas d'accès direct.

La création de services centralisés, bénéficiant de modalités innovantes d'accès aux informations contenues dans les fichiers, représente indéniablement une avancée. Il convient à présent de **poursuivre l'évolution de l'organisation des enquêtes administratives en confiant au SNEAS un champ plus large d'enquêtes**. Cette réflexion semble engagée au ministère de l'intérieur. Il a ainsi été indiqué aux rapporteurs que le SNEAS se verrait confier à brève échéance certaines enquêtes relevant de l'article L. 114-1 du code de la sécurité intérieure.

Proposition n° 18 : Confier au service national des enquêtes administratives de sécurité (SNEAS) un champ plus large d'enquêtes administratives relevant actuellement des services de police et des unités de gendarmerie.

c. L'exigence de préserver les droits des personnes

L'utilisation des fichiers dans le cadre des enquêtes administratives est encadrée par différentes dispositions législatives et réglementaires.

La **consultation du TAJ** est autorisée dans les différents types d'enquête administrative. Les informations pouvant être consultées sont celles relatives à des procédures judiciaires en cours ou closes, à l'exception des cas où sont intervenues des mesures ou décisions de classement sans suite, de non-lieu, de relaxe ou d'acquittement devenues définitives, ainsi que des données relatives aux victimes [(1)]. L'article 230-8 du code de procédure pénale prévoit que les décisions de relaxe ou d'acquittement devenues définitives entraînent l'effacement des données, tandis que les décisions de non-lieu et de classement sans suite font l'objet d'une mention, rendant impossible leur consultation à des fins d'enquête administrative.

(1) Article R. 40-29 du code de procédure pénale.

Lorsque la consultation du TAJ par les agents des préfectures ou du CNAPS dans le cadre d'enquêtes administratives révèle qu'une personne est inscrite en tant que mise en cause, ces agents sont tenus de saisir, pour complément d'information, les services de police ou les unités de gendarmerie compétents et, aux fins de demandes d'information sur les suites judiciaires, le procureur de la République compétent.

Malgré cette garantie, **la consultation du TAJ dans le cadre d'enquêtes administratives soulève plusieurs difficultés**.

Comme l'a souligné M. Rémy Heitz, directeur des affaires criminelles et des grâces, **le TAJ s'éloigne de sa finalité première** – faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs – **pour se rapprocher du rôle du casier judiciaire**.

Si les rapporteurs prennent acte de cette évolution, liée à l'extension du champ des enquêtes administratives, ils estiment d'autant plus nécessaire de renforcer la fiabilité des informations contenues dans ce fichier. Le fait que le TAJ contienne **de nombreuses informations inexactes** (erreurs diverses, absence de prise en compte de suites judiciaires favorables par l'effacement des données ou l'ajout d'une mention) peut en effet avoir **des conséquences extrêmement lourdes pour les personnes concernées** par une enquête administrative.

En outre, **la complexité des procédures de rectification ou d'effacement anticipé des données**, en application de l'article 230-8 du code de procédure pénale, peut être un obstacle à l'exercice de leurs droits par les personnes concernées. Ainsi que l'a relevé M. Paul Michel, ancien magistrat référent chargé du contrôle du TAJ, il arrive également que les personnes concernées n'aient même pas connaissance de leur inscription dans le TAJ et ne l'apprennent que lorsqu'elles font l'objet d'une décision administrative défavorable mentionnant cette inscription.

La mise en œuvre des propositions précédemment formulées par les rapporteurs s'agissant du TAJ (interconnexion avec CASSIOPEE, voire avec le casier judiciaire, renforcement des moyens humains et techniques des parquets pour mettre en œuvre leurs missions de contrôle) sont de nature à remédier à ces difficultés.

Il conviendra également de **veiller à ce que la mise en œuvre du droit à l'information prévu par l'article 70-18 de la loi du 6 janvier 1978 soit effective** pour les personnes concernées au moment de leur inscription dans le TAJ. Or, selon les éléments communiqués par le ministère de l'intérieur aux rapporteurs, l'information relative aux différents traitements pourrait se limiter à une publication sur le site internet du ministère. Compte tenu des conséquences que peut avoir une inscription au TAJ, les rapporteurs jugent nécessaire d'aller plus loin et de prévoir la communication systématique aux personnes concernées d'informations sur la durée de conservation des données, leur utilisation possible

dans le cadre d'enquêtes administratives ainsi que sur les possibilités de demander leur effacement anticipé.

Proposition n° 19 : Prévoir, s'agissant du fichier TAJ, une mise en œuvre effective du droit à l'information des personnes au moment de leur inscription dans le fichier, incluant notamment la communication d'informations sur la durée de conservation des données, leur utilisation possible dans le cadre d'enquêtes administratives ainsi que sur les possibilités de demander leur effacement anticipé.

Au-delà des difficultés propres au fichier TAJ, la question de la légalité de décisions défavorables se fondant uniquement sur l'inscription d'une personne dans un fichier de renseignement peut se poser.

La CNIL a ainsi souligné, dans son bilan d'activité pour 2017, à propos du traitement ACCReD que « *l'avis rendu sur la compatibilité du comportement de l'agent avec l'accès à des missions, zones ou produits spécifiques ne* [devait] *pas découler de la seule inscription d'une personne dans un fichier* », en raison des « *risques liés à l'absence de mise à jour récente ou à l'absence de vérification des informations enregistrées dans cet unique traitement* ». La commission a donc préconisé qu'en cas de réception automatique par le traitement ACCReD d'un message indiquant « levée de doute », ce qui révèle qu'une personne est inscrite dans les traitements GESTEREXT ou CRISTINA, un complément d'informations soit recherché et que celui-ci ne se limite pas à la consultation des informations inscrites dans ces traitements.

S'agissant de la consultation du FPR, il a été indiqué aux rapporteurs que la simple inscription d'une personne ne pouvait justifier une décision défavorable mais que le Conseil d'État acceptait que des « notes blanches » des services de renseignement puissent fonder une telle décision.

III. RENFORCEMENT DE LA COOPÉRATION EUROPÉENNE ET ÉVOLUTIONS TECHNOLOGIQUES : DE NOUVEAUX ENJEUX

A. L'UTILISATION DES FICHIERS : UN AXE ESSENTIEL DE LA COOPÉRATION POLICIÈRE DANS L'UNION EUROPÉENNE

Le contexte international de lutte contre le terrorisme et de renforcement des contrôles aux frontières fait de la coopération européenne en matière de sécurité un enjeu de premier plan. Le bon fonctionnement et l'adaptation des fichiers utilisés dans le cadre de cette coopération sont donc essentiels.

Principal outil utilisé par les forces de sécurité, le Système d'Information Schengen (SIS) est au cœur de ce dispositif.

Le Système d'information Schengen de deuxième génération (SIS II)

Fondé sur le règlement (UE) 1987/2006 du 20 décembre 2006 et la décision du Conseil 2007/533/JAI du 12 juin 2007, le Système d'information Schengen de deuxième génération (SIS II) a pour finalité principale « *d'assurer un niveau élevé de sécurité dans l'espace de liberté, de sécurité et de justice de l'Union européenne* ».

Il intègre des **signalements concernant des personnes recherchées ou des objets ou documents** perdus, volés, invalidés ou surveillés.

Le SIS II se compose :

– d'un **système central** (le SIS II central) ;

– d'une **section nationale** (le N-SIS II) dans chaque État membre, constituée des systèmes nationaux reliés au SIS II central ;

– d'une infrastructure de communication entre le SIS II central et les N-SIS II.

Le SIS II est alimenté par chaque État membre de manière automatisée et en temps réel depuis ses bases nationales. En France, **il est interconnecté à douze applications nationales**.

Parmi celles-ci, certaines alimentent et consultent le SIS II tandis que d'autres le consultent ou l'alimentent seulement.

Interconnexion « alimentation et consultation »

– FOVeS ;

– FPR ;

– SIRENE (supplément d'information requis à l'entrée nationale).

Alimentation uniquement

– TES ;

– DOCVERIF (vérification de la validité des cartes d'identité et des passeports).

Interconnexion « consultation uniquement »

– COVADIS (contrôle et vérification automatiques des documents d'identité sécurisés) ;

– PARAFE (passage automatisé rapide aux frontières extérieures) ;

– RMV (réseau mondial visas) ;

– SETRADER (système européen de traitement des données d'enregistrement et de réservation) ;

– PNR : *Passenger Name Record* (registre des passagers aériens) ;

– AGDREF (application de gestion des dossiers des ressortissants étrangers en France) ;

– SAT VV (interface de consultation sur les véhicules volés) ;

– STCL (service de traitement central du traitement LAPI de lecture automatisée des plaques d'immatriculation).

1. Assurer le bon fonctionnement des dispositifs existants et la bonne alimentation du SIS II

Différentes difficultés ont été relevées par la Commission européenne lors de l'évaluation de la mise en œuvre de l'acquis de Schengen par la France à l'automne 2016. Celles-ci ont fait l'objet de recommandations du Conseil, qui ont conduit à l'élaboration d'un plan d'action national présenté le 13 avril 2018.

Il s'agit en premier lieu de **problèmes d'accès technique**, liés au nombre des applications nationales connectées au SIS II et à la complexité de l'architecture informatique actuelle. Ces difficultés peuvent être extrêmement dommageables dans le cadre, par exemple, des contrôles aux frontières, où l'accès aux données du SIS II est soumis au bon fonctionnement simultané de CHEOPS, COVADIS (ou PARAFE selon les cas), VISABIO, FPR et N-SIS II.

La DCPJ a indiqué aux rapporteurs que des travaux réalisés depuis l'été 2017 avaient permis d'améliorer la disponibilité générale du SIS II, notamment aux frontières, et de procéder à une première simplification. Le projet de refonte technique de l'architecture N-SIS lancé en juillet 2017 doit permettre, d'ici le début de l'année 2019, de limiter les interdépendances entre fichiers, chaque application accédant aux données du SIS II de manière autonome.

Un deuxième enjeu concerne **l'introduction dans le SIS II d'une photographie et d'empreintes digitales chaque fois qu'elles sont disponibles**, comme le prévoit la réglementation européenne [(1)].

L'introduction automatisée des photographies dans le SIS II depuis le FPR 2 est maintenant opérationnelle. La nécessité de fournir les photographies disponibles a été rappelée aux services demandeurs d'inscriptions au FPR 2 et la mise en œuvre d'un dispositif de préalimentation dématérialisée par ces services est prévue pour faciliter cette transmission.

En revanche, l'insertion des empreintes digitales disponibles associées aux signalements s'effectue pour l'instant manuellement, ce qui n'est pas satisfaisant au regard des exigences de fiabilité et d'exhaustivité des informations transmises au SIS II. Les rapporteurs rappellent à cet égard la **nécessité d'interconnecter les fichiers FPR et FAED** afin de permettre l'alimentation automatisée du FPR et du SIS II s'agissant des empreintes digitales des personnes signalées [(2)].

La Commission européenne a également souligné, dans le cadre de l'évaluation de la mise en œuvre de l'acquis Schengen par la France, **le caractère incomplet de l'alimentation du SIS II avec les numéros des documents volés**. Ces numéros ne peuvent en effet que rarement être enregistrés dans FOVeS au moment du dépôt d'une plainte, la victime ne disposant pas en général du numéro du document. Seule une interconnexion entre FOVeS et le fichier TES permettrait

(1) Articles 20 du règlement SIS II et de la décision SIS II.

(2) Cf. supra*, proposition n° 13.*

d'alimenter automatiquement FOVeS, et donc le SIS II, par les numéros des documents volés. Si les rapporteurs ne souhaitent pas que le fichier TES soit utilisé à des fins d'identification des personnes [1], ils considèrent en revanche que le recours à ce fichier pour compléter les informations relatives aux documents volés pourrait être autorisé car il ne présente pas de risques comparables en matière de libertés individuelles.

Proposition n° 20 : Interconnecter le fichier TES et le fichier FOVeS afin d'alimenter automatiquement le SIS II par les numéros des documents volés.

2. Renforcer l'interopérabilité des systèmes d'informations européens

Dans le prolongement des travaux d'un groupe d'experts de haut niveau piloté en 2016-2017 par la Commission européenne, deux propositions de règlements sur l'interopérabilité des bases centralisées européennes sont discutées depuis décembre 2017 au Parlement européen et au Conseil [2].

Ces propositions de règlement ont pour objectif de renforcer la lutte contre la fraude à l'identité des ressortissants des pays tiers et de faciliter les recherches des services répressifs, notamment grâce à la création d'un « portail de recherche européen » qui rendrait possibles :

– des recherches alphanumériques et biométriques, simultanées en mode *hit/no hit*, dans le SIS II, le système d'information des visas (VIS), la base EURODAC [3] et les deux futurs systèmes d'entrée/de sortie (EES) [4] et d'information et d'autorisation concernant les voyages (ETIAS) [5] ;

– des comparaisons biométriques automatisées au moment de la création de signalements dans le SIS II, le VIS, EURODAC et le Système EES ;

– un détecteur d'identités multiples ;

– la possibilité d'associer des profils ADN à des signalements de personnes.

---

(1) Cf. supra.

(2) Proposition de règlement portant établissement d'un cadre pour l'interopérabilité entre les systèmes d'information de l'Union européenne (coopération policière et judiciaire, asile et migration) COM (2017) 794 final et proposition de règlement portant établissement d'un cadre pour l'interopérabilité entre les systèmes d'information de l'Union européenne (frontières et visas) COM (2017) 793 final, 12 décembre 2017.

(3) Le système EURODAC enregistre les empreintes digitales des demandeurs d'asile et des immigrants illégaux se trouvant sur le territoire de l'UE.

(4) Prévu par le règlement (UE) 2017/2226 du 30 novembre 2017, le système d'entrée/de sortie (EES) sera opérationnel à partir de 2020. Il enregistrera les données relatives aux entrées et aux sorties ou aux refus d'entrée des ressortissants de pays tiers franchissant les frontières extérieures de l'espace Schengen.

(5) Créé par le règlement (UE) 2018/1241 du 12 septembre 2018, le système d'information et d'autorisation concernant les voyages (ETIAS) s'inspire du système ESTA mis en œuvre aux États-Unis. Il permettra de réaliser des contrôles avant la délivrance d'une autorisation de voyage aux ressortissants de pays tiers exemptés de l'obligation de visa qui se rendent dans l'espace Schengen. Le système ETIAS sera opérationnel en 2021.

Les rapporteurs approuvent l'objectif de mise en œuvre de l'interopérabilité des fichiers européens. Ils soulignent que celle-ci impliquera **une évolution profonde du dispositif national**, s'agissant en particulier de la possibilité d'effectuer des recherches à partir des empreintes digitales et d'associer des profils ADN aux signalements.

Des efforts d'interopérabilité sont également menés au niveau national. La France participe ainsi, aux côtés de l'Allemagne, de la Finlande, de l'Espagne et de l'Irlande, au projet pilote ADEP (*Automation of Data Exchange Process*). Ce projet vise à permettre une consultation simultanée de type *hit/no hit* des antécédents judiciaires d'une personne à partir des bases de données nationales.

Les rapporteurs souhaitent que le projet ADEP, qui va prochainement entrer dans sa phase expérimentale sur des données réelles, puisse être, en fonction de ses résultats, étendu à l'ensemble de l'Union européenne.

Proposition n° 21 : Généraliser à l'ensemble des États membres de l'Union européenne la transmission automatisée des antécédents judiciaires à partir des bases de données nationales (projet ADEP), si les résultats de l'expérimentation de cette transmission sont concluants.

B. DE NOUVELLES PERSPECTIVES OUVERTES PAR LES AVANCÉES TECHNOLOGIQUES

Les progrès technologiques vont permettre dans les prochains mois la modernisation d'un certain nombre de fichiers de police. Le fichier central de la criminalité organisée (F2CO) va ainsi remplacer le fichier des brigades spécialisées (FBS) de la police nationale, en principe au premier trimestre 2019 : des ateliers fonctionnels permettent actuellement de valider la mise à jour de ses spécifications. De nouveaux logiciels de rédaction des procédures sont en cours de finalisation pour la police nationale (SCRIBE [(1)]) et la gendarmerie nationale (LRPGN – NG [(2)]). Une nouvelle application dite « *Main courante police nationale* » (MCPN), destinée à remplacer les logiciels actuels de main courante informatisées (« MCI v6 » et « N-MCI »), sera déployée sur des sites pilotes au mois de juillet de l'année prochaine. Plus généralement, au-delà de la refonte de certaines bases existantes, les évolutions technologiques en cours sont appelées à faire naître de nouveaux enjeux en termes d'adaptation technique et juridique des fichiers de police.

1. Les possibilités offertes par le traitement de données de masse et l'intelligence artificielle

Des capacités de rapprochement sont aujourd'hui développées, à partir de données issues de différents fichiers, afin d'évaluer les possibilités offertes par les

(1) Offrant des progrès en termes de partage de l'information opérationnelle et d'ergonomie de rédaction.

(2) Nouvelle génération du logiciel adaptée à la mobilité.

technologies de traitement de données de masse (« *Big Data* ») et d'intelligence artificielle (IA), actuellement en plein essor. Selon le ST(SI)², « *les technologies actuelles permettraient de sécuriser ces opérations, notamment en « pseudonymisant » les données d'identité* ». Cette procédure est cependant lourde et techniquement contraignante. Pour le ST(SI)², seule « *la mise en œuvre d'une véritable procédure d'expérimentation permettrait une meilleure valorisation des nouvelles technologies de data sciences dans un cadre opérationnel, tout en étant encadrée* ».

M. Éric Morvan, directeur général de la police nationale, a indiqué aux rapporteurs que les projets d'intelligence artificielle étaient très attendus au sein des services de la police nationale qui espèrent pouvoir être libérés de certaines tâches à faible valeur ajoutée. Ces projets pourraient aussi permettre de traiter des flux d'informations croissants, trop importants pour être pris en charge par les seules capacités humaines, de comparer les informations émanant de bases différentes, d'enrichir les données, de créer des modèles prédictifs, *etc*. Des projets sont déjà identifiés en matière de gestion et d'analyse d'images en masse (vidéo), de gestion des appels d'urgence (modernisation des centres d'information et de commandement [(1)], mise en œuvre des plates-formes d'appels d'urgence unifiées), de gestion de crise, de sécurité routière ou encore de lutte contre la fraude. Selon M. Éric Morvan, « *plus qu'une simple intelligence artificielle, les projets s'orienteront vers de l'intelligence augmentée pour dépasser la dimension strictement technologique et aller dans le sens d'une véritable assistance aux agents* ».

2. Le développement des techniques de reconnaissance faciale

Le TAJ comporte déjà une fonctionnalité de reconnaissance faciale permettant, dans le cadre d'investigations judiciaires, d'opérer des rapprochements avec les photographies de personnes mises en cause déjà inscrites dans ce fichier [(2)]. Cette fonctionnalité permet également de proposer des « tapissages » de photos faciales de suspects afin de les soumettre aux victimes.

Quant au FPR, il comporte lui aussi certaines photographies d'individus recherchés. S'il n'offre pas à ce jour les mêmes fonctionnalités que le TAJ, des progrès sur ce point pourraient toutefois être enregistrés à brève échéance. En effet, selon le ST(SI)², « *les technologies de reconnaissance faciale sont matures aujourd'hui et permettent à partir de la photo faciale une recherche d'individus. La photo faciale est une biométrie qui présente moins de contraintes dans sa capture et son traitement que l'empreinte digitale. Aussi* ***il nous paraît techniquement envisageable de permettre dans un avenir proche une consultation du FPR à partir d'une photo*** ».

(1) M-CIC 2.

(2) Le TAJ comprend entre 7 et 8 millions de photos de face.

3. L'augmentation des potentialités des équipements mobiles

L'accès aux fichiers via des équipements mobiles (tablettes, téléphones portables) permet d'ores et déjà la transmission sécurisée de données par les réseaux mobiles de communication (3G/4G) et par des protocoles de communication sans fil tels que Wi-Fi et Bluetooth. M. Pascal Lalle, directeur central de la sécurité publique, a indiqué aux rapporteurs que des études techniques ou des développements d'applications étaient en cours en vue d'augmenter encore les potentialités offertes par l'utilisation de ces outils de type « Néo ». Des progrès sont attendus notamment en matière :

— de fonctionnalité de géolocalisation des terminaux ;

— de messagerie instantanée de type « WhatsApp » ;

— d'applications bureautiques, permettant la rédaction de document ;

— de chiffrement de la voix.

4. Le recours à la biométrie en mobilité

En matière de contrôle « en bord de route », si les applications Néo/Néogend permettent la consultation des fichiers de police à partir de données alphanumériques (nom, prénom, date, lieu de naissance), elles ne permettent pas encore en revanche le contrôle à partir de la biométrie. Toutefois, l'appareil photo intégré dans ces outils offre des perspectives intéressantes peu explorées et qui pourraient être prometteuses, surtout si la reconnaissance faciale était autorisée sur FPR ou sur SBNA [(1)]. Il permet la prise de photographie faciale mais aussi la capture directe d'empreintes digitales. Selon le ST(SI)², « *des projets en laboratoire chez certains industriels en ont déjà démontré la faisabilité. D'ici deux ans, sans ajout d'appareil de capture biométrique, NEO pourrait être un vecteur de contrôle et d'identification des personnes recherchées, ou des étrangers en situation irrégulière, et de contrôle aux frontières* ».

Par ailleurs, d'autres outils biométriques pourraient voir le jour, sous l'impulsion notamment de la Commission européenne. Celle-ci travaille par exemple à la mise en œuvre de contrôles par l'iris de l'œil [(2)].

---

(1) Système biométrique national de l'application de gestion des dossiers des ressortissants étrangers en France.

(2) L'OACI (Organisation de l'aviation civile internationale) reconnaît trois biométries normalisées pour les documents de voyage : l'empreinte digitale, la photo faciale et l'iris de l'œil.

SYNTHÈSE DU RAPPORT

Au terme de cette mission d'information, les rapporteurs formulent plusieurs propositions d'évolution portant sur le cadre juridique des fichiers mais aussi sur leur architecture et les modalités concrètes de leur utilisation.

Ils souhaitent tout d'abord la mise en œuvre effective **du droit à l'information des personnes inscrites dans les fichiers** des forces de sécurité. Celle-ci est particulièrement urgente s'agissant du fichier TAJ, qui contient près de 19 millions de fiches relatives à des personnes mises en cause et qui est largement utilisé dans le cadre des enquêtes administratives pour l'accès à certains emplois, avec des conséquences potentiellement très lourdes pour les personnes. Chaque personne mise en cause devrait être informée de son inscription dans le TAJ, ainsi que de la durée pendant laquelle les données pourront être conservées et des possibilités de demander leur effacement anticipé. De manière plus générale, les rapporteurs souhaitent qu'une réflexion soit menée sur les modalités concrètes de l'information des personnes inscrites dans les différents fichiers car il s'agit d'un enjeu essentiel de protection des libertés individuelles.

L'approfondissement des avancées déjà intervenues en matière de **sécurisation des fichiers** et de **traçabilité** est une deuxième priorité. Il s'agit par exemple de généraliser l'accès aux fichiers par l'authentification grâce à la carte professionnelle ou de rendre plus systématiques les contrôles de l'utilisation des fichiers, par le recours à des procédés algorithmiques permettant l'analyse massive des traces de consultation.

Les rapporteurs souhaitent également que soit mieux garantie **la sécurité juridique**. Le foisonnement et la complexité des normes applicables aux fichiers, par exemple en matière d'effacement anticipé des données, nuisent à la bonne compréhension de leurs droits par les personnes. La jurisprudence de la Cour européenne des droits de l'homme sur les durées de conservation des données doit par ailleurs être prise en compte.

L'architecture des fichiers est trop complexe : les rapporteurs ont recensé plus d'une centaine de fichiers utilisés par les forces de sécurité. Ils souhaitent donc que le ministère de l'intérieur engage **une réflexion globale sur la rationalisation de ces fichiers,** en se fondant sur une analyse de leurs finalités et de leur utilisation.

La **cohérence des informations** et la **fiabilité des identités** enregistrées dans les différents fichiers doivent être améliorées. Il est pour cela urgent de relier les fichiers TAJ, FAED et FNAEG, soit par une base commune d'identité, soit par l'utilisation d'un identifiant commun. Dans un objectif de fiabilisation des informations enregistrées dans le fichier TAJ, les rapporteurs demandent de

généraliser à l'ensemble du territoire l'interconnexion avec l'application CASSIOPEE du ministère de la justice, actuellement expérimentée dans sept juridictions. Ils proposent également d'interconnecter le TAJ avec le casier judiciaire national, afin que les condamnations pénales figurent dans le TAJ.

Les moyens informatiques et humains des parquets doivent être renforcés, pour leur permettre d'accomplir les missions importantes qui leur sont confiées en matière de contrôle des fichiers de police judiciaire. L'information des procureurs de la République en matière de suivi de la radicalisation doit être complétée en autorisant leur accès au FSPRT.

Il est nécessaire de **développer les interconnexions entre fichiers** pour remédier à leur cloisonnement. Des interconnexions devraient, par exemple, être mises en œuvre entre les fichiers SIS II, FPR et FAED, pour intégrer les empreintes digitales des personnes signalées, et entre TES et FOVeS pour permettre l'alimentation automatique de ce dernier par les numéros des documents d'identité volés. Ces évolutions sont nécessaires pour respecter les obligations de la réglementation Schengen. De manière plus générale, les rapporteurs souhaitent **la mise en œuvre d'une interface permettant l'accès simultané aux différents fichiers** qu'un agent peut consulter. Une telle solution permettrait des gains de temps significatifs dans le cadre des enquêtes judiciaires et éviterait que la consultation de certains fichiers soit oubliée. La possibilité que cette interface permette également à un agent d'être alerté sur l'inscription d'une personne dans d'autres fichiers, auxquels il n'a pas accès, devrait également être étudiée.

Des évolutions sont également souhaitables afin d'élargir le champ des données auxquelles **les services de renseignement spécialisés** ont accès, notamment dans le cadre de leurs missions de prévention du terrorisme. Ces services devraient ainsi être autorisés à consulter les fichiers de prévention des atteintes à la sécurité publique PASP et GIPASP, la partie « victimes » du TAJ et le fichier national des personnes incarcérées.

Enfin, la multiplication des **enquêtes administratives,** menées pour autoriser l'accès à certains emplois ou à des lieux sensibles, et qui s'appuient sur la consultation de plusieurs fichiers, doit conduire à une réorganisation des acteurs chargés de ces enquêtes. Le service national des enquêtes administratives de sécurité (SNEAS), créé en 2017, a été chargé de certaines de ces enquêtes, pour lesquelles il dispose d'une application spécifique, ACCReD, permettant la consultation simultanée de plusieurs fichiers. Les rapporteurs proposent que ce service se voie confier un champ plus large d'enquêtes relevant actuellement des services de police et des unités de gendarmerie.

TRAVAUX DE LA COMMISSION

Lors de sa réunion du mercredi 17 octobre 2018, la commission des Lois a examiné ce rapport d'information et en a autorisé la publication [(1)].

(1) Ces débats font l'objet d'un compte-rendu audiovisuel et sont accessibles sur le portail vidéo du site de l'Assemblée à l'adresse suivante : http://videos.assemblee-nationale.fr/video.6758787_5bc7454187f56.commission-des-lois--fichiers-mis-a-la-disposition-des-forces-de-securite-rapport-de-la-mission-d--17-octobre-2018

LISTE DES PROPOSITIONS

Proposition n° 1 : Mieux associer les services de la CNIL en amont du dépôt officiel des demandes d'avis sur les actes réglementaires de création des fichiers, de façon à résoudre les difficultés juridiques ou techniques susceptibles de se poser.

Proposition n° 2 : Supprimer l'authentification par identifiants et mots de passe, et généraliser l'authentification par la carte professionnelle.

Proposition n° 3 : Développer, notamment par des procédés algorithmiques, l'analyse massive des données recueillies grâce à la traçabilité pour détecter plus largement les comportements irréguliers d'utilisation des fichiers.

Proposition n° 4 : Mener, au sein du ministère de l'intérieur, une réflexion globale sur la rationalisation des fichiers existants, s'appuyant sur une analyse de leur finalité et de leur utilisation par les forces de sécurité.

Proposition n° 5 : Publier dans les plus brefs délais un décret prévoyant une modulation de la durée de conservation des données enregistrées dans le FNAEG au regard de la nature et de la gravité de l'infraction en cause tout en tenant compte des spécificités de la délinquance des mineurs.

Proposition n° 6 : Légiférer dans de brefs délais sur les conditions d'effacement des données enregistrées dans le FNAEG pour les personnes condamnées.

Proposition n° 7 : Accentuer l'informatisation des parquets et les doter de moyens suffisants.

Proposition n° 8 : Rappeler aux parquets, par la voie d'une circulaire, la faculté offerte par l'article 230-8 du code de procédure de pénale d'ordonner l'inscription d'une mention au TAJ.

Proposition n° 9 : Généraliser dans de brefs délais l'interconnexion de CASSIOPEE vers TAJ, en remplacement des fiches-navettes, actuellement expérimentée dans sept juridictions.

Proposition n° 10 : Relier le TAJ, le FAED et le FNAEG par une base-pivot, ou créer un identifiant commun (lié à un numéro d'empreinte digitale) à ces différentes applications, afin de garantir la cohérence des informations entre les fichiers et de fiabiliser les identités des personnes mises en cause.

Proposition n° 11 : Autoriser l'accès des services de renseignement spécialisés :

– aux fichiers « Prévention des atteintes à la sécurité publique » (PASP) et « Gestion de l'information et prévention des atteintes à la sécurité publique » (GIPASP) ;

– à la partie « victimes » du TAJ.

Proposition n° 12 : Autoriser l'accès de la DGSI au fichier national des personnes incarcérées.

Proposition n° 13 : Développer les interconnexions entre fichiers et étudier en particulier la possibilité d'interconnexions :

– entre les traitements SIS, FPR et FAED pour se conformer aux obligations du règlement Schengen ;

– entre les logiciels de rédaction des procédures LRPPN et LRGGN et le système d'immatriculation des véhicules pour permettre l'alimentation automatisée de la partie « véhicules » du FOVeS.

Proposition n° 14 : Mettre en œuvre une interconnexion entre le TAJ et le casier judiciaire national pour permettre l'inscription dans le TAJ des condamnations pénales.

À défaut d'une telle interconnexion, autoriser l'accès des policiers et des gendarmes ainsi que des agents des services chargés des enquêtes administratives au bulletin n° 1 du casier judiciaire.

Proposition n° 15 :

– Mettre en œuvre une interface entre les différents fichiers auxquels un agent a accès, permettant leur consultation simultanée à partir de la saisie d'une identité ou d'un identifiant technique ;

– Étudier la possibilité de mettre en œuvre, dans le cadre de cette interface, un système d'alerte de présence, indiquant uniquement si une personne est inscrite au sein d'autres fichiers auxquels l'agent n'a pas accès.

Proposition n° 16 : Faire ressortir visuellement sur la fiche S, de manière immédiate, la « conduite à tenir » face à la personne contrôlée.

Proposition n° 17 : Donner accès au FSPRT aux procureurs de la République.

Proposition n° 18 : Confier au service national des enquêtes administratives de sécurité (SNEAS) un champ plus large d'enquêtes administratives relevant actuellement des services de police et des unités de gendarmerie.

Proposition n° 19 : Prévoir, s'agissant du fichier TAJ, une mise en œuvre effective du droit à l'information des personnes au moment de leur inscription dans le fichier, incluant notamment la communication d'informations sur la durée de conservation des données, leur utilisation possible dans le cadre d'enquêtes administratives ainsi que sur les possibilités de demander leur effacement anticipé.

Proposition n° 20 : Interconnecter le fichier TES et le fichier FOVeS afin d'alimenter automatiquement le SIS II par les numéros des documents volés.

Proposition n° 21 : Généraliser à l'ensemble des États membres de l'Union européenne la transmission automatisée des antécédents judiciaires à partir des bases de données nationales (projet ADEP), si les résultats de l'expérimentation de cette transmission sont concluants.

ANNEXE N° 1 :
LISTE DES PERSONNES ENTENDUES PAR LES RAPPORTEURS [(1)]

- **Inspection générale de la police nationale (IGPN)**
  - — Mme Marie-France Monéger-Guyomarc'h, directrice
- **Commission nationale de l'informatique et des libertés (CNIL)**
  - — M. Paul Hébert, directeur-adjoint à la direction de la conformité
  - — Mme Émilie Seruga-Cau, chef du service des affaires régaliennes et des collectivités territoriales
  - — Mme Tiphaine Havel, conseillère pour les questions institutionnelles et parlementaires
- **Direction centrale de la sécurité publique au ministère de l'Intérieur**
  - — M. Pascal Lalle, directeur central
- **Inspection générale de la gendarmerie nationale (IGGN)**
  - — Général Michel Labbé, chef
- **Direction des affaires criminelles et des grâces (DACG)**
  - — M. Rémy Heitz, directeur
  - — M. Éric Serfass, chef du service du casier judiciaire national
  - — Mme Caroline Gaudefroy, adjointe au chef du bureau de la législation pénale générale
  - — Mme Sabrina Palmier, magistrate au bureau de la police judiciaire
- **Direction générale de la police nationale (DGPN)**
  - — M. Éric Morvan, directeur général de la police nationale
  - — M. Laurent Monbrun, conseiller juridique
  - — M. Philippe Saunier, conseiller technologies de sécurité intérieure

(1) Les auditions sont présentées par ordre chronologique.

- **Service des technologies et des systèmes d'information de la sécurité intérieure (STSISI)**
  - — Général Bruno Poirier-Coutansais, chef de service
  - — M. Christophe Fichot, contrôleur général
  - — Général Alain Kerboull
- **Direction générale de la gendarmerie nationale (DGGN)**
  - — Général Richard Lizurey, directeur général
  - — Lieutenant-colonel Mark Evans, chef du département de la protection et de la gouvernance des données au sein de la mission du pilotage et de la performance de la gendarmerie nationale
  - — Mme Sandrine Guillon, conseillère juridique et judiciaire
- **Conférence nationale des procureurs de la République (CNPR)**
  - — Mme Marie-Madeleine Alliot, procureur de la République à Bordeaux
  - — Mme Emmanuelle Bochenek, procureur de la République à Cherbourg
- **Direction centrale de la police judiciaire)**
  - — Mme Mireille Ballestrazzi, directrice centrale
  - — M. Frédéric Trannoy, chef de la division des études et de la prospective
  - — M. Bernard Manzoni, adjoint au chef de la division nationale de la documentation criminelle et de la coordination de la police technique
- **Conseil de la fonction militaire de la gendarmerie (CFMG)**
  - — Major Philippe Antoni
  - — Adjudant-chef Samia Bakli
  - — Lieutenant-colonel Sébastien Baudoux
  - — Adjudant Raoul Burdet
  - — Major Emmanuel Franchet
  - — Maréchal des logis chef Frédéric Le Louette
  - — Adjudant-chef Laurent Lemeilleur
  - — Adjudant-chef Erick Verfaillie
  - — Chef d'escadron Frédéric Colard
  - — Adjudant-chef Régis Poulet
  - — Gendarme Stéphane Gautier
  - — Lieutenant-colonel Mark Evans
  - — Capitaine Fabien Lacombe

- **Conseil national des activités privées et de sécurité (CNAPS)**
  - — M. Jean-Paul Celet, directeur
  - — M. Pierre-Frédéric Bertaux, directeur de cabinet
  - — Mme Margaux Monnoyeur, conseillère juridique
- **M. Ange Mancini, ancien coordonnateur national du renseignement**
- **Direction générale de la sécurité intérieure (DGSI)**
  - — M. Laurent Nuñez, directeur général
  - — Mme Carine Henry, chef de cabinet
  - — M. Maxime Feghouli, chargé de la mission juridique
- **M. Jean-Marc Manach, journaliste**
- **Groupe de travail « Les exégètes amateurs »**
  - — M. Alexis Fitzjean O Cobhthaigh, avocat
  - — Mme Alicia Bruley, juriste
- **Table ronde de syndicats d'officiers de police**

  Synergie Officiers
  - — M. David Alberto, conseiller technique
  - — M. Anthony Lope, conseiller technique

  Syndicat des cadres de la sécurité intérieure
  - — M. Guillaume Ryckewaert, délégué national
  - — M. Christophe Rouget, secrétaire national
  - — Mme Sabrina Rigolle, secrétaire nationale
- **Table ronde des syndicats de gradés et gardiens de la paix de la police**

  Unité SGP Police
  - — M. Franck Fievez, secrétaire national
  - — M. Christophe Pichenot, délégué syndical

  UNSA POLICE
  - — M. Thierry Clair, secrétaire national
  - — M. Stéphane Immery, délégué pôle préfecture de police
  - — M. Thomas Toussaint, délégué national pôle CRS

Alliance Police nationale

— M. Stanislas Gaudon, secrétaire administratif général adjoint

— M. David Olivier Reverdy, conseiller technique investigation

- **M. Paul Michel, ancien magistrat chargé du contrôle des fichiers de police judiciaire, et Mme Blandine Devallois, greffière**

- **Table ronde d'avocats**

Conseil national des barreaux

— Mme Sophie Ferry-Bouillon, membre de la commission « Libertés et droits de l'homme »

— M. Étienne Papin, avocat

Barreau de Paris

— M. Basile Ader, vice-bâtonnier

— M. Emmanuel Daoud, membre du Conseil de l'Ordre

Conférence des bâtonniers

— M. Stéphane Campana, membre

- **Syndicat indépendant des commissaires de police (SICP)**

— M. Olivier Boisteaux, président

— M. Jean-Paul Megret, secrétaire national

— M. Mickaël Trehen, secrétaire national

- **Syndicat des commissaires de la police nationale (SCPN)**

— M. David Le Bars, secrétaire général

— M. Pierrick Agostini, secrétaire général adjoint

- **Ministère de l'Intérieur**

— M. Thomas Campeaux, directeur des libertés publiques et des affaires juridiques

— M. Fabrice Mattatia, délégué à la protection des données

- **Commission nationale de contrôle des techniques de renseignement (CNTCR)**

— M. Francis Delon, président

— M. Patrick Puges, membre

— M. Samuel Manivel, conseiller auprès du président

— Mme Céline Gay, chargée de mission

ANNEXE N° 2 :
LISTE DES DÉPLACEMENTS EFFECTUÉS PAR LES RAPPORTEURS

- **Service Central de Renseignement Criminel (SCRC) de Pontoise (13 septembre 2018)**
  - — Général de Brigade Patrick Touron, commandant du Pôle Judiciaire de la gendarmerie nationale (PJGN)
  - — Colonel Jérôme Servettaz, chef du Service central de renseignement criminel
  - — Colonel Joël Dromard, chef de la division des fichiers du SCRC
  - — Lieutenant-colonel Frédérick Rehault, adjoint au chef de la division des fichiers
  - — Capitaine Catherine Anguille-Blanc, cheffe du département des fichiers de recherches
  - — Capitaine Christophe Larousse, chef du département du fichier d'antécédents judiciaires
  - — Adjudant-chef Sandrine Hameau, cheffe du département du droit d'accès indirect
  - — Lieutenant-colonel Mark Evans, chef du département de la protection et de la gouvernance des données
  - — Capitaine Marie Morellec, bureau de la police judiciaire
- **Préfecture de police de Paris (13 septembre 2018)**
  - — M. Jérôme Guerreau, chef de cabinet du Préfet de Police
  - — M. Étienne Genet, secrétaire général pour l'administration à la préfecture de police
  - — M. Philippe Dalbavie, conseiller juridique auprès du préfet de police
  - — M. Jérôme Mazzariol, commissaire de police, conseiller adjoint au cabinet du préfet de police
  - — M. Denis Cottin, correspondant délégué à la protection des données
  - — M. Frédéric Dupuch, directeur de la sécurité de proximité de l'agglomération parisienne
  - — M. Thierry Huguet, chef d'état-major à la direction régionale de la police judiciaire de Paris
  - — Mme Françoise Bilancini, contrôleuse générale, directrice du renseignement

— Mme Anne-Sophie Briec-Brugat, commissaire divisionnaire, cheffe d'état-major de la direction du renseignement

— M. Éric Belleut, directeur adjoint de l'ordre public et de la circulation (DOPC)

— M. Jean-Claude Corneau, responsable de la sécurité des systèmes d'information (DOPC)

- **Unité de coordination de la lutte antiterroriste (UCLAT) (13 septembre 2018)**

  — M. Yves Joannesse, commissaire divisionnaire, chef adjoint de l'UCLAT

  — Mme Monique Boudet, commissaire de police (UCLAT)

  — M. Laurent Monbrun, conseiller juridique auprès du DGPN

  — Mme Marie-Paule Repaire, conseiller juridique auprès du DGPN

- **Cour d'Appel de Lyon (14 septembre 2018)**

  — Mme Sylvie Moisson, procureure générale près la Cour d'Appel de Lyon, chargée du contrôle des fichiers FAED et FNAEG

- **Tribunal de grande instance de Lyon (14 septembre 2018)**

  — M. Marc Cimamonti, procureur de la République

  — M. Bernard Reynaud, procureur adjoint, chef de la division de l'action publique spécialisée

  — Mme Audrey Quey, vice-procureure, secrétaire générale du parquet

  — Mme Hélène Moreau, vice-procureure, magistrat à la section de l'exécution des peines (plus spécialement en charge du contrôle des fichiers de police judiciaire)

- **Service central de la police technique et scientifique (SCPTS) d'Écully (14 septembre 2018)**

  — M. Éric Angelino, inspecteur général, chef du service central de la police technique et scientifique

  — Mme Marie Gallais, commandant divisionnaire

  — Mme Sylvie Lassale, technicienne en chef de police technique et scientifique (FAED)

  — M. Alexandre Bedel, technicien principal de police technique et scientifique (FAED)

  — M. Tsara Couvert, agent spécialisé de police technique et scientifique (FAED)

  — Mme Claudie Nerbollier, commandant

— Mme Lindsay Legeay, agent spécialisé de police technique et scientifique (FNAEG)

— Mme Estelle Davet, commissaire divisionnaire, cheffe de la division nationale de la documentation criminelle et de la coordination de la police technique (DND2CPT)

— M. Bernard Manzoni, commissaire divisionnaire, adjoint à la cheffe de la division nationale de la documentation criminelle et de la coordination de la police technique

— Mme Jennifer Deseigne, commissaire de police, cheffe du service des systèmes nationaux d'information criminelle

— M. Jean-Jacques Soboul, commandant divisionnaire fonctionnel, adjoint à la cheffe du service des systèmes nationaux d'information criminelle

— M. Xavier Bitaud, capitaine, chef de la cellule d'administration fonctionnelle unique TAJ

— Mme Stéphanie Beguet, capitaine, adjointe au chef du groupe objectif et recherche des personnes

— Mme Murielle Durochat, commandant, cheffe du groupe juridique

— Mme Nathalie Millard, commandant, cheffe de la section du traitement des droits d'accès et du contentieux

ANNEXE N° 3 :
GLOSSAIRE

A

ACCReD : Automatisation de la consultation centralisée de renseignements et de données
AGDREF : Application de gestion des dossiers des ressortissants étrangers en France
AGRIPPA : Application de gestion du répertoire informatisé des propriétaires et possesseurs d'armes

B

BDSP : Base de données de sécurité publique
BNDP : Base nationale de données patrimoniales

C

CASSIOPEE : Chaîne applicative supportant le système d'information orienté procédure pénale et enfants
CJN : Casier judiciaire national
CNIL : Commission nationale de l'informatique et des libertés
CNCTR : Commission nationale de contrôle des techniques de renseignement
COSSEN : Commandement spécialisé pour la sécurité nucléaire
COVADIS : Fichier de contrôle et vérification automatique des documents d'identité sécurisés
CRISTINA : Centralisation du renseignement intérieur pour la sécurité du territoire et les intérêts nationaux

D

DCPJ : Direction centrale de la police judiciaire
DCSP : Direction centrale de la sécurité publique
DGPN : Direction générale de la police nationale
DGGN : Direction générale de la gendarmerie nationale
DGSI : Direction générale de la sécurité intérieure
DLPAJ : Direction des libertés publiques et des affaires juridiques
DACG : Direction des affaires criminelles et des grâces
DOCVERIF : Fichier de contrôle de la validité des documents (carte nationale d'identité et passeports) émis par les autorités françaises

E

EASP : Fichier des enquêtes administratives liées à la sécurité publique
EURODAC : Système de comparaison des empreintes digitales des demandeurs d'asile et de plusieurs catégories d'immigrants clandestins

F

FAED : Fichier automatisé des empreintes digitales
FBS : Fichier des brigades spécialisées
FICOBA : Fichier national des comptes bancaires
FICOVIE : Fichier des contrats de capitalisation et d'assurance-vie
FIJAIS : Fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes
FIJAIT : Fichier judiciaire national automatisé des auteurs d'infractions terroristes
FINIADA : Fichier national des interdits d'acquisition et de détention d'armes
FNAEG : Fichier national automatisé des empreintes génétiques
FNFM : Fichier national du faux monnayage
FNPC : Fichier national des permis de conduire
FNPI : Fichier national des personnes incarcérées
FOVeS : Fichier des objets et des véhicules signalés
FPR : Fichier des personnes recherchées
FSPRT : Fichier de traitement des signalements pour la prévention de la radicalisation à caractère terroriste

G

GASPARD-NG : Gestion automatisée des signalements et des photographies anthropométriques répertoriées et distribuables (Nouvelle génération)
GESTEREXT : Gestion du terrorisme et des extrémismes violents
GIPASP : Gestion de l'information et prévention des atteintes à la sécurité publique

I

IGGN : Inspection générale de la gendarmerie nationale
IGPN : Inspection générale de la police nationale

L

LRPGN : Logiciel de rédaction des procédures de la gendarmerie nationale
LRPPN : Logiciel de rédaction des procédures de la police nationale

P

PARAFE : Traitement du passage automatisé rapide des frontières extérieures
PASP : Prévention des atteintes à la sécurité publique
PNR : *Passenger Name Recorder* (enregistrement des passagers aériens)

R

REDEX : Répertoire des expertises
RMV : Réseau mondial visas
RNCPS : Répertoire national commun de la protection sociale

S

SALVAC : Système d'analyse des liens de la violence associée aux crimes
SCPPB : Service central de préservation des prélèvements biologiques
SCRT : Service central du renseignement territorial
SETRADER : Système européen de traitement des données d'enregistrement et de réservation
SIRENE : Supplément d'information requis à l'entrée nationale
SIS : Système d'information Schengen
SIV : Système d'immatriculation des véhicules
SNEAS : Service national des enquêtes administratives de sécurité
SRDC : Service régional de documentation criminelle
STIC : Système de traitement des infractions constatées
ST(SI)^2 : Service des technologies et des systèmes d'information de la sécurité intérieure

T

TAJ : Traitement des antécédents judiciaires
TES : Fichier des titres électroniques sécurisés

U

UCLAT : Unité de coordination de la lutte antiterroriste

V

VISABIO/VIS : Système d'information sur les visas

ANNEXE N° 4 :
TABLEAU DES FICHIERS MIS À LA DISPOSITION DES FORCES DE SÉCURITÉ

Nom des fichiers	Gestionnaire du fichier	Fondement juridique	Finalités
ACCRED (automatisation de la consultation centralisée de renseignements et de données)	DGPN-DGGN	Décret n° 2017-1224 du 3 août 2017	Faciliter la conduite des enquêtes administratives réalisées en application des articles L. 114-1, L. 114-2 et L. 211-11-1 du code de la sécurité intérieure et exploiter les informations recueillies dans ce cadre
ADOC (accès au dossier des contraventions)	Ministère de l'intérieur	Arrêté du 13 octobre 2004 portant création du système de contrôle automatisé	Constater, au moyen d'appareils de contrôle automatique homologués, les infractions à la réglementation sur les vitesses maximales autorisées, sur le respect des distances de sécurité entre les véhicules, sur l'usage des voies et chaussées réservées à certaines catégories de véhicules et sur les signalisations imposant l'arrêt des véhicules ; Procéder à l'enregistrement et à la conservation des données recueillies par l'agent verbalisateur au moyen d'appareils électroniques à l'occasion de la constatation des contraventions des quatre premières classes liées à la circulation routière ; Gérer les opérations relatives à l'identification des conducteurs de véhicule, auteurs d'infractions visées ; Gérer les opérations nécessaires au traitement des infractions visées en vue de la notification des avis de contravention ; Gérer les réponses des contrevenants aux avis de contravention qui leur sont notifiés ; Faciliter la gestion du paiement des consignations, le recouvrement des amendes et le remboursement des consignations par les services compétents ; Faciliter l'établissement des retraits de points par le service chargé de la gestion du système national des permis

Nom des fichiers	Gestionnaire du fichier	Fondement juridique	Finalités
			de conduire ; Assurer la transmission des dossiers relatifs aux infractions visées au 1° et au 2° aux tribunaux et autorités judiciaires compétents ; Gérer le parc des appareils électroniques d'enregistrement
AGDREF (application de gestion des dossiers des ressortissants étrangers en France)	Ministère de l'intérieur	Articles R 611-1 et s. du CESEDA Décret du 18 février 2013 Décret du 08 juin 2011	Garantir le droit au séjour des ressortissants étrangers en situation régulière et lutter contre l'entrée et le séjour irréguliers en France des ressortissants étrangers
AGRIPPA (application de gestion du répertoire informatisé des propriétaires et possesseurs d'armes)	Ministère de l'intérieur	Arrêté du 15 novembre 2007 portant création de l'application de gestion du répertoire informatisé des propriétaires et possesseurs d'armes	Enregistrer et suivre les autorisations et récépissés de déclarations et d'enregistrements délivrés par l'autorité administrative relatifs au régime des matériels de guerre, armes et de leurs éléments ainsi que des munitions des catégories A et B et des armes et éléments d'arme de la catégorie C et du 1° de la catégorie D
ANACRIM ATRT (logiciel d'analyse criminelle ANACRIM Application de traitement des relations transactionnelles)	DGGN/DGPN	Décret n° 2012-687 du 7 mai 2012 relatif à la mise en œuvre de logiciels de rapprochement judiciaire à des fins d'analyse criminelle	Exploiter et rapprocher les informations sur les modes opératoires réunis au cours d'une même enquête par les unités de gendarmerie et les services de police chargés d'une mission de police judiciaire dans le cadre : 1° Des enquêtes de flagrance ou des enquêtes préliminaires et des investigations exécutées sur commission rogatoire relatives à des crimes et délits punis d'une peine d'emprisonnement ; 2° Des procédures de recherche des causes de la mort ou d'une disparition prévues par les articles 74 et 74-1 du code de procédure pénale
Analyst notebook	DGPN (DCPJ)	Engagement de conformité du 13 mars 2014 au décret du 7 mai 2012 autorisant les logiciels de rapprochement judiciaire	Logiciel de représentation graphique pour l'exploitation et le rapprochement d'informations sur les modes opératoires réunies au cours d'une même enquête
API-PNR France	Ministères chargés de l'économie, de la défense et des transports	Articles L. 232-7 et R. 232-12 et suivants du CSI	Recueil et traitement des données commerciales de réservation et d'embarquement des passagers aériens des vols entrants et sortants de France (vols DOM-COM compris)
Appels à témoins	DGPN-DGGN-PP	Arrêté cadre du 22 août 2012	Enregistrement et exploitation des communications

Nom des fichiers	Gestionnaire du fichier	Fondement juridique	Finalités
			reçues dans le cadre de procédures d'appel à témoins ouvertes par les services de la police et les unités de la gendarmerie nationales
ASPC (application de stockage des procédures clôturées)	DGGN	Projet de décret	Transmettre aux magistrats et archiver les procédures rédigées par leurs services et unités
Assignation à résidence	DGPN-DGGN PP	Arrêté cadre du 22 août 2012 autorisant la création de traitements de données à caractère personnel dénommés « assignation à résidence »	Assurer le suivi des dossiers des personnes qui, dans le cadre d'une mesure d'assignation à résidence prononcée par le JLD ou par arrêté préfectoral, doivent périodiquement se signaler aux autorités responsables du traitement
ATRC (application de traitement de renseignement criminel)	DGGN/DGPN	Décret n° 2014-187 du 20 février 2014 relatif à la mise en œuvre de traitements de diffusion de l'information opérationnelle au sein des services et unités de la police et de la gendarmerie nationales	Faciliter la diffusion et le partage d'informations opérationnelles détenues par les différents services ou de la police et de la gendarmerie nationale investis de missions de police judiciaire, sur les enquêtes en cours ou les personnes qui en font l'objet ainsi que l'activité judiciaire de ces services ou unités
BABCO (base atteintes aux biens et criminalité organisée)	DGGN	Décret n° 2013-1054 du 22 novembre 2013 relatif aux traitements automatisés de données à caractère personnel dénommés « bases d'analyse sérielle de police judiciaire »	Identifier les auteurs, co-auteurs ou complices de faits sériels nationaux et transfrontaliers pour toutes les infractions sérielles afférentes aux atteintes aux biens (VAMA, vols quelle que soit la nature du butin, cambriolages, recels en tout genre) punies d'une peine d'emprisonnement d'au moins 5 ans
BAM (base anti-mafia)	DGGN	Décret n° 2013-1054 du 22 novembre 2013 relatif aux traitements automatisés de données à caractère personnel dénommés « bases d'analyse sérielle de police judiciaire »	Identifier les auteurs, co-auteurs ou complices de faits sériels régionaux et transfrontaliers pour toutes les infractions afférentes aux phénomènes mafieux et de criminalité organisée au sein de la RGPACA punies d'une peine d'emprisonnement d'au moins 5 ans
Base de l'OCLDI (office central de lutte contre la délinquance itinérante)	DGGN	Décret n° 2013-1054 du 22 novembre 2013 relatif aux traitements automatisés de données à caractère personnel dénommés « bases d'analyse sérielle de police judiciaire »	Analyser, exploiter et transmettre toute documentation relative aux faits et infractions liés à la délinquance itinérante et punis d'une peine d'emprisonnement d'au moins 5 ans
Base escroqueries	DGGN	Décret n° 2013-1054 du 22 novembre 2013 relatif aux traitements automatisés de données à	Identifier les auteurs, co-auteurs ou complices de faits sériels nationaux et transfrontaliers pour toutes

Nom des fichiers	Gestionnaire du fichier	Fondement juridique	Finalités
		caractère personnel dénommés « bases d'analyse sérielle de police judiciaire »	les infractions sérielles afférentes aux escroqueries en tout genre punies d'une peine d'emprisonnement d'au moins 5 ans
Base Harpie (base Harpie du COMGEND Guyane)	DGGN	Décret n° 2013-1054 du 22 novembre 2013 relatif aux traitements automatisés de données à caractère personnel dénommés « bases d'analyse sérielle de police judiciaire »	lutte contre l'orpaillage illégal, infractions relatives à des exploitations minières illicites susceptibles de causer des dommages écologiques sévères punies d'une peine d'emprisonnement d'au moins 5 ans
Base satellite VV	DGPN (DCPJ)	Arrêté du 10 décembre 2008	Accéder aux informations relatives à l'état de vol et de mise sous surveillance d'un véhicule afin : — d'informer les agents des autorités administratives mentionnées au troisième alinéa de l'article 3, pour les besoins exclusifs de leurs missions, de l'état de vol d'un véhicule ; — d'informer les services de police et de gendarmerie nationales compétents de la nature des opérations d'immatriculation effectuées sur un véhicule surveillé
Bases d'analyse sérielle de police judiciaire	DGPN-PP DGGN	Articles 230-12 et suivants du CPP - Décret cadre n° 2013-1054 du 22 novembre 2013 relatif aux traitements automatisés de données à caractère personnel dénommés « bases d'analyse sérielle de police judiciaire »	Rassemblement de preuves et identification des auteurs des crimes ou délits présentant un caractère sériel, grâce à l'établissement de liens entre les individus, les événements ou les infractions
CALIOPE (base de comparaison et analyse logicielles des images d'origine pédopornographiques)	DGGN	Décret n° 2013-1054 du 22 novembre 2013 relatif aux traitements automatisés de données à caractère personnel dénommés « bases d'analyse sérielle de police judiciaire »	Trier et rapprocher les éléments relatifs à l'exploitation sexuelle de mineurs, fournir des contenus illicites utilisés lors des actions de « cyberpatrouille »
Caméra piéton	Services de la DGPN, de la DGGN et de la PP	Acte cadre – Art. L. 241-1 et R. 241-1 et suivants du CSI	Prévention des incidents au cours des interventions des agents de la police nationale et des militaires de la gendarmerie nationale ; constat des infractions et poursuite de leurs auteurs par la collecte de preuves ; formation et pédagogie des agents
CHEOPS / PASSAGE	DGPN	Arrêté du 19 octobre 2001	Portail d'accès aux traitements réglementaires du ministère de l'intérieur et gestion sécurisée des habilitations
Contrôle judiciaire	DGPN	Arrêté cadre du 22 août 2012 autorisant la	Assurer le suivi des personnes soumises à des

Nom des fichiers	Gestionnaire du fichier	Fondement juridique	Finalités
	PP	création de traitements de données à caractère personnel dénommés « contrôle judiciaire »	obligations de contrôle judiciaire qui, en exécution d'une ordonnance d'un magistrat, doivent se présenter périodiquement aux autorités
CORAIL (cellule opérationnelle de rapprochement et d'analyse des infractions liées)	Préfecture de police de Paris		Rapprochement d'informations sur les modes opératoires des infractions aux fins d'identification de leurs auteurs
CRISTINA	DGSI	Décret non publié	
Diffusion de l'information opérationnelle au sein des services de police ou unités de gendarmerie	DGPN-DGGN-PP	Décret cadre n° 2014-187 du 20 février 2014 relatif à la mise en œuvre de traitements de diffusion de l'information opérationnelle au sein des services et unités de la police et de la gendarmerie	Diffusion et partage d'informations opérationnelles détenues par les différents services ou unités de la police et de la gendarmerie nationales investis de missions de police judiciaire, sur les enquêtes en cours ou les personnes qui en font l'objet ainsi que l'activité judiciaire de ces services ou unités
DOCVERIF	Ministère de l'intérieur	Arrêté ministériel du 10 août 2016 autorisant la création d'un traitement automatisé de données à caractère personnel dénommé « DOCVERIF »	Faciliter le contrôle de la validité des documents émis par les autorités françaises et de lutter contre l'utilisation indue de tels documents, leur falsification ou leur contrefaçon
EASP	DGPN (DCSP)	Articles R. 236-1 à R. 236-10 du code de la sécurité intérieure	Faciliter la réalisation des enquêtes administratives pour la conservation des données issues de précédentes enquêtes relatives à la même personne
F2CO (fichier central de la criminalité organisée)	DGPN (DCPJ)	Décret en cours d'élaboration	Recueil, centralisation et partage de données et informations relatives à des personnes participant ou susceptibles d'être impliquées directement ou indirectement dans une entreprise criminelle relevant de la délinquance ou de la criminalité organisées
FAED (fichier automatisé des empreintes digitales)	DGPN (SCPTS)	Décret n° 87-249 du 8 avril 1987	Centralisation des traces relevées sur les scènes d'infractions punies d'une peine d'emprisonnement et des empreintes digitales et palmaires d'individus mis en cause dans le cadre d'un crime ou d'un délit afin de faciliter la recherche et l'identification des auteurs d'infractions - permettre l'identification des personnes disparues, décédées ou découvertes grièvement blessées - permettre l'identification d'un étranger ou d'une personne dans le cadre d'une vérification d'identité

Nom des fichiers	Gestionnaire du fichier	Fondement juridique	Finalités
FCJ (fichier des courses et jeux)	DGPN (DCPJ)	Arrêté du 8 novembre 2010	Assurer la surveillance de la régularité et de la sincérité des jeux, des courses et des paris
FIJAIS (fichier judiciaire national automatisé des auteurs d'infractions sexuelles)	Ministère de la justice	Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité	Prévenir le renouvellement des infractions mentionnées à l'art. 706-25-4 du CPP et faciliter l'identification de leurs auteurs (art. 706-25-3 CPP)
FIJAIT (fichier judiciaire national automatisé des auteurs d'infractions terroristes)	Ministère de la justice	Loi n° 2015-912 du 24 juillet 2015 relative au renseignement Décret n° 2015-1840 du 29 décembre 2015 modifiant le code de procédure pénale et relatif au FIJAIT	Prévenir le renouvellement des infractions mentionnées à l'art. 706-25-4 du CPP et faciliter l'identification de leurs auteurs (art. 706-25-3 CPP)
FIMPAT (fichier des mesures de police administrative destinées à prévenir les actes liés au terrorisme)	DGPN	Arrêté du 7 août 2017	Centraliser la gestion et le suivi des propositions des mesures de police administrative, faciliter leur mise en œuvre en réunissant les éléments de motivation, émanant des services chargés de la prévention ou de la répression du terrorisme, destinées à prévenir et à lutter contre les actes liés au terrorisme
FNAEG (fichier national automatisé des empreintes génétiques)	DGPN (SCPTS)	Articles 706-55 et suivants et R 53-9 et suivants du CPP	Centralisation des traces relevées sur les scènes d'infractions définies à l'article 706-55 du CPP et les personnes mises en cause pour ces mêmes infractions afin de faciliter la recherche des auteurs d'infractions et l'identification des personnes disparues ou décédées
FNFM (fichier national du faux monnayage)	DGPN (DCPJ)	Règlement (CE) n° 1338/2001	Centraliser l'ensemble des procédures judiciaires en matière de faux monnayage et opérer des rapprochements
FNIS (fichier national des personnes interdites de stade)	DGPN (DCSP)	Arrêté du 28 août 2007	Prévenir et lutter contre les violences lors de manifestations sportives notamment en garantissant la pleine exécution des mesures d'interdictions administratives et judiciaires de stade
FNOS (fichier national des objectifs en matière de stupéfiants)	DGPN (DCPJ)-DGGN-DGDDI	Arrêté du 11 juillet 2012	Coordonner l'action des services concourant à la répression du trafic de stupéfiants en répertoriant les personnes faisant l'objet d'investigations judiciaires ou douanières dans ce domaine
FNPI (fichier national automatisé des personnes incarcérées)	Ministère de la justice	Arrêté du 20 février 2003	Gérer les affectations pénitentiaires des détenus ainsi que la production de statistiques sur la population pénale

Nom des fichiers	Gestionnaire du fichier	Fondement juridique	Finalités
FOJ (fichier des objectifs judiciaires)	DGPN DGGN PP	Arrêté cadre du 5 mai 2017	Répertorier les personnes faisant l'objet d'investigations dans le cadre d'une enquête judiciaire relative à certains crimes et délits
FOJAG (fichier des objectifs judiciaires aux Antilles Guyane)	DGPN (DCPJ)-DGGN	Engagement de conformité PN-GN à l'arrêté cadre FOJ du 5 mai 2017	Répertorier les personnes faisant l'objet d'investigations dans le cadre d'une enquête judiciaire relative à certains crimes et délits sur le territoire des Antilles Guyane
FOVeS (fichier des objets et des véhicules signalés)	DGPN (DCPJ)-DGGN	Arrêté du 7 juillet 2017	Faciliter les recherches et les contrôles de la police, de la gendarmerie et des douanes dans le cadre de leurs attributions respectives pour la découverte et la restitution des véhicules volés et objets perdus ou volés ainsi que la surveillance des véhicules et objets signalés
FPNID (fichier des personnes non identifiées ou disparues)	DGGN	Décret n° 2013-1054 du 22 novembre 2013 relatif aux traitements automatisés de données à caractère personnel dénommés « bases d'analyse sérielle de police judiciaire »	Retrouver et identifier les personnes disparues et les victimes lorsque celles-ci ont fait l'objet d'infractions à caractère sériel afférentes aux homicides, enlèvements, séquestrations, actes de tortures et de barbarie commis en tous lieux et punis d'une peine d'emprisonnement d'au moins 5 ans
FPR (fichier des personnes recherchées)	DGPN (DCPJ)	Décret n° 2010-569 du 28 mai 2010 modifié	Faciliter les recherches, les surveillances et les contrôles effectués par les services de la police nationale, les unités de la gendarmerie nationale et les agents des douanes exerçant des missions de police judiciaire ou de police administrative
FSPRT (fichier du traitement des signalements pour la prévention de la radicalisation à caractère terroriste)	DGPN-UCLAT	Décret du 5 mars 2015 modifié non publié	Recensement et centralisation des informations relatives aux personnes qui, engagées dans un processus de radicalisation, sont susceptibles de vouloir se rendre à l'étranger sur un théâtre d'opérations de groupements terroristes ou de vouloir prendre part à des activités à caractère terroriste, en vue de l'information des autorités compétentes et du suivi de ces personnes par les services de renseignement

Nom des fichiers	Gestionnaire du fichier	Fondement juridique	Finalités
GDEP (gestion du dépôt)	DGPN-DGGN-PP	Arrêté cadre du 4 février 2013	Gestion administrative des personnes déférées ou gardées à vue dans le but d'être présentées à un magistrat
GECI (gestion électronique des courriers internationaux)	DCPJ	Arrêté du 21 septembre 2017	Outil de traitement et de conservation des demandes et réponses de coopération émises et reçues par les services français compétents
GEDReT (gestion électronique des documents du renseignement territorial)	DCSP	Décret n° 2016-1045 du 29 juillet 2016 relatif à la mise en œuvre de traitements de conservation, de gestion et d'exploitation électroniques des documents des services du ministère de l'intérieur chargés des missions de renseignement territorial	Outil de gestion et de partage des notes de renseignement du Service Central de Renseignement Territorial
GEMFI (gestion des effectifs et des moyens des forces d'intervention)	FIPN	Déclaration simplifiée n°46 du 26 septembre 2012	Outil de gestion des effectifs et des moyens disponibles de la FIPN (force d'intervention de la Police Nationale)
GERRPOL	DCPJ	Décret en cours d'élaboration	Traiter et conserver les demandes d'arrestation provisoire actives émises par les autorités judiciaires françaises ou étrangères
GESTEL (gestion de l'éloignement)	DCPAF	Arrêté	Gestion des étrangers faisant l'objet d'une mesure d'éloignement
GESTEREXT (gestion du terrorisme et des extrémismes violents)	Préfecture de police de Paris	Décret non publié	
GIPASP (gestion de l'information et prévention des atteintes à la sécurité publique)	DGGN	Décret n° 2011-340 du 29 mars 2011 portant création d'un traitement de données à caractère personnel relatif à la gestion de l'information et la prévention des atteintes à la sécurité publique	Recueillir, conserver et analyser les informations qui concernent des personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique
GIPI (gestion informatisée des procédures d'immigration)	DGPN (DCPAF)	Arrêté du 14 février 2013	Faciliter la gestion des procédures de non-admission des étrangers qui ne remplissent pas les conditions d'entrée dans l'espace de libre circulation des personnes entre les États signataires de l'accord de Schengen et le suivi des amendes infligées aux entreprises de transport
GSI (gestion des sollicitations et des interventions)	DGGN	Décret n° 2013-696 du 30 juillet 2013 modifiant le décret n° 2011-341 du 29 mars 2011 portant création d'un traitement de données à caractère personnel intitulé « gestion	Apporter une réponse adaptée aux sollicitations des usagers notamment faites auprès d'un centre d'appel et d'assurer l'engagement des personnels et des moyens de la gendarmerie dans les meilleures

Nom des fichiers	Gestionnaire du fichier	Fondement juridique	Finalités
		des sollicitations et des interventions »	conditions d'efficacité
GTEAGAV (gestion technique des enregistrements audiovisuels de garde à vue)	DGPN	Arrêté du 11 décembre 2009	Gestion technique des enregistrements audiovisuels de garde à vue
Ibase	DGPN (DCPJ)	Engagement de conformité du 13 mars 2014 au décret du 7 mai 2012 autorisant les logiciels de rapprochements judiciaires	Logiciel de gestion des données permettant d'extraire des informations sur les modes opératoires réunies au cours d'une même enquête, de les recouper et les exploiter aux fins de rapprochement
iGAV	DGPN/DGGN	Décret du 26 octobre 2016	Rationaliser la gestion des gardes à vue et améliorer le contrôle hiérarchique en fiabilisant le suivi et la traçabilité du déroulement de chaque mesure
Interface de désanonymisation (IDPV)	DGPN-DGGN-DGDDI	Arrêté du 30 mars 2018	Permettre l'identification des agents PN,GN ou douanes anonymisés par un numéro d'immatriculation administrative dans les procédures judiciaires ou douanières
LAPI (lecture automatisée des plaques d'immatriculation)	DGPN DGGN DGDDI	Articles L. 233-1 et suivants du CSI - Arrêté cadre du 18 mai 2009	Mise en œuvre par la PN,GN et services des douanes de dispositifs de lecture automatisée de plaques d'immatriculation de véhicules afin de déterminer par consultation du FOVeS et du SIS s'ils sont volés ou surveillés. Déploiement autorisé en matière de lutte contre le terrorisme, la criminalité organisée, le vol et de recel de véhicules volés, d'infractions de contrebande, d'importation ou d'exportation commises en bande organisée de ces mêmes infractions, de réalisation ou de tentative de réalisation des opérations financières afin de permettre le rassemblement des preuves de ces infractions et la recherche de leurs auteurs ainsi qu' à titre temporaire, pour la préservation de l'ordre public, à l'occasion d'événements particuliers ou de grands rassemblements de personnes, par décision de l'autorité administrative
Logiciels de rapprochements judiciaires à des fins d'analyse criminelle	DGPN-DGGN-PP	Articles 230-20 et suivants du CPP - Décret cadre n° 2012-687 du 7 mai 2012	Permettre l'exploitation et le rapprochement d'informations sur les modes opératoires réunis au cours d'une même enquête par les unités de gendarmerie et les services de police chargés d'une

Nom des fichiers	Gestionnaire du fichier	Fondement juridique	Finalités
			mission de police judiciaire dans le cadre leurs enquêtes
LOGICRA (logiciel de gestion individualisée des centres de rétention administrative)	DCPAF	Arrêté du 6 mars 2018	Outil de gestion informatique quotidienne de la rétention administrative et de suivi statistique des mesures
LRPGN (logiciel de rédaction des procédures de la gendarmerie nationale)	DGGN	Décret n° 2011-111 du 27 janvier 2011 autorisant la mise en œuvre par le ministère de l'intérieur (direction générale de la gendarmerie nationale) d'un traitement automatisé de données à caractère personnel d'aide à la rédaction des procédures (LRPGN)	Permettre aux unités de gendarmerie, dans l'exercice de leurs missions de police judiciaire et de police administrative, d'assurer la clarté et l'homogénéité de la rédaction des procédures judiciaires et administratives
LRPPN (logiciel de rédaction de procédures de la PN)	DGPN (DCPJ)	Décret n° 2011-110 du 27 janvier 2011 modifié	Rédaction de procédures judiciaires et administratives de la PN
LUPIN (logiciel d'uniformisation des procédures d'identification)	DGGN/DGPN	Arrêté du 15 octobre 2014 relatif à la mise en œuvre de traitements automatisés de données à caractère personnel dénommés « logiciel d'uniformisation des procédures d'identification »	Identifier dans le cadre des enquêtes préliminaires ou de flagrance les auteurs des infractions prévues aux articles 311-1 à 311-13 et 322-5 à 322-11-1 du code pénal par l'enregistrement d'informations collectées par les officiers et les agents de police judiciaire ainsi que par les agents spécialisés, techniciens ou ingénieurs de police scientifique sur les lieux de commission de ces infractions
MCI (main courante informatisée)	DGPN-PP	Arrêté du 24 février 1995 modifié	Gérer les événements de manière chronologique pour faciliter ensuite les recherches opérationnelles et la production de statistiques, d'autre part, de permettre une gestion nominative de l'activité du personnel en fonction des règles d'emploi en vigueur et enfin de faciliter la diffusion et le partage d'informations dans le cadre de missions de police judiciaire et du traitement de l'information criminelle
MERCURE	DGPN PP	Engagement de conformité DGPN du 14 décembre 2012 au décret n° 2012-687 autorisant les logiciels de rapprochements	Traitement d'analyse des données de téléphonie recueillies au cours d'une procédure judiciaire
N-MCI (nouvelle main courante informatisée)	DGPN-PP	Arrêté du 22 juin 2011 modifié	Faciliter le traitement des déclarations et événements pour assurer une meilleure efficacité des interventions ; faciliter la direction opérationnelle

Nom des fichiers	Gestionnaire du fichier	Fondement juridique	Finalités
			des services de police et de leurs agents ainsi que le contrôle et l'évaluation de leur activité (gestion d'emploi des effectifs) ; faciliter la diffusion et le partage d'informations dans le cadre de missions de police judiciaire et du traitement de l'information criminelle
N-SIS II (système national d'information Schengen 2)	DGPN (DCPJ)	Articles R. 231-5 et suivants du CSI	Centralisation d'informations concernant les personnes et objets signalés par les autorités administratives et judiciaires des États membres Schengen afin de permettre aux autorités désignées par ces États de décider de la conduite à tenir à l'égard des personnes et objets signalés
ODICOP (outil d'investigation et de communication opérationnelle de police)	DGPN (DCSP)	Engagement de conformité DGPN du 19 novembre 2014 au décret cadre du 20 février 2014 relatif à la diffusion de l'information opérationnelle	Faciliter la diffusion et l'échange d'informations opérationnelles sur certaines affaires judiciaires en cours de traitement au sein des services chargés d'une mission de police judiciaire
ORCA (outil de recherche de contamination ADN)	DGPN-DGGN	Décret cadre n° 2013-406 du 16 mai 2013	Identifier, lors des analyses génétiques effectuées par les laboratoires, à la demande des autorités judiciaires et des services de police ou des unités de gendarmerie, une éventuelle contamination des échantillons analysés
OSA (outil de suivi de l'activité)	DGPN (DCPAF)	Arrêté cadre du 20 mars 2014	Outil de suivi de l'activité des centres de coopération policière et douanière
OSIRIS (outil et système d'informations relatives aux infractions sur les stupéfiants)	DGPN-DGGN-PP	Arrêté du 12 janvier 2016	Évaluation de la situation nationale et de l'activité des services en matière d'usage et de trafic illicites de produits stupéfiants dans le cadre de la lutte contre ces phénomène et élaboration de statistiques opérationnelles et descriptives
PARSIFAL (plateforme automatisée de reconstruction de scripts informatiques de FREE appliquée à la localisation)	DGPN (DCPJ)	Engagement de conformité à l'arrêté cadre n° autorisant les traitements permettant la mise en œuvre des mesures de géolocalisation en temps réel dans un cadre judiciaire également en cours d'élaboration	Outil de suivi en temps réel des mesures de géolocalisation de téléphones portables
PASP (prévention des atteintes à la sécurité publique)	DCSP	Articles R. 236-11 à R. 236-20 du code de la sécurité intérieure	Conservation et analyse des informations sur les personnes susceptibles d'être impliquées dans des actions de violence collective

Nom des fichiers	Gestionnaire du fichier	Fondement juridique	Finalités
PEGASE	DCSP	Arrêté du 21 janvier 2008	Améliorer la gestion des appels d'urgence police secours
PERCEVAL	DGGN	Arrêté du 23 mai 2018 portant création d'un traitement automatisé de données à caractère personnel dénommé « plate-forme électronique de recueil des coordonnées bancaires et de leurs conditions d'emploi rapportées par les victimes d'achats frauduleux en l	Permettre à une victime d'effectuer un signalement depuis un téléservice mis à disposition sur le site « service-public.fr » contre un auteur inconnu pour des faits constitutifs des infractions suivantes : contrefaçon ou falsification d'un instrument de paiement ayant un dispositif de sécurité personnalisé, usage ou tentative d'usage, en connaissance de cause, d'un instrument de paiement ayant un dispositif de sécurité personnalité contrefait ou falsifié, acceptation, en connaissance de cause, de recevoir un paiement au moyen d'un instrument de paiement ayant un dispositif de sécurité contrefait ou falsifié Permettre d'exploiter les signalements mentionnés ci-dessus afin d'effectuer des rapprochements Faciliter et uniformiser les démarches administratives des victimes auprès de leurs établissements bancaires
Permissions de sortir	DGFPN-DGGN-PP	Arrêté cadre du 22 août 2012	Assurer la centralisation des informations relatives aux permissions de sortir des établissements pénitentiaires ou de placement en semi-liberté, accordées par le juge de l'application des peines et de disposer des informations statistiques liées à ce suivi
PeSMS (plateforme d'envoi de SMS)	DGGN		Envoyer des SMS en masse aux contacts disponibles ou enregistrés dans l'application dans le cadre de la sécurisation des casernes et plus largement dans le cadre de l'information de certaines populations (élus, commerçants, réservistes, autorités, candidats au concours, etc)
PHAROS (plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements)	DGPN (DCPJ)	Arrêté du 16 juin 2009 modifié	Traitement centralisé des signalements de toutes formes d'activités illicites sur internet signalés par les internautes afin d'effectuer des rapprochements et de saisir les services compétents pour les exploiter

Nom des fichiers	Gestionnaire du fichier	Fondement juridique	Finalités
PIO (diffusion et partage de l'information opérationnelle)	DGGN/DGPN	Décret n° 2014-187 du 20 février 2014 relatif à la mise en œuvre de traitements de diffusion de l'information opérationnelle au sein des services et unités de la police et de la gendarmerie nationales	Faciliter la diffusion et le partage d'informations opérationnelles détenues par les différents service sou unités de la police et de la gendarmerie nationale investis de missions de police judiciaire, sur les enquêtes en cours ou les personnes qui en font l'objet ainsi que l'activité judiciaire de ces services ou unités, informations collectées au cours des enquêtes préliminaires ou de flagrance ou des investigations exécutées sur commission rogatoire et concernant tout crime, délit ou contravention connexe à ce crime ou délit ou des procédures de recherche des causes de la mort ou d'une disparition prévues aux articles 74 et 74-1 du code de procédure pénale ou des procédures de recherche des personnes en fuite ou des actes visant à assurer l'exécution d'une peine diligentés en application des articles 74-2 et 709 du code de procédure pénale
PITEH (base personnes impliquées dans la traite des êtres humains)	DGGN	Décret n° 2013-1054 du 22 novembre 2013 relatif aux traitements automatisés de données à caractère personnel dénommés « bases d'analyse sérielle de police judiciaire »	Identifier les auteurs, co-auteurs ou complices de faits sériels nationaux et transfrontaliers pour toutes les infractions sérielles afférentes à la traite des êtres humains, dans toutes ses composantes (sexuelle, économique, frauduleuse, …) commis en tous lieux et punis d'une peine d'emprisonnement d'au moins 5 ans
PNIJ (plate-forme nationale des interceptions judiciaires)	Ministère de la justice	Décret n° 2014-1162 du 9 octobre 2014 portant création d'un traitement automatisé de données à caractère personnel dénommé « Plate-forme nationale des interceptions judiciaires »	Faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs par l'enregistrement et la mise à disposition des magistrats, des OPJ et des APJ PN et GN chargés de les seconder ainsi que des agents des douanes et des services fiscaux habilités à effectuer des enquêtes judiciaires le contenu des communications électroniques interceptées sur le fondement des articles 74-2,80-4,100 à 100-7 et 706-95 et les données et les informations communiquées en application des articles 60-1, 60-2, 77-1-1, 77-1-2, 99-3, 99-4, 230-32, des articles R. 10-13 et R. 10-14

Nom des fichiers	Gestionnaire du fichier	Fondement juridique	Finalités
			du code des postes et des communications électroniques et du décret n° 2011-219 du 25 février 2011
Pré-plainte en ligne	DGPN (DCSP)-DGGN-PP	Arrêté du 30 novembre 2011	Téléservice permettant d'effectuer une déclaration en ligne pour des faits d'atteinte aux biens contre auteur inconnu et d'obtenir un RDV auprès d'un service de police ou d'une unité de gendarmerie pour déposer et signer sa plainte. Élargissement à titre expérimental pour les faits de discriminations, de diffamation ou d'injures, à l'égard d'une personne, à raison de son origine ou de son appartenance ou de sa non-appartenance à une ethnie, une nation, une race, une religion, ou à raison de son sexe, de son orientation sexuelle ou de son identité de genre ou de son handicap et de provocation à la discrimination, à la haine ou à la violence
Projet de refonte des bases sérielles	DGGN	Décret n° 2013-1054 du 22 novembre 2013 relatif aux traitements automatisés de données à caractère personnel dénommés « bases d'analyse sérielle de police judiciaire »	Rassembler les preuves et identifier les auteurs des crimes ou délits présentant un caractère sériel, grâce à l'établissement de liens entre les individus, les événements ou les infractions
Registre des fourrières et des immobilisations	DCSP		Enregistrement et gestion des véhicules mis en fourrière ou immobilisés par les services de police
Résidents des zones de sécurité	DGPN DGGN	Arrêté du 2 mai 2011	Gestion des titres d'accès aux zones à l'intérieur desquelles sont apportées des restrictions de circulation afin de prévenir les troubles à l'ordre public et garantir la sécurité d'un événement majeur
RLOPPA (répertoires locaux pour les opérations de protection des personnes âgées)	DGPN (DCSP)-PP	Arrêté du 20 juin 2011	Recenser les personnes de soixante-cinq ans et plus souhaitant bénéficier d'une vigilance particulière de la part des services de police
SALVAC (système d'analyse des liens de la violence associée aux crimes)	DGPN (DCPJ)	Décret n° 2009-786 du 23 juin 2009	Faciliter la constatation des crimes et délits portant atteinte aux personnes et présentant un caractère sériel, rassembler les preuves et identifier les auteurs, grâce à l'établissement de liens entre les individus, les événements ou les infractions pouvant mettre en évidence ce caractère sériel

Nom des fichiers	Gestionnaire du fichier	Fondement juridique	Finalités
Sécurisation et contrôle des accès aux locaux et emprises relevant du ministère de l'intérieur	DGGN	Arrêté du 14 août 2014 portant autorisation de mise en œuvre de systèmes de vidéoprotection et création de traitements automatisés de données à caractère personnel destinés à la sécurisation et au contrôle des accès aux locaux et emprises relevant du min (arrêté -cadre)	Assurer la gestion des prélèvements biologiques effectués dans le cadre d'affaires judiciaires concernant l'une des infractions mentionnées à l'art. 706-55 du code de procédure pénale
SERAFIM (système d'exploitation, de recherche et d'analyse sur les filières d'immigration)	DGPN (DCPAF)	Engagement de conformité du 28 janvier 2014 au décret cadre du 22 novembre 2013 relatif aux bases d'analyse sérielle	Mettre à disposition de l'ensemble des enquêteurs des services d'investigation de la DCPAF, les données judiciaires inhérentes à la lutte contre les filières d'immigration irrégulière issues des enquêtes judiciaires en cours, en vue d'effectuer des recoupements
Service central de préservation des prélèvements biologiques	DGGN	Arrêté du 13 septembre 2002 portant création d'un traitement automatisé d'informations nominatives relatif à la gestion des prélèvements biologiques par le service central de préservation des prélèvements biologiques	Assurer la gestion des prélèvements biologiques effectués dans le cadre d'affaires judiciaires concernant l'une des infractions mentionnées à l'art. 706-55 du code de procédure pénale
SETRADER	DCPAF	Arrêté du 11 avril 2013	Collecte et traitement des données d'enregistrement et d'embarquement (API) des passagers de vols internationaux extra-européens
SIDPP (sécurisation des interventions et demandes particulières de protection)	DGGN	Décret n° 2011-342 du 29 mars 2011 portant création d'un traitement de données à caractère personnel relatif à la sécurisation des interventions et demandes particulières de protection	Collecter des données destinées à une gestion des interventions des forces de gendarmerie adaptée soit aux personnes dont la dangerosité ou l'agressivité, à travers manifestations de violence physique ou verbale, a été déjà constatée lors d'une précédente intervention, soit aux personnes demandant une intervention ainsi qu'aux personnes se trouvant dans une situation de vulnérabilité particulière
SINUS (système d'information numérique standardisé)	DGPN	Arrêté ministériel du 17 février 2010 portant création d'un traitement automatisé de données à caractère personnel dénommé « Système d'information numérique standardisé »	Faciliter les recherches effectuées par les services de police et de gendarmerie à la demande des autorités judiciaires ou administratives et faciliter les recherches, surveillances et contrôles effectués dans le cadre de leurs attributions respectives, par les services de la police nationale, les unités de la gendarmerie nationale et les agents des douanes

Nom des fichiers	Gestionnaire du fichier	Fondement juridique	Finalités
			exerçant des missions de police judiciaire ou des missions administratives ainsi que par les agents du service mentionné à l'art. L 561-23 du code monétaire et financier (TRACFIN)
SiPOL	DGPN	Décret en cours d'examen par le Conseil d'État	Le traitement a pour finalités : 1° De recueillir et centraliser les informations collectées par les services territoriaux des directions concernées ; 2° De faciliter et de fiabiliser l'analyse, la production, la diffusion et le partage de ces informations ; 3° D'apporter une aide à la prise de décision du directeur général de la police nationale et des directeurs centraux de la direction générale de la police nationale (DGPN)
SIV (système d'immatriculation des véhicules)	Ministère de l'intérieur	Arrêté ministériel du 10 février 2009 portant création d'un traitement automatisé de données à caractère personnel dénommé « système d'immatriculation des véhicules » ayant pour objet la gestion des pièces administratives du droit de circuler des véhicules	Gérer les pièces administratives du droit de circuler des véhicules sur les voies ouvertes à la circulation publique
SNPC (système national des permis de conduire)	Ministère de l'intérieur	Arrêté ministériel du 29 juin 1992 portant création du Système national des permis de conduire	Traiter les informations nominatives relatives aux permis de conduire un véhicule terrestre à moteur
STADE	Ministère de l'intérieur	Arrêté du 15 avril 2015 portant autorisation d'un traitement automatisé de données à caractère personnel dénommé « fichier STADE »	Prévenir les troubles à l'ordre public, les atteintes à la sécurité des personnes et des biens ainsi que les infractions susceptibles d'être commises à l'occasion des manifestations sportives et des rassemblements en lien avec ces manifestations se tenant dans le ressort des départements de Paris, des Hauts-de-Seine, de la Seine-Saint-Denis et du Val-de-Marne, et des manifestations sportives du club du Paris Saint Germain et des rassemblements liés à ces manifestations se tenant à l'extérieur des départements précités ; faciliter la constatation de ces infractions et la recherche de leurs auteurs

Nom des fichiers	Gestionnaire du fichier	Fondement juridique	Finalités
STDC (système de traitement de captations de données)	DGPN DGGN PP DGSI DGDDI	Décret cadre n° 2015-1700 du 18 décembre 2015 relatif à la mise en œuvre de traitements de données informatiques captées en application de l'article 706-102-1 du code de procédure pénale	Recueil et exploitation des données captées (capture écran, frappes clavier, skype) dans le cadre d'une information judiciaire pour l'une des infractions de l'article 706-73 du CPP (délinquance et criminalité organisées)
SYANS (caméras individuelles des agents de la police nationale et des militaires de la gendarmerie nationale)	DGGN/DGPN	Loi n° 2016-731 du 3 juin 2016 Déclaration normale CNIL n° 2088882	Prévenir les incidents au cours des interventions des agents de la police nationale et des militaires de la gendarmerie nationale, constater les infractions et la poursuite de leurs auteurs par la collecte des preuves, former les agents
TAJ (traitement d'antécédents judiciaires)	DGPN (DCPJ) DGGN	Décret n° 2012-652 du 4 mai 2012 modifié	Centralisation des données recueillies dans le cadre des procédures établies par les services de la police et les unités de la gendarmerie nationales, ou par des agents des douanes habilités à exercer des missions de police judiciaire lorsqu'un service de police ou une unité de gendarmerie est appelé à en assurer la continuation ou la conduite commune
TES (titres électroniques sécurisés)	Ministère de l'intérieur	Décret n° 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement de données à caractère personnel relatif aux passeports et aux cartes nationales d'identité	Établir, délivrer, renouveler et invalider les cartes nationales d'identité et passeport et prévenir et détecter leur falsification et contrefaçon
THESEE (Traitement harmonisé des enquêtes et des signalements pour les e-escroqueries)	DGPN (DCPJ)	Arrêté en cours d'élaboration	Recueillir et centraliser les plaintes et signalements relatifs aux escroqueries commises sur internet afin de procéder à des rapprochements et permettre l'identification de leurs auteurs
Traitements de données à caractère personnel permettant la mise en œuvre des mesures de géolocalisation en temps réel dans un cadre judiciaire	DGPN-DGGN-PP-DGSI	Arrêté cadre en cours d'élaboration	Permettre sur autorisation et sous le contrôle de l'autorité judiciaire, la collecte, l'enregistrement, l'exploitation et la conservation de données destinées à la localisation en temps réel d'une personne, d'un véhicule ou de tout autre objet
Vidéoprotection dans les locaux et enceintes du MI non ouverts au public	DGPN	Acte cadre du 14 août 2014 portant autorisation de mise en œuvre de systèmes de vidéoprotection et création de traitements automatisés de données à caractère personnel destinés à la sécurisation et au contrôle des accès aux locaux et emprises relevant du	Traitements automatisés de données à caractère personnel destinés à la sécurisation et au contrôle des accès aux locaux et emprises relevant du ministère de l'intérieur mais non ouverts au public

Nom des fichiers	Gestionnaire du fichier	Fondement juridique	Finalités
		ministère de l'intérieur	
VISABIO	Ministère de l'intérieur	Décret n° 2013-147 du 18 février 2013 relatif à l'application de gestion des dossiers de ressortissants étrangers en France et au traitement automatisé de données à caractère personnel relatives aux étrangers sollicitant la délivrance d'un visa	Mieux garantir le droit au séjour des personnes en situation régulière et lutter contre l'entrée et le séjour irréguliers des étrangers en France, en prévenant les fraudes documentaires et les usurpations d'identité ; permettre l'instruction des demandes de visas en procédant notamment à l'échange d'informations avec des autorités nationales et avec les autorités des États Schengen au travers du système d'information sur les visas (VIS) pour les données biométriques se rapportant aux visas pour un séjour d'une durée inférieure à 3 mois délivrés par les autorités françaises

ANNEXE N° 5 :
MODÈLE DE FICHE-NAVETTE UTILISÉE POUR LA MISE À JOUR DU FICHIER TAJ (1)

BULLETIN OFFICIEL DU MINISTÈRE DE LA JUSTICE

Annexe 6

Modèle de « fiche-navette »

SUITES JUDICIAIRES

Imprimé à retourner par le parquet au service gestionnaire du traitement des antécédents judiciaires (TAJ)

PERSONNE MISE EN CAUSE : Madame/Monsieur .....
né le ..... à .....
de nationalité .....
demeurant à .....

PROCEDURE N° ...../..... établie par .....

Transmise à Madame/Monsieur le procureur de la République près le tribunal de grande instance de.....

Le .....

INFRACTION(S) : 1 - VOL SIMPLE commis le ..... à .....

Le procureur de la République
Près le tribunal de grande instance
de.....

informe

Madame/Monsieur le directeur du Service régional de police judiciaire/
le commandant de la Brigade départementale de renseignements et d'investigations judiciaires

□ qu'est intervenue, au profit de la personne mise en cause dans la procédure judiciaire concernant la ou les infractions mentionnées ci-dessus et enregistrées dans le TAJ :

1 [....] une décision de requalification judiciaire en date du ..... modifiant la qualification des faits initialement retenue ..... (Code Natinf) pour les requalifier de ..... (Code Natinf)

2 [....] une décision définitive de relaxe ou d'acquittement, en date du .....
[] Effacement (principe)
[] Ajout de la mention (exception)

3 [....] une décision définitive de non-lieu, en date du .....
[] Ajout de la mention (principe)
[] Effacement (exception)

4 [....] une décision de classement sans suite motivée par l'insuffisance de charges (motifs 11, 21 ou 71), en date du .....
[] Ajout de la mention (principe)
[] Effacement (exception)

5 [....] une décision de classement sans suite autre que celle figurant au point 4, en date du .....
[] Ajout de la mention

□ qu'il lui appartient de mettre à jour le STIC/le JUDEX, dans lequel les données relatives à la personne mise en cause ont été initialement enregistrées.

□ autres observations :

Cachet de la juridiction et signature de l'autorité

(1) Annexée à la circulaire de la garde des sceaux du 18 août 2014 relative aux fichiers d'antécédents judiciaires (NOR : JUSD1419980C).