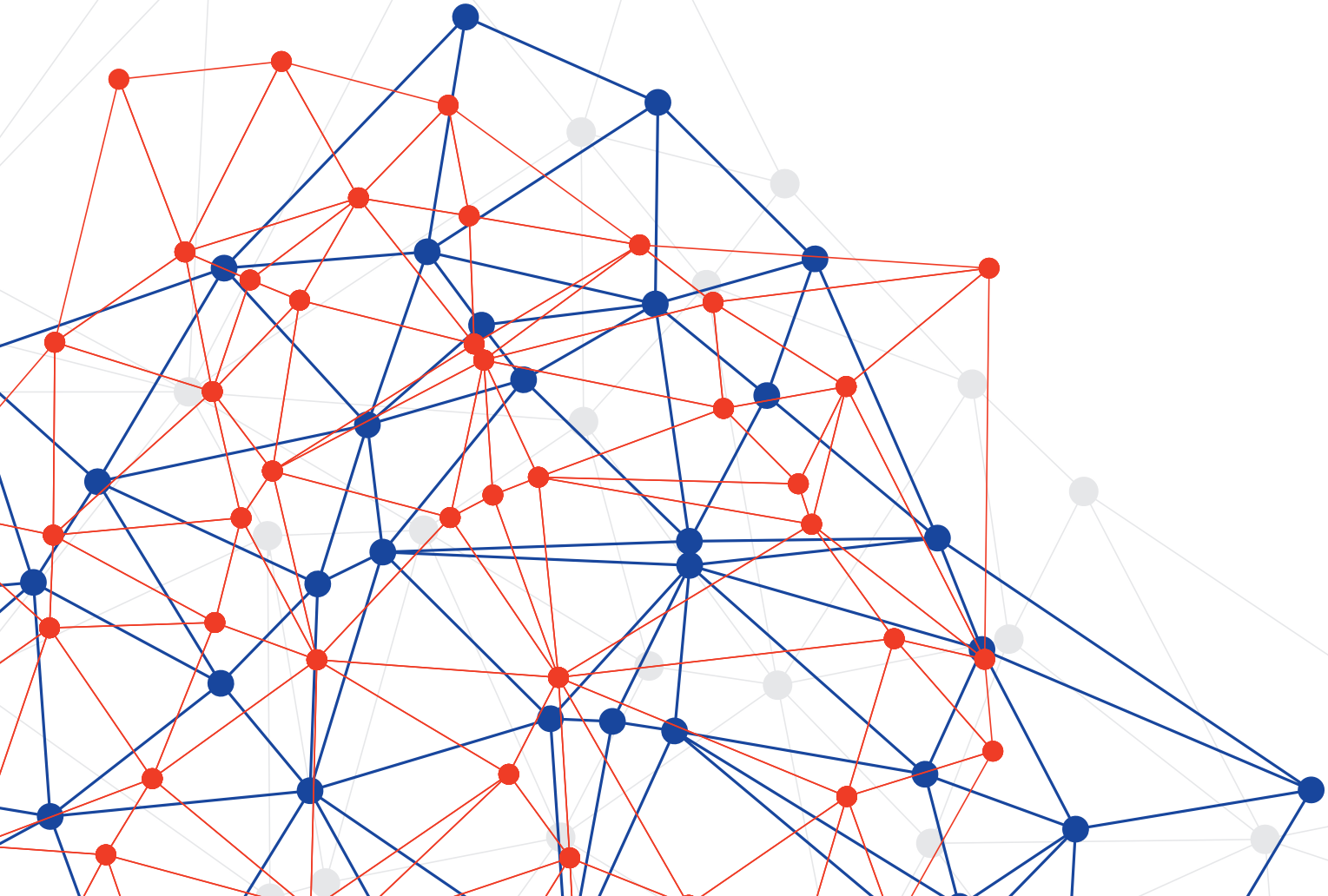
Cf2R
Centre Français de Recherche sur le Renseignement

LES FICHIERS DE POLICE ET DE RENSEIGNEMENT EN FRANCE

Jean-Marie COTTERET

Rapport de recherche #21
Octobre 2017



PRÉSENTATION DE L'AUTEUR

Professeur émérite à la Sorbonne (Paris I), **Jean-Marie Cotteret** est docteur en droit, docteur en science politique, agrégé de droit public et diplômé de la Fondation nationale des sciences politiques (FNSP).

Il a été professeur de droit public et de science politique à l'Université de Nice, de 1964 à 1975, puis professeur de sciences politiques à l'Université de Paris I Panthéon-Sorbonne et directeur du Centre de recherche sur l'information et la communication de la Sorbonne (1975-2001).

Jean-Marie Cotteret a également été membre du Conseil supérieur de l'audiovisuel (CSA), où il fut responsable des campagnes électorales et du pluralisme politique, et membre de la Commission Informatique et Liberté (CNIL) où il a été en chargé des fichiers de police.

Il est l'auteur de nombreux ouvrages, parmi lesquels :
- *Parlement 2.0*, Fauves éditions, 2015.
- *Les avatars de la volonté générale*, Michalon, 2011.
- *La démocratie télé-guidée*, Michalon, 2006.
- *Giscard d'Estaing/Mitterrand*, Presses universitaires de France, 2005.
- *Le marché électoral* avec Claude Émeri, Michalon, 2004.
- La bataille des images *avec Gérard Mermet, Larousse, 20*03.
- *La magie du discours*, Michalon, 2000.
- *Gouverner c'est paraître*, Presses universitaires de France, 1991.
- *Droit budgétaire et comptabilité publique*, Dalloz, 1985.
- *La démocratie cathodique l'élection présidentielle de 1981 et la télévision*, avec Jacques Gerstle, Gérard Ayache et Nicole Casile, Dunod, 1981
- *Les systèmes électoraux*, avec Claude Emeri, Presses universitaires de France, 1978.
- *Le vocabulaire du général de Gaulle*, avec René Moreau Presses de la Fondation nationale des sciences politiques, 1969.

Enfin, Jean-Marie Cotteret est membre du Conseil scientifique du Centre Français de Recherche sur le Renseignement (CF2R).

RÉSUMÉ

LES FICHIERS DE POLICE ET DE RENSEIGNEMENT EN FRANCE

L'informatisation des fichiers de police et de renseignement augmente la possibilité de collecter, traiter et mettre à disposition des policiers, des gendarmes et des services de renseignement et de sécurité une grande quantité de données. Il n'est donc pas étonnant que les citoyens perçoivent ces fichiers comme un instrument de pouvoir, voire comme une menace.

Mais comme le constatent les parlementaires Delphine Batho et Jacques-Alain Benisti dans leur rapport *Fichiers de Police, les Défis de la République, « interdire aux services de police de vivre avec leur temps et d'utiliser les outils d'aujourd'hui pour traquer délinquants et criminels reviendrait à se tirer rune balle dans le pied* ». Et s'il y a eu une multiplication des fichiers de police et de renseignement au cours de ces dernières années la Commission nationale informatique et libertés (CNIL), créée par la loi du 6 janvier 1978, en assure le contrôle.

Ainsi l'État est-il confronté au double défi de protéger les données personnelles des citoyens, tout en assurant leur sécurité face à un terrorisme qui agit sans règles.

Face à la menace terroriste, la presse ne cesse d'évoquer les désormais tristement célèbres « fiches S », sans vraiment savoir à quoi correspond cette dénomination, ni le fichier correspondant. Force est de constater la méconnaissance et la méfiance qu'ont les médias et le public des fichiers de police et de renseignement dans notre pays, et des règles d'utilisation qui sont les leurs.

Le but de ce rapport est d'en dresser un inventaire aussi précis que possible, afin de porter à la connaissance des journalistes, des chercheurs et de l'opinion des éléments factuels ayant pour but d'éviter certains propos infondés ou analyses fantaisistes.

SOMMAIRE

INTRODUCTION

« Constatant que les sociétés démocratiques se trouvent menacées de nos jours par des formes très complexes d'espionnage et par le terrorisme, la Cour a estimé que l'existence de dispositions législatives accordant des pouvoirs de surveillance secrète de la correspondance, des envois postaux et des télécommunications était, devant une situation exceptionnelle, nécessaire dans une société démocratique à la sécurité nationale ».

Cour européenne des droits de l'homme, Klass et autres c., Allemagne, 6 septembre 1978.

On fait remonter la notion de société de surveillance au XVIIIe siècle. Et bien évidemment, elle est liée à la mise en place de fichiers de police. En 1752 est mis en place à Paris un « Livre rouge » consignant l'identité et le signalement des coupables. Puis Fouché est crédité d'avoir mis en fiches un nombre important de citoyens. Mais les vrais fichiers de police voient le jour avec le début de la police scientifique et la création en 1882 du service anthropométrique et photographique à la préfecture de police de Paris. Cette précision accrue des fichiers de police allait évidemment entraîner le développement de la défense des libertés individuelles et les accusations de pratiques non démocratiques du pouvoir.

Au début du XXe siècle, les fichiers de police allaient déclencher la fameuse « Affaire des fuites ». Nommé ministre de la Guerre en 1900, le général André entreprend de mettre sur fiches 25 000 officiers de son état-major.
Il se vantait de vouloir « républicaniser » l'armée. Mais le scandale fut tel qu'il fut obligé de démissionner en 1904. Depuis, l'opposition entre la défense des libertés et la multiplication des fichiers de police ne s'est jamais atténuée.

Le nombre de ces derniers n'a cessé d'augmenter et, en mars 2009, le rapport de la Mission d'information sur les fichiers de police[1] les évaluait à 58, dont environ un quart ne faisait l'objet d'aucune loi. Leur nombre se rapprocherait en réalité de la centaine. Aujourd'hui, des millions de personnes sont fichées sans que semble-t-il, il y ait des conséquences pour les libertés individuelles.
Les moyens de protection de la personne - sauf exception, par exemple pour le terrorisme - ne sont pas affectés.

Améliorer le recueil des données et faciliter leur consultation sont des objectifs permanents des services de police. Comme plusieurs rapporteurs de l'Assemblée nationale et du Sénat l'ont constaté, les fichiers de police sont par nature un instrument de pouvoir. L'arrivée de l'informatique a complètement changé la donne.
En effet, grâce à l'informatique et au développement de l'analyse sérielle, une grande quantité de données peuvent être traitées, collectées et mises à la disposition des services de renseignement et du pouvoir. Et l'interconnexion des fichiers peut fournir des renseignements inédits jusqu'alors.

Il faut noter aussi une évolution de la nature des données collectées. La biométrie marque une nouvelle façon de concevoir les données et va même jusqu'à modifier le concept d'identité. Dans une période où les identifiants traditionnels sont les moins stables - sexe, nom, nationalité, profession - et semblent donner plus de libertés aux individus, les données biométriques figent l'identité en lui conférant certitude et permanence.

Il est évident que ces fichiers informatiques demandent une vigilance toute particulière, surtout avec la possibilité d'interconnexion. Mais si l'informatique permet la constitution de fichiers de masse, elle permet aussi une plus grande traçabilité pour vérifier qui a eu accès aux fichiers.

Car l'État n'a pas qu'un aspect totalitaire, il doit à la fois protéger le citoyen et lutter contre l'arbitraire selon le principe défini par Montesquieu, ce qui consiste à la fois à défendre la vie contre les menaces extérieures, mais aussi à protéger l'individu contre l'arbitraire du despote.
L'État est donc confronté au double défi de protéger les données personnelles des citoyens, tout en assurant leur sécurité face à un terrorisme qui agit sans règles.

Confronté à la menace terroriste, le pouvoir politique, via le renseignement, recherche moins ce que pense l'individu dans son intériorité qu'à surveiller sa mobilité : ce qui est devenu essentiel, c'est de pouvoir localiser un individu et opérer une véritable traçabilité en temps réel de l'ensemble de ses déplacements. Et bien évidemment on assiste à une remise en cause nouvelle de la liberté. Mais la localisation de l'individu est un moyen efficace de la lutte antiterroriste pour assurer la sécurité des Français.

Depuis plusieurs années, la presse ne cesse d'évoquer les désormais tristement célèbres « fiches S », sans vraiment savoir à quoi correspond cette dénomination, ni le fichier correspondant.
L'utilisation des fichiers de renseignement, comme le Fichier des personnes recherchées (FPR) ou le Fichier des signalements pour la prévention et la radicalisation à caractère terroriste (FSPRT), fait régulièrement l'objet de débats et de polémiques comme l'a encore montré le cas d'Adam Djaziri, auteur de l'attentat raté en juin 2017, sur les Champs-Élysées. Fiché S en 2015, il avait pu renouveler son autorisation de détention d'armes en 2017, et acquérir en toute légalité deux pistolets automatiques et une carabine de chasse de catégorie B.
Suite à cet incident, depuis le 3 août 2017, un décret permet aux agents autorisant la détention d'armes de consulter le fichier des personnes recherchées dans lequel se trouvent les fichés S. D'autres décrets permettant une plus large consultation des fichiers, à des fins d'enquête administrative, ont également été publiés au cours de l'été 2017.

[1] *Delphine Batho et Jacques-Alain Benisti, Rapport d'information sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police, Assemblée nationale, n° 1548, 24 mars 2009.*

Pour Hélène L'Heuillet[1], la police ne doit pas être l'esclave du pouvoir mais au contraire « *elle se doit pour être efficace de participer de la souveraineté, c'est-à-dire d'agir souverainement. La culture policière n'est pas seulement une culture d'obéissance, mais aussi de souveraineté. Le renseignement participe aussi du domaine du secret. Alors que la justice est du domaine de la transparence, la police en général et le renseignement en particulier est du domaine de l'opacité* ».

Mais il est évident que dans nos sociétés qui prônent la transparence, cette opacité génère le soupçon. Ce qui explique les réactions de l'opinion aux actions de la police et du renseignement. D'où le statut spécial réservé aux fichiers de renseignement par la loi de 1978 qui crée la CNIL.

Le but de ce rapport est de dresser un inventaire précis des différents fichiers de police ou de renseignement existant dans notre pays et de leurs conditions d'utilisation par les services de sécurité et les forces de l'ordre.

[1] *Basse politique, haute police: Une approche historique et philosophique de la police, Fayard, Paris, 2001.*

1. LES FICHIERS DE POLICE

Les fichiers de police peuvent être classés en plusieurs familles en fonction de leurs finalités : fichiers administratifs, d'antécédents judiciaires, d'identification judiciaire et de rapprochement.

LES FICHIERS ADMINISTRATIFS

Une première catégorie de fichiers de police a un caractère administratif. Ces fichiers sont destinés à enregistrer des données administratives sur des personnes, des objets ou des moyens de transport. Les plus connus sont les fichiers relatifs à la carte d'identité et aux passeports. Ils ont fait l'objet d'un regroupement au sein du fichier TES (Titres électroniques sécurisés) par un décret du 28 octobre 2016 qui a fait l'objet de violentes polémiques.
C'est le cas aussi des fichiers d'immatriculation des véhicules (Fichier national des immatriculations/FNI) ou de celui des propriétaires ou possesseurs d'armes (AGRIPPA/Application nationale de gestion du répertoire informatisé des propriétaires et possesseurs d'armes).

Une seconde catégorie regroupe les fichiers administratifs à vocation judiciaire qui sont destinés à centraliser des renseignements pour lutter contre les infractions bien déterminées. C'est le cas du fichier national de faux monnayage (FNFM) et du fichier des véhicules volés (FVV).

Le fichier Application de gestion du répertoire informatisé des propriétaires et possesseurs d'armes (AGRIPPA)
AGRIPPA[1] est le fichier qui recense tous les détenteurs d'armes en France. Pour chacun d'eux, il comprend les informations suivantes :
- date de délivrance de l'autorisation
- date d'expiration,
- le cas échéant, date du refus,

Détenu par les préfectures sous tutelle de la Direction des libertés publiques du ministère de l'Intérieur (DLPJ), ce fichier est consultable par les services de police, de gendarmerie et des douanes.

Le Fichier national des personnes interdites d'acquisition et de détention d'armes (FINIADA)
Le FINIADA[2], recense toutes les personnes ne pouvant acquérir ou détenir une arme. Elles y sont inscrites à la suite d'une décision, le plus souvent préfectorale - pour des raisons de sécurité, de sûreté nationale -, à une condamnation ou un traitement psychiatrique, ou encore pour des motifs d'ordre psychologique. Les armuriers et la Fédération nationale de la chasse peuvent le consulter via un code personnalisé, ainsi que les services de police et de gendarmerie.

Le fichier Titres électroniques sécurisés (TES)
Nature des données recueillies
Le TES est une immense base de données regroupant les informations personnelles et biométriques de près de 60 millions de Français. Pour chaque citoyen titulaire ou ex-titulaire d'une carte d'identité ou d'un passeport, des données à caractère personnel (nom de famille, prénom, date et lieu de naissance, sexe, couleur des yeux, taille, adresse, image numérisée du visage et des empreintes digitales, adresse de messagerie électronique, etc.), sont enregistrées dans un fichier unique.

Conservation des données
L'ensemble des informations seront conservées pendant 15 ans pour les passeports et 20 ans pour les cartes d'identité. Les agents chargés de la réalisation de ces documents pourront accéder aux données et les exploiter à l'instar de la police judiciaire, des services de renseignement, ainsi que la police et la gendarmerie « pour les besoins exclusifs de leurs missions ». En cas de vol ou de pertes des titres, Interpol et le système d'information Schengen pourront également accéder à certaines informations contenues dans le TES.

À quoi sert-il ?
Pour le gouvernement, la création d'un tel fichier se justifie au nom de la simplification administrative. En effet, le regroupement des informations personnelles vise à faciliter « l'établissement, la délivrance, le renouvellement et l'invalidation des cartes nationales d'identité (...) et des passeports ». Dans le même temps, le TES doit permettre de prévenir et détecter la falsification et la contrefaçon des papiers d'identité. Il est amené à remplacer le précédent TES (qui se référait jusqu'alors aux passeports) et le Fichier national de gestion (dédié aux cartes d'identité).

Usage du système pour les forces de l'ordre
Les forces de l'ordre accèdent à une application permettant de consulter les données à l'exception des empreintes. Elles ont notamment accès aux données d'identité, y compris aux photographies qui sont des données biométriques.

---

[1] Décret du 16 octobre 2007, en cours de révision.
[2] Décret du 5 avril 2011.
[3] Décret n° 2016-1460 du 28 octobre 2016 autorisant la création d'un traitement des données à caractère personnel relatif aux passeports et aux cartes nationales d'identité

Usage du système pour les forces de l'ordre dans le cadre des réquisitions judiciaires
La réquisition judiciaire prévue par le code de procédure pénale permet aux officiers de police judiciaire, procureurs et juges d'instruction d'obtenir communication des informations détenues par le TES ou par les préfectures.

Dans ce cadre, les officiers de police judiciaire peuvent obtenir auprès de l'Agence nationale des titres sécurisés (ANTS) toutes les informations collectées lors des demandes de titres correspondant à une identité donnée. Cela comprend notamment les photographies et les empreintes digitales.

LES FICHIERS D'ANTÉCÉDENTS JUDICIAIRES

La seconde catégorie regroupe les fichiers d'antécédents judiciaires qui ont pour but de collecter les informations extraites des procédures de police judiciaire. Ces fichiers facilitent le rassemblement des preuves d'infractions et la recherche de leurs auteurs.

Le fichier Traitement des antécédents judiciaires (TAJ)
Deux fichiers principaux ont longtemps existé : le STIC (Système de traitement des infractions constatées) pour la police et JUDEX (Système judiciaire de documentation et d'exploitation) pour la gendarmerie. Ils ont été supprimés et remplacés par un fichier unique, le TAJ.

En application des articles 230-6 à 230-11 du Code de procédure pénal, le TAJ est un fichier d'antécédents commun à la police et à la gendarmerie nationales, en remplacement des fichiers STIC et JUDEX, qui ont été définitivement supprimés. Il est utilisé dans le cadre des enquêtes judiciaires (recherche des auteurs d'infractions) et d'enquêtes administratives (enquêtes préalables à certains emplois publics ou sensibles).

Le TAJ présente en outre des évolutions par rapport aux fichiers qu'il remplace : plus de catégories de personnes concernées et nouvelles fonctionnalités, comme des outils d'analyse et de rapprochement des données permettant de faire des recherches d'éléments communs dans des procédures différentes ou reconnaissance faciales à partir de photographies des personnes.

On estime à 9 500 000 le nombre de personnes présentes dans le TAJ en qualité de « mis en cause ».
C'est le ministère de l'Intérieur qui est responsable de ce fichier (DGPN et DGGN).

Nature des données recueillies
Les données du TAJ sont recueillies dans le cadre de procédures établies par les services de la police nationale et les unités de la gendarmerie nationale, ou par des agents des douanes habilités à exercer des missions de police judiciaire. Plusieurs catégories de données à caractère personnel peuvent être enregistrées.

▪ Concernant les « mis en cause », personnes à l'encontre desquelles sont réunis, lors de l'enquête préliminaire, de l'enquête de flagrance ou sur commission rogatoire, des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer, comme auteurs ou complices, à la commission d'un crime, délit ou contraventions de cinquième classe :
- identité, surnom, alias, situation familiale, filiation, nationalité, adresse,
- date et lieu de naissance,
- profession,
- état de la personne,
- signalement,
- photographie comportant des caractéristiques techniques permettant de recourir à un dispositif de reconnaissance faciale,
- pour des personnes morales : raison sociale, enseigne commerciale, sigle, forme juridique, IRCS, SIREN, SIRET, lieu du siège social, secteur d'activité, adresses.

▪ Concernant les victimes des infractions :
- identité, situation familiale, nationalité, adresse,
- date et lieu de naissance,
- profession,
- état de la personne,
- pour des personnes morales : raison sociale, enseigne commerciale, sigle, forme juridique, IRCS, lieu du siège social, secteur d'activité, adresses

▪ Concernant les personnes faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort, de blessures graves ou d'une disparition au sens de l'article 74 et 74-1 du code de procédure pénale :
- identité, situation familiale, nationalité, adresse,
- date et lieu de naissance,
- profession,
- état de la personne,
- signalement (personnes disparues et corps non identifiés),
- photographie comportant des caractéristiques techniques permettant de recourir à un dispositif de reconnaissance faciale,

Des données à caractère non personnel sont également enregistrées : cela concerne les faits, objets de l'enquête, lieux, dates de l'infraction, modes opératoires, données et images relatives aux objets, sont autorisés par dérogation.

Le TAJ n'indique pas le jugement ou la sanction finale. La plupart du temps, les services de police et de gendarmerie n'ont pas connaissance des sanctions prises.

Qui a accès au TAJ ?

▪ Les personnes ayant accès à TAJ sont :
- les membres de la police et de la gendarmerie nationales exerçant des missions de police judiciaire individuellement désignés,
- la douane judiciaire,
- les magistrats du parquet,
- les agents des services judiciaires, habilités par le Procureur de la République.

▪ Les personnes qui procèdent à une inscription ont accès à TAJ. Sont également destinataires des données :
- les agents de l'État investis d'attributions de police judiciaire,
- les magistrats instructeurs, pour des recherches relatives aux infractions dont ils sont saisis,
- les organismes de coopération internationale en matière de police judiciaire et les services de police étrangers, dans le cadre de l'article 24 de la loi du 18 mars 2003.

Enfin, le TAJ peut être consulté dans le cadre d'enquêtes administratives (cf. décret n° 2005-1124 du 6 septembre 2005) :
- en cas de recrutement pour des fonctions mentionnées à l'article L. 114-1 du code de la sécurité intérieure,
- en cas de demande d'acquisition de la nationalité française,
- les agents spécifiquement habilités réalisant une mission de police administrative.

Le droit d'information ne s'applique pas (art 32-VI).

Le droit d'opposition (art.38) est exclu, à l'exception des victimes dès lors que l'auteur des faits a été condamné définitivement.

Conservation des données
- Les données concernant les personnes mises en cause sont conservées 20 ans. Par dérogation, elles sont conservées 5 ans (pour certains délits et contraventions) et 40 ans pour certaines infractions (crimes et certains délits).
- Les données concernant les mineurs mis en cause sont conservées 5 ans. Par dérogation, elles sont conservées : 10 ans (pour certains délits) et 20 ans (crimes et certains délits).
- Les données concernant les victimes sont conservées au maximum 15 ans.
- Les données concernant les personnes faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort, de blessures graves ou d'une disparition au sens de l'article 74 et 74-1 du code de procédure pénale sont conservées jusqu'à ce que l'enquête ait permis de retrouver la personne disparue ou d'écarter toute suspicion de crime ou délit.

Interconnexion avec d'autres fichiers

Les interconnexions se font avec CASSIOPEE (Chaîne applicative supportant le système d'information orienté procédure pénale et enfants). Une interconnexion avec FOVeS (Fichier des objets volés et signalés) est également envisagée.

Les dysfonctionnements du TAJ

Les contrôles du STIC réalisés par la Commission informatique et libertés (CNIL) en 2007 et 2008, puis en 2012 et 2013, ont permis de révéler plusieurs types de dysfonctionnement (erreurs de saisie, utilisation du profil de consultation judiciaire lors des enquêtes administratives, réelles carences en matière de mise à jour du fichier, etc.).

Dès lors que le projet d'interconnexion avec CASSIOPEE (ministère de la Justice) sera achevé, le TAJ devrait être l'une des solutions à ces dysfonctionnements, notamment en ce qu'il permettra une mise à jour automatisée des données en fonction des suites judiciaires (et notamment de rendre inaccessibles des données en cas de classement sans suite lors d'enquêtes administratives, conformément aux dispositions en vigueur).

Des solutions imparfaites, néanmoins assez nombreuses ont été mises en œuvre par le ministère de l'Intérieur pour pallier les difficultés constatées par la CNIL.

Fichier du casier judiciaire national informatisé (FCJNI)

Le FCJNI, tenu au centre de traitement à Nantes sous l'autorité du ministère de la Justice, est celui qui contient le plus d'informations concernant les citoyens. En effet, toutes les condamnations pénales et les peines ou mesures d'accompagnement, y compris civiles, y figurent. Il émane de son ancêtre créé en 1848, mais a été organisé dans sa version actuelle à partir de 1966.

Trois casiers le composent :
- Casier 1, où figurent toutes les condamnations, y compris civiles et administratives. Seuls les juges y ont accès.
- Casier 2, où sont enlevés les mineurs, les contraventions, les sanctions étrangères, les condamnations avec sursis. Les autorités militaires et administratives, et judiciaires y ont accès notamment pour l'emploi public ou les distinctions honorifiques, et quelques employeurs (pour les mineurs).
- Casier 3, contient les condamnations à des crimes et délits à 1 an d'emprisonnement et à moins de deux ans si la juridiction a ordonné leur mention au bulletin. Est ouvert aux citoyens ou leurs représentants légaux. C'est le seul fichier accessible et voué aux citoyens.

LES FICHIERS D'IDENTIFICATION JUDICIAIRE

Troisième catégorie des fichiers de police, les fichiers d'identification judiciaire. Ces fichiers servent à l'identification d'un auteur d'infraction ou d'une personne disparue. Ces fichiers bénéficient de progrès considérables grâce à l'informatique et à la biométrie. Grâce à ces nouveaux outils, les résultats obtenus par la police scientifique et technique se sont considérablement améliorés.

Le Fichier automatisé des empreintes digitales (FAED)

Le FAED sert à la recherche et à l'identification des auteurs de crimes et de délits, ainsi qu'à la poursuite, à l'instruction et au jugement des affaires criminelles et délictuelles dont l'autorité judiciaire est saisie.

Le FAED permet de s'assurer de la véritable identité des personnes mises en cause dans une procédure pénale ou condamnée à une peine privative de liberté, afin d'éviter les erreurs judiciaires, de détecter les fausses identités et d'établir les cas de récidive. Il s'agit également d'identifier, par comparaison, les traces de personnes inconnues relevées sur des lieux d'infractions.

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

Enfin, il permet de vérifier l'identité de personnes retenues en application de l'article 78-3 du code de procédure pénale ou dans les conditions prévues par l'article L.611-4 du code de l'entrée et du séjour des étrangers et du droit d'asile.

Au 20 juin 2016, il y avait 4 682 387 personnes enregistrées et 237 457 traces non identifiées.

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

Le FIJAIT comprend toute personne susceptible de porter atteinte à la sécurité publique, y compris les mineurs de plus de treize ans.

Durée de conservation des données

Les données ne peuvent être conservées plus de 10 ans (3 ans pour les mineurs) après l'intervention du dernier événement de nature à faire apparaître un risque d'atteinte à la sécurité publique ayant donné lieu à un enregistrement.

Modalités de consultation

Peuvent accéder à ce fichier :

- les fonctionnaires relevant de la Sous-direction de l'information générale (SDIG[1]) individuellement désignés et spécialement habilités par le directeur central de la sécurité publique ;
- les fonctionnaires des directions départementales de la sécurité publique affectés dans les services d'information générale (SDIG) individuellement désignés et spécialement habilités par le directeur départemental ;
- les fonctionnaires affectés dans les services de la préfecture de police en charge du renseignement individuellement désignés et spécialement habilités par le directeur départemental ;
- les fonctionnaires des groupes spécialisés dans la lutte contre les violences urbaines ou les phénomènes de bandes, individuellement désignés et spécialement habilités par le directeur départemental de la sécurité publique ou par le préfet de police, sont autorisés à accéder à certaines données.
- peut également être destinataire des données, dans la limite du besoin d'en connaître, tout autre agent d'un service de la police nationale ou de la gendarmerie nationale, sur demande expresse précisant l'identité du demandeur, l'objet et les motifs de la consultation.

À noter que le droit d'information et le droit d'opposition sont exclus.

Cadre juridique

La CNIL est particulièrement attentive aux éventuelles évolutions de ces dispositions législatives ainsi qu'aux conditions effectives de mise en œuvre de ce fichier.
Elle a demandé le respect en Conseil d'État des engagements pris par le gouvernement devant la Commission quant au contrôle du fichier par un magistrat, sur les données enregistrées dans le FIJAIT, sur les modalités et les cadres d'accès à ce dernier, sur les modalités d'information des personnes concernées et d'exercice de leurs droits, etc.

La CNIL s'est prononcée, lors de la séance plénière du 7 avril 2015, sur un projet de dispositions législatives visant à modifier le code de procédure pénale (CPP) en y insérant une section relative au Fichier national des auteurs d'infractions terroristes (FIJAIT), dans leur version envisagée par le gouvernement.

Il s'agit ainsi de créer un fichier d'adresses spécifiques à une catégorie particulière d'infractions liées au terrorisme afin d'assurer un suivi des personnes qui y sont inscrites au travers de différentes obligations (justification d'adresse et des déplacements à l'étranger, etc.).
Dans la mesure où des garanties identiques au Fichier judiciaire national automatisé des auteurs d'infractions sexuelles (FIJAISV) ont été prévues pour le FIJAIT, la Commission a considéré que celles-ci étaient a priori de nature à assurer un équilibre entre le respect de la vie privée et la sauvegarde de l'ordre public.

Toutefois, la Commission a considéré qu'il lui appartenait de s'assurer, de manière effective, qu'il n'était pas porté une atteinte excessive au respect des droits et libertés fondamentaux. En particulier, elle a formulé des observations sur les points suivants :

[1] *Devenue Service central du renseignement territorial (SCRT) en 2014.*

- Sur la durée de conservation des données, la CNIL a notamment relevé[1] que dans la mesure où, par nature, le FIJAIT constitue un fichier d'adresses utilisé aux fins de suivi des personnes concernées, la conservation d'adresses non mises à jour n'apparaît pas utile, ce qui est le cas des adresses conservées au-delà de la date de fin des obligations des personnes concernées. De même, la conservation de données qui pourraient déjà figurer dans d'autres fichiers judiciaires (TAJ et casier judiciaire, par exemple) ou de renseignement (tel CRISTINA, *cf. infra*) au-delà de la fin des obligations n'apparaît pas davantage nécessaire à la poursuite des finalités du FIJAIT. Elle a estimé que le dispositif projeté ne serait conforme aux dispositions de la loi du 6 janvier 1978 modifiée que dans la mesure où seules des données exactes et pertinentes y seraient conservées après cette date.

- Sur l'inscription automatique des personnes inscrites au FIJAIT dans le FPR (*cf. infra),* le gouvernement justifie cette inscription automatique par la nécessité pour les services du ministère de l'Intérieur en charge du contrôle aux frontières d'identifier si la personne se trouve en violation de ses obligations. La CNIL a dès lors considéré que seuls ces personnels devraient avoir accès à la situation des personnes inscrites au FIJAIT, à cette seule fin, et non l'ensemble des forces de sécurité publique ayant accès au FPR.

- Sur les destinataires des données, la CNIL a tout d'abord précisé que les autorités judiciaires et les services spécialisés de renseignement ne devaient pouvoir accéder au FIJAIT que dans le seul cadre de leurs missions de lutte contre le terrorisme, ce qui devrait figurer expressément dans les dispositions législatives projetées. Elle a également relevé que s'agissant des préfets et administrations de l'État, le périmètre des enquêtes leur permettant de recevoir communication des données était imprécis et a appelé l'attention du gouvernement sur la nécessité de le restreindre à certaines activités ou professions en lien avec les infractions pouvant donner lieu à une inscription dans le fichier.

Le Fichier national des empreintes génétiques (FNAEG)

L'ADN (acide désoxyribonucléique) est une macromolécule découverte en 1944. En 1953, MM. Watson et Crick établirent le schéma de la structure en double hélice de l'ADN. Puis, en 1984, le professeur Alec Jeffreys découvrit ce que l'on appelle communément « l'empreinte génétique ».

L'ADN constitue le support de l'information génétique héréditaire réunissant toutes nos caractéristiques organiques, morphologiques et parfois pathologiques comme constituant un élément essentiel du matériel héréditaire. L'ADN détermine notre identité et permet de différencier un individu d'un autre.

Le Fichier national des empreintes génétiques (FNAEG) sert à faciliter l'identification et la recherche
- des auteurs d'infractions à l'aide de leur profil génétique,
- de personnes disparues à l'aide du profil génétique de leurs descendants ou de leurs ascendants.

En 2015, le FNAEG contenait les profils génétiques de plus de 3 millions d'individus dont :
- 2 540 000 personnes mises en cause
- 472 500 personnes condamnées.

Il a permis de résoudre près de 75 000 affaires.

Que contient ce fichier ?

Le FNAEG centralise les empreintes génétiques concernant :
- les personnes non identifiées (empreintes issues de prélèvements sur les lieux d'une infraction),
- les personnes identifiées (personnes condamnées ou mises en cause pour une des infractions listées à l'article 706-55 du code de procédure pénal).
- Les empreintes sont complétées des informations suivantes :
- nom, prénoms, date et lieu de naissance, filiation et sexe ;
- services ayant procédé à la signalisation ;
- date et lieu d'établissement de la fiche signalétique ;
- nature de l'affaire et référence de la procédure.

Critères d'inscription dans ce fichier

L'enregistrement des empreintes ou traces est réalisé dans le cadre d'une enquête pour crime ou délit, d'une enquête préliminaire, d'une commission rogatoire ou de l'exécution d'un ordre de recherche délivré par une autorité judiciaire.

Combien de temps sont conservées les informations ?
- 40 ans pour les personnes définitivement condamnées, les personnes décédées, les personnes disparues, pour les personnes ayant bénéficié d'une décision de classement sans suite, non-lieu, relaxe ou acquittement pour trouble mental ainsi que les traces biologiques,
- 25 ans pour les personnes mises en cause,
- 25 ans pour les empreintes génétiques des ascendants ou descendants.

Qui est responsable de ce fichier ?

La Direction centrale de la police judiciaire (DCPJ) du ministère de l'Intérieur, sous le contrôle d'un magistrat.

Qui peut consulter ce fichier ?
- Les personnels habilités de la Sous-direction de la police technique et scientifique de la Direction centrale de la police judiciaire, de la Police nationale et ceux de la Gendarmerie nationale,
- Les personnes affectées au Service central de préservation des prélèvements biologiques,
- Les agents spécialement habilités d'organismes de coopération internationale en matière de police judiciaire ou des services de police ou de justice d'états étrangers dans les conditions prévues par l'article R.53-19-1 du code de procédure pénale.

[1] *CNIL, avis du 7 avril 2015, portant sur un projet de dispositions législatives visant à créer un Fichier national des auteurs d'infractions terroristes (FIJAIT).*

Comment obtenir communication et/ou rectification des données ?
Pour accéder aux données du FNAEG, il faut écrire au Directeur central de la police judiciaire.

Pour obtenir l'effacement des données du FNAEG, avant l'expiration de la durée de conservation, il faut faire une demande d'effacement au procureur de la République par lettre recommandée avec demande d'avis de réception ou déclaration au greffe.

En cas de refus d'effacement, il existe une possibilité de recours devant le Juge des libertés et de la détention puis, en cas de nouveau refus, devant le Président de la chambre de l'instruction.

Le ministère de la Justice a mis en ligne des formulaires de demande d'effacement d'un signalement au FNAEG et de demande d'effacement de données enregistrées concernant les parents de personnes disparues (à adresser au procureur de la République, au Juge des libertés et de la détention, au Président de la chambre de l'instruction).

Le refus de personnes concernées de se soumettre à un prélèvement destiné à obtenir une empreinte génétique constitue une infraction.

Lorsque le prélèvement concerne les ascendants ou les descendants d'une personne disparue, leur accord préalable doit être recueilli par procès-verbal.

La CNIL est destinataire d'un rapport annuel d'activité mentionnant notamment les résultats des opérations de mise à jour et d'apurement du fichier.

Le Système d'analyse et de liens de la violence associée au crime (SALVAC)
Cadre juridique et finalités
Le SALVAC trouve son fondement dans l'article 21-1 de la loi du 18 mars 2003 pour la Sécurité intérieure, introduit par l'article 30 de la loi du 12 décembre 2005 relative au traitement de la récidive des infractions pénales.

Son champ d'application est limité aux crimes et délits les plus graves, passibles de plus de cinq ans de prison (pour les atteintes aux personnes) ou sept ans de prison (pour les atteintes aux biens).

La finalité du traitement consiste à opérer des rapprochements entre les procédures judiciaires afin d'identifier et poursuivre les auteurs des crimes ou délits commis « en série », dans le domaine de la criminalité violente (meurtre, assassinat, actes de tortures et de barbarie, viol, agression sexuelle, atteinte sexuelle sur mineur, etc.).

Données enregistrées et durées de conservation
- Concernant les suspects et les tiers (témoins et relations de l'agresseur), les données enregistrées sont : état civil, adresse, photographie.
- Concernant la victime et le mis en cause les données enregistrées sont : état civil, adresse, lieux fréquentés, numéros de téléphone, apparence physique, photographie, mode de vie.
- La durée de conservation des données est de 40 ans.

Modalités d'alimentation et de consultation
L'alimentation et les consultations sont effectuées par une équipe qui comprend 15 policiers et gendarmes de l'Office central pour la répression des violences aux personnes (OCRVP), spécialement habilités. Les données alimentant chaque dossier sont fournies par les services enquêteurs à partir d'un questionnaire détaillé.

Exemple d'affaire
En 2009, le SALVAC a permis d'identifier et d'interpeller un violeur pédophile récidiviste, dit le « violeur des stades », auteur de plusieurs viols d'enfants en région parisienne. Cette affaire a été traitée en collaboration avec les enquêteurs de la sûreté départementale de la Seine-Saint-Denis et de la brigade de protection des mineurs de la direction régionale de la police judiciaire de Paris.

LES FICHIERS DE RAPPROCHEMENT

Ces logiciels permettent, à travers une base de données aux entrées multiples, de créer des relations entre toutes les informations contenues dans les fichiers.

CORAIL, LUPIN et ANACRIM
La Cellule de rapprochement et d'analyse des infractions liées (CORAIL) diffuse aux services d'enquêtes les fiches relatives à des faits sériels, sous forme d'états opérationnels tirés des infractions afin de faciliter les rapprochements.
Elle exploite un Logiciel d'uniformisation des procédures d'identification nommé LUPIN, qui permet aux policiers et aux gendarmes de procéder à des rapprochements à partir de données de police technique et scientifique relatives aux modes opératoires observés et aux éléments recueillis sur les scènes d'infraction.

La gendarmerie dispose parallèlement d'un logiciel d'analyse criminelle (ANACRIM) qui fonctionne à partir de fichiers temporaires d'investigation criminelle élaborés exclusivement dans le cadre de procédures judiciaires. La Préfecture de police de Paris dispose aussi de son propre logiciel de traitement des informations sensibles.

Le principe retenu est celui de leur conservation « pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées ». En fait, ces fichiers sont des fichiers de souveraineté. En effet, ils intéressent « la sûreté de l'État, la défense ou la sécurité publique ».

Le fichier Automatisation de la consultation centralisée de renseignements et de données (ACCRED)

ACCRED autorise le ministre de l'Intérieur à mettre en œuvre un traitement de données à caractère personnel ayant pour objet de faciliter la réalisation des enquêtes administratives prévues aux articles L. 114-1, L. 114-2 et L. 211-11-1 du Code de la Sécurité intérieure par le Service national des enquêtes administratives de sécurité de la DGPN et par le Commandement spécialisé pour la sécurité nucléaire de la DGGN et d'exploiter les informations recueillies dans ce cadre.
Il définit les finalités de ce traitement, la nature et la durée de conservation des données enregistrées, les catégories de personnes ayant accès aux données ainsi que celles qui en sont destinataires.
Il précise également le droit d'accès aux données ainsi que les modalités de traçabilité de ces accès.

2. LES FICHIERS DE RENSEIGNEMENT

Un fichier de renseignement n'est pas un fichier judiciaire. Le simple fait de figurer dans un fichier de renseignement ne veut pas dire grand-chose en soi, ce qui compte ou peut poser problème, c'est l'exploitation qui est faite des informations qu'il contient.

Les fichiers de renseignement entrent dans le champ d'application de l'article 26 de la loi du 6 janvier 1978 modifiée, et plus précisément dans les finalités définies au 1° du I dudit article. Il s'agit des traitements de données à caractère personnel « mis en œuvre pour le compte de l'État qui intéressent la sûreté de l'État, la Défense ou la sécurité publique ».

Dès lors, ces fichiers doivent être autorisés par un texte réglementaire pris après avis de la CNIL. Le régime général est la création par arrêté du ministre compétent : le ministère de l'Intérieur le plus souvent, mais cela peut être également le ministère de la Défense, de l'Économie, ou de la Justice.
Cependant, si le traitement porte sur des données sensibles, un décret en Conseil d'État est nécessaire.

Dans la majorité des cas, le pouvoir exécutif fait également application, pour les fichiers de renseignement, des dispositions du III de l'article 26 de la loi, qui permettent de dispenser de publication les actes en portant création. Cette dispense doit intervenir par décret en Conseil d'État.

Étrangement, aucune précision sur le champ d'application exact des dispositions du III de l'article 26 ne figure dans la Loi « informatique et libertés » ou dans le décret d'application.
Potentiellement, tous les traitements relevant du I ou du II du même article pourraient donc ainsi être dispensés de publication, alors même qu'il s'agit d'une exception majeure à l'équilibre du texte de la loi du 6 janvier 1978 telle qu'elle a été modifiée en 2004.

En outre, l'absence de publication d'un tel acte a pour corollaire l'absence de publication de l'avis motivé de la CNIL sur ce texte. Ainsi, le III de l'article 26 dispose : « pour ces traitements, est publié, en même temps que le décret autorisant la dispense de publication de l'acte, le sens de l'avis émis par la commission ».

Dans ce cas, conformément aux dispositions de l'article 83 du décret d'application, le sens de l'avis de la CNIL ne peut porter que trois mentions : «favorable », « favorable avec réserve » ou « défavorable ».
Ainsi, pour les fichiers dispensés de publication, la Commission adopte une délibération similaire aux autres délibérations portant sur des traitements relevant de l'article 26 (c'est-à-dire motivées), dans laquelle elle doit indiquer le sens de l'avis qui devra être publié en même temps que le décret en Conseil d'État dispensant de publication l'acte réglementaire créant le fichier en question.

Pour rappel, la CNIL dispose d'un pouvoir de contrôle sur tous les traitements de données qui relèvent de la loi « informatique et libertés ». Ses pouvoirs et ses modalités d'exercice sont définis à l'article 44 de la loi « informatique et libertés », et aux articles 57 à 69 du décret d'application.

Le dernier alinéa de l'article 44 prévoit cependant une exception pour « les traitements intéressant la sûreté de l'État et qui sont dispensés de la publication de l'acte réglementaire qui les autorise ».

Dans ce cas, le décret en Conseil d'État qui prévoit cette dispense peut également prévoir que le traitement n'est pas soumis au pouvoir de contrôle a posteriori de la CNIL.

Enfin, certains fichiers grâce à leurs interconnexions permettent de reconstituer le profil des délinquants. C'est le cas du SALVAC (cf. supra) et du FBS (Fichier des Brigades Spécialisées).

Le Fichier des Brigades Spécialisées (FBS)

Cadre juridique et finalités

Le FBS est à la fois un, « fichier d'objectifs » et un « fichier de travail » créé en 1991 pour les services de police spécialisés luttant contre la grande délinquance et le crime organisé (banditisme, terrorisme, stupéfiants, proxénétisme, trafics d'œuvres d'art, de fausse monnaie, blanchiment, grande délinquance financière, immigration clandestine).

Les finalités du FBS sont :
- de collecter des informations sur l'environnement et les habitudes des délinquants spécialisés ;
- de favoriser la coopération des services en assurant la confidentialité nécessaire grâce aux notions de visibilité, sensibilité et de « copropriété ».

Il a pour objectif d'utiliser au mieux les diverses informations collectées à l'occasion de la surveillance du milieu criminel, de permettre des échanges confidentiels entre services spécialisés et d'autoriser tous les croisements de recherche possibles entre les informations figurant dans la base

Données enregistrées et durées de conservation

Les informations collectées à l'occasion de la surveillance du milieu criminel sont conservées 20 ans.

Modalités d'alimentation et de consultation

Le FBS est actuellement utilisé par les directions interrégionales de la police judiciaire, par la plupart des offices centraux de police judiciaire (DCPJ) et par les brigades centrales de la préfecture de police de Paris.

Le FBS n'est jamais utilisé dans le cadre d'enquêtes administratives. Il est alimenté et consulté exclusivement dans un cadre judiciaire pour la lutte contre la grande délinquance et la criminalité organisée.

Exemple d'affaire

Le 26 février 2008, l'Office central de lutte contre le crime organisé (OCLCO) était sollicité par la Belgique pour identifier une femme auteur d'un vol à main armée commis dans une agence bancaire. Une photographie extraite de la vidéosurveillance était jointe à la demande.

Le mode opératoire était le suivant : la femme se présentait une première fois sous prétexte de prendre rendez-vous afin d'ouvrir un compte, repérait les lieux et revenait le lendemain s'emparer de la caisse en exhibant une arme de poing. Les recherches conduites pour faire suite à la demande des autorités belges ont entraîné une consultation du FBS en utilisant comme critère les mots « téléphone » et « banque » dans la rubrique « banditisme ».

Le FBS a alors fait apparaître l'affaire de la synthèse de l'OCRB et a permis d'identifier la femme recherchée, interpellée le 18 juin 2008 alors qu'elle s'apprêtait à commettre un autre vol à main armée.

Précédemment, en 1998, l'Office central pour la répression du banditisme (OCRB) avait assisté la PJ de Bordeaux pour interpeller un couple de braqueurs qui utilisait le même mode opératoire du rendez-vous préalable. Cette affaire avait fait l'objet d'une synthèse nationale de l'OCRB.

Le fichier Centralisation du renseignement intérieur pour la sécurité du territoire et des intérêts nationaux (CRISTINA)

Ce fichier est moins connu que sa sœur EDVIGE (Exploitation documentaire et valorisation de l'information générale[1]) et de ce fait paraît comme plus dangereux.
Très peu d'informations sont disponibles, hormis le fait que sa gestion relève de la responsabilité Direction générale de la sécurité intérieure (DGSI).
En effet, CRISTINA est issue de la fusion, en 2008, des fichiers de la Direction centrale des Renseignements Généraux (DCRG) et la Direction de la Surveillance du Territoire (DST).
Nous savons que ce fichier contient des données personnelles sur les personnes fichées et leur entourage, mais étant classé « secret-défense », il n'est pas soumis à la vigilance de CNIL, à qui il a été permis ce seul commentaire apparaissant dans le JO : « avis favorable avec réserves ».

CRISTINA couvre l'ensemble des champs d'intérêt de la DGSI, dont les quatre missions principales, relevant de l'intérêt de la Nation, sont :
- la lutte contre l'espionnage et les ingérences étrangères ;
- la lutte contre le terrorisme ;
- la protection du patrimoine et la sécurité économique ;
- la surveillance des mouvements subversifs violents et des phénomènes de société précurseurs de menaces.

Ce fichier qui n'échappe pas à la vigilance de la CNIL mais est toutefois dispensé de contrôle a posteriori. Les informations qu'il contient ne sont évidemment pas publiques tout en ne relevant pas du secret-défense.

Le fichier Prévention d'atteinte à la sécurité publique (PASP)

Le PASP a pour finalité de recueillir, conserver et analyser les informations qui concernent des personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique, notamment les personnes susceptibles d'être impliquées dans des actions de violence collectives, en particulier en milieu urbain ou à l'occasion de manifestations sportives. C'est le ministère de l'Intérieur qui est responsable de ce fichier.

[1] Projet de fichier de police informatisé créé en juin 2008 et retiré en novembre de la même année. Le fichier EDVIGE devait recenser les personnes « ayant sollicité, exercé ou exerçant un mandat politique, syndical ou économique ou qui jouent un rôle institutionnel, économique, social ou religieux significatif ». Les données n'auraient pu être collectées que pour des personnes « dont l'activité individuelle ou collective » peut « porter atteinte à la sécurité publique » et pour celles « entretenant ou ayant entretenu des relations non fortuites avec elles ». Il aurait visé également « des personnes travaillant dans des secteurs ou des domaines sensibles », faisant à ce titre l'objet d'enquêtes administratives

Informations contenues dans ce fichier
Les catégories de données à caractère personnel suivantes peuvent être enregistrées :
- motif de l'enregistrement ;
- informations ayant trait à l'état civil, à la nationalité et à la profession, adresses physiques, numéros de téléphone et adresses électroniques ;
- signes physiques particuliers et objectifs, photographies ;
- titres d'identité ;
- immatriculation des véhicules ;
- informations patrimoniales ;
- agissements susceptibles de recevoir une qualification pénale ;
- personnes entretenant ou ayant entretenu des relations directes et non fortuites avec l'intéressé.

Par dérogation au I de l'article 8 de la loi du 6 janvier 1978 modifiée, pour les seules fins et dans le strict respect des conditions définies par le décret, la collecte, la conservation et le traitement des données dites sensibles peuvent avoir lieu :
- signes physiques particuliers et objectifs comme éléments de signalement des personnes ;
- origine géographique ;
- activités politiques, philosophiques, religieuses ou syndicales.

Cadre juridique
Dans sa délibération, la CNIL a rappelé que la « sécurité publique » peut s'analyser comme « l'élément de l'ordre public caractérisé par l'absence de périls pour la vie, la liberté ou le droit de propriété des individus ».

Le GIPASP
Le PASP est complété par le GIPASP (Gestion de l'information et la prévention des atteintes à la sécurité publique), logiciel qui en permet le traitement des données.

Le Fichier des signalements pour la prévention et la radicalisation à caractère terroriste (FSPRT)
Le FSPRT est considéré par le décret du 7 octobre 2016 comme un fichier de renseignement et contient environ 17 000 noms. Ce fichier, peu connu, a un rôle essentiel dans la lutte contre le terrorisme. Outre l'identité de la personne, il contient sa localisation, ses antécédents judiciaires et éventuellement sa situation psychiatrique. Il y aurait dans ce fichier environ 20 000 mineurs dont le plus jeune aurait onze ans. Il est alimenté par l'Unité de coordination de lutte antiterroriste (UCLAT) et par la plateforme de signalement du Centre national d'assistance et de prévention de la radicalisation (CNAPR), qui gère la plateforme téléphonique nationale de signalement[1]. Ils sont suivis par le SCRT et les gendarmes. Les plus dangereux d'entre eux sont fichés « S » dans une liste qui est une sous-catégorie du fichier des personnes recherchées « FPR ».

La mesure de la radicalisation n'est pas une science exacte. On ne peut guère se fonder que sur les signalements traités par l'UCLAT pour avoir une vue globale de la situation.

Les chiffres qui suivent sont actualisés à la date du 1er mars 2017.

Individus inscrits au fichier de traitement des signalements pour la prévention de la radicalisation à caractère terroriste (FSPRT)
Au total, 17 393 individus étaient inscrits au FSPRT, dont :
- 7 400 individus signalés par les préfectures via les états-majors de sécurité (EMS) ;
- 5 346 individus signalés par le public via le CNAPR ;
- 5 799 objectifs inscrits par des services de police ou gendarmerie.

Tous ces individus ne sont pas nécessairement contrôlés en permanence. Un certain nombre d'entre eux sont dits « clôturés » : les services estiment qu'ils ne nécessitent plus de surveillance, mais ils demeurent dans le FSPRT du fait des signes de radicalisation ayant été constatés.
D'autres encore sont dits « en veille » : ils ne nécessitent plus de suivi actif mais restent néanmoins attribués à un service.

Origine des signalements validés par le CNAPR
Sur 5 651 signalements validés par le CNAPR :
- 3 939 provenaient d'appels au numéro vert ;
- 770 provenaient du formulaire internet du site du ministère de l'Intérieur ;
- 941 provenaient des courriels des services de police et de gendarmerie.

Par ailleurs, 2 046 individus ont été formellement identifiés sur une zone de combat en Syrie et en Irak et 249 individus présumés décédés ont été recensés[2].

Le Fichier des personnes recherchées (FPR)
Le FPR est davantage un outil pour les services de renseignement qu'un véritable fichier. C'est un fichier de signalement qui ne permet pas d'accumuler des informations sur les personnes surveillées. En recensant toutes les personnes faisant l'objet d'une mesure de recherche ou de vérification de leur situation juridique, le FPR sert à faciliter les recherches effectuées par les services de police et de gendarmerie à la demande des autorités judiciaires, militaires ou administratives. Le ministère de l'Intérieur est responsable de ce fichier.

Données enregistrées et durées de conservation
L'inscription au FPR intervient 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 (étrangers : mesure d'expulsion, opposition à l'entrée sur le territoire) ; législation fiscale ; protection des personnes (recherches de personnes disparues à la demande d'un membre de leur famille, etc.)
- d'ordre public (prévention de menaces contre la sécurité publique ou la sûreté de l'État).

[1] *Jean-Marie Bockel et Luc Carvounas, Les collectivités territoriales et la prévention de la radicalisation, Rapport d'information n° 483 (2016-2017), fait au nom de la Délégation aux collectivités territoriales, Assemblée nationale, 29 mars 2017.*
[2] *Ibid*

Sans donner lieu à inscription, le FPR est également consulté lors de l'instruction des demandes de carte nationale d'identité, de passeport, de titre de séjour ou encore de visa.
Les informations enregistrées sont :
- l'identité de la personne recherchée,
- son signalement et éventuellement sa photographie,
- le motif de la recherche,
- la conduite à tenir en cas de découverte des personnes recherchées.

Le FPR est divisé en vingt et un sous-fichiers regroupant les personnes concernées en fonction du fondement juridique de la recherche.

Modalités de consultation et d'alimentation
Ont accès au FPR les services dûment habilités de la Direction générale de la police nationale ou la Direction générale de la gendarmerie nationale, ainsi que, dans le cadre de leurs attributions, les préfectures.

La mise à jour des informations est réalisée à l'initiative du service ayant demandé l'inscription. La radiation des personnes inscrites doit en particulier être effectuée sans délai en cas de découverte ou d'extinction du motif de la recherche.
- Les durées de conservation dépendent du motif d'enregistrement.
- Les radiations sont opérées sans délai en cas de découverte de la personne ou d'extinction du motif de l'inscription.

Peuvent seuls être destinataires de la totalité ou d'une partie de ces informations dans le cadre de leurs compétences :
- les autorités judiciaires,
- les services de police, de gendarmerie et des douanes,
- les autorités administratives pour les seules recherches relevant de leurs attributions
- les services de police d'États liés à la France par une convention ou un accord international leur autorisant l'accès à tout ou partie des informations enregistrées dans le fichier des personnes recherchées.

Comment obtenir communication et/ou rectification des données ?
Le droit d'accès au FPR est mixte. Le droit d'accès est direct pour les personnes inscrites pour des raisons n'intéressant par la sûreté de l'État, la défense ou la sécurité publique (personnes faisant l'objet d'une décision judiciaire mentionnée à l'article 230-19 2 à 13 du code de procédure pénale), les personnes mineures faisant l'objet d'une opposition à la sortie de territoire ou ayant quitté le domicile/soustraites à l'autorité des personnes en ayant la garde, les personnes débitrices de l'État, les personnes disparues, les personnes interdites de stade et les personnes mentionnées à l'article 2 IV du décret du 28 mai 2010. Dans les autres cas, le droit d'accès est indirect et doit passer par la CNIL.

GESTEREXT
Le décret n° 2017-1218 du 2 août 2017[1] porte création d'un traitement automatisé de données à caractère personnel dénommé GESTEREXT (Gestion du terrorisme et des extrémismes violents) mis en œuvre par la préfecture de police.

Il est inscrit dans la liste des traitements de données à caractère personnel bénéficiant d'une déclaration simplifiée, bénéficie de la dispense de publication de l'acte réglementaire et ne peut faire l'objet d'un contrôle sur pièce et sur place de la Commission nationale de l'informatique et des libertés (CNIL). Le décret prévoit que les requêtes relatives à la mise en œuvre du droit d'accès de ce traitement relèvent de la compétence du Conseil d'État.

Les fichiers de Défense
Les fichiers relevant du ministère de la Défense sont ceux de la Direction générale de la sécurité extérieure (DGSE) - en charge du renseignement extérieur -, de la Direction du renseignement et de la sécurité de la Défense (DRSD) - en charge de la contre-ingérence dans les unités et installations relevant du ministère de la Défense - et de la Direction du renseignement militaire (DRM).

Le Décret n° 2007-914 du 15 mai 207[2] liste les traitements automatisés de données à caractère personnel intéressant la sûreté de l'État, la défense ou la sécurité publique. Parmi ceux-ci il identifie six fichiers de renseignement relevant des services du ministère de la Défense :
- *Fichiers d'informations nominatives mis en œuvre par la DGSE,*
- *Traitement automatisé d'informations nominatives « fichier de la DGSE » mis en œuvre par la DGSE,*
- *Traitement automatisé d'informations nominatives « fichier du personnel de la DGSE » mis en œuvre par la DGSE,*
- *Traitement automatisé de données à caractère personnel dénommé SIREX mis en œuvre par la DRSD,*
- *Fichier d'informations nominatives mis en œuvre par la DRM,*
- *Traitement automatisé d'informations nominatives de personnes étrangères mis en œuvre par la DRM.*

Aucun de ces fichiers n'est « secret-défense » en tant que tel, mais les informations qui y figurent peuvent être couvertes par le secret de la Défense nationale.
Ces fichiers ne sont pas accessibles aux policiers ni aux gendarmes. Ils ne peuvent être consultés que par les membres de chacun des services concernés dès lors que leur fonction les y autorise (besoin d'en savoir, habilitation).

---

[1] *Décret n° 2017-1218 du 2 août 2017 modifiant les articles R. 211-32 et R. 841-2 du code de la sécurité intérieure et le 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 (JORF n°0180 du 3 août 2017, texte n° 8).*

[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 (version consolidée au 10 octobre 2017).*

Niveaux de classification
Ces fichiers Défense comprennent trois niveaux de classification :
- Très Secret-Défense, qui est réservé aux informations et supports concernant les priorités gouvernementales en matière de défense et de sécurité nationale et dont la divulgation est de nature à nuire très gravement à la défense nationale ;
- Secret-Défense, qui est réservé aux informations et supports dont la divulgation est de nature à nuire gravement à la défense nationale ;
- Confidentiel-Défense, qui est réservé aux informations et supports dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale classifié au niveau Très Secret-Défense ou Secret-Défense.

Les informations et supports classifiés portent la mention de leur niveau de classification outre, le cas échéant, une mention particulière précisant les États, leurs ressortissants ou les organisations internationales pouvant y avoir accès. Les informations et supports classifiés qui ne doivent en aucun cas être communiqués totalement ou partiellement à des organisations internationales, à des États étrangers ou à leurs ressortissants portent, en sus de la mention de leur niveau de classification, la mention particulière « Spécial France ». Nul n'est qualifié pour connaître des informations et supports classifiés s'il n'a pas fait au préalable l'objet d'une décision d'habilitation.

En derniers recours, la Commission consultative du secret de la Défense nationale (CCSDN) est l'autorité administrative indépendante chargée de donner un avis sur la classification du secret-défense.

Les autres fichiers de renseignement
Le Décret n° 2007-914 du 15 mai 2007 signale également l'existence de deux fichiers de renseignement au sein du ministère de l'Économie et des finances et d'un au sein du ministère de la Justice.
- *Traitement automatisé de données à caractère personnel dénommé BCR-DNRED* au profit de la Direction nationale du renseignement et des enquêtes douanières (DNRED) ;
- *Traitement automatisé de données à caractère personnel dénommé STARTRAC* mis en œuvre par le service à compétence nationale TRACFIN (Traitement du renseignement et action contre les circuits financiers clandestins) ;
- *Traitement automatisé de données à caractère personnel relatif au suivi des personnes placées sous main de justice et destiné à la prévention des atteintes à la sécurité pénitentiaire et à la sécurité publique dénommé CAR* mis en œuvre par la Direction de l'administration pénitentiaire.

CONCLUSION

Le secret est-il compatible avec la démocratie ?

La Cour européenne des Droits de l'Homme répond par l'affirmative dans un arrêt du 6 septembre 1978 (Klass et autres c., Allemagne) : « *Les sociétés démocratiques qui se trouvent menacées de nos jours par des formes très complexes d'espionnage et par le terrorisme doivent être capables pour combattre efficacement ces menaces de surveiller en secret les éléments subversifs opérant sur son territoire* ».
Néanmoins, tout citoyen doit être attentif aux fichiers de police afin de se protéger des risques d'intervention de l'État.

L'informatisation des fichiers est bien évidemment l'élément essentiel qui a bouleversé le recueil des données personnelles et les possibilités d'interconnexion entre les fichiers.
Mais les principes posés en 1978 en créant la CNIL n'ont pas vieilli. Les données collectées dans les traitements automatisés doivent l'être « *pour des finalités pertinentes déterminées explicites et légitimes* » ; elles doivent être « *adéquates pertinentes et non excessives* » au regard de ces finalités, tout en étant « *exactes complètes et, si nécessaire, mises à jour* » ; enfin, elles doivent être conservées « *pendant une durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées* ». Le tableau qui vient d'être présenté montre que ces grands principes ont été respectés.

En septembre 2017, le ministre de l'Intérieur, Gérard Collomb a déclaré vouloir poursuivre la réflexion sur l'utilisation des fichiers de renseignement dans le cadre de la lutte anti-terroriste. « *Le cadre juridique et technique de l'utilisation des fichiers, notamment du FSPRT, pour prévenir les actes terroristes et empêcher l'exercice de certains emplois, l'accès à certains lieux, ou encore l'acquisition et la détention d'armes par des personnes dont le comportement justifie ces restrictions, sera consolidé* », souligne la feuille de route transmise aux préfets, sans donner davantage de précisions sur les modalités de cette réflexion. Cela traduit néanmoins la préoccupation du gouvernement de ne pas déroger à la loi.

GLOSSAIRE

ACCRED	Automatisation de la consultation centralisée de renseignements et de données
ADN	Acide désoxyribonucléique
AGRIPPA	Application nationale de gestion du répertoire informatisé des propriétaires et possesseurs d'armes.
ANACRIM	Logiciel d'analyse criminelle (gendarmerie)
BCR-DNRED	Traitement automatisé de données à caractère personnel au profit de la DNRED
CAR	Traitement automatisé de données à caractère personnel relatif au suivi des personnes placées sous main de justice et destiné à la prévention des atteintes à la sécurité pénitentiaire et à la sécurité publique
CASSIOPEE	Chaine applicative supportant le système d'information orienté procédure pénale et enfants
CCSDN	Commission consultative du secret de la Défense nationale
CNIL	Commission Informatique et Libertés
CNPR	Centre national de la prévention de la radicalisation
CCSDN	Commission consultative du secret de la Défense nationale
CORAIL	Cellule de rapprochement et d'analyse des infractions liées
CPP	Code de procédure pénale
CRISTINA	Centralisation du renseignement intérieur pour la sécurité du territoire et des intérêts nationaux
DCPJ	Direction centrale de la police judiciaire
DCRG	Direction centrale des Renseignements généraux
DCSP	Direction centrale de la sécurité publique
DGGN	Direction générale de la gendarmerie nationale
DGPN	Direction générale de la police nationale
DGSE	Direction générale de la sécurité extérieure
DGSI	Direction générale de la sécurité intérieure
DNRED	Direction nationale du renseignement et des enquêtes douanières
DRM	Direction du renseignement militaire
DRSD	Direction du renseignement et de la sécurité de la Défense
DST	Direction de la surveillance du territoire
EDVIGE	Exploitation documentaire et valorisation de l'information générale
FAED	Fichier automatisé des empreintes digitales (FAED)
FBS	Fichier des Brigades Spécialisées
FFV	Fichier des véhicules volés
Fiches « S »	Sous-catégorie du fichier des personnes recherchées (FPR).
FIJAISV	Fichier judiciaire national automatisé des auteurs d'infractions sexuelles
FIJAIT	Fichier judiciaire national automatisé des auteurs d'infractions terroristes
FINIADA	Fichier national des personnes interdites d'acquisition et de détention d'armes
FNAEG	Fichier national des empreintes génétiques
FCJNI	Fichier du casier judiciaire national informatisé
FNFM	Fichier national de faux monnayage
FNI	Fichier national des immatriculations
FOVeS	Fichier des objets volés et signalés
FPR	Fichier des personnes recherchées
FSPRT	Fichier des signalements pour la prévention et la radicalisation à caractère terroriste
GESTEREXT	Gestion du terrorisme et des extrémismes violents
GIPASP	Gestion de l'information et la prévention des atteintes à la sécurité publique
JUDEX	Système judiciaire de documentation et d'exploitation (gendarmerie)
JO	Journal officiel

GLOSSAIRE (suite)

LUPIN	Logiciel d'uniformisation des procédures d'identification
LOPPSI	Loi d'orientation et de programmation pour la performance de la sécurité intérieure
OCLCO	Office central de lutte contre le crime organisé
OCRB	Office central pour la répression du banditisme
OCRVP	Office central pour la répression des violences aux personnes
PASP	Prévention d'atteinte à la sécurité publique
SALVAC	Système d'analyse et de liens de la violence associée au crime
SCRT	Service central du renseignement territorial
STARTRAC	Traitement automatisé de données à caractère personnel mis en œuvre par TRACFIN
STIC	Système de traitement des infractions constatées (police)
TAJ	Traitement des antécédents judiciaires
TES	Titres électroniques sécurisés
TRACFIN	Traitement du renseignement et action contre les circuits financiers clandestins
UCLAT	Unité de coordination de lutte antiterroriste

ANNEXE

PRÉSENTATION DE LA CNIL ET DE SES MISSIONS

Autorité administrative indépendante créée en 1978 par la loi Informatique et Libertés, la Commission Nationale Informatique et Libertés (CNIL) accompagne les professionnels dans leur mise en conformité et aide les particuliers à maîtriser leurs données personnelles et exercer leurs droits. Elle analyse l'impact des innovations technologiques et des usages émergents sur la vie privée et les libertés. Enfin, elle travaille en étroite collaboration avec ses homologues européens et internationaux pour élaborer une régulation harmonisée.

Missions de la CNIL
La CNIL a 4 missions principales :

Informer/protéger
La CNIL informe les particuliers et les professionnels et répond à leurs demandes. Elle met à leur disposition des outils pratiques et pédagogiques et intervient très régulièrement pour animer des actions de formation et de sensibilisation, notamment dans le cadre de l'éducation au numérique. Toute personne peut s'adresser à la CNIL en cas de difficulté dans l'exercice de ses droits.

Elle a pour mission de promouvoir l'utilisation des technologies protectrices de la vie privée, notamment les technologies de chiffrement des données.

Accompagner/conseiller
La régulation des données personnelles passe par différents instruments qui poursuivent tous un objectif de mise en conformité des organismes : avis sur des projets de loi ou de décret, autorisation pour les traitements les plus sensibles, recommandations fixant une doctrine, cadres juridiques simplifiant les formalités préalables, réponse à des demandes de conseils.
La CNIL propose également une boîte à outils aux organismes qui souhaitent aller plus loin dans leur démarche de conformité : correspondants informatique et libertés (CIL), labels, packs de conformité (référentiels sectoriels), BCR (Binding Corporate Rules) qui encadrent les transferts de multinationales hors de l'Union Européenne.

Elle certifie la conformité des processus d'anonymisation des données personnelles dans la perspective de leur mise en ligne et de leur réutilisation.

Contrôler et sanctionner
Le contrôle sur place, sur pièces, sur audition ou en ligne permet à la CNIL de vérifier la mise en œuvre concrète de la loi.

Un programme des contrôles est élaboré en fonction des thèmes d'actualité, des grandes problématiques identifiées et des plaintes dont la CNIL est saisie.

La CNIL est compétente pour contrôler les systèmes de vidéoprotection autorisés par les préfectures.

Lors d'un contrôle sur place, la CNIL peut :
- accéder à tous les locaux professionnels,
- demander communication de tout document nécessaire et d'en prendre copie,
- recueillir tout renseignement utile et entendre toute personne,
- accéder aux programmes informatiques et aux données.

À l'issue des contrôles, le président de la CNIL peut décider des mises en demeure. La formation restreinte de la CNIL, composée de 5 membres et d'un Président distinct du président de la CNIL, peut prononcer diverses sanctions à l'issue d'une procédure contradictoire : une sanction pécuniaire (sauf pour les traitements de l'État) d'un montant maximal de 3 millions d'euros. Cette sanction peut être rendue publique ; la formation restreinte peut également ordonner l'insertion de sa décision dans la presse, ou ordonner que les organismes sanctionnés informent individuellement les personnes concernées aux frais de l'organisme sanctionné. Le montant des amendes est perçu par le Trésor Public et non par la CNIL.

La formation restreinte de la CNIL peut également prononcer :
- Une injonction de cesser le traitement.
- Un retrait de l'autorisation accordée par la CNIL.

En cas d'atteinte grave et immédiate aux droits et libertés, le président de la CNIL peut demander, par référé, à la juridiction compétente, d'ordonner toute mesure nécessaire. Il peut également dénoncer au Procureur de la République les infractions à la législation dont il a connaissance.

Anticiper
Dans le cadre de son activité d'innovation et de prospective, la CNIL met en place une veille pour détecter et analyser les technologies ou les nouveaux usages pouvant avoir des impacts importants sur la vie privée. Elle dispose d'un laboratoire lui permettant d'expérimenter des produits ou applications innovants. Elle contribue au développement de solutions technologiques protectrices de la vie privée en conseillant les entreprises le plus en amont possible, dans une logique de Privacy by Design. Pour renforcer sa réflexion, elle a créé un comité de la prospective faisant appel à des experts extérieurs qui la conseillent pour élaborer un programme annuel d'études et d'explorations.

ANNEXE (suite)

Elle a pour mission de conduire une réflexion sur les problèmes éthiques et les questions de société soulevés par l'évolution des technologies numériques.

Fonctionnement de la CNIL
L'indépendance de la CNIL est garantie par sa composition et son organisation.

Composition de la CNIL
La CNIL se compose d'un collège pluridisciplinaire de 18 membres. 12 de ses 18 membres sont élus ou désignés par les assemblées ou les juridictions auxquelles ils appartiennent.

- 4 parlementaires (2 députés, 2 sénateurs)
- 2 membres du Conseil économique, social et environnemental
- 6 représentants des hautes juridictions (2 conseillers d'État, 2 conseillers à la Cour de cassation, 2 conseillers à la Cour des comptes)
- 5 personnalités qualifiées désignées par le Président de l'Assemblée nationale (1 personnalité), le Président du Sénat (1 personnalité), en Conseil des Ministres (3 personnalités).
- 1 membre de la Commission d'accès aux documents administratifs.

Le mandat des commissaires est de 5 ans ou, pour les parlementaires, d'une durée égale à leur mandat électif.

Organisation
La CNIL élit son Président parmi ses membres ; elle ne reçoit d'instruction d'aucune autorité. Les ministres, autorités publiques, dirigeants d'entreprises, publiques ou privées, ne peuvent s'opposer à son action. Le Président de la CNIL recrute librement ses collaborateurs (195 agents contractuels de l'État).

En 2017, la présidence de la CNIL est assurée par Madame Isabelle Falque-Pierrotin.

Séance plénière
Les membres de la CNIL se réunissent en séances plénières une fois par semaine sur un ordre du jour établi à l'initiative de son Président.

Une partie importante de ces séances est consacrée à l'examen de projets de loi et de décrets soumis à la CNIL pour avis par le Gouvernement. La CNIL autorise également les traitements les plus sensibles.

Formation restreinte
Pour prendre des mesures à l'encontre des responsables de traitement qui ne respectent pas la loi informatique et libertés, la CNIL siège dans une formation spécifique composée de 5 membres et d'un Président distinct du Président de la CNIL.

À l'issue de contrôles ou de plaintes, elle peut prononcer diverses sanctions qui peuvent être rendues publiques : avertissement, sanction pécuniaire, etc.

Adresse
Commission nationale de l'informatique et des libertés (CNIL)
3 Place de Fontenoy
TSA 80715
75334 Paris Cedex 07
Tél : 01 53 73 22 22
www.cnil.fr/fr

Pour plus d'informations sur le suivi par la CNIL des fichiers de police et de renseignement :
www.cnil.fr/fr/thematique/police-justice
www.cnil.fr/fr/tag/Police
www.cnil.fr/fr/tag/Fichiers+de+Police
www.cnil.fr/fr/tag/Renseignement
www.cnil.fr/fr/tag/Justice

Centre Français de Recherche sur le Renseignement

VOCATION /

Fondé en 2000, le CENTRE FRANÇAIS DE RECHERCHE SUR LE RENSEIGNEMENT (CF2R) est un Think Tank indépendant, régi par la loi de 1901, spécialisé sur l'étude du renseignement et de la sécurité internationale.

Il a pour objectifs :

- *le développement de la recherche académique et des publications consacrées au renseignement et à la sécurité internationale,*
- *l'apport d'expertise au profit des parties prenantes aux politiques publiques (décideurs, administration, parlementaires, médias, etc.),*
- *la démystification du renseignement et l'explication de son rôle auprès du grand public.*

ORGANISATION /

Le CF2R est organisé en trois pôles spécialisés, regroupant une vingtaine de chercheurs.

■ **HISTOIRE DU RENSEIGNEMENT qui étudie les activités de renseignement à travers l'histoire :**
- Renseignement et contre-espionnage,
- Actions clandestines et opérations spéciales,
- Interceptions et décryptements,
- Guerre psychologique,
- Tromperie et stratagèmes.

■ **OBSERVATOIRE DU RENSEIGNEMENT qui analyse le fonctionnement du renseignement moderne :**
- Organisation et coordination des services,
- Budget et effectifs,
- Analyses d'opérations,
- Technologies du renseignement,
- Gouvernance et éthique du renseignement,
- Intelligence économique et privatisation du renseignement,
- Contrôle parlementaire.

■ **SÉCURITÉ INTERNATIONALE qui a pour objet l'analyse des grands enjeux de la sécuriét internationale :**
- Terrorisme,
- Conflits,
- Crises régionales,
- Extrémisme politique et religieux,
- Criminalité internationale,
- Cybermenaces,
- Nouveaux risques, etc.

ACTIVITÉS /

■ **RECHERCHE ACADÉMIQUE ET ENCADREMENT DE THÈSES**

L'équipe du CF2R compte 8 docteurs dans des disciplines diverses (droit, science politique, histoire, sciences de l'information, sociologie, psychologie), dont 2 HDR, et encadre des thèses en cotutelle avec plusieurs universités françaises et étrangères.

■ **ORGANISATION DE COLLOQUES, CONFÉRENCES ET DINERS-DÉBAT**

■ **SOUTIEN À LA RECHERCHE**

Chaque année, le CF2R décerne deux prix universitaires qui récompensent les meilleurs travaux académiques francophones consacrés au renseignement :
- le « Prix Jeune chercheur » prime un mémoire de mastère,
- le « Prix universitaire » récompense une thèse de doctorat.

■ **PARTICIPATION À DES RÉUNIONS SCIENTIFIQUES ET COLLOQUES EN FRANCE ET À L'ÉTRANGER**

■ **ACTIONS DE SENSIBILISATION À L'INTENTION DES PARLEMENTAIRES ET DES DÉCIDEURS POLITIQUES ET ÉCONOMIQUES**

■ **FORMATIONS SPÉCIALISÉES**

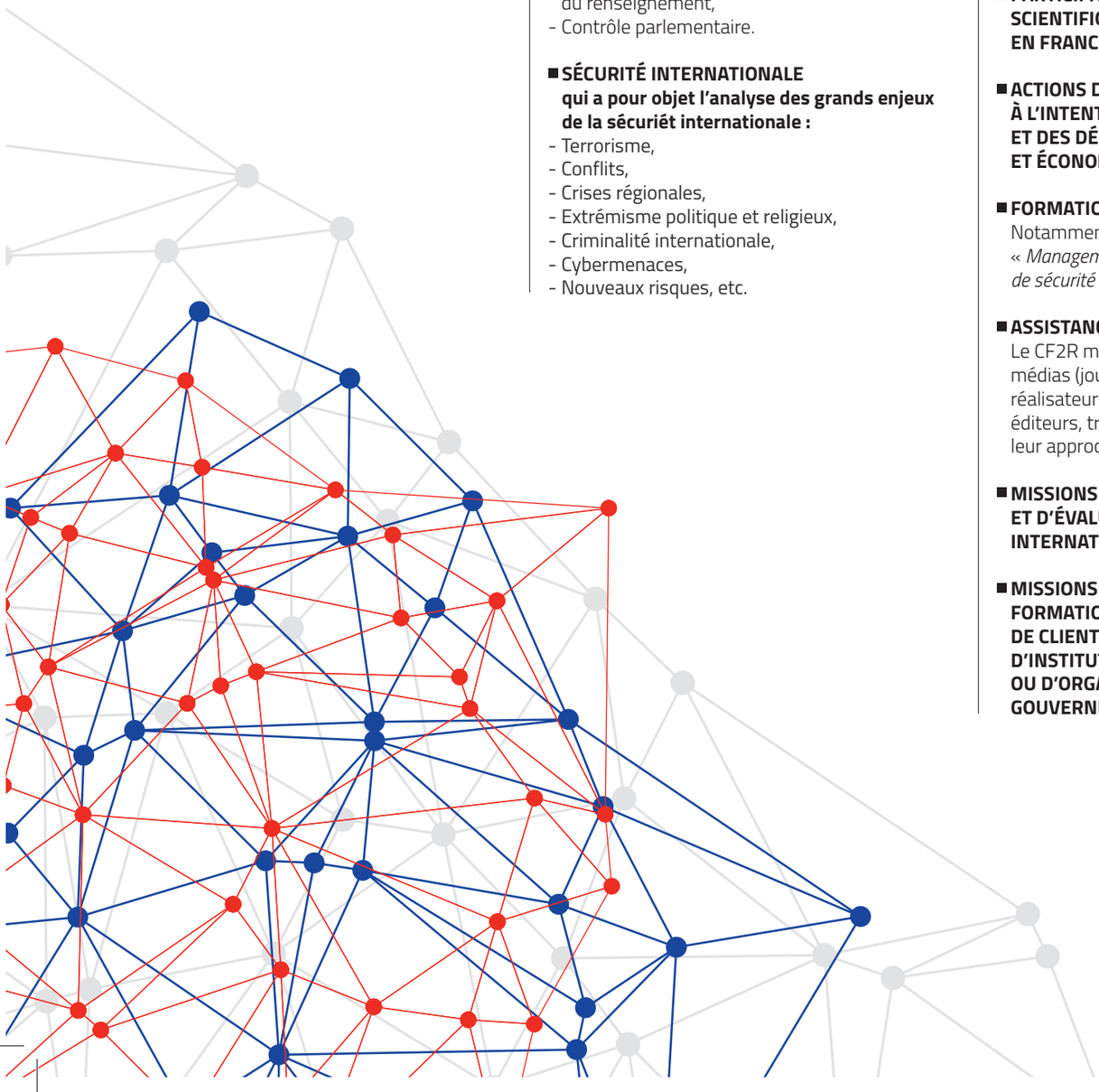
Notamment une session internationale « *Management des agences de renseignement et de sécurité (MARS)* ».

■ **ASSISTANCE AUX MÉDIAS**

Le CF2R met son expertise à la disposition des médias (journalistes), du cinéma (scénaristes, réalisateurs) et de l'édition (romanciers, éditeurs, traducteurs) afin de les éclairer dans leur approche du renseignement.

■ **MISSIONS D'EXPERTISE DE TERRAIN ET D'ÉVALUATION DES CONFLITS INTERNATIONAUX**

■ **MISSIONS DE CONSEIL, D'ÉTUDE ET DE FORMATION AU PROFIT D'ENTREPRISES, DE CLIENTS GOUVERNEMENTAUX, D'INSTITUTIONS INTERNATIONALES OU D'ORGANISATIONS NON GOUVERNEMENTALES**



Centre Français de Recherche sur le Renseignement (CF2R)
21 boulevard Haussmann
75 009 Paris - FRANCE
Courriel : info@cf2r.org
Tel. 33 (1) 53 43 92 44
Fax 33 (1) 53 43 92 00

www.cf2r.org

Centre Français de Recherche sur le Renseignement

RAPPORTS DE RECHERCHE

RAPPORTS DE RECHERCHE DU CF2R

Les Rapports de recherche (RR) publiés par le Centre Français de Recherche sur le Renseignement (CF2R) sont des travaux de recherche approfondis menés par un ou plusieurs de ses chercheurs, afin d'apporter des éléments d'information nouveaux sur un sujet d'actualité. Ces rapports sont téléchargeables sur notre site www.cf2r.org.

- **Jean-Marie COTTERET**
  Les fichiers de Police et de renseignement en France
  Rapport de recherche n°21, octobre 2017.

- **Général Alain LAMBALLE**
  Les services de renseignement et de sécurité d'Asie du Sud
  Rapport de recherche n°20, juin 2017.

- **Eric DENÉCÉ, Général Michel MASSON, Michel NESTERENKO et Jean-François LOEWENTHAL**
  Quelle contribution de l'arme aérienne aux besoins en renseignements civils et militaires à l'horizon 2035 ?
  Rapport de recherche n°19, juin 2016 (confidentiel).

- **Gérald ARBOIT**
  Quelles armées secrètes de l'OTAN ?
  Rapport de recherche n°18, mai 2016.

- **CHLOÉ AEBERHARDT ET ALII**
  Des femmes dans le renseignement belge : un défi permanent
  Rapport de recherche n°17, mars 2016.

- **CHRISTIAN DARGNAT**
  2015-2016 : années d'inflexion de la stratégie géo-économique chinoise
  Rapport de recherche n°16, février 2016.

- **OLIVIER DUJARDIN**
  Le renseignement technique d'origine électromagnétique appliqué au radar (ELINT)
  Rapport de recherche n°15, octobre 2015.

- **OLIVIER GUILMAIN**
  Le Smart Power au secours de la puissance américaine
  Rapport de recherche n°14, mars 2015.

- **LESLIE VARENNE ET ERIC DENÉCÉ**
  Racket américain et démission d'Etat. Le dessous des cartes du rachat d'ALSTOM par General Electric
  Rapport de recherche n°13, décembre 2014.

- **DR FARHAN ZAHID**
  Operation Cyclone and its Consequences
  Rapport de recherche n°12 (en anglais), août 2014.

- **DR FARHAN ZAHID AND HAIDER SULTAN**
  The US Objectives in GWOT and their Effects on AfPak Theater
  Rapport de recherche n°11 (en anglais), juillet 2014.

- **DR FARHAN ZAHID**
  Islamist Radicalization in South Asia. Origins, Ideologies and Significance of Radical Islamist Violent Non-State Actors
  Rapport de recherche n°10 (en anglais), mai 2014.

- **GÉRALD ARBOIT**
  Le renseignement, dimension manquante de l'histoire contemporaine de la France
  Rapport de recherche n°9, mars 2013.

- **ERIC DENÉCÉ & GÉRALD ARBOIT**
  Les études sur le renseignement en France
  Rapport de recherche n°8, novembre 2009.

- **NATHALIE CETTINA**
  Communication et gestion du risque terroriste
  Rapport de recherche n°7, mars 2009.

- **PHILIPPE BOTTO**
  Noukhaev et le nationalisme tchétchène
  Rapport de recherche n°6, septembre 2008.

- **ALAIN RODIER**
  La menace iranienne
  Rapport de recherche n°5, janvier 2007.

- **NATHALIE CETTINA**
  Specificités de la gestion organisationnelle de la lutte antiterroriste en Corse
  Rapport de recherche n°4, mars 2006.

▪ **GÉNÉRAL ALAIN LAMBALLE**
Terrorism in South Asia
Rapport de recherche n°3 (en anglais), novembre 2005.

▪ **MICHEL NESTERENKO**
Project for a New American Century : la politique des néoconservateurs derrière la guerre contre la terreur
Rapport de recherche n°2, octobre 2005.

▪ **ERIC DENÉCÉ**
Le développement de l'islam fondamentaliste en France : conséquences sécuritaires, économiques et sociales
Rapport de recherche n°1, septembre 2005.

RAPPORTS DE RECHERCHE CF2R/CIRET-AVT

Les rapports publiés en partenariat avec le Centre international de recherche et d'étude sur le terrorisme et d'aide aux victimes du terrorisme (CIRET-AVT) font suite à des missions d'évaluation de terrain réalisées dans le cadre d'une mission internationale francophone.

▪ **GROUPE MILITAIRE DE HAUT NIVEAU**
Évaluation du conflit de Gaza en 2014, Israël, octobre 2015.
À l'instigation de Friends of Israel Initiative, un Groupe militaire de haut niveau (High Level Military Group/HLMG) a été créé au début de l'année 2015 avec pour mandat d'examiner la conduite d'Israël lors du conflit de Gaza en 2014.
Le rapport final, évalue le fait de savoir si Israël a agi dans ce conflit comme un pays responsable, soucieux du respect des normes et des lois régissant la guerre, en adoptant des attitudes appropriées dans les domaines juridique, opérationnel et moral.
Dans le cadre de ses activités d'évaluation des conflits internationaux, le Centre Français de Recherche sur le Renseignement (CF2R) a envoyé l'un de ses directeurs de recherche, le général Alain Lamballe, participer à ce travail d'évaluation du conflit de Gaza.

▪ **Yves-Marie PEYRY**
Problemi et prospettivi della cyberwarfare
Centre Français de Recherche sur le Renseignement (CF2R)/Centro Studi Strategici Carlo De Cristoforis (CESTUDEC), Italie, 2012.

▪ **Éric DENÉCÉ et Valéry GAUDIN**
Sous-traitance et externalisation : quels risques pour les établissements financiers et les entreprises de services et de conseil ?
Centre Français de Recherche sur le Renseignement (CF2R)/Groupe Synergie Globale, Paris, avril 2009.

▪ **SOUS LA DIRECTION D'ÉRIC DENÉCÉ**
Syrie : une libanisation fabriquée. Compte rendu de mission d'évaluation auprès des protagonistes de la crise syrienne"
Centre international de recherche et d'études sur le terrorisme et d'aide aux victimes du terrorisme (CIRET-AVT) et Centre Français de Recherche sur le Renseignement (CF2R), Paris, janvier 2012 (traduit en anglais et en arabe).

▪ **YVES BONNET**
Iran : l'oublié du printemps
Centre international de recherche et d'études sur le terrorisme et d'aide aux victimes du terrorisme (CIRET-AVT) et Centre Français de Recherche sur le Renseignement (CF2R), Paris, décembre 2011.

▪ **SOUS LA DIRECTION D'ÉRIC DENÉCÉ (CF2R) ET D'YVES BONNET (CIRET/AVT)**
Libye : un avenir incertain, compte rendu de mission d'évaluation auprès des belligérants libyens
Centre international de recherche et d'études sur le terrorisme et d'aide aux victimes du terrorisme (CIRET-AVT) et Centre Français de Recherche sur le Renseignement (CF2R), Paris, avril 2011 (traduit en anglais et en italien).

Cf2R
Centre Français de Recherche sur le Renseignement

Centre Français de Recherche sur le Renseignement (CF2R)
21 boulevard Haussmann
75009 Paris
FRANCE
Courriel : info@cf2r.org
Tel. 33 (1) 53 43 92 44
Fax 33 (1) 53 43 92 00

www.cf2r.org

Centre Français de Recherche sur le Renseignement

Centre Français de Recherche
sur le Renseignement (CF2R)
21 boulevard Haussmann
75009 Paris
FRANCE
Courriel : info@cf2r.org
Tel. 33 (1) 53 43 92 44
Fax 33 (1) 53 43 92 00

www.cf2r.org