FICHAGE
INSTITUTIONNEL

Quels risques pour le citoyen ?

Monographie | FRANCE

Ligue des droits de l'Homme
FONDÉE EN 1898

aedh FIDH

Humanistische Union

HUNGARIAN CIVIL LIBERTIES UNION
HCLU

Ligue des Droits de l'Homme
Action Luxembourg Ouvert et Solidaire

MEDEL
Magistrats Européens pour la Démocratie et les Libertés

Avril 2014

PRESENTATION DU PROJET

Les citoyens de l'Union européenne ignorent souvent l'étendue du fichage institutionnel dont leurs proches et eux-mêmes peuvent être l'objet : fichiers liés à l'éducation, fichiers liés à la santé et aux soins médicaux, fichiers de police, fichiers de justice, etc. Ce fichage est souvent abusif et peut avoir des conséquences sur leur vie quotidienne et leur avenir.

L'objectif de notre projet est d'informer et de sensibiliser les citoyens sur le fichage, sur les moyens qu'ils ont de se protéger et de se défendre en cas d'abus avéré.

Notre projet fait référence aux principes de la Convention européenne de sauvegarde des droits de l'Homme et des libertés (article 8 : « *toute personne a le droit au respect de sa vie privée* ») et, au niveau de l'Union européenne, de la Charte des droits fondamentaux dont la force contraignante a été consacrée par le Traité de Lisbonne en 2009 (article 7 : « *toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications* » et article 8 : « *toute personne a droit à la protection des données à caractère personnel la concernant. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. Le respect de ces règles est soumis au contrôle d'une autorité indépendante* »). Notre projet fait également référence aux textes généraux ou spécifiques de l'Union européenne, ainsi que du Conseil de l'Europe, sur la protection des personnes à l'égard du traitement des données à caractère personnel, qui y puisent leur fondement ou en sont à l'origine. Parmi ces textes, il convient de mentionner la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, dite Convention 108, qui a pour objet de garantir « *sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant* » (article 1er).

L'objet de nos organisations est de réaliser un état des lieux en vue d'une analyse comparative dans plusieurs pays (comparaison des fichiers, de la législation qui s'y applique, des pouvoirs des autorités de protection des données personnelles et des moyens de recours), puis de concevoir des outils de sensibilisation et de lancer une campagne d'information et d'alerte visant à informer les citoyens européens de l'utilisation qui est faite de leurs données personnelles et de leurs droits dans ce domaine, tout en prenant en compte les changements qui pourraient découler d'une part de la révision de la directive européenne de 1995, d'autre part du processus de modernisation de la Convention 108 du Conseil de l'Europe.

Pour plus d'informations, voir le site de la Ligue des droits de l'Homme concernant le projet : http://www.ldh-france.org/Fichage-institutionnel-Quels/

SOMMAIRE

1. LA LEGISLATION

LES GARANTIES POUR LA VIE PRIVEE EN FRANCE

La protection de la vie privée est une liberté individuelle qui est garantie par l'article 66 de la Constitution.

Article 9 du Code civil : droit au respect de la vie privée

Chacun a droit au respect de sa vie privée. Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé.

Les articles 226-1 et suivants du Code pénal sanctionnent la violation de la vie privée

Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :

1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;

2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.

Lorsque les actes mentionnés au présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé.

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « Informatique et Libertés »

Conçue sur des principes généraux et universels, la loi « Informatique et Libertés » a fait l'objet d'une dizaine de modifications dont la dernière le 6 août 2004 pour la mettre en conformité avec la directive européenne 95/46/CE du 24 octobre 1995. Elle définit **les principes à respecter** lors de la collecte, du traitement et de la conservation des données personnelles quel que soit le secteur d'activité. Elle précise les droits des personnes dont les données personnelles ont été recueillies. Ces principes répondent à l'ensemble **des risques présentés par la numérisation de l'information : facilité de copie, conservation, modification, transmission, possible réutilisation à l'insu des personnes, problème de sécurité etc.**

La révision de 2004 a sensiblement modifié la portée de la loi dans des domaines qui ne relevaient pas de la directive : sécurité publique, défense… Les pouvoirs de la Cnil ont été réduits par la suppression de l'autorisation préalable (l'avis conforme préalable et donc opposable à l'administration en matière de création de fichiers) dans ces domaines, remplacée par l'avis « consultatif » non opposable à l'administration. Elle a également libéralisé la création de fichiers portant sur les données dites « sensibles ».

- **Les principes de la loi « Informatique et Libertés »**

• L'article 1er définit le cadre de la loi

« L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'Homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».

• L'article 2 définit notamment les notions de données personnelles et de traitements

Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou tout autre personne.

Constitue un **traitement de données à caractère personnel** toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

- **Les articles 6 et 7 définissent les principes s'appliquant aux données personnelles**
  - **Le principe de finalité** : un traitement ne peut être mis en œuvre que pour une finalité déterminée, explicite et légitime.
  - **Le principe de pertinence et de proportionnalité des données :** les données doivent être adéquates, pertinentes et non excessives par rapport à la finalité du traitement.
  - **Le principe d'une durée de conservation limitée:** les données ne doivent être conservées que le temps nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées.
  - **L'obligation de ne communiquer les données qu'aux destinataires et aux tiers autorisés. L'obligation de sécurité :** tout responsable de traitement de données doit prendre toutes précautions utiles afin de préserver la sécurité des informations
  - **Le principe de loyauté et de transparence :** toute personne doit être informée des conditions d'utilisation de ses données. Elle a un droit d'accès à ses informations, de les faire rectifier voire supprimer et, sous certaines conditions, de s'opposer au traitement de ses données.
  - **Les interconnexions :** qui, constituent de fait un nouveau traitement justifient l'application du principe de finalité et doivent faire l'objet d'une autorisation de la CNIL (article 25 loi I&L). L'interconnexion peut se définir comme la mise en relation automatisée d'informations provenant de fichiers ou de traitements qui étaient au préalable distincts, donnant ainsi une nouvelle finalité aux fichiers.

2. L'AUTORITE DE PROTECTION DES DONNEES (LA COMMISSION NATIONALE INFORMATIQUE ET LIBERTES - CNIL)

Statut

La Commission Nationale de l'Informatique et des Libertés (CNIL) a été créée par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite Informatique et Libertés, une des premières lois en Europe (après le land de Hesse en Allemagne en 1971 et la Suède en 1973) issue des réflexions d'une commission ad hoc mise en place pour répondre à une campagne de citoyens opposés au projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus) d'interconnexion des fichiers administratifs grâce au n° identifiant national géré par l'Institut National de la Statistique et des Etudes Economiques INSEE (appelé aussi n° de sécurité sociale). Cette loi a été amendée à plusieurs reprises, notamment en 2004 pour répondre à l'obligation de transposition de la directive européenne 95/46/CE de 1995.

L'article 1er de la loi définit comme principe que « *L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'Homme, ni à la vie privée, ni aux libertés individuelles ou publiques* ».

En 72 articles, la loi définit les principes de cette protection (voir rappel des principes de la loi ci-dessus) et les moyens pour les mettre en œuvre. La CNIL et ses missions sont définies aux articles 11 à 21. Elle doit notamment veiller à un équilibre entre les intérêts des responsables de traitement et les droits des personnes concernées.

La CNIL a un statut **d'autorité administrative indépendante**.

Elle est composée de personnalités diverses (17) nommées pour 5 ans (ou pour la durée de leur mandat électif) renouvelables une fois. Elle comprend 12 membres désignés par leur instance : 4 élus (2 députés et 2 sénateurs) ; 2 membres du Conseil économique, social et environnemental ; 2 conseillers d'État (cour suprême administrative) ; 2 conseillers à la Cour de cassation (cour suprême judiciaire) ; 2 conseillers maîtres à la Cour des comptes (assurant le contrôle financier des organismes publics) ; 5 membres sont nommées pour leurs compétences en Informatique ou sur les questions de libertés, par le gouvernement par décret ministériel (3), par le Président de l'Assemblée nationale (1) et celui du Sénat (1).

Les membres élisent le/la président(e) en leur sein. Cette fonction est incompatible avec une activité professionnelle, un mandat électif national, et tout intérêt direct ou indirect dans une entreprise du secteur des communications électroniques ou de l'informatique. Sauf démission, il ne peut être mis fin aux fonctions d'un membre que par la commission elle-même dans les conditions qu'elle définit. C'est dans le règlement intérieur qu'elle fixe les règles relatives à son organisation et son fonctionnement, notamment les règles relatives aux délibérations, à l'instruction des dossiers et à leur présentation devant la commission, ainsi que les modalités de mise en œuvre de la procédure de labellisation (10 labels ont été attribués en 2012 notamment à des formations et à une procédure d'audit).

La CNIL ne reçoit d'instruction d'aucune autorité. Les ministres, autorités publiques, dirigeants d'entreprises, publiques ou privées, ne peuvent pas s'opposer à son action.

Les décisions de la CNIL peuvent faire l'objet de recours devant le Conseil d'Etat.

Budget et moyens

Le budget de la CNIL relève du budget de l'Etat, il était d'environ 16 millions d'euros en 2012 (dont 10 millions pour salaires).

Le président de la CNIL recrute librement ses collaborateurs. On comptait, en juillet 2013, 174 collaborateurs (avec statut d'agent contractuel) pour assurer les missions quotidiennes de la CNIL, ce qui est tout à fait insuffisant au regard de la charge qui lui incombe. Les membres et agents de la CNIL sont astreints par la loi au secret professionnel, les personnels amenés à traiter des dossiers sensibles doivent aussi être habilités « secret défense ».

Fonctionnement

Les membres de la CNIL se réunissent régulièrement en séances plénières pour examiner les projets de loi et de décrets soumis pour avis ainsi que les projets de fichiers les plus sensibles (notamment les fichiers biométriques).

Les contentieux sont examinés en formation restreinte. Celle-ci est composée d'un président et de 5 membres élus parmi les 17. Le président et les deux vice-présidents (qui constituent le Bureau de la CNIL) ne peuvent pas faire partie de la formation restreinte. La formation restreinte peut prononcer après une procédure contradictoire, un avertissement à l'égard du responsable d'un traitement qui ne respecte pas les obligations de la loi. Cet avertissement a le caractère d'une sanction.

Le président de la commission peut mettre en demeure ce responsable de se conformer à la loi dans un délai qu'il fixe. En cas d'urgence, ce délai peut être ramené à 5 jours. Si le responsable du traitement obtempère, le président de la commission prononce la clôture de la procédure. Dans le cas contraire la formation restreinte peut prononcer, après une procédure contradictoire, les sanctions suivantes (sauf dans les cas où le traitement est mis en œuvre par l'État) :

- une sanction pécuniaire qui ne peut dépasser 150 000 € lors du premier manquement ;
- en cas de nouvelle infraction dans les cinq années la sanction ne peut excéder 300 000 € ;
- une injonction de cesser le traitement ;
- ou un retrait de l'autorisation accordée.

Le bureau décide de la publicité des mises en demeure, et la formation restreinte est libre de publier les sanctions.

La CNIL agit aussi par voie de recommandations pour une catégorie de traitements dans un secteur, élaborées généralement après consultations des parties prenantes.

En dehors des séances plénières, les commissaires travaillent chacun dans un domaine particulier ou un secteur d'activités économiques en lien avec les services.

Les correspondants « informatique et libertés » (CIL)

La révision de la loi en 2004 a intégré la création de la fonction de correspondant à la protection des données (CIL[1]) dans les entreprises qui le souhaitent. Ce salarié est chargé de s'assurer de manière indépendante de la conformité des fichiers mis en œuvre par l'entreprise avec la loi et ainsi, l'entreprise est dispensée de déclaration et/ou autorisation préalable sauf en cas de transfert envisagé de données à caractère personnel vers un Etat non membre de l'Union européenne. En 2012 plus de 10 000 organismes ont désigné un CIL, ils étaient 10 709 fin 2012**.**

Les missions et pouvoirs de la CNIL

La CNIL a pour mission générale de conseiller les personnes (particuliers et professionnels) et de leur délivrer toute information utile en ce qui concerne notamment les démarches à accomplir pour l'exercice de leurs droits et les procédures à suivre pour les formalités déclaratives.

Information / communication / anticipation

La CNIL doit veiller à ce que les citoyens soient informés des données contenues dans les traitements les concernant et qu'ils puissent y accéder facilement. Elle informe toutes les personnes concernées et tous les responsables de traitements de leurs droits et obligations concernant la protection des données personnelles.

Elle a un rôle d'information prospective par son analyse des évolutions technologiques et sociétales, elle informe sur les conséquences possibles pour les droits et les libertés et propose au gouvernement des mesures pour adapter la protection de la vie privée.

Depuis 2004, la CNIL a la possibilité de délivrer des labels à des produits ou à des procédures ayant trait à la protection des personnes à l'égard du traitement des données à caractère personnel. Dix labels ont été attribués en 2012.

La CNIL présente chaque année au président de la République, au Premier ministre et au Parlement un rapport public rendant compte de l'exécution de sa mission, ce rapport est disponible sur son site.

On trouve sur son site en français, anglais et espagnol une présentation de l'autorité, des documents d'information, de formation et de conseils ainsi que des modèles de courriers et la possibilité de porter plainte en ligne.

Les références des avis qu'elle rend sur les projets de fichiers qui lui sont soumis sont indiquées sur son site internet, ils sont publiés sur le site Légifrance (http://www.legifrance.gouv.fr/), service gouvernemental de la diffusion du droit.

La CNIL a remplacé récemment sa devise, qui était auparavant l'article 1er de la loi[1], pour : « *Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles* ».

Réguler / Contrôler

La CNIL veille à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions de la loi Informatique et libertés.

La CNIL recense les fichiers, autorise certaines catégories de traitements avant leur mise en place, notamment quand il s'agit de données sensibles[i].

La CNIL établit des « normes simplifiées » (description de règles à respecter pour des traitements par catégories), afin que les traitements les plus courants fassent l'objet de formalités allégées (déclaration « simplifiées »), elle établit des autorisations uniques pour des catégories de traitements « à risques » mais ainsi réglementés (exemple autorisation de système de lecture des empreintes palmaires dans les cantines scolaires, etc.). Elle peut aussi décider de dispenser de toute déclaration des catégories de traitement sans risque pour les libertés individuelles.

Elle peut faire des investigations de sa propre initiative ou pour instruire les plaintes et analyser certains fichiers (exactitude des contenus, légitimité des finalités, sécurité, etc. - voir exemples de plaintes[ii]).

Dans le cadre de ses pouvoirs d'investigation la CNIL peut :

- demander des informations et des documents ;
- accéder à des banques de données et à des fichiers ;
- perquisitionner dans les locaux et procéder à des saisies avec mandat judiciaire ;
- mener des audits.

Elle fait procéder aux rectifications, effacements des données inexactes, elle peut aussi enquêter dans toute entreprise, procéder à des vérifications de sa propre initiative, mais elle ne peut pas perquisitionner dans les locaux et procéder à des saisies sans mandat judiciaire.

Elle vérifie la sécurité des systèmes d'information (personnes autorisées à y accéder, mesures pour empêcher que les données ne soient déformées ou communiquées à des personnes non-autorisées).

Le gouvernement doit lui soumettre pour avis, avant présentation au Parlement, tout projet de loi relatif à la protection des données personnelles; son avis doit aussi être sollicité par le gouvernement avant d'autoriser les traitements intéressant la sûreté de l'État, la défense ou la sécurité publique mais **depuis 2004 la compétence d'autorisation préalable qui lui donnait la possibilité de refuser notamment la constitution de fichiers de police lui a été retirée, elle ne peut plus s'opposer à la création de fichiers de police**, mais rend un avis consultatif, publié au Journal officiel qui n'influera pas sur leur création.

La CNIL établit des normes simplifiées, afin que les traitements les plus courants fassent l'objet de formalités allégées (exemple autorisation de système de lecture des empreintes palmaires dans les cantines scolaires…). Elle peut aussi décider de dispenser de toute déclaration des catégories de traitement sans risque pour les libertés individuelles.

1. *voir page 6*

Assurer le droit d'accès aux données

Toute personne justifiant de son identité a le droit d'interroger le responsable d'un traitement de données personnelles pour obtenir communication des informations la concernant et, le cas échéant, de demander leur correction ou leur suppression. La CNIL instruit les plaintes des personnes qui souhaitent exercer ce droit et qui n'obtiennent pas satisfaction auprès des responsables des fichiers.

Elle assure le droit d'accès indirect[2] à certains fichiers nationaux de souveraineté (fichiers intéressant la sûreté de l'État, la défense et la sécurité publique : fichiers de police et de gendarmerie, fichiers de renseignement, fichier Schengen, etc.), notamment les traitements mis en œuvre par les administrations publiques et les personnes privées chargées d'une mission de service public qui ont pour mission de prévenir, rechercher ou constater des infractions, ou de contrôler ou recouvrer des impositions (principalement les fichiers de la police judiciaire, tels que le STIC, JUDEX, le FNAEG ou les fichiers des renseignements généraux, le fichier des comptes bancaires FICOBA, tenu par la direction générale des finances publiques, qui recense les ouvertures et les mouvements de comptes). Seuls les membres ayant la qualité de magistrats ou d'anciens magistrats peuvent enquêter sur ces fichiers. En 2012 la CNIL a reçu **3 682 demandes de droit d'accès indirect** (+ 75 % par rapport à 2011).

Sanctionner

Lorsqu'elle constate un manquement à la loi, la CNIL peut, après avoir mis en demeure les responsables d'y mettre fin, utiliser diverses mesures : l'avertissement, les sanctions pécuniaires pouvant atteindre 300 000 €, l'injonction de cesser le traitement, elle peut saisir également le procureur de la République des violations de la loi dont elle a connaissance. Elle peut aussi demander en référé à la juridiction compétente d'ordonner toute mesure de sécurité nécessaire. Le Président ou son représentant peut présenter des observations dans des procédures pénales.

Toutefois ces sanctions peuvent être contestées devant le Conseil d'Etat (exemple : en 2009, le Conseil d'Etat a annulé deux sanctions prononcées en 2006 par la CNIL à l'encontre de plusieurs sociétés. Elles ont exercé un recours contre ces sanctions devant le Conseil d'Etat, au motif que les contrôles n'avaient pas été « *préalablement autorisés par un juge* »).

Par ailleurs la loi I&L prévoit (article 51) que le fait d'entraver l'action de la Commission nationale de l'informatique et des libertés (en s'opposant à l'exercice de ses missions, en refusant de lui communiquer ou en faisant disparaitre les renseignements et documents utiles, en communiquant des informations inexactes ou non conformes) est puni d'un an d'emprisonnement et de 15 000 € d'amende.

La CNIL en quelques chiffres pour l'année 2012 avec un budget de 16 millions d'euros

88 990 traitements déclarés	458 contrôles	4 sanctions financières
113 avis	316 autorisations	2 078 décisions et délibérations
3 682 demandes d'accès indirect aux fichiers de police et de renseignement	Plus de 6 000 plaintes (8 % portant sur les libertés publiques)	43 mises en demeure et 9 avertissements
Formalités préalables		
8 946 déclarations relatives à la vidéosurveillance	5 483 déclarations relatives à la géolocalisation	795 autorisations de systèmes biométriques
Demandes d'accès indirect	STIC : 1 523 ; JUDEX : 1 523	SIS : 306

2. La personne concernée doit adresser une demande à la CNIL pour savoir si elle est fichée dans un fichier «sensible». C'est un membre de la CNIL, magistrat ou ancien magistrat qui interviendra en son nom auprès du responsable du fichier pour vérifier l'existence d'informations la concernant, vérifier l'exactitude de ces données, en demander la rectification si nécessaire et communiquer à la personne les informations la concernant, sous réserve de l'accord du gestionnaire du fichier concerné.

Le rôle de la CNIL pour les fichiers étudiés

Compte tenu de la modification de la loi I&L de 2004, les avis de la CNIL sur la création de fichiers de police ne sont plus contraignants pour le gouvernement mais publiés en même temps que la réglementation du fichier

Extrait de la loi Informatique et libertés (modifiée 2004)

I. - Sont autorisés par arrêté du ou des ministres compétents, **pris après avis motivé et publié de la CNIL**, les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat et :

1° Qui intéressent la sûreté de l'Etat, la défense ou la sécurité publique ;

2° 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.

L'avis de la commission est publié avec l'arrêté autorisant le traitement.

II. - Ceux de ces traitements qui portent sur des données mentionnées au I de l'article 8 sont autorisés par décret en Conseil d'Etat pris après avis motivé et publié de la commission ; cet avis est publié avec le décret autorisant le traitement.

3. ANALYSE CRITIQUE DES FICHIERS ETUDIES

A. JUSTICE

Parmi les nombreux fichiers de Justice nous avons choisi d'étudier ceux qui nous semblent les plus susceptibles d'atteintes à la vie privée notamment parce qu'ils contiennent des données sensibles, que la sécurité de traitement peut laisser à désirer, que les personnes ne sont pas systématiquement informées et enfin qu'ils peuvent concerner des enfants.

1. Résumé des fichiers étudiés et leur but

Casier judiciaire national

Créé en 1980, le fichier des casiers judiciaires est un traitement informatisé qui recense l'ensemble des condamnations pénales prononcées par les autorités judiciaires, pour les besoins des juridictions et des administrations[3]. Il est placé sous le contrôle et l'autorité de la Direction des affaires criminelles et des grâces du ministère de la Justice.

(Code de procédure pénale : voir art.768 et suivants[4]).

Les informations contenues dans le casier judiciaire permettent d'obtenir un compte-rendu du passé judiciaire d'une personne. Ces informations sont communiquées sous forme de trois bulletins dont les contenus suivent des règles relatives aux destinataires.

Le bulletin n° 1, communicable aux autorités judiciaires et aux greffes des établissements pénitentiaires, contient l'ensemble des condamnations pénales prononcées par une juridiction française ou celle d'un Etat membre de l'Union européenne à l'encontre d'une personne.

Le bulletin n° 2, communicable à certaines autorités administratives et militaires pour des motifs précis (notamment en vue de l'accès à certaines professions), contient la plupart des condamnations pour crimes et délits, à l'exception entre autres de celles prononcées à l'encontre de mineurs, des contraventions, et des condamnations avec sursis lorsque le délai d'épreuve a expiré. Il peut également contenir des condamnations prononcées par des juridictions étrangères.

Le bulletin n° 3, communicable uniquement à la personne concernée[5], contient les condamnations pénales les plus graves prononcées à l'encontre d'une personne par une juridiction française ou de l'Union européenne ou une autre juridiction étrangère. Un employeur ne peut pas demander directement communication du casier judiciaire de son employé.

Le délai maximum de conservation des informations contenues dans le casier judiciaire est de 40 ans, sauf pour les crimes contre l'humanité, qui ne sont jamais effacés. Les fiches sont également automatiquement effacées au décès du titulaire ou lorsqu'il atteint l'âge de 100 ans.

A noter que la **décision-cadre 2009/315/JAI** de l'UE et la **décision2009/316/JAI** du Conseil ont mis en œuvre la création du **système européen d'information sur les casiers judiciaires (ECRIS).** Ce système permet l'interconnexion des casiers judiciaires par voie électronique, dans le cadre d'échanges d'informations sur les condamnations entre les Etats membres de manière uniforme et informatisée. Depuis avril 2012 ce système interconnecte les bases de données des casiers judiciaires de tous les Etats membres.

Le public peut s'informer sur le site internet du ministère de la Justice[6].

3. C'est un casier devenu national et automatisé après 1981, en application de la loi n° 80-2 du 4 janvier 1980 relative à l'automatisation du casier judiciaire (JO du 5 janvier 1980, p. 40) et du décret en Conseil d'Etat n° 81-1003 du 6 novembre 1981 pris pour l'application de la loi 80-2 du 4 janvier 1981 relative à l'automatisation du casier judiciaire et modifiant certaines dispositions du Code de procédure pénale. Avant 1981, le casier judiciaire était tenu auprès du Tribunal de grande instance proche du lieu de naissance de l'individu. (http://fr.jurispedia.org/index.php/Casier_judiciaire_(fr))

4. http://www.legifrance.gouv.fr/affichCode.

5. Ou à son représentant légal s'il s'agit d'un mineur.

6. http://www.vos-droits.justice.gouv.fr/casier-judiciaire-11942/casier-judiciaire-contenu-de-casier-20250.html

Cassiopée (Chaîne Applicative Supportant le Système d'Information Orienté Procédure pénale Et Enfants)

Créé en 2009[7] dans le but de moderniser la gestion de la chaîne pénale, ce traitement a pour fonction de faciliter la gestion des procédures au sein des tribunaux de grande instance grâce à l'enregistrement de toutes les informations relatives aux procédures judiciaires en cours. L'objectif est de faciliter la gestion des procédures pénales grâce à une vision complète de chaque dossier judiciaire et permettre la fluidité des transmissions entre les différents acteurs (notamment pour la mise à jour du STIC par la transmission des suites judiciaires), d'assurer la qualité et le délai du traitement des procédures, l'information des victimes.

Il concerne donc toutes les personnes engagées dans les procédures judiciaires concernées : personnes mises en examen, témoins, prévenus, accusés, victimes, témoins assistés, parties civiles, mineurs, personne faisant l'objet d'une procédure d'extradition ou d'un mandat d'arrêt européen, avocats, personnels du ministère de la Justice, certains membres des associations d'aide aux victimes conventionnées.

Il contient des informations (conservées de 10 à 30 ans selon les cas) relatives à :

- la personne concernée : identité, filiation, adresse, vie professionnelle, niveau d'étude, situation familiale, et, sauf pour les témoins, les données bancaires ;
- la procédure judiciaire : situation de la personne concernée au cours de la procédure, mode de comparution devant la juridiction, nature du jugement, le montant demandé pour les dommages-intérêts ou la provision, les infractions sur lesquelles porte la procédure, la peine prononcée. Peuvent y accéder directement, dans le cadre du traitement des infractions ou des procédures dont ils sont saisis : les procureurs et les magistrats du siège ; le représentant national auprès d'Eurojust ; les magistrats ainsi que les agents de greffe ; les délégués du procureur de la République ; les éducateurs de la protection judiciaire de la jeunesse dans le cadre des procédures pénales dont ils sont saisis ou pour l'accomplissement des missions ; les avocats ; les personnes concourant à la procédure (c'est-à-dire tenues au secret professionnel) ; les administrations et les personnes qui participent à l'instruction des dossiers, à la signification, à la notification et à l'exécution des décisions judiciaires ; certains membres des associations d'aide aux victimes conventionnées.

Ces informations sont énumérées à l'article R15-33-66-3 du code de procédure pénale.

FIJAIS : Fichier Judiciaire Automatisé des Auteurs d'Infraction Sexuelle

Créé en 2004, ce fichier a pour objectif la prévention de la récidive des auteurs d'infractions sexuelles et des auteurs de crimes graves, ainsi que leur identification et leur localisation rapide. A l'origine, il ne concernait que les auteurs d'infractions sexuelles, mais son champ d'application a été étendu en 2005 aux auteurs d'infractions particulièrement graves (meurtre ou assassinat d'un mineur avec viol ; tortures ou actes de barbarie ; viol sur mineur ; agression ou atteinte sexuelle sur mineur ; proxénétisme à l'égard d'un mineur ; recours à la prostitution d'un mineur ; meurtre ou assassinat commis avec actes de torture ou de barbarie ; crime commis avec actes de torture ou de barbarie ; meurtre et assassinat en récidive légale[8]).

Textes encadrant ce fichier : loi (n°2004-204) du 9 mars 2004 créant le FIJAIS[9] ; articles 706-53-1 à 706-53-12 du code de procédure pénale[10] ; décret (n°2005-627) du 30 mai 2005[11] ; décret n°2008-1023 du 6 octobre 2008[12].

7. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020605929
8. http://www.jcomjeune.com/les-fichiers-de-police/le-fichier-judiciaire-automatise-des-auteurs-d-infractions-sexuelles-ou-violentes-fijaisv
9. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000249995
10. http://www.legifrance.gouv.fr/affichCode.do;jsessionid=9E608DF4BDA9D645A9045286A76C15F0.tpdjo03v_1?idSectionTA=LEGISCTA000006151994&cidTexte=LEGITEXT000006071154&dateTexte=20140305
11. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006051832
12. http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000019585170&dateTexte

En 2011 le FIJAIS contenait les informations d'environ 54 900 personnes. Ces informations sont relatives à :

- la personne concernée : nom, prénom, sexe, date et lieu de naissance, nationalité, le cas échéant alias, changement de nom et nom d'usage, filiation, adresses, le cas échant la commune de rattachement ;
- la/les décision(s) ayant donné lieu à l'enregistrement : nature et date de la décision, juridiction ayant prononcé la décision, peines principales ou complémentaires ou mesures prononcées, nature de l'infraction, lieu et date des faits, caractère exprès de l'enregistrement, date de notification des obligations prévues, date d'exécution ou de fin d'exécution de la peine, le cas échéant, dates de mise sous écrou et de libération.

Ces données sont conservées pour une durée de 20 à 30 ans maximum selon la gravité de l'infraction. La demande de retrait du FIJAIS est irrecevable tant que la condamnation figure au bulletin n° 1 du casier judiciaire.

A noter : l'inscription au fichier implique des obligations pour les personnes concernées, elles doivent justifier (auprès du commissariat ou de la gendarmerie) de leur adresse au moins une fois par an et déclarer leur changement d'adresse éventuel dans les quinze jours. Pour les auteurs des infractions les plus graves, la justification d'adresse s'effectue tous les six mois, voire tous les mois. Toutefois, l'extension du fichier aux auteurs de crimes violents nuit à cette fonction, car les services de police n'ont pas la capacité de surveiller les non-justifications d'adresse qui pourraient se révéler inquiétantes.

2. Garanties prévues par la législation

Casier judiciaire

- Aucune interconnexion n'est possible entre le casier judiciaire national automatisé et tout autre fichier ou traitement national de données à caractère personnel, ce qui évite les risques de divulgation du passé judiciaire d'une personne.
- Un service du casier judiciaire national automatisé est entièrement dédié à sa gestion et son contrôle. Il est dirigé par un magistrat de l'administration centrale du ministère de la Justice.

Cassiopée : un magistrat du parquet assisté d'un comité de trois membres nommés pour trois ans par le ministre de la Justice est chargé du contrôle du traitement. Ce magistrat peut ordonner toutes les mesures nécessaires à l'exercice de son contrôle (saisies, copies d'informations, effacement d'enregistrements illicites).

FIJAIS : il est tenu par le service du casier judiciaire, sous l'autorité du ministre de la Justice et sous le contrôle du magistrat dirigeant le service du casier judiciaire.

3. Rôle de la CNIL

Fichier des casiers judiciaires

Depuis 1979 la CNIL a rendu de nombreux avis : délibération 79-02 du 08 août 1979 ; délibération 81-100 du 15 septembre 1981 ; délibération 85-21 du 18 juin 1985 ; délibération 88-45 du 26 avril 1988 ; délibération 88-145 du 06 décembre 1988 ; délibération 01-049 du 18 septembre 2001 ; délibération n°2007-326 du 8 novembre 2007[13].

La CNIL a toujours donné des avis favorables à la création puis aux nombreuses modifications du fichier et de ses modes de consultation tout en insistant sur les mesures de sécurisation des accès, les droits d'information des personnes et les délais excessifs de mise à jour.

13. http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000019796105&fastReqId=1851354861&fastPos=1

Chaîne Applicative Supportant le Système d'Information Oriente Procédure pénale Et Enfants (CASSIOPEE)

La délibération de la CNIL est intervenue après la mise en place du fichier[14].

La CNIL n'a pas contesté la finalité du fichier. Elle regrette l'absence de précisions sur le traitement des données sensibles et estime que les personnes concernées devraient être informées de l'existence du traitement et des modalités d'exercice de leurs droits. Elle déplore le manque de sécurisation des données (qui pourraient se faire par le chiffrement des données, un mécanisme d'authentification sûr, une analyse des journaux d'exploitation et des remontées d'alertes).

FIchier Judiciaire automatisé des Auteurs d'Infractions Sexuelles (FIJAIS)

Etendu aux auteurs de certaines infractions particulièrement graves, après leur sortie de prison, il est rebaptisé **FIJAISV.**

Il a été créé par la loi Perben II du 9 mars 2004 dont les modalités d'application ont été fixées par un décret du 30 mai 2005, pris après avis de la CNIL, mais ensuite modifié par la loi du 12 décembre 2005 sur la récidive des infractions pénales, qui étendait le contenu et la finalité du FIJAIS, et sans que la CNIL ait pu se prononcer sur les modifications envisagées.

Délibération n°2007-326 du 8 novembre 2007[15] ; délibération n° 2011-179 du 16 juin 2011[16].

La CNIL déplore que la loi n'indique pas les conséquences individuelles des personnes postulant ou exerçant des professions ou des activités en contact avec des mineurs et soumises à un agrément de l'Etat qui seraient inscrites dans le FIJAIS, et que ne soient pas listées dans la loi les professions et activités concernées.

La CNIL demande que les personnes concernées par le FIJAIS puissent être informées des destinataires des données. Elle estime nécessaire que les décisions de refus d'agrément prises à la suite d'une consultation du FIJAIS, lorsqu'elles sont notifiées, comportent également une information sur le fait que ce fichier ait été consulté, tout comme pour les décisions de refus d'embauche faisant suite à une consultation du STIC.

La CNIL regrette de ne pas avoir d'information précise sur le nombre de personnes susceptibles d'accéder au FIJAIS au titre de la consultation administrative, qui s'ajouteront aux **39 000 personnes** déjà autorisées au titre des missions de police judiciaire. Elle demande que soient précisément définies les modalités de la délivrance des habilitations et que chaque ministère concerné lui fasse connaitre les procédures mises en œuvre.

Concernant l'obligation pour les personnes inscrites au FIJAIS de justifier de leur adresse régulièrement (en fonction de leur « dangerosité ») et d'en déclarer tout changement, la CNIL a souligné que toutes les garanties doivent être prises pour assurer la confidentialité de ces notifications dans les commissariats et les gendarmeries et rappelle que ces notifications ne doivent pas donner lieu à l'enregistrement d'informations dans des fichiers locaux, distincts du FIJAIS.

Concernant le droit des personnes inscrites dans le FIJAIS à demander rectification ou effacement, la CNIL a indiqué ses réticences à l'allongement de deux à quatre mois des délais de réponses (justifiés par les enquêtes nécessaires) compte tenu de l'importance que peut avoir la consultation de ce fichier par les employeurs potentiels.

Après avoir donné un avis favorable en 2004, la CNIL déplore de n'avoir pu se prononcer sur les modifications intervenues par la suite.

14. Délibération n°2009-170 du 26 mars 2009 : http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000020972757&fastReqId=1161854227&fastPos=1

15. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000019585369

16. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024909935

4. Risques

Risques dus aux dangers contenus dans la législation

‣ Risques dus à l'interconnexion des fichiers

L'interconnexion des casiers judiciaires dans le cadre du système ECRIS risque de poser des difficultés concernant la distinction crime/délit/contravention, qui n'existe pas dans tous les Etats membres de l'UE. Par exemple, certaines condamnations étrangères pourraient être enregistrées pour des faits qui seraient seulement classés en contraventions, ou même pour des faits qui ne seraient pas constitutifs d'une infraction en France.

‣ Risques dus à l'absence d'information des personnes concernées

- Cassiopée : la CNIL[17] regrette que le droit d'information ne s'applique pas au traitement Cassiopée, ce qui ne permet pas aux personnes concernées d'être informées de l'existence du traitement, de l'enregistrement de leurs données et des modalités d'exercice de leurs droits.
- FIJAIS : le formulaire remis aux personnes condamnées n'est pas facilement compréhensible[18].

‣ Risques dus au manque de sécurisation des données

Cassiopée : la CNIL[19] regrette que le décret ne comporte aucune mention particulière relative à la collecte et au traitement de données sensibles, qui pourtant nécessitent une protection particulière. Elle déplore également le manque de mesures de sécurisation des données telles que : chiffrement des données, mécanisme d'authentification sûr, analyse des journaux d'exploitation (qui a accédé à quelles données), remontées d'alertes.

‣ Risques dus à l'extension du nombre de personnes accédant au FIJAISV

La CNIL a regretté que tout officier de police judiciaire puisse accéder aux données dans le cadre de toute enquête de flagrance même si celle-ci ne concerne pas la répression d'infractions sexuelles ou d'actes de violence ; que ne soient pas précisées les professions impliquant un contact avec des mineurs pour lesquelles les préfets et certaines administrations de l'Etat peuvent utiliser ce fichier ; et que ne soit pas précisé si ce contrôle concerne l'ensemble des professions impliquant un contact avec des mineurs. Ceci, sans qu'un premier bilan ait pu être tiré de sa première version et sans qu'elle ait pu se prononcer sur les modifications envisagées.

Risques dus au non-respect des garanties prévues par la législation

‣ Risques dus aux manquements liés à l'obligation d'information des personnes concernées

Selon un rapport remis à l'Assemblée nationale le 21 décembre 2011[20], toutes les personnes ne sont pas informées de leur inscription dans le FIJAIS, notamment celles qui n'ont pas été incarcérées : seulement 15 % des notifications sont réalisées à l'audience, ce qui fait que près de 9 000 personnes sont inscrites au FIJAIS sans pour autant être informées de leurs obligations, faute de notification.

17. Délibération de la CNIL n°2009-170 du 26 mars 2009
18. Voir « La machine à fabriquer des délinquants » blog de Maitre Eolas.
http://www.maitre-eolas.fr/post/2007/04/03/592-la-machine-a-fabriquer-des-delinquants
19. Délibération de la CNIL n°2009-170 du 26 mars 2009
20. http://www.assemblee-nationale.fr/13/rap-info/i4113.asp

Risques dus aux manquements liés à l'obligation d'exactitude des données

Risques concernant l'accès à l'emploi : l'obtention d'un poste est parfois conditionnée à la consultation préalable des informations figurant dans certains fichiers de l'Etat. Par exemple, l'accès à certaines professions est soumis à l'existence d'un casier judiciaire vierge ou sans mention incompatible avec la profession. C'est le cas pour les métiers de la fonction publique, les emplois dans les domaines de la santé (médecin, pharmacien, infirmier, etc.), de l'enfance et des personnes âgées (animateurs, éducateurs, instituteurs, etc.), de la sécurité (agent de sécurité, policier, militaire, etc.), de l'aéroportuaire, ainsi qu'une série de professions telles que les avocats, chauffeurs de taxi, agents immobiliers… Or, même si la loi pose l'obligation d'exactitude des données enregistrées dans les fichiers, ils peuvent contenir des erreurs. Il est donc important pour les intéressés de faire rectifier les informations erronées ou de faire supprimer celles qui n'ont plus lieu d'être inscrites dans leur casier judiciaire.

Risque de refus ou de difficultés pour l'obtention d'un visa (après consultation du casier judiciaire)

Risques dus au manque ou à l'absence de formation des utilisateurs des fichiers

Cassiopée : la législation prévoit que les données enregistrées doivent être exactes, or la difficulté d'utilisation du fichier Cassiopée et l'absence ou le manque de formation de ses utilisateurs entrainent un grand nombre d'erreurs dans la saisie des données. Ces erreurs potentielles peuvent porter préjudice aux personnes concernées, d'autant plus graves du fait de l'interconnexion de Cassiopée avec d'autres fichiers : des données erronées peuvent ainsi être transférées dans le STIC, le TAJ, APPI (Application Des Peines, Probation et Insertion) via Cassiopée.

5. Abus

Abus potentiels selon des organisations de la société civile

Les fonctionnaires de justice du TGI de Bordeaux se sont mis en grève « anti-Cassiopée » en 2009, afin de dénoncer les risques engendrés par la mise en œuvre de Cassiopée : informations peu fiables voire fausses, manque de fonctionnalité et lenteur de l'outil, défauts de conception et impréparation des juridictions à son implantation.

6. Les recours contre ces fichiers

Pour le casier judiciaire

Des recours administratifs ont déjà eu lieu suite à la perte du statut de fonctionnaire ou au refus de nomination suite à la consultation du casier judiciaire.

Pour le FIJAIS

Dans une décision n°2004-492 DC du 2 mars 2004 sur la loi portant adaptation de la justice aux évolutions de la criminalité, le Conseil constitutionnel a estimé que les dispositions relatives à la création du FIJAIS ne portaient pas atteinte à la vie privée.

7. Points forts / points faibles / bonnes pratiques

Développements actuels et prévisibles

Dans un projet de loi portant diverses dispositions d'adaptation dans le domaine de la justice en application du droit de l'Union européenne, et des engagements internationaux de la France du 20 février 2013, la ministre de la Justice a proposé de nouvelles dispositions concernant le FIJAIS :
- l'extension de son champ d'application aux auteurs de crimes de génocide, crime contre l'humanité et crimes et délits de guerre dans les mêmes conditions que celles prévues pour les auteurs d'infractions de crimes et délits de droit commun ;
- un accès au FIJAIS aux autres Etats membres de l'Union européenne via Eurojust[21], dans des conditions identiques à celles des autorités judiciaires.

Evolution de la situation

- On constate un mouvement d'extension du fichage : selon une ancienne présidente du Syndicat de la Magistrature, l'élargissement du champ d'application du FIJAIS illustre « le mouvement naturel et perpétuel du fichage ». Elle fait la comparaison avec le Fichier national automatisé des empreintes génétiques (FNAEG), d'abord conçu pour les auteurs d'infractions sexuelles et qui, au fur et à mesure, s'est étendu à une vaste série de délits.
- Les difficultés d'implantation et d'utilisation dans le cas de Cassiopée conduit à des erreurs alors même que le traitement est sensé faciliter l'enregistrement des informations relatives aux procédures.

21. Agence européenne chargée de renforcer la coopération judiciaire entre les Etats membres de l'Union européenne.

B. POLICE

Parmi plus de 80 fichiers de police ayant une existence légale, notre choix pour cette étude s'est porté sur ceux qui nous semblent les plus susceptibles de porter atteinte à la vie privée avec des conséquences graves en matière d'emploi ou de vie sociale, qui concernent le plus de personnes, ou encore qui contiennent des données sensibles (ADN, empreintes digitales, etc.).

1. Résumé des fichiers étudiés et leur but

AGDREF 2 : Application de Gestion des Dossiers des Ressortissants Etrangers en France

Créé en 2011 (décret n° 2011-638 du 8 juin 2011 relatif à l'application de gestion des dossiers des ressortissants étrangers en France et aux titres de séjour et aux titres de voyage des étrangers[22]), le fichier AGDREF 2 est le résultat de la fusion entre l'ancien fichier AGDREF, devenu obsolète, et le fichier ELOI (pour « éloignement » signifiant l'obligation pour un étranger de quitter le territoire français) qui avait pour but le suivi des procédures d'éloignement. Il a pour objet la gestion des titres de séjour et de voyage des étrangers (délivrance des titres de séjour, demandes de renouvellement ou de délivrance, etc.), la meilleure coordination des services chargé de l'immigration, les vérifications et les contrôles des titres de séjour, ainsi que la gestion des différentes étapes de la procédure applicable aux mesures d'éloignement[23]. Le but est de garantir le droit au séjour des ressortissants étrangers en situation régulière et de lutter contre l'entrée et le séjour irréguliers en France des ressortissants étrangers. Il permet également d'établir des statistiques en matière de séjour et d'éloignement des ressortissants étrangers.

Le traitement concernait, en 2011, environ 7 millions de personnes, qui peuvent être : des étrangers demandeurs ou titulaires d'un titre de séjour ou d'un titre de voyage d'une durée de validité supérieure à un an ; des étrangers en situation irrégulière ; des étrangers faisant l'objet d'une mesure d'éloignement.

Les images numérisées de la photographie et des empreintes digitales des dix doigts des personnes concernées sont automatiquement enregistrées dans le fichier.

De nombreuses données peuvent être enregistrées :

- des données générales telles que : l'état civil, la nationalité, le numéro AGDREF2[24] et autres numéros de dossiers administratifs, la taille, la couleur des yeux pour les titulaires d'un titre de voyage, les références des documents d'identité et de voyage détenus et du visa d'entrée délivré, le pays de résidence et l'adresse du parent bénéficiaire pour le regroupement familial, l'état civil de l'enfant étranger mineur dont les parents font l'objet d'une mesure d'éloignement, l'état civil et adresse du garant (personne qui s'engage en faveur d'un ressortissant étranger), l'état civil et adresse du responsable du mineur étranger, la situation familiale, le plus haut niveau de diplôme obtenu, l'adresse complète, le nom de l'hébergeant, l'ancienne adresse, le pays de résidence antérieure, l'acceptation du dispositif d'hébergement par le demandeur d'asile, l'adresse e-mail, le téléphone, les langues parlées, la signature du titulaire du titre de séjour ou du titre de voyage, etc. ;

22. http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=1770DAEB264BBFD544AE75C6961B4C5A.tpdjo05v_3?cidTexte=JORFTEXT000024147941&dateTexte=20110610

23. Les mesures d'éloignement sont diverses : obligation de quitter le territoire français, reconduite à la frontière, expulsion, extradition, etc.

24. Numéro national d'identification attribué à un étranger lors de sa première immatriculation en France pour la demande d'un titre de long séjour ou d'asile.

- des données en rapport avec les procédures et les décisions administratives ou juridictionnelles (par exemple la délivrance/refus/retrait du titre de séjour, demande d'asile, interdiction judiciaire, mesure d'éloignement, etc.).

Ces informations peuvent être conservées de 5 ans (quand le dossier n'a fait l'objet d'aucune mise à jour, ou qu'il contient des données relatives à une peine d'interdiction du territoire temporaire, ou une interdiction de retour) à 40 ans (dans les cas d'arrêté d'expulsion ou de peine d'interdiction définitive du territoire.)

A noter : les données enregistrées dans AGDREF 2 peuvent être consultées par les agents d'organismes de coopération internationale en matière de lutte contre l'immigration irrégulière dans les conditions prévues par tout engagement liant la France à des organismes internationaux ou à des Etats étrangers. Toutefois, ces organismes et ces Etats doivent assurer un niveau de protection suffisant de la vie privée, des libertés et des droits fondamentaux des personnes à l'égard de données personnelles (c'est notamment le cas de l'ensemble des pays de l'Union européenne, soumis à la législation européenne)[25].

OSCAR: Outil de Statistique et de Contrôle de l'Aide au Retour

Créé en 2009, dans le but de déceler les demandes d'aide au retour d'une personne étrangère qui en aurait déjà bénéficié. Il permet également d'effectuer le suivi administratif, budgétaire et comptable des procédures d'aide au retour gérées par l'Office français de l'immigration et de l'intégration, ainsi que d'établir des statistiques relatives à ces procédures et à leur exécution[26].

Le fichier contient les images numérisées des empreintes des dix doigts du bénéficiaire et de ses enfants mineurs âgés d'au moins douze ans, ainsi que certaines données à caractère personnel relatives aux bénéficiaires (coordonnées en France et dans le pays de retour, numéro national d'identification mentionné dit n°AGDREF, les motifs de la demande, etc.), et d'autres informations relatives à la gestion administrative et comptable du dossier de demande d'aide et à l'organisation du voyage. Ces données sont conservées pour un délai de 5 ans maximum. Il concerne environ 12 000 personnes par an ayant fait la demande d'une aide au retour.

FAED : Fichier Automatisé des Empreintes Digitales

Le fichier est créé en 1987 suite à l'affaire d'un tueur en série qui aurait pu être arrêté plus rapidement si la police avait disposé de ses empreintes digitales collectées dans le cadre d'autres affaires pour lesquelles il avait été emprisonné. Il entre officiellement en service en 1992, sous la responsabilité de la Direction centrale de la police judiciaire du ministère de l'Intérieur. Le FAED est commun à la police, la gendarmerie et la douane, dans le but de faciliter la recherche et l'identification des auteurs de crimes et de délits ainsi que la poursuite, l'instruction et le jugement des affaires dont l'autorité judiciaire est saisie. Il permet aussi de s'assurer de la véritable identité des personnes mises en cause dans une procédure pénale ou condamnées à une peine privative de liberté. Cela évite les erreurs judiciaires en détectant les fausses identités et les cas de récidive. Le FAED permet également d'identifier par comparaison les traces de personnes inconnues relevées sur des lieux d'infractions.

25. Art. R. 611-7 du CESEDA
http://www.legifrance.gouv.fr/affichCode.do;jsessionid=2BC77B3D4C05790A15E9088995D7614E.tpdjo17v_1?idSectionTA=LEGISCTA000024149380&cidTexte=LEGITEXT000006070158&dateTexte=
20130813

26. http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070158&idArticle=LEGIARTI000006335277&dateTexte=&categorieLien=cid

En 2010, il contenait les empreintes de plus de 3,4 millions de personnes mises en cause dans une procédure pénale ou condamnées à une peine privative de liberté, ou disparues.

Ces empreintes digitales sont accompagnées:

- des noms, prénoms, date et lieu de naissance, filiation et sexe ;
- du service ayant procédé à la signalisation ;
- de la date et le lieu d'établissement de la fiche ;
- de la nature de l'affaire et la référence de la procédure ;
- des clichés anthropométriques.

Ces données sont conservées pour une durée maximum de 25 ans.

A noter : le FAED alimente le fichier européen Eurodac (un système d'information contenant les empreintes digitales des demandeurs d'asile et immigrants illégaux se trouvant sur le territoire de l'UE) et peut également être consulté via Europol (agence de l'UE pour la lutte contre la criminalité transfrontalière).

FNAEG: Fichier National Automatisé des Empreintes Génétiques[27]

Créé en 1988, le fichier naît de la volonté du ministre de la Justice, suite à une série de viols et crimes dont l'auteur avait déjà été condamné pour d'autres délits sexuels et avait été libéré sans que le rapprochement avec des viols précédents ait pu être fait. Placé sous la responsabilité de la Direction centrale de la police judiciaire au ministère de l'Intérieur, il a pour objectif de faciliter l'identification et la recherche des auteurs d'infractions, ainsi que des personnes disparues, à l'aide de leur profil génétique. Initialement, le FNAEG était uniquement destiné à centraliser les empreintes génétiques des délinquants sexuels. Au fur et à mesure, six textes de lois vont étendre son champ d'application à d'autres infractions, jusqu'aux **délits de vols, d'extorsions, de destructions et détériorations, de menaces d'atteinte aux biens** ainsi qu'aux simples suspects[iii]. La question de l'élargissement du champ d'application du FNAEG est toujours d'actualité. De plus le refus de se soumettre aux opérations de prélèvement ordonnées par l'officier de police judiciaire est passible d'un an d'emprisonnement et de 15 000 euros d'amende.

Le fichier centralise essentiellement les empreintes génétiques des personnes déclarées coupables ou pénalement irresponsables, poursuivies, ou suspectées en raison d'indices graves pour l'une des (nombreuses) infractions énumérées par la loi. Ces empreintes sont complétées :

- des nom, prénoms, date et lieu de naissance, filiation et sexe (pour les empreintes identifiées) ;
- du numéro de la procédure ;
- de l'autorité judiciaire ou l'officier de police judiciaire ayant demandé l'enregistrement au fichier ;
- de la date de la demande d'enregistrement ou de la condamnation ;
- du nom de la personne physique ou morale habilitée ayant réalisé l'analyse de la nature de l'affaire.

Ces informations sont conservées pour une durée de 25 ans à 40 ans maximum selon les cas.

A noter : le FNAEG ne fait l'objet d'aucune interconnexion au niveau national. Cependant, les fichiers génétiques des 28 Etats membres de l'Union européenne sont mis en réseau. De plus, certaines empreintes génétiques enregistrées peuvent être transmises par des organismes de coopération internationale en matière de police judiciaire ou des services de police étrangers. Inversement, les données enregistrées au FNAEG peuvent être consultées par des agents d'organismes de coopération internationale en matière de police judiciaire ou par les agents des services de police ou de justice d'Etats étrangers pour effectuer des rapprochements (notamment via Interpol[28]).

27. http://www.legifrance.gouv.fr/affichCodedo;jsessionid=D60621176232F5D3B8653AA6B60EC750.tpdjo08v_1?idSectionTA=LEGISCTA000006137412&cidTexte=LEGITEXT000006071154&dateTexte=20040601

28. Organisation de police internationale regroupant 190 pays.

STIC: Système de Traitement des Infractions Constatées

Créé officiellement le 5 juillet 2001[29], le STIC est le résultat d'un projet de modernisation de la police nationale initié en 1985. Il a d'abord fonctionné de manière expérimentale, puis a commencé à être exploité à partir de 1994. Ce n'est qu'en 1998, suite à une fuite de la presse, que la CNIL va pouvoir émettre un avis favorable contraignant assorti de plusieurs réserves, dont l'interdiction de l'utiliser à des fins administratives (par exemple dans le cadre de vérifications pour l'exercice de certaines professions réglementées). En 2001, il bénéficie enfin d'une existence légale, après une utilisation « clandestine » de plus de 6 ans. Cette absence de législation empêchait les personnes concernées d'exercer leur droit d'accès et de rectification. D'abord utilisé dans le cadre des enquêtes de police, le STIC présente à nouveau une fonction administrative suite au vote de la loi relative à la sécurité quotidienne du 15 novembre 2001 (votée sous l'influence de l'émotion suscitée par les attentats du 11/09/2001), puisqu'il peut à nouveau être consulté à des fins administratives dans le cadre du recrutement, de l'habilitation ou de l'agrément de personnels de professions diverses en relation avec la sécurité (personnels de surveillance et de gardiennage, personnes souhaitant travailler dans les zones aéroportuaires, agents de police municipale, gardes champêtres, préfets, ambassadeurs, directeurs et chefs de cabinets des préfets, magistrats…), ainsi que dans le cadre des procédures de naturalisation et des attributions de décorations honorifiques.

L'article R40-23 Code de procédure pénale prévoit la fusion prochaine du STIC avec Judex, le fichier équivalent de la gendarmerie, sous un même traitement automatisé dénommé « traitement d'antécédents judiciaires » (TAJ). Le 31 décembre 2013 le STIC aurait donc dû être supprimé définitivement.

Le STIC est sous la responsabilité de la Direction générale de la police nationale, et est utilisé afin de faciliter la constatation des infractions à la loi pénale (dépôt de plaintes), le rassemblement des preuves et la recherche de leurs auteurs. Il permet aussi de produire des statistiques.

Il contient des informations concernant plus de 6,8 millions de personnes à l'encontre desquelles ont été réunis des indices ou des éléments graves et concordants attestant de leur participation à la commission d'un crime, d'un délit ou de certaines contraventions de 5e catégorie lors d'une enquête, ou victime de l'une de ces infractions.

Pour les personnes mises en cause, les données pouvant être enregistrées sont : l'identité (nom, nom marital, nom d'emprunt officiel, prénoms, sexe), le surnom, l'alias, la date et le lieu de naissance, la situation familiale, la filiation, la nationalité, l'adresse(s), la profession(s), l'état de la personne, le signalement, la photographie.

Pour les victimes, les données pouvant être enregistrées sont **:** l'identité (nom, nom marital, nom d'emprunt officiel, prénoms, sexe), la date et le lieu de naissance, la situation familiale, la nationalité, l'adresse, la profession, l'état de la personne, le signalement et la photographie des personnes disparues et des corps non identifiés.

Des données sensibles peuvent également être inscrites si elles résultent de la nature ou des circonstances de l'infraction ou si elles se rapportent à des signes physiques particuliers, objectifs et permanents, en tant qu'éléments de signalement des personnes. Ces informations doivent être nécessaires à la recherche et à l'identification des auteurs d'infractions pénales.

Toutes ces données sont également accompagnées des informations concernant les faits, l'objet de l'enquête, les lieux, les dates de l'infraction et les modes opératoires, ainsi que les informations relatives aux objets.

Les informations sont conservées de 5 à 40 ans selon la gravité de l'infraction. Les informations concernant les mis en cause mineurs sont conservées cinq ans.

29. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000589796

TAJ : Traitement des Antécédents Judiciaires

Créé le 4 mai 2012 par le décret n° 2012-652[30] , le TAJ est un « super-fichier » de la Direction générale de la police nationale et de la Direction générale de la gendarmerie nationale ayant pour objectif de fournir des informations aux enquêteurs de la police, de la gendarmerie nationale et de la douane judiciaire afin de faciliter la constatation des infractions, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs. Il provient de la fusion du STIC (Système de traitement des infractions constatées de la police nationale) et de JUDEX (Système judiciaire de documentation et d'exploitation de la gendarmerie nationale). Cependant, il va plus loin que la simple réunion de ces deux fichiers puisqu'il contient de nouvelles données (la photographie des personnes physiques). En juin 2013, il contenait les informations de plus de douze millions (12,2 millions) de personnes (personnes mises en cause, victimes, et personnes faisant l'objet d'une enquête), 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.

TES : Titres Electroniques Sécurisés

Créée en 2005, la base de données TES a pour fonction la prise en compte des procédures d'établissement, de délivrance, de renouvellement et de retrait des passeports. Elle sert également à prévenir et détecter la falsification et la contrefaçon des passeports. Elle concerne toutes les personnes faisant une demande de passeport biométrique et contient :

- des données relatives au titulaire du passeport : le nom de famille, les prénoms, le nom dont l'usage est autorisé par la loi, la date et le lieu de naissance, le sexe, la couleur des yeux, la taille, le domicile ou la résidence ou la commune de rattachement de l'intéressé ou l'adresse de l'organisme d'accueil auprès duquel il est domicilié le cas échéant, la décision attestant la capacité juridique du demandeur et **l'image numérisée du visage et celle des empreintes digitales** ;
- des informations relatives au passeport ;
- des données relatives au fabricant du passeport et aux agents chargés de la délivrance du passeport ;
- les images numérisées des pièces du dossier de demande de passeport.

Ces données sont conservées pendant 15 ans pour les titres délivrés à des majeurs, soit au-delà de la durée de validité du titre, et pendant 10 ans pour les titres délivrés à des mineurs.

Dans le texte définitif de la proposition de loi relative à la « protection de l'identité » (texte adopté le 6 mars 2012), il était prévu de regrouper toutes les données biométriques des citoyens français demandant un passeport ou une carte d'identité dans la base TES. Le fichier aurait pu être consulté par les services de police, permettant ainsi d'identifier les personnes au cours d'enquêtes relatives à certaines infractions à partir de leurs données biométriques. Cependant, le Conseil constitutionnel a censuré ces dernières dispositions au nom du droit au respect de la vie privée, considérant que l'atteinte portée à ce droit n'était pas proportionnée au but poursuivi (« *préserver l'intégrité des données requises pour la délivrance du passeport français et de la carte nationale d'identité* »[31]) [32].

Par ailleurs, le règlement (CE) n° 444/2009 du Parlement européen et du Conseil du 28 mai 2009[33] modifiant le règlement (CE) n° 2252/2004 du Conseil établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les Etats membres **ne demande que 2 empreintes et une photo** enregistrées dans le passeport.

30. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025803463&categorieLien=id
31. Article 5 de la proposition de loi relative à la protection de l'identité. http://www.assemblee-nationale.fr/13/ta/ta0883.asp
32. Décision n° 2012-652 DC du 22 mars 2012 : *« Considérant, (…) ; que les dispositions de la loi déférée autorisent la consultation ou l'interrogation de ce fichier non seulement aux 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 également à d'autres fins de police administrative ou judiciaire ; Considérant qu'il résulte de ce qui précède qu'eu égard à la nature des données enregistrées, à l'ampleur de ce traitement, à ses caractéristiques techniques et aux conditions de sa consultation, les dispositions de l'article 5 portent au droit au respect de la vie privée une atteinte qui ne peut être regardée comme proportionnée au but poursuivi ».* http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=CEF2E0C98643596D19E7BF1B9FE1F5E7.tpdjo17v_1&dateTexte=?cidTexte=JORFTEXT000025582452&categorieLien=cid
33. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:142:0001:01:FR:HTML

A noter : le fichier est notamment mis en relation lors de l'instruction des demandes de passeport avec le Fichier des Personnes Recherchées (FPR) afin de vérifier qu'aucune décision judiciaire ni aucune circonstance particulière ne s'oppose à sa délivrance. De même, le système de fabrication et de gestion informatisée des cartes nationales d'identité est consulté afin de vérifier si des titres ont déjà été sollicités ou délivrés sous l'identité du demandeur.

La base TES est également interconnectée avec les systèmes d'information Schengen (SIS II) et INTERPOL. Cette interconnexion porte sur les informations relatives aux numéros des passeports perdus ou volés ainsi que sur l'indication relative au pays émetteur, au type et au caractère vierge ou personnalisé du document[34].

2. Garanties prévues par la législation

- **FAED :**
  - le fichier est sous le contrôle d'un magistrat de l'ordre judiciaire ;
  - le FAED ne peut faire l'objet d'aucune interconnexion avec un autre traitement automatisé d'informations nominatives.

- **FNAEG :**
  - le fichier est sous le contrôle d'un magistrat du parquet assisté d'un comité de trois personnes, nommées pour trois ans par le ministre de la justice ;
  - le 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, sauf avec ceux conservant les scellés des traces et échantillons biologiques ;
  - les empreintes génétiques conservées dans le fichier sont réalisées à partir de segments d'acide désoxyribonucléique réputés non codants, à l'exception du segment correspondant au marqueur du sexe (c'est-à-dire qu'ils doivent permettre d'identifier les personnes mais n'apporter aucune autre information). Toutefois des chercheurs ont découvert que ce n'est plus exact, voir le § « *Risques dus aux possibilités d'utilisation* ».

- **OSCAR :** les données biométriques n'ont aucun destinataire, car elles sont uniquement utilisées à des fins de comparaison.

- **STIC :**
  - le fichier est sous le contrôle du procureur de la République territorialement compétent ;
  - les consultations font l'objet d'un enregistrement comprenant l'identifiant du consultant, la date et l'heure de la consultation ainsi que sa nature administrative ou judiciaire. Ces données sont conservées pendant un délai de trois ans ;
  - le directeur général de la police nationale doit rendre compte chaque année à la CNIL de ses activités de vérification, de mise à jour et d'effacement des informations enregistrées dans le traitement.

34. Article 23 du décret n°2005-1726 du 30 décembre 2005 relatif aux passeports
http://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=1076B8D1300A6FA4A04DD5D837413928.tpdjo17v_1?idArticle=LEGIARTI000006286513&cidTexte=LEGITEXT000018763666&dateTexte=20140305

3. Rôle de la Cnil

Traitement des Antécédents Judiciaires (TAJ)

Malgré le fait que le TAJ présente des garanties qui faisaient défaut au STIC et au JUDEX, la CNIL a émis **certaines réserves** à son sujet dans sa délibération n° 2011-204 du 7 juillet 2011.

Tout d'abord, elle craint que le nouveau fichier TAJ contienne les **nombreuses erreurs déjà présentes dans le STIC et le JUDEX,** et demande que des mesures concrètes soient prises pour que les **données reprises soient exactes et mises à jour**. De plus, le traitement TAJ peut porter sur des données **sensibles** (origines raciales ou ethniques, opinions politiques, philosophiques ou religieuses ou appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci) qui ne doivent pas permettre de sélectionner des personnes en fonction de ces critères. Le TAJ contient également une nouvelle fonctionnalité d'identification des personnes à partir de l'analyse biométrique de la morphologie de leur visage. La CNIL estime que cette fonctionnalité présente des **risques importants pour les libertés individuelles**, et demande le contrôle de son utilisation. Elle rappelle aussi que le « **droit à l'oubli** » doit être particulièrement garanti, notamment concernant les mineurs, et remarque que les **délais de conservation sont parfois très importants** et supérieurs aux délais de prescription.

La CNIL estime que la sécurité du TAJ est assurée par des mesures particulièrement appropriées :

- hébergement dans des conditions de sécurité physique d'un niveau élevé ;
- sécurité renforcée de l'infrastructure technique et des logiciels ;
- l'accès à l'application n'est possible qu'après identification puis authentification des utilisateurs.

Pour plus de sécurité, la CNIL recommandait un audit de sécurité du TAJ dès sa mise en œuvre.

Contrôles : le directeur général de la police nationale et le directeur général de la gendarmerie nationale doivent **rendre compte tous les ans à la CNIL des opérations de vérification, de mise à jour et d'effacement des informations** enregistrées dans le TAJ.

De plus, **la mise à jour des données enregistrées** devrait être garantie par **l'interconnexion du TAJ avec le traitement Cassiopée,** qui permettra la transmission automatique des suites des procédures judiciaires.

Concernant la transmission des données des fichiers STIC et JUDEX dans le TAJ, la CNIL estime qu'une **mise à jour préalable des données est indispensable**, afin que le TAJ ne soit pas affecté des erreurs contenues dans ces deux fichiers. Cependant**, il n'a pas été prévu de mettre à jour les fiches issues du STIC et de JUDEX,** avant leur versement dans TAJ. C'est le « vain » constat qu'a encore fait la CNIL dans ses contrôles de 2012-2013 (voir partie STIC). La CNIL estime que le TAJ concernera 61 194 991 procédures, 12 057 515 personnes physiques mises en cause et 39 819 811 personnes physiques victimes.

Système de Traitement des Infractions Constatées (STIC)

En 1998 et 2000, alors que son avis était contraignant, la CNIL a donné « *un avis favorable sous réserves* ». Un nouvel avis en 2005 (délibération 2005-187 du 8 septembre 2005), non contraignant, donnait **autorisation** des modifications apportées par le projet de loi n° 2003-239 du 18 mars 2003.

Utilisé de manière expérimentale, puis exploité à partir de 1994, sans avis de la CNIL, le STIC a reçu **un avis favorable contraignant assorti de quelques réserves** de la CNIL en 1998. La CNIL demandait l'interdiction de l'utiliser à des fins administratives (par exemple pour l'exercice de certaines professions réglementées). Ce n'est qu'en 2001 que le décret d'application (du 5 juillet 2001) lui donne une existence légale. Pendant plus de 6 ans, les personnes concernées n'ont pas eu la possibilité d'exercer leurs droits d'accès et de rectification, elles ne pouvaient alors que procéder à une demande de contrôle auprès de la CNIL, sans plus d'indications sur la suppression ou la modification des données.

En 2007, une décision du président de la CNIL n°207049C, prévoyait un mécanisme de contrôle du STIC. Cependant, lors des vérifications du STIC effectuées par la CNIL en 2007/2008 (publié en 2009), celle-ci a établi que **80 % des fiches contenaient des erreurs** (inversion victime/auteur, absence des suites judiciaires, requalification des faits non-enregistrée, etc.).

Ces erreurs sont souvent dues à des défauts de mise à jour. De nouveaux contrôles ont été effectués fin 2012 et début 2013 par la CNIL qui a constaté que le fonctionnement du STIC n'a pas connu d'évolution réelle et les défaillances relevées en 2009 persistent. Aucune mise à jour n'est prévue, et des millions de fiches contiennent toujours des erreurs qui seront donc répercutées dans le TAJ. Pour remédier à ces « *dysfonctionnements* », la CNIL a soumis 10 propositions aux ministères de l'Intérieur et de la Justice avec lesquels selon elle, la coopération a été « *très bonne* ». Elle préconise avant tout une mise à jour prioritaire des fiches « *les plus sensibles* » reprises dans le TAJ, celles concernant les mineurs, les faits de nature criminelle, et les infractions les plus récentes. La CNIL met aussi en cause les procureurs de la République qui respectent de manière « *très imparfaite* » leur obligation de transmettre au ministère de l'Intérieur les mesures favorables aux personnes initialement mises en cause : classement sans suite, non-lieu, relaxe, acquittement. Or, cette mise à jour, une fois réalisée, peut pourtant conduire à l'effacement de la fiche.

Il n'est toutefois pas possible de trouver des réactions du ministère de l'Intérieur ou de la Justice concernant ce rapport de la CNIL

Fichier National Automatisé des Empreintes Génétiques (FNAEG)

Délibération n° 99-052 du 28 octobre 1999 donnait un avis favorable.

Délibération n° 2008-113 du 14 mai 2008[35].

Lors de l'extension des infractions pouvant conduire au fichage dans le FNAEG, en 2002, la CNIL a émis un avis **favorable.** Cette extension ajoutait aux infractions de nature sexuelles les crimes d'atteintes volontaires à la vie de la personne, de torture et actes de barbarie et de violences volontaires, les actes de terrorisme, ajoutait aussi subrepticement les actes de destructions, dégradations et détériorations dangereuses, ce qui ouvrait la porte aux dérives que l'on connait de fichage de militants.

Dans sa délibération, la CNIL estimait que les modalités techniques prévues pour assurer la concordance entre un profil ADN transmis et un profil ADN enregistré dans le fichier d'analyse de la partie contractante sont conformes aux stipulations du traité de Prüm et aux accords d'exécution. Elle prenait acte de ce que l'accès au système serait réservé à des agents habilités, et les accès (aux locaux, au réseau informatique) protégés et sécurisés. Mais elle relevait que les préconisations en matière de traçage des accès (journalisation d'un certain nombre de données) n'étaient pas conformes aux dispositions du traité dans la mesure où le processus ne permet pas d'identifier l'agent qui est à l'origine de la demande. Elle demandait au ministère de l'Intérieur (en application de l'article 39-5 du traité de Prüm) de prendre toutes les dispositions pour lui permettre d'exercer des contrôles aléatoires pour vérifier la légitimité des transmissions, et d'exercer les droits d'accès indirect pour les contrôles sur ce fichier.

Pourtant le Conseil constitutionnel saisi (septembre 2010) sur la conformité aux droits et libertés que la Constitution garantit par rapport à certaines dispositions du Code de procédure pénale relatives au FNAEG a estimé (se fondant sur l'article 9 de la Déclaration de 1789 qui, en matière de procédure pénale, proscrit « *toute rigueur qui ne serait pas nécessaire* ») que, concernant les infractions permettant un prélèvement d'empreintes génétiques aux fins de rapprochement avec les données du fichier, en raison du principe de proportionnalité, la commission d'une simple contravention ou d'un délit non visé par l'article du CPP ne peut donc conduire à un tel prélèvement aux fins de rapprochement et que la durée de conservation, qui doit être fixée par décret, doit être proportionnée à la nature ou à la gravité des infractions concernées, avec adaptation de ces modalités à la délinquance des mineurs. Réserves qui auraient dû être relevées par la CNIL lors de ses délibérations.

Fichier automatisé des Empreintes Digitales (FAED)

En octobre 1986 la CNIL a émis un avis favorable au projet qui lui était soumis, considérant la finalité légitime et que toutes les garanties seraient apportées à l'exercice du droit des personnes et notamment :
- l'enregistrement des personnes ne se ferait que dans le cadre d'une enquête pour crime ou délit flagrant, d'une enquête préliminaire, d'une commission rogatoire ou de l'exécution d'un ordre de recherche délivré par une autorité judiciaire ;

38. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020788622

- les informations enregistrées ne concerneraient que les personnes mises en cause dans une procédure judiciaire ou celles contre lesquelles des indices graves auront été réunis ;
- le Procureur Général près la Cour d'Appel de Paris pourra demander la destruction des informations lorsque leur conservation ne paraîtrait manifestement plus utile ;
- seul le personnel dûment habilité du service d'identité judiciaire du ministère de l'Intérieur et des unités de recherches de la gendarmerie nationale pourront avoir accès aux informations enregistrées.

Elle attirait toutefois l'attention sur les conséquences d'éventuelles intrusions lors de la transmission des informations du site central vers les sites régionaux ou locaux et vice-versa tant en ce qui concerne la consultation que la saisie création.

La CNIL est destinataire d'un rapport annuel par la direction centrale de la police judiciaire du ministère de l'Intérieur (responsable du FAED, sous le contrôle d'un magistrat de l'ordre judiciaire). Elle a, dans un communiqué du 28 décembre 2008, rappelé la nécessité d'encadrer et de limiter l'usage des empreintes digitales dans le traitement de données à caractère personnel. En avril 2013, cette conservation abusive a valu à la France une condamnation par la CEDH[36].

4. Risques

Risques dus aux dangers contenus dans la législation

‣ Risques dus au nombre excessif de données pouvant être enregistrées

- AGDREF 2 : la longue liste de données susceptibles d'être enregistrées suppose le risque d'un enregistrement excessif de données au vu des finalités du fichier.

‣ Risques dus à l'étendue des personnes pouvant être enregistrées

- AGDREF 2 : le fichier cible les étrangers, mais contient également des informations sur leur famille, entourage et personnes les hébergeant. Pour les hébergeants, cela pose le risque de se voir suspectés d'avoir organisé un séjour irrégulier.
- FNAEG : au 31 août 2012, le FNAEG contenait les profils génétiques de plus de 2 millions d'individus dont 1 641 176 personnes mises en causes et 398 698 personnes condamnées. Cela signifie que 80 % des empreintes génétiques enregistrées concernent des personnes présumées innocentes.

‣ Risques dus aux possibilités d'utilisation

- FNAEG : utilisation de la technique de la « familial search » ou recherche familiale (notamment utilisée dans l'affaire du meurtre d'Elodie Kulik). Il s'agit, à partir d'un ADN retrouvé sur les lieux d'une infraction, de procéder à un rapprochement permettant d'identifier un membre de la famille possiblement enregistré au FNAEG. L'usage de cette technique signifierait qu'indirectement, des millions de personnes peuvent être enregistrées au FNAEG sans le savoir.
- FNAEG : alors que la loi prévoit que les empreintes génétiques sont réalisées à partir de segments d'acide désoxyribonucléique non codants, les progrès de la génétique démontrent que les marqueurs génétiques sélectionnés pour l'inscription dans le FNAEG pourraient donner des informations sur l'origine géographique de la personne concernée ou sur certaines prédispositions pathologiques**.**
- STIC : le STIC est aussi utilisé pour les enquêtes administratives, ce qui peut avoir et a déjà eu des conséquences graves au niveau de l'emploi et du recrutement (notamment dans le secteur des services privés de sécurité), de la présentation aux concours administratifs, ou des attributions de décorations honorifiques. En effet, des données erronées ont déjà conduit à des pertes d'emploi ou des refus de recrutement dans le domaine de la sécurité sur base d'erreurs ou d'enquêtes sur des affaires familiales sans aucun lien. De plus**,** les mesures adoptées pour limiter l'accès aux données dans le cadre d'enquêtes administratives ne sont pas toujours appliquées, ce qui peut porter préjudice aux personnes concernées (le profil judiciaire permet d'accéder à l'ensemble des informations enregistrées dans le STIC contrairement au profil administratif. Il faut savoir qu'au total, la consultation du STIC à des fins d'enquête administrative est susceptible de concerner aujourd'hui plus d'un million d'emplois.

36. http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-118597#{«itemid»:[«001-118597»]}. Voir aussi « Fichiers : la France condamnée par la Cour européenne des droits de l'Homme (CEDH) », Patrick Canin. http://www.ldh-france.org/Fichiers-la-France-condamnee-par.html

- TAJ : le fichier contient une fonctionnalité d'identification des personnes à partir de l'analyse biométrique de la morphologie de leur visage (reconnaissance faciale). Cette fonctionnalité peut présenter des risques importants pour les libertés individuelles, et un contrôle de son utilisation est nécessaire.

‣ Risques dus aux oublis de la législation

- FNAEG : le fichier ne contient aucune disposition protectrice pour les mineurs (durée de conservation, information, consentement des détenteurs de l'autorité parentale), dont les empreintes génétiques peuvent être enregistrées.

‣ Risques dus aux possibilités d'interconnexion

- STIC : le STIC est mis en relation avec JUDEX (Système judiciaire de documentation et d'exploitation), le TAJ (Traitement d'antécédents judiciaires, fusion du STIC et Judex), VISABIO (traitement informatisé de données personnelles biométriques avec photographie numérisée et empreintes digitales des 10 doigts des demandeurs de visas), Cassiopée (Chaîne applicative supportant le système d'information orienté procédure pénale et enfants), et le Casier National Judiciaire or, le STIC contient de nombreuses erreurs qui peuvent « contaminer » les autres fichiers.

‣ Risques dus au traitement de données sensibles

- TAJ : le fichier peut contenir des données concernant les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci. Ces données sensibles ne devraient pas permettre de sélectionner des personnes dans le fichier en fonction de ces données.

‣ Risques dus aux délais de conservation

- TAJ : les délais de conservations au sein de ce fichier sont parfois très importants et supérieurs aux délais de prescriptions pour l'infraction commise. La CNIL a rappelé à ce sujet l'importance du droit à l'oubli, surtout concernant les mineurs.

Risques dus au non-respect des garanties prévues par la législation

‣ Risques dus aux manquements liés au respect de la finalité du fichier

- AGDREF 2 : le nombre important d'entités pouvant consulter le fichier (préfectures, consulats, services de police et unités de gendarmerie, Office français de protection des réfugiés et apatrides, Office français de l'intégration et de l'immigration, caisses de sécurité sociale et Pôle emploi) risque d'entraîner des utilisations du fichier non prévues par la loi.

Risques dus aux absences de mise à jour

- STIC : si le STIC contient de nombreuses erreurs, cela est surtout dû à l'absence de mise à jour des informations, conséquence de la mauvaise communication entre la police et la justice. De ce fait, le fichier n'est pas toujours modifié lors d'une requalification des faits ou d'un non-lieu prononcé par la justice par exemple, ce qui signifie que de nombreuses personnes sont inscrites au STIC alors qu'elles ne devraient pas y être.

‣ Risques dus au non-accomplissement des garanties de sécurité prévues par la loi

- STIC *:* alors que la loi prévoit que les consultations du fichier font l'objet d'un enregistrement, dans son rapport de 2009, la CNIL constate que cette traçabilité n'est pas exploitée car cette fonction de contrôle n'est quasiment jamais utilisée**,** et aucun système d'alerte ne permet d'avertir d'une utilisation anormale**.**

‣ Risques dus au non-respect des modalités d'inscription

- FNAEG *:* le FNAEG serait alimenté de manière illégale. Aors que les empreintes génétiques de personnes mises en garde à vue ne peuvent pas être conservées mais seulement utilisées pour faire des rapprochements, les officiers de police judiciaire cochent systématiquement la case « suspect : indices graves ou concordants » dans les réquisitions qu'ils adressent au FNAEG, ce qui permet leur enregistrement. Même si, dans les textes, les procureurs de la République et les juges d'instruction doivent effacer les empreintes abusivement conservées, cela ne garantit pas que cet effacement soit effectué dans les faits (d'autant plus que cela concerne un grand nombre de personnes).

5. Abus

Les exemples d'abus

▸ **FNAEG** : la police relève quasi systématiquement l'ADN de toutes les personnes en garde à vue alors qu'une personne non condamnée à titre définitif est présumée innocente.

▸ **STIC. D**e nombreuses affaires ont démontré le manque de sécurisation, de mise à jour et de contrôle des fichiers :
- divulgation des fiches STIC de célébrités. Exemple : début 2013, des informations au sujet de rappeurs français ont été soustraites par téléphone à des commissariats et diffusées sur Internet ;
- accès aux informations au bénéfice d'entreprises privées (affaire Ikéa : en 2003, la Direction Risque d'Ikea aurait passé un accord avec des enquêteurs privés, anciens policiers, dans le but d'obtenir des informations issues du fichier STIC concernant certains de ses salariés, mais aussi certains clients dans le cadre de recouvrement de dettes. En mars 2012, une nouvelle enquête a été ouverte par le parquet de Versailles pour les mêmes faits de la part de l'enseigne Ikéa) ;
- en 2008, l'ex-commandant Philippe P. divulgue volontairement les fiches STIC de deux personnalités du « show-business » afin de dénoncer les irrégularités et le fonctionnement illégal du STIC et alerter l'opinion publique des dangers liés à l'existence de ce fichier. Il a été révoqué de la Police nationale pour cette raison. Poursuivi pour « *violation du secret professionnel* » pour avoir communiqué des fiches du STIC (il avait lui-même souffert d'une homonymie dans le Judex qui a retardé sa promotion au grade de commandant), le tribunal correctionnel de Paris ne l'a condamné qu'à une peine symbolique de 1 500 euros d'amende avec sursis en 2013 ;
- certaines qualifications des personnes fichées touchent à la dignité des personnes : « autiste », « homosexuel », « travesti », etc.

Le site de la CNIL relate quelques expériences d'individus ayant recouru à la CNIL afin d'obtenir la suppression de leurs données après avoir subi un préjudice suite à leur inscription dans le STIC[37] :
- refus d'agrément d'agent de recherche suite à une accusation d'usurpation d'état civil dont le classement sans suite n'avait pas été transmis à la police par la justice ;
- licenciement d'un agent de surveillance suite à son inscription dans le STIC pour violence volontaires. Or, entre temps, l'affaire avait été requalifiée en violences légères et le délai de conservation des informations pour ce type d'infraction était expiré : ses données auraient dues être supprimées ;
- avenir professionnel compromis pour un mineur enregistré au STIC alors qu'aucune charge n'avait été retenue contre lui : son signalement dans le STIC n'aurait pas dû avoir lieu.

(Voir aussi la note en fin de document : exemples de plaintes instruites par la CNIL[ii]).

Abus potentiels selon des organisations de la société civile

▸ **AGDREF 2** : mobilisation de certaines associations de défense des droits de l'Homme et des droits des étrangers (GITSI, Cimade, LDH, etc.).

▸ **FNAEG** : mobilisation de la LDH et du Syndicat de la Magistrature. Le communiqué du 21 novembre 2011 « *FNAEG ne vous en fichez pas* » appelle à s'opposer au développement illégitime du FNAEG et demande :
- que ne soient inscrites au FNAEG que les personnes effectivement condamnées ;
- que le nombre d'infractions pouvant conduire à une inscription soit réduit ;
- que les délais de conservation soient mieux adaptés ;
- que toute forme de réhabilitation permette l'effacement des données au fichier.

▸ **STIC** : campagnes de la Ligue des droits de l'Homme et articles de presse suite aux différentes affaires mettant en cause le fichier STIC.

37. http://www.Cnil.fr/les-themes/police-justice/fiche-pratique/article/stic-histoires-vecues/

6. Les recours contre ces fichiers

▸ **AGDREF 2** : demande d'annulation du décret de création d'AGDREF 2 par le GITSI, la Cimade et la LDH devant le Conseil d'Etat le 7 mai 2012. Les trois associations soulèvent les points suivants :

- les possibilités de mise en relation avec d'autres traitements et de consultation envisagées par le décret pourraient aboutir à des utilisations du fichier incompatibles avec finalités du traitement (notamment par la police qui pourrait utiliser certaines informations pour procéder à des enquêtes ou arrestations) ;
- elles estiment que l'enregistrement d'images numérisées de la photographie et des empreintes digitales des dix doigts porte atteinte à la vie privée et à la liberté individuelle des personnes ;
- elles soulèvent le caractère excessif de la liste de données enregistrées, de la liste des destinataires et de la durée de conservation des données.

L'ensemble des points soulevés a cependant été rejeté par le Conseil d'Etat (Cour suprême administrative) qui a déclaré le décret valide.

▸ **FAED** : la CEDH, dans une décision du 18 avril 2013, M.K contre France, devenue définitive le 18 juillet 2013, a considéré que la conservation des empreintes au fichier automatisé des empreintes digitales (FAED) d'une personne qui n'a fait l'objet d'aucune condamnation, constituait une atteinte disproportionnée au droit au respect de la vie privée garanti par l'article 8 de la Convention européenne des droits de l'Homme. La Cour a aussi considéré que la règlementation n'est pas assez précise. Elle fait référence à son propre arrêt du 4/12/2008 S et MARPER/Royaume Uni qui reconnaissait déjà que la conservation illimitée des données de personnes non condamnées est une violation du droit à la protection de la vie privée.

Cette décision est une avancée concernant le fichage biométrique et essentielle car elle fixe des limites à la « simple conservation » des données personnelles.

▸ **FNAEG**

• En 2010, saisi d'une question prioritaire de constitutionnalité sur la loi mettant en place le FNAEG (décision n° 2010-25 QPC du 16 septembre 2010), le Conseil constitutionnel a émis deux réserves :

- la liste des infractions doit être strictement limitée a certains crimes et délits définis par l'article 706-55 du code de procédure pénale (crimes sexuels ou crimes de sang principalement), les simples contraventions ou les délits non spécifiés dans cet article ne pouvant conduire à un prélèvement et l'expression « *crime ou délit* » devant être comprise comme renvoyant à **une liste limitative d'infractions ;**
- il a demandé à ce que la durée de conservation des données soit fixée par décret et qu'elle soit « raisonnable », proportionnelle à la gravité de l'infraction et adaptée à l'âge de l'auteur de l'infraction (mineur ou majeur).

• De nombreuses affaires judiciaires liées au refus de prélèvement ADN, notamment par des militants syndicalistes. Par exemple, fin 2006, des faucheurs d'OGM refusent de se soumettre à un prélèvement biologique en vue d'une inscription au FNAEG**,** et dénoncent une atteinte aux libertés individuelles. Craignant qu'un recours devant la Cour européenne des droits de l'Homme (CEDH) ne mette en cause la légalité du FNAEG, le gouvernement français initie un règlement à l'amiable et propose 1 500 euros aux faucheurs en réparation du préjudice subi. La négociation est dévoilée dans la presse par les faucheurs concernés, violant le principe de confidentialité. De ce fait, la CEDH, dans une décision du 20 janvier 2012, déclare irrecevable le recours des faucheurs d'OGM contre la décision d'obligation de se soumettre à un prélèvement génétique (CEDH ; Mandil ; Barreau et A. ; Deceuninck contre France du 20 janvier 2012).

• Dans une question écrite du 19/01/2012 le sénateur J. Mézard s'inquiétait, à propos de l'extension des données figurant dans le FNAEG, du danger que « *cette immense base de données soit détournée de sa finalité première, grâce aux progrès technologiques qui permettront d'établir d'autres types de fichage à partir du profil génétique d'une personne* »[38].

38. http://www.senat.fr/questions/base/2012/qSEQ120121911.html

▸ **OSCAR** : recours de la Ligue des droits de l'Homme, du Groupe d'information et de soutien des immigrés, et de Imaginons un réseau Internet solidaire, devant le Conseil d'Etat, **rejeté le 20 octobre 2010**. Les trois associations contestaient principalement la collecte dans Oscar des données biométriques du bénéficiaire de l'aide au retour et de ses enfants de plus de 12 ans, ainsi que la durée excessive de conservation des données qu'elles jugeaient arbitraires et disproportionnées. Selon la LDH, « *le fichier Oscar constitue un instrument supplémentaire de contrôle et de stigmatisation de l'ensemble des étrangers susceptibles de bénéficier d'une aide au retour dite volontaire ou humanitaire, qu'ils soient ressortissants communautaires ou non* ».

▸ **TES**

• Dans une décision du 26 octobre 2011, le Conseil d'Etat, saisi par plusieurs recours (notamment de la Ligue des droits de l'Homme) a annulé partiellement l'article 5 du décret du 30 avril 2008. Celui-ci autorisait la conservation de huit empreintes digitales de chaque détenteur d'un passeport biométrique dans le fichier TES. Le Conseil d'Etat « *a jugé que la collecte et la conservation d'un plus grand nombre d'empreintes digitales que celles figurant dans le composant électronique ne sont ni adéquates, ni pertinentes et apparaissent excessives au regard des finalités du traitement informatisé. Il a donc annulé partiellement l'article 5 du décret, en tant qu'il prévoit la conservation des empreintes digitales qui ne figurent pas dans le composant électronique du passeport* ». Il a d'ailleurs rappelé que le règlement européen du 13 décembre 2004 (établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les Etats membres) ne prévoyait que le stockage de deux empreintes digitales. Par cette décision, le Conseil d'Etat exprime implicitement son refus de voir la base TES se transformer en un fichier de police utilisé à des fins judiciaires.

• Le 22 mars 2012, le Conseil constitutionnel, saisi dans le cadre de la loi relative à la protection de l'identité, annule les dispositions rendant possible l'identification d'une personne à partir de ses empreintes digitales et permettant que les données enregistrées à partir des cartes d'identité et des passeports soient consultées à des fins de police administrative ou judiciaire. Il estime que ces dispositions constituent une atteinte inconstitutionnelle au droit au respect de la vie privée, et sont insuffisantes contre le risque d'arbitraire. Suite à cette décision, le projet de carte d'identité biométrique semble avoir été abandonné. En France la carte d'identité est facultative mais très répandue.

7. Points forts / points faibles / bonnes pratiques

Bonnes pratiques

▸ **FAED** : l'enregistrement des empreintes fait l'objet d'un contrôle de légalité (motif de signalisation) ainsi que d'un contrôle qualité (mentions alphanumériques et relevés digitaux) avant toute insertion en base de données. Les autres données (état civil, etc.) font l'objet d'une double saisie pour être ensuite associées aux empreintes digitales correspondantes.

▸ **OSCAR** : le fichier ne comporte pas de dispositif logiciel permettant d'indiquer, à partir d'empreintes présentées, l'identité d'une personne. Le but de l'exploitation du fichier des empreintes est seulement de vérifier que la personne qui présente une demande n'a pas déjà bénéficié d'une aide au retour par comparaison de ses empreintes à celles des empreintes enregistrées. Mais la présence de dix empreintes digitales reste tout à fait disproportionnée. Par ailleurs, les intéressés sont informés par écrit dans une langue qu'ils comprennent, des conditions de conservation des données les concernant, de leur droit d'accès à ces données et des destinataires de ces données. Cela permet de véritablement garantir le droit d'information des personnes concernées (qui ne comprennent pas forcément le français).

▸ **TES** : le traitement ne comporte pas de dispositif de reconnaissance faciale ni de dispositif d'identification à partir de l'image numérisée des empreintes digitales enregistrées dans le fichier qui ne comporte plus que 2 empreintes digitales. Néanmoins la nécessité de les conserver dans ce fichier central se pose. Voir l'exemple de l'Allemagne dont la loi ne prévoit pas de les conserver.

Evolution de la situation

Plutôt qu'une amélioration ou une aggravation : une absence de changement

- STIC : malgré les contrôles, il n'y a pas eu d'améliorations ni de changements positifs notables : lors du bilan publié en 2009 des vérifications du STIC effectuées par la CNIL en 2007/2008, celle-ci a établi que **80 % des fiches contenaient des erreurs** (inversion victime/auteur, absence des suites judiciaires, requalification des faits non-enregistrée…). Ces erreurs sont souvent dues à des défauts de mise à jour. Suite à ce contrôle, la CNIL avait émis dix recommandations aux autorités publiques dans le but de garantir une meilleure confidentialité et une meilleure qualité des données contenues dans le fichier. Parmi elles, la CNIL insistait notamment sur la mise en œuvre d'une procédure de sécurisation des opérations de saisie afin d'éviter les erreurs. Elle incitait également au respect des profils d'interrogation du fichier, en particulier en utilisant uniquement le profil administratif dans le cadre des enquêtes administratives. Enfin, elle invitait le ministère de la Justice à être en mesure de détecter et de prévenir les cas d'utilisation détournée du fichier grâce à une meilleure traçabilité des accès et à mettre en œuvre l'obligation de mise à jour du STIC en fonction des suites judiciaires concernant chaque mis en cause fiché lors de l'enquête.
- De nouveaux contrôles ont été effectués entre fin 2012 et début 2013 par la CNIL : elle constate que le fonctionnement du STIC n'a pas connu d'évolution réelle et les défaillances relevées en 2009 persistent. Aucune mise à jour n'est prévue, et des millions de fiches contiennent toujours des erreurs.
  Concernant le TAJ : bien qu'il présente des garanties qui faisaient défaut au STIC et au JUDEX, la CNIL a émis certaines réserves à son sujet[39]. Elle craint que le nouveau fichier TAJ contienne les nombreuses erreurs déjà présentes dans le STIC et le JUDEX, et demande que des mesures concrètes soient prises pour que les données reprises soient exactes et mises à jour (voir § suivant).

Développements actuels et prévisible

FNAEG : dans une réponse écrite au député Patrice Carvalho en avril 2013, le ministre de l'Intérieur indique que l'élargissement de la liste des délits pouvant conduire à un enregistrement au FNAEG, tels que les délits routiers et financiers, n'est pas envisagé car cela « *risquerait de soumettre les personnes concernées à une rigueur qui ne serait pas nécessaire au regard de la nature des faits commis* ».

STIC

• En réponse à la question écrite du député de la Seine-Saint-Denis, Daniel Goldberg, au sujet du STIC (publiée au Journal Officiel le 11/09/2012), le ministre de l'Intérieur, Manuel Valls, a promis une amélioration rapide de l'exactitude des informations et des indications de mise hors de cause grâce à la mise en service prochaine du fichier TAJ (traitement d'antécédents judiciaires). Un magistrat sera affecté à plein temps pour veiller à la mise à jour des fichiers de police en fonction de la décision judiciaire. Les procédures judiciaires faisant l'objet d'un classement sans suite ne seront plus consultables dans le cadre des enquêtes administratives afin d'éviter de porter préjudice à des personnes dans le cadre de leur recherche d'emploi (publiée au Journal officiel le 30/10/2012).

• Suite au contrôle du STIC, la CNIL a publié en juin 2013 dix recommandations à suivre pour résoudre les dysfonctionnements du STIC et du TAJ (son successeur). Ces recommandations visent à :

- sensibiliser les procureurs de la République à leurs obligations d'information sur les mesures favorables ;
- mettre à jour et corriger les fiches reprises dans TAJ, tout particulièrement les plus sensibles (mineurs notamment) ;
- renforcer les règles de confidentialité ;
- imposer aux autorités administratives de s'assurer des suites judiciaires en cas d'antécédents ;
- généraliser la coopération entre les différents services de police et de gendarmerie pour améliorer la mise à jour des fichiers ;
- limiter dans le temps l'accès aux données dans le cadre administratif et envisager la diminution de certaines durées de conservation.

39. Délibération n° 2011-204 du 7 juillet 2011 portant avis sur un projet de décret en Conseil d'Etat relatif à la mise en œuvre d'un traitement de données à caractère personnel dénommé « traitement de procédures judiciaires » (TPJ).

▸ **TAJ** : des échanges inter applicatifs entre la police, la gendarmerie et les parquets devraient permettre une mise à jour automatique des données (et non plus par le biais de fiches papier) et rendre ainsi les informations plus fiables. Cependant, seules les affaires à venir bénéficieront de ces améliorations : aucune mise à jour totale n'est prévue pour les affaires anciennes et déjà classées.

C. EDUCATION

1. Résumé des fichiers étudiés et leur but

BNIE/RNIE : Répertoire National des Identifiants Elèves, étudiants et apprentis

Créé en 2012, le RNIE est un fichier du ministère de l'Education nationale géré au niveau académique, qui a pour fonction l'attribution d'un identifiant national (INE) à chaque élève, étudiant ou apprenti au moyen d'une procédure automatisée. Cet identifiant unique permet de faciliter la gestion du système éducatif et le suivi statistique des élèves. Il remplace la « base nationale des identifiants élèves » (BNIE) créée en 2004 par un arrêté publié le 20 octobre 2008[40] (portant création d'un traitement automatisé de données à caractère personnel relatif au pilotage et à la gestion des élèves de l'enseignement du premier degré) mais sans jamais avoir été l'objet d'une réglementation publiée au Journal Officiel (l'application avait seulement fait l'objet d'une simple déclaration à la CNIL). Suite à de nombreuses critiques et de nombreuses polémiques relatives au contenu de la BNIE, plusieurs recours ont été formés devant le Conseil d'Etat. Ce dernier, dans un arrêt du 19 juillet 2010, avait donné trois mois au ministère de l'Education nationale pour légaliser la BNIE. Ce n'est que deux ans plus tard qu'est enfin publié l'arrêté portant création du RNIE qui apportait les modifications nécessaires à la BNIE (arrêté du 16 février 2012 portant création d'un traitement dénommé « répertoire national des identifiants élèves, étudiants et apprentis », nor : MENG1135335A, version consolidée au 24 mars 2012[41]).

Toutes les personnes suivant une scolarité dans un établissement d'enseignement scolaire ou d'enseignement supérieur, une formation dans un centre de formation d'apprentis, sont enregistrées dans le RNIE. Il contient, à leur sujet, l'identifiant national élève, étudiant ou apprenti (nombre aléatoire non signifiant), le nom de famille, le nom d'usage, les prénoms, le sexe, la date de naissance et le lieu de naissance et l'établissement fréquenté. Les données de Base élèves 1er degré sont conservées au maximum un an après la fin de la scolarité (dans le premier degré). Les parents peuvent s'adresser au directeur de l'école pour avoir accès aux informations les concernant (eux et leurs enfants).

Données à caractère personnel enregistrées dans le répertoire national des identifiants élèves, étudiants et apprentis :

- identifiant national élève, étudiant ou apprenti. Ce numéro est constitué de l'année scolaire d'immatriculation et d'un numéro d'ordre non signifiant ;
- nom de famille ;
- nom d'usage ;
- prénoms ;
- sexe ;
- date de naissance ;
- lieu de naissance (mention du « code commune » pour les personnes nées en France ou indication d'une « naissance à l'étranger » pour les autres).

40. http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=A417AE9E8D6F82D35AAD74CEDFC7256F.tpdjo15v_3?cidTexte=LEGITEXT000019713352&dateTexte=20091221

41. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025554438

LPC : Livret Personnel de Compétences expérimental

Créé et réglementé en 2009[42], le livret de compétences s'inscrit dans le projet d'une orientation positive des jeunes et fait suite à la recommandation 2006/962/CE du Parlement européen et du Conseil, du 18 décembre 2006, sur les compétences clés pour l'éducation et la formation tout au long de la vie[43]. Il doit permettre à chaque jeune, élève ou apprenti de valoriser ses compétences acquises dans le cadre scolaire et extrascolaire et de le rendre acteur de sa formation et de son orientation. Le livret de compétences doit aussi servir à établir un lien entre les établissements scolaires et d'autres partenaires extérieurs (associations, partenaires économiques). Il pourra également être utilisé lors des phases d'orientation, d'affectation et d'admission de l'élève. Le livret de compétences est construit progressivement par le jeune lui-même, ses enseignants, les associations ou organisations professionnelles partenaires de l'établissement, le tout en collaboration étroite avec les parents. Il s'agit en fait d'une sorte de CV de l'élève, regroupant ses compétences, diplômes, aptitudes, stages, échanges, etc., ainsi que des éléments d'autoévaluation et de réflexion sur le projet d'orientation.

Il est pour le moment en phase d'expérimentation, mais il devrait devenir obligatoire pour tous les élèves jusqu'au lycée. Devenu obligatoire à la rentrée 2011-2012, il est aussi depuis 2011 obligatoire pour obtenir le diplôme national du brevet. L'article 11 de la loi prévoit que « *lorsque l'élève entre dans la vie active, il peut, s'il le souhaite, intégrer les éléments du livret de compétences au passeport orientation et formation prévu à l'article L. 6315-2 du code du travail.* »

2. Garanties prévues par la législation

La législation concernant ces deux fichiers a connu de nombreuses modifications, notamment suite aux débats et recours qu'ils ont suscités.

3. Risques

Risques dus aux dangers contenus dans la législation

‣ Risques dus à l'attribution d'un numéro identifiant

- RNIE : grâce au numéro INE (Identification Nationale Elève), il est facile de lier le RNIE aux fiches base élèves du 1er et du 2nd degré qui contiennent beaucoup plus d'informations, dont les activités périscolaires (1er degré), la nationalité, les bourses, l'identité bancaire, les vœux d'affectation (2nd degré). De plus, ce numéro suit l'élève pendant toute sa vie scolaire et étudiante, mais aussi professionnelle. L'INE pourrait devenir un outil d'interconnexions permettant la traçabilité des élèves et porter préjudice à leurs choix d'orientation. La divulgation ou la dissémination de telles informations pourrait conduire à des situations d'orientation automatique dues au passé de l'élève. Elles constitueraient également une source d'informations précieuse pour la prospection commerciale et le ciblage des élèves (notamment les sociétés d'aide aux devoirs).

‣ Risques dus au contenu du fichier

- LPC : risque de discriminations par l'orientation automatique selon les compétences affichées dans le livret et ses détracteurs considèrent que l'Etat prépare un fichier informatique centralisé des compétences de tout individu dès sa petite enfance.

42 LOI n° 2009-1437 du 24 novembre 2009 relative à l'orientation et à la formation professionnelle tout au long de la vie http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021312490&categorieLien=id

43. http://europa.eu/legislation_summaries/education_training_youth/lifelong_learning/c11090_fr.htm

Risques dus au non-respect des garanties prévues par la législation

Risques dus aux détournements de finalité du fichier

- RNIE. Il existe un risque de détournement de la finalité du fichier : il pourrait permettre le contrôle de l'immigration et des familles sans-papiers, ou encore de l'absentéisme. Le RNIE a seulement une fonction de gestion, et il est donc important qu'il reste limité à cette fonction, et qu'il ne permette pas de rendre les élèves identifiables sur d'autres fichiers ayant des finalités différentes.

4. Rôle de la Cnil

Répertoire National des Identifiants Elèves, étudiants et apprentis (BNIE – RNIE)

- Récépissé de la CNIL délivré le 6 octobre 2011 pour RNIE.
- Son implantation, à titre expérimental, a débuté en 2005 et a été généralisé en 2009.
- Ce dispositif a fait l'objet d'une simple déclaration auprès de la CNIL. Un arrêté du 20 octobre 2008[4] a été pris par le ministère de l'Education nationale pour encadrer cette application par voie réglementaire.
- La CNIL a pu effectuer plusieurs vérifications sur le fonctionnement de ce système. Elle a demandé à être régulièrement informée des bilans de la phase d'expérimentation.

Livret Personnel de Compétences expérimental (LPC)

- Selon le Ministère de l'Education nationale, ce traitement aurait été déclaré à la CNIL le 5 novembre 2010. Mais la CNIL ne donne aucune information sur son site…

5. Abus

Abus potentiels selon des organisations de la société civile

BNIE / RNIE

- Certaines associations et syndicats se sont inquiétés des détournements possibles des informations contenues dans les différents fichiers élèves. En 2008, de nombreux fonctionnaires de l'Education nationale se sont mobilisés pour la suppression de ces fichiers, et surtout des champs controversés tels que la nationalité, l'année d'arrivée en France, l'enseignement de la langue et la culture d'origine, contenus alors dans la base élèves 1er degré. Ces rubriques ont été supprimées en 2007 et 2008.
- Le Collectif national de résistance à « Base élèves » (CNRBE) conteste le fichier Base élèves depuis ses premières expérimentations, et a réussi à obtenir des modifications. Le collectif a même porté l'affaire devant le Comité des droits de l'enfant de l'ONU. Celui-ci s'est déclaré préoccupé par l'utilisation de Bases élèves à des « f*ins telles que la détection de la délinquance et des enfants migrants en situation irrégulière et par l'insuffisance de dispositions légales propres à prévenir son interconnexion avec les bases de données d'autres administrations* ». Le CNRBE continue de lutter pour la suppression des fichiers élèves.
- Question du sénateur Marcel Rainaud au ministre de l'Education nationale sur le BNIE le 4 octobre 2012 : le sénateur se déclare inquiet de la constitution d'un « *gigantesque répertoire national de la population* » possible grâce à l'interconnexion des fichiers et au numéro INE. Il estime que les conditions d'existence et de fonctionnement du BNIE ne sont pas claires. Selon le ministre de l'Education nationale, l'utilisation de Base élèves est légitime, légale et sécurisée, et elle est nécessaire au bon fonctionnement de l'enseignement public.

LPC

- Certaines associations de parents d'élèves, dont le collectif national de résistance à Base élèves, s'élèvent contre cette expérimentation. Le CNRBE considère que ce livret de compétences n'est rien d'autre qu'un super CV numérique aux mains de l'Etat, et elle craint la traçabilité, le contrôle social et l'orientation automatique des élèves. Elle parle de marchandisation de l'éducation au profit du marché du travail.
- Appel au boycott du Livret personnel de compétences, déjà existant, à l'initiative du syndicat SUD Education.

6. Les recours contre ces fichiers

RNIE

- Recours en annulation contre la BNIE. La décision du Conseil d'Etat du 19 juillet 2010 n° 334014 annule la décision de création du fichier BNIE. Le Conseil d'Etat enjoint le ministère de l'Education nationale à effectuer des modifications sur la durée de conservation estimée excessive des données (35 ans). Ces modifications ont été prises en compte lors de la création du RNIE. La décision précise également que le droit d'opposition peut s'exercer avec des « *motifs légitimes* ». On peut supposer qu'il en est de même pour le RNIE. Cependant jusqu'à aujourd'hui aucun des motifs qui ont pu être invoqués n'a été reconnu « légitime ».
- Recours administratifs contre l'inscription dans le RNIE : tribunal administratif de Bastia, 14 juin 2012, n° 1101179 et n° 1101205. Suite au refus de l'inspecteur d'académie de Corse-du-Sud de faire suite à la demande de suppression des données concernant leurs enfants dans le RNIE, des parents forment un recours en annulation, considérant que leur droit d'opposition n'a pas été respecté. En effet, l'inspecteur avait motivé son rejet en indiquant que, dès lors qu'un parent souhaite scolariser son enfant, il ne peut s'opposer à la saisie d'informations nécessaires à la gestion du dossier de l'élève, considérant que ces fichiers ne comportent pas de données sensibles et répondent à une mission d'intérêt public. Le TA a jugé dans ces deux affaires similaires que le droit d'opposition avait ainsi été nié et a prononcé l'annulation pour excès de pouvoir des décisions de rejet de l'inspecteur[44].

7. Points forts / points faibles / bonnes pratiques

Bonnes pratiques

RNIE : en cas de rapprochements de fichiers **à des fins statistiques**, l'INE est préalablement soumis à une double procédure de cryptage-hachage afin de rendre anonymes les informations recueillies, évitant ainsi une possible identification du jeune concerné.

Développements actuels et prévisible

Le LPC pourrait rapidement être généralisé et obligatoire au niveau national.

Aggravation de la situation ou améliorations?

Améliorations

RNIE : suite aux modifications apportées, le RNIE est moins menaçant pour les libertés individuelles que ne l'était la BNIE. Reste la question de l'application effective des nouvelles dispositions.

44. http://bastia.tribunal-administratif.fr/communiques/jugements-n-k3g.html

D. SANTE

La collecte et l'enregistrement de données de santé doivent faire l'objet de mesures de protection particulières, notamment en matière de consentement et de sécurité des données car il s'agit de données sensibles. Cette préoccupation est d'autant plus importante que les enjeux financiers liés à la santé et à l'accès aux soins sont énormes.

1. Résumé des fichiers étudiés et leur but

DMP : Dossier Médical Personnel

Créé par la loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie et réglementé par les articles L1111-14 à L1111-24 du Code de la santé publique[45], le DMP, sous la responsabilité de l'ASIP Santé (Agence nationale des systèmes d'information partagés de santé[46]) a été mis en place afin de permettre une meilleure coordination des professionnels de santé, une meilleure qualité et continuité des soins dispensés, une meilleure information des assurés, et une plus grande maîtrise des dépenses de l'assurance maladie. Son expérimentation a commencé en 2006. Il fait alors l'objet d'évaluations, d'audits, de rapports et d'avis, notamment de la CNIL, qui ont freiné sa généralisation, en particulier à cause du choix d'utiliser le NIR (ou n° de sécurité sociale) comme identifiant, ce qui aurait permis de nombreuses interconnexions. En 2008, le gouvernement relance le DMP, avec l'idée de le rendre obligatoire à chaque bénéficiaire de l'assurance maladie, sous peine de sanctions financières. Mais compte tenu de l'avis négatif du Comité consultatif national d'éthique sur le DMP (il estimait qu'au vu de ses objectifs, le DMP ne pouvait pas être généralisé à l'ensemble des citoyens du fait de son coût très élevé, et des risques liés à sa mise en place pour la confidentialité des données et le respect des libertés individuelles et que le patient devrait avoir le choix d'en disposer ou pas). La Ministre de la santé envisageait alors son déploiement jusqu'en 2012 de manière facultative.

Finalement, la législation concernant le DMP sera modifiée[47], et il sera déployé à partir de décembre 2010. Depuis, tout bénéficiaire de l'assurance maladie **peut choisir de bénéficier d'un DMP** en demandant à un professionnel de santé. Le fichier contient des données d'identification[48] (identifiant national de santé – INS – différent du NIR : c'est un numéro unique, pérenne, non déductible et non signifiant), ainsi que des données médicales générales et de soins, des documents d'imagerie médicale dématérialisés, et des données de prévention (comptes rendus hospitaliers et radiologiques, résultats d'analyses, antécédents, allergies, actes importants réalisés, médicaments prescrits et délivrés). Seuls les professionnels titulaires d'une Carte de Professionnel de Santé (CPS) peuvent accéder au DMP d'un patient. Cette CPS porte l'identification du praticien et permet de tracer ses accès au DMP. La totalité du DMP n'est pas accessible à tous les professionnels de santé. Les accès sont autorisés en fonction de leur profession selon une matrice d'habilitation. Par exemple, un pharmacien ne peut pas lire les comptes-rendus de consultation, un pédicure podologue ne peut pas accéder aux comptes-rendus d'hospitalisation.

45. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000625158 http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=0CECEAE5684CF35E53A6CB64F5B5BB95.tpdjo15v_3?cidTexte=LEGITEXT000006072665&idArticle=LEGIARTI000020889189&dateTexte=&categorieLien=cid

46. Agence gouvernementale chargée notamment de la certification, la production, la gestion et le déploiement du DMP – et la maîtrise d'ouvrage de son hébergement – et de la Carte de Professionnel de Santé (CPS). Elle assure les fonctions d'autorité administrative et d'autorité de certification du répertoire partagé des professionnels de santé (RPPS), dispositifs assurant les fonctions d'identification, d'authentification, de signature et de chiffrement pour la sécurité et la confidentialité requises pour les échanges électroniques qu'ils utilisent.

47. Loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie (1) Version consolidée au 26 février 2010 http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000625158

48. http://www.dmp.gouv.fr/patient/decouvrir-le-dmp/confidentiel-et-securise

Il est conservé pendant une durée de 10 ans à compter de sa clôture. Il peut toujours être réactivé pendant cette période, à la demande de la personne concernée. Il est également possible pour le titulaire de demander la suppression définitive de son DMP.

En octobre 2013 le site officiel[49] annonçait près de 400 000 dossiers ouverts (sur un objectif de 60 millions…) qui plus est, vides dans 50 % des cas selon le site Rue89. Par ailleurs, les médecins estiment que le DMP est un outil qui ne leur apporte rien. Ils considèrent que c'est une perte de temps et un moyen potentiel de les surveiller.

DP : **Dossier Pharmaceutique**

Créé officiellement en 2008 par le décret n° 2008-1326 du 15 décembre 2008 relatif au dossier pharmaceutique[50], sa mise en œuvre est assurée par le Conseil national de l'ordre des pharmaciens mentionné à l'article L. 4231-2 du Code de la santé publique. Le DP a d'abord suivi une phase d'expérimentation initiée en juin 2007, avant d'être généralisé en décembre 2008 après accord de la CNIL et sous le contrôle du Conseil national de l'ordre des pharmaciens. Le Dossier Pharmaceutique est un dossier informatique qui recense les médicaments délivrés au patient au cours des quatre derniers mois ainsi que les traitements et prises en cours. Les médicaments figurant sur le dossier peuvent avoir été prescrits par un médecin ou avoir été achetés librement par le patient. Le pharmacien peut ainsi contrôler d'éventuels risques de contre-indication et conseiller le client.

L'objectif du Dossier Pharmaceutique est de faciliter la coordination, la qualité, la continuité des soins et la sécurité de la dispensation des médicaments, produits et objets médicaux. Le DP permet ainsi d'éviter les risques d'interactions dangereuses entre médicaments, les redondances de traitement et de mieux respecter les doses et les prescriptions. Le DP est accessible par les pharmaciens d'officine et, depuis fin 2012, par les pharmaciens exerçant dans les pharmacies hospitalières. L'accès au DP par certains médecins hospitaliers est en phase d'expérimentation (décret n° 2013-31 du 9 janvier 2013[51]**)**.

Le DP est créé sur proposition du pharmacien, **avec le consentement explicite du patient**. Un certificat électronique en atteste et une copie du certificat lui est remise. Si le patient refuse, le pharmacien enregistre ce refus (pour éviter que cette proposition lui soit réitérée). Le dossier comporte : le nom de famille ou nom d'usage, le prénom usuel, la date de naissance du bénéficiaire, le sexe et, en cas de naissance multiple le rang de naissance, le numéro INS (idem DMP) l'identification et la quantité des médicaments, les produits et objets dispensés pour l'usage du bénéficiaire, avec ou sans prescription médicale et les dates de dispensation. L'ensemble des traitements médicamenteux délivrés en pharmacie sont enregistrés pour une période de 4 mois. Cependant, à l'expiration du délai, ces données sont archivées par l'hébergeur pendant une durée complémentaire de trente-deux mois afin de permettre d'informer les patients en cas d'alerte sanitaire relative à un médicament.

HOPSY (HOPSY Web dans sa version modernisée) pour le suivi des personnes hospitalisées sans leur consentement

Créé et réglementé en 1994, le fichier HOPSY, sous l'autorité des Agences régionales de santé (ARS) a pour fonction d'assurer le suivi des personnes hospitalisées sans leur consentement en raison de troubles mentaux. Il permet une meilleure gestion des dossiers, l'harmonisation des pratiques, l'établissement de statistiques, mais également d'éviter les contentieux. A l'origine, le fichier HOPSY était d'utilisation facultative, puis son usage a été rendu obligatoire dans toutes les DDASS (Directions départementales des affaires sanitaires et sociales), et aujourd'hui les ARS (Agences régionales de santé) suite à la suppression des DDASS. Il contient des informations concernant les personnes ayant fait l'objet de soins psychiatriques sans consentement, soit à la demande d'un tiers ou en cas de péril imminent, soit à la demande d'un représentant de l'Etat ou de l'autorité judiciaire.

49. http://www.dmp.gouv.fr/web/dmp/
50. http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=ECED7C1FE48C56644EBABE455A62B3D3.tpdjo14v_1&dateTexte=?cidTexte=JORFTEXT000019938177&categorieLien=cid
51. http://legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000026924340&categorieLien=id

Ces informations sont relatives à l'identité de la personne hospitalisée sans consentement (nom, prénoms, date et lieu de naissance, profession, adresse, mais pas de n° d'identifiant), à l'identité de la personne ayant demandé l'hospitalisation (nom, prénoms, profession, adresse), à l'identité des médecins auteurs des certificats (nom, adresse professionnelle). Elles sont accompagnées d'informations en rapport avec la justice et avec la situation administrative des personnes hospitalisées (lieu d'hospitalisation, date des certificats médicaux, date des arrêtés préfectoraux d'hospitalisation d'office, date et mode de sortie).

Ces informations sont conservées pendant toute la durée de l'hospitalisation sans consentement et jusqu'à la fin de l'année civile de l'admission en établissement hospitalier.

RIM-Psy : Recueil d'Information Médicalisée en Psychiatrie

Créé en 2006, RIM-Psy recense les personnes ayant à faire à une structure psychiatrique. Le but du fichier est d'améliorer la connaissance et l'évaluation de l'activité et des coûts de la prise en charge psychiatrique, et de favoriser l'optimisation de l'offre de soins. D'abord facultatif, RIM-Psy est devenu obligatoire pour l'ensemble des établissements publics et privés exerçant une activité de psychiatrie en 2007. De ce fait, ils ont l'obligation d'enregistrer un minimum d'informations dans le RIM-Psy, parmi lesquelles le numéro de l'établissement de santé, l'identifiant permanent du patient (numéro permettant de référencer sous un identifiant unique et permanent l'ensemble des informations relatives à un patient), la date de naissance, le sexe, le code postal du lieu de résidence, la date d'entrée et de sortie du séjour, le mode d'entrée et de sortie, la provenance et la destination de sortie ainsi que des informations sur le diagnostic et les soins. S'ils le souhaitent, les établissements peuvent recueillir des informations supplémentaires, sous réserve d'une demande d'avis ou d'une déclaration particulière auprès de la CNIL. Chaque établissement concerné détient un fichier qui est sous la responsabilité d'un médecin désigné responsable de l'information médicale. Les informations y sont conservées pour une durée minimum de 20 ans.

Toutes les données préalablement anonymisées[52], sont également transmises et conservées par l'ATIH (Agence technique de l'information hospitalière), établissement public national, pendant une durée de 5 ans.

RNCPS/SGNI : Répertoire National Commun de la Protection Sociale/Système National de Gestion des Identifiants

Créé en 2006 et installé fin 2011, le RNCPS a pour objectif de renforcer la lutte contre les fraudes, grâce à un contrôle du versement des prestations sociales, et de simplifier les démarches administratives des allocataires sociaux, grâce aux données d'identification du système de gestion national des identifiants (numéro d'inscription au répertoire des personnes physiques[53]). C'est donc une hyper-base de données sociales, de contrôle et de lutte contre la fraude, qui contient des informations sur l'ensemble des assurés sociaux (c'est-à-dire la quasi-totalité de la population en France), notamment concernant leur identité, leurs organismes de rattachement et les droits ouverts (maladie, chômage, retraite, etc.) et/ou les prestations dont ils bénéficient : sécurité sociale ou aide sociale (environ 96 organismes de protection sociale entrent dans le champ du RNCPS).

Les principaux objectifs du RNCPS sont d'assurer une qualité de service renforcée, se traduisant notamment par la simplification des démarches et des procédures ; d'assurer une efficacité accrue dans le contrôle du versement des prestations ; et d'assurer une productivité accrue pour les différents régimes. En particulier, le RNCPS facilite et rationalise les échanges de données et accélère l'ouverture de droits.

Le fichier est sous la responsabilité de la CNAV (Caisse nationale d'assurance vieillesse), et est potentiellement utilisé par plus de 70 000 personnes habilitées de la Sécurité sociale.

52. Avec le logiciel MAGIC (module d'anonymisation et de gestion des informations de chaînage mis à disposition depuis 2006), permettant la génération irréversible, par hachage du numéro d'assuré social, de la date de naissance et du sexe des malades

53. ou communément le numéro de sécurité sociale. Le NIR est utilisé notamment par les organismes d'assurance maladie pour la délivrance des cartes vitales.

A noter : le RNCPS est également utilisé pour l'échange de données entre les organismes de protection sociale, et entre les organismes et les administrations fiscales. Des agents des collectivités territoriales peuvent le consulter.

2. Garanties prévues par la législation

DMP : Dossier Médical Personnel

Etant donné qu'il contient des données sensibles, des mesures de sécurité et des garanties adéquates sont nécessaires.

- Le DMP n'est pas obligatoire, ce qui signifie qu'une personne ne dispose d'un DMP que si elle le souhaite, dans le respect du secret médical.
- Le fait pour une personne de révéler les données contenues dans un DMP alors qu'elle est tenue au secret est puni d'un an d'emprisonnement et de 15 000 euros d'amende. Un décret en Conseil d'Etat, pris après avis de la CNIL, des conseils nationaux de l'ordre des professions de santé, doit fixer les conditions d'accès aux différentes catégories d'informations qui figurent au dossier médical personnel, les conditions dans lesquelles certaines informations peuvent être rendues inaccessibles par le titulaire du dossier médical personnel ou son représentant légal ainsi que les modalités selon lesquelles le professionnel de santé accédant au dossier médical personnel a connaissance de l'inscription au dossier d'informations rendues inaccessibles par son titulaire ou son représentant légal. Or, selon le rapport de la Cour des comptes de juillet 2012, ce décret n'avait toujours pas été adopté à cette date.
- Au niveau de la sécurité informatique, afin que le DMP puisse être utilisé par les professionnels de santé, ceux-ci doivent se doter d'un logiciel spécialisé compatible avec l'utilisation de la plateforme nationale du DMP et être titulaires d'une Carte de Professionnel de Santé (CPS) – voir p 39. Il doit aussi être hébergé auprès d'un hébergeur de santé agréé[54].
- L'accès aux informations contenues dans le DMP à des tiers non-autorisés pourrait porter préjudice au patient concerné (par exemple pour l'obtention d'un travail, d'une assurance, d'un prêt, etc.). C'est pourquoi tout acte de cession à titre onéreux de données de santé identifiantes, directement ou indirectement, y compris avec l'accord de la personne concernée, est interdit sous peine de sanctions.

DP Dossier pharmaceutique

Tout comme le DMP, le DP contient des données sensibles, qui nécessitent une protection et des garanties accrues.

- Le bénéficiaire de l'assurance maladie ou son représentant légal peut demander la clôture du DP à tout moment auprès d'un pharmacien d'officine ou d'hôpital. Le pharmacien remet au bénéficiaire ou à son représentant légal une attestation de clôture mentionnant qu'elle a été réalisée à sa demande. En cas d'inactivité, le dossier pharmaceutique est automatiquement clos par l'hébergeur s'il n'a fait l'objet d'aucun accès pendant une durée de trois ans.
- Toutes les informations contenues dans le DP sont enregistrées, conservées et transférées dans des conditions de sécurité garanties par des moyens de chiffrement.
- Les DP sont hébergés chez un hébergeur unique de données de santé, agréé par la CNIL et sélectionné par le Conseil national de l'ordre des pharmaciens et lié par contrat. Ce contrat précise entre autre les conditions techniques nécessaires pour assurer la qualité et la continuité du service rendu, la conservation, la sécurité, dont la confidentialité et l'intégrité des données, ainsi que leur interopérabilité avec le dossier médical personnel.
- Le bénéficiaire du dossier pharmaceutique, ou son représentant légal, peut s'opposer à ce que le pharmacien consulte son dossier ou à ce que certaines informations y soient enregistrées. Dans ce cas, le pharmacien mentionne ce refus.

57. Le groupement Santéos, Atos Worldline, Extelia est agréé pour l'hébergement du dossier médical personnel.

HOPSY

- La mise en place du fichier HOPSY par un établissement doit faire l'objet d'une déclaration à la CNIL accompagnée d'une annexe détaillant les mesures adoptées pour garantir la sécurité du traitement et la confidentialité des informations.

RIM-Psy

- Chaque membre du personnel détient ses propres identifiants et mots de passe. Des systèmes d'alerte et de vérification sont également mis en place chaque fois qu'une personne non-autorisée consulte le dossier d'un patient.
-,La mise en œuvre du recueil est soumise à une déclaration auprès de la CNIL.
- Une plateforme d'échanges « e-PMSI » est développée par l'ATIH permet les échanges sécurisés de données (déjà anonymisées). Ce programme permet de crypter le numéro d'identifiant du patient au moment de la transmission des données, ce cryptage étant indéchiffrable. Cependant, les données étant remises tous les trimestres, la question se pose de savoir si les données d'un même patient sur plus de 3 mois peuvent être réunies malgré le cryptage.
- En cas de défaut de qualité de l'information, le directeur de l'établissement en question est responsable des informations transmises. Mais en pratique, il est difficile d'exercer des contrôles de qualité sur la pertinence et l'exactitude des données, et cela demanderait des investissements importants pour les établissements.

RNCPS : Répertoire National Commun de la Protection Sociale/Système National de Gestion des Identifiants

- Dans un but de sécurité, l'usage du RNCPS garantit la reconnaissance de l'émetteur et du destinataire des données échangées, l'identification et, si nécessaire, le rattachement des personnes auxquelles sont attachées les informations échangées, ainsi que la confidentialité du contenu des informations échangées et la traçabilité des échanges.
- Chaque organisme utilisateur du RNCPS conclut avec la Cnav une convention précisant les modalités de sa participation au RNCPS. Celle-ci décrit notamment les caractéristiques techniques des systèmes d'informations garantissant la sécurité du RNCPS, et les exigences de qualité des données transmises.

3. Rôle de la Cnil

Dossier Médical Personnel (DMP)

Dans sa délibération n°2010-449 du 2 décembre 2010, la CNIL a autorisé le DMP.

- **Le recueil du consentement du patient à la création du dossier médical personnel** : elle a veillé à ce que le patient soit clairement informé des spécificités du DMP et mis en mesure d'apprécier les conséquences de l'accord qu'il donne. La personne habilitée à ouvrir un DMP attestera avoir procédé à l'information du patient et recueilli son consentement exprès, une copie papier du document électronique sera remise au patient.
- **L'information du patient** : le patient devra être informé de la possibilité d'accéder à son DMP depuis son ordinateur personnel et du rôle spécifique dévolu au médecin traitant dans la gestion de son DMP et l'exercice de ses droits.
- **Les conditions de sécurité du DMP** : (chez les professionnels et établissements de santé ainsi que chez l'hébergeur) les informations enregistrées dans le DMP sont couvertes par le secret professionnel. Elles ne sont consultables que moyennant l'utilisation d'une carte de professionnel de santé. Une trace de tous les accès et consultations du DMP est gardée. Un chiffrement des données de santé contenues dans le DMP et des communications est effectué, conformément aux recommandations de la CNIL.

La Commission a considéré que l'utilisation d'un identifiant national de santé, calculé automatiquement par les logiciels professionnels à partir des données d'identification de la Carte Vitale pouvait être admise à titre temporaire, dans l'attente de l'identifiant national de santé aléatoire prévu à terme.

‣ Dossier pharmaceutique (DP)

Dans sa délibération n° 2008-487 du 2 décembre 2008[55], la CNIL a autorisé la création du DP car elle a constaté que les conditions de sécurité qu'elle préconisait étaient respectées : sécurité logique de l'infrastructure d'hébergement reposant sur une dissociation des données d'identité et des données de santé, deux bases de données étanches ont été créées, l'une contenant les informations relatives à l'état civil des assurés et l'autre regroupant les données sur les médicaments, le lien entre les deux étant assuré via le calcul d'un identifiant mettant en œuvre une fonction de hachage et un boîtier cryptographique. La CNIL a relevé que les données sont conservées sous forme cryptée dans les serveurs de l'hébergeur. Les conditions à remplir par l'hébergeur de données de santé sont définies dans le code de la santé publique[V].

‣ Suivi des personnes hospitalisées en psychiatrie sans leur consentement (HOPSY)

La CNIL a donné un avis favorable à la création de ce fichier (avis en date du 29 mars 1994 n° 94-24[56]) considérant que la finalité était légitime ; que l'information du patient était respectée (« *la personne hospitalisée sans son consentement "doit être informée dès l'admission et, par la suite, à sa demande de sa situation juridique et de ses droits", il est essentiel que les personnes hospitalisées sans y avoir consenti ainsi que, le cas échéant, leurs représentants légaux soient informés dès l'admission en établissement psychiatrique de l'existence de l'application "HOPSY" et du droit d'accès et de rectification au dit traitement* ») ; que les accès étaient conformes à l'article 34 de la loi I&L (« *considérant (…) que l'accès sera sélectif en fonction des informations concernées, les patients hospitalisés, les personnes ayant demandé l'hospitalisation et les médecins auteurs des certificats médicaux ayant respectivement accès aux seules informations les concernant* ») ; et que la **sécurité serait respectée** dans la mesure où « *l'accès au traitement est protégé par des procédures de mots de passe individuels établies suivant les recommandations de la CNIL* ». Elle a pris acte de ce que les responsables (DDASS puis ARS) devront lui adresser une déclaration simplifiée de référence, accompagnée d'un engagement de conformité et d'une annexe précisant les caractéristiques techniques locales du traitement et les mesures de sécurité adoptées.

Pourtant, il semble que cette maitrise de la sécurité ait échappé aux autorités en charge d'HOPSY puisqu'en 2011 le ministère de la santé a lancé une vaste enquête pour recenser tous les personnels en charge du suivi des soins sans consentement dans les ARS afin d'identifier les comptes utilisateurs du logiciel HOPSY valides ou invalides.

‣ Répertoire National Commun de la Protection Sociale/Système National de Gestion des Identifiants (RNCPS)

Dans sa délibération n° 2009-211 du 30 avril 2009 portant avis sur un projet de décret en Conseil d'Etat relatif au Répertoire national commun de la protection sociale (RNCPS)[57], du fait du caractère sensibles des informations contenues dans le fichier, et du nombre important de personnes pouvant le consulter, la CNIL insiste sur :

- le suivi et le contrôle des habilitations, essentiels pour garantir la sécurité et la confidentialité des données ;
- la traçabilité des accès et l'existence de mécanismes d'alerte ;
- le suivi des habilitations d'utilisation du fichier ;
- la sécurisation des mécanismes de consultation ;
- l'information complète des personnes sur leurs droits d'accès et de rectification.

Elle a donc émis de nombreuses réserves ou recommandations pour améliorer le respect des droits des millions de citoyens inscrits dans ce fichier.

55. http://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000020022185
56. http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017652418&fastReqId=888895730&fastPos=3
57. http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000021895450&fastReqId=1228994879&fastPos=4

4. Risques

Risques dus aux dangers contenus dans la législation

‣ Risques dus à l'inscription dans le fichier

• DMP et DP

Selon le site « ticsante »[58] (professionnels de l'informatique de santé), il existe des risques de piratage de grosses structures avec en jeu des dizaines de milliers, ou plus, de dossiers, rendant la reprise en main quasi impossible et les dégâts humains irréparables, ainsi que des risques de substitution de données dans les dossiers médicaux, laissant le dossier et les sécurités intactes, mais où certaines données seraient modifiées à des fins de nuire aux patients ou aux soignants.

• HOPSY :

- une inscription dans un fichier psychiatrique peut porter préjudice à la personne concernée dans de nombreux domaines si cette information venait à être divulguée, d'où la nécessité de mesures de sécurité adéquates ;
- la consultation du fichier Hopsy est systématique dans le cadre des demandes d'autorisation relatives des pots d'armes.

‣ Risques relatifs à l'information des patients

- RIMP-Psy : des réflexions éthiques sont menées sur la question de l'information, mais aussi sur le caractère nominatif du fichier. En effet, il n'est pas certain que les patients aient véritablement conscience de leurs droits.

‣ Risques relatifs à l'absence du droit d'opposition

- RIMP-Psy : le droit d'opposition ne s'applique pas : cela peut poser le problème du refus de soin par des patients qui ne souhaiteraient pas être inscrits dans un fichier psychiatrique.

‣ Risques dus au manque de transparence de la législation

- HOPSY : il est difficile de rendre compte de la véritable portée et de l'usage du fichier HOPSY du fait du peu d'informations existant à son sujet.

‣ Risques dus à l'étendue du fichier

- RNCPS : il s'agit d'un gigantesque croisement de fichiers, regroupant des informations issues des fichiers des nombreux organismes concernés, et où toute personne est inscrite à partir du moment où elle a des droits ouverts à des prestations sociales. De fait, cela signifie que le RNCPS contient des données à caractère personnel concernant l'ensemble de la population française ainsi que les ressortissants étrangers résidant de façon stable en France. Pour certains, il s'agit d'un dangereux outil de surveillance globale, d'autant plus qu'il est accessible à différents services (fiscaux, sociaux, territoriaux).

‣ Risques dus à l'existence d'un identifiant unique

- RNCPS : l'utilisation du numéro de sécurité sociale (NIR), qui permet déjà l'interconnexion de nombreux fichiers, ne doit être ni généralisée ni systématique. Il représente d'autant plus de risques qu'il s'agit d'un numéro stable, identifiant et signifiant (composé à partir du sexe, mois et année de naissance, département et commune de naissance). Cela signifie que l'identité d'une personne pourrait en être déduite assez facilement.

58. http://www.ticsante.com/story.php?story=1280&story=1280#ixzz2jodZKO4j

Risques dus au non-respect des garanties prévues par la législation

‣ Risques dus au non-respect de la confidentialité des informations

- DMP : les déclarations de l'ASIP santé (en charge de la gestion du DMP) dans *Repères Juridiques* du 22 août 2012[59] semblent démontrer, sous prétexte du développement des technologies de l'information et de la communication, une volonté de favoriser les échanges des données de santé plutôt que de protéger ces données sensibles : « *Les données de santé et les données médico-sociales sont aujourd'hui des données destinées à être partagées, même si elles relèvent de la vie privée de la personne.* »
- HOPSY : la loi prévoit que les destinataires du fichier sont le préfet du département, le procureur de la République et les membres de la commission départementale des hospitalisations psychiatriques. Dans certains cas, le maire du domicile ainsi que la famille de la personne hospitalisée sont informés de toute hospitalisation, de tout renouvellement et de toute sortie. Cependant, selon certains professionnels de santé interrogés, dans la pratique, la police et la gendarmerie auraient accès à certaines informations contenues dans le fichier, alors qu'ils n'en sont pas destinataires.

‣ Risques du fait du contenu du fichier

- RIM-Psy : l'existence du RIM-Psy constitue un risque d'atteinte à la vie privée et aux libertés individuelles des personnes soignées en psychiatrie. En effet, les données qu'il contient sont très convoitées sur le plan commercial, ou dans le cadre d'une politique sécuritaire.

5. Abus

Les exemples d'abus

‣ **DMP** : selon un sondage de 2012[60], 45 % des personnes interrogées possédant un DMP indiquaient qu'on ne leur avait pas demandé leur consentement pour ouvrir leur DMP.

‣ **HOPSY** : des patients hospitalisés sans leur consentement ont rapporté avoir reçu la visite de la police ou de la gendarmerie consécutivement à leur séjour, alors que les policiers et gendarmes ne sont pas destinataires des informations contenues dans le fichier.

Abus potentiels selon des organisations de la société civile

‣ **RIM-Psy**

- L'association Droits et libertés face à l'informatisation de la société Santé mentale en Rhône-Alpes (DELIS-SM-RA) a tenté d'alerter l'opinion sur les dangers de RIM-Psy depuis sa création. En février 2008, elle a saisi le Comité consultatif national d'éthique « *sur les atteintes au respect de la vie privée (...) et à l'éthique médicale liées aux pratiques actuelles en matière de recueil informatique des "données personnelles" dans les établissements de santé privés et publics ayant une activité en psychiatrie* », qui lui a donné raison. L'association souhaite obtenir à la source l'anonymisation des données personnelles recueillies en psychiatrie.
- Le fichier a également fait l'objet d'un appel au boycott de certains syndicats de psychiatres et quelques médecins ont mené des actions de résistance, en refusant de remplir le fichier (ce qui est sanctionné par la loi) et en informant les patients sur les dangers du fichage psychiatrique.

59. http://esante.gouv.fr/services/reperes-juridiques/le-cadre-juridique-du-partage-d-informations-ns-les-domaines-sanitaire

60. LH2 réalisé pour le Comité interassociatif sur la santé (Ciss) http://www.ticsante.com/story.php?story=1202#ixzz2jzksQ4SM

RNCPS

Certaines organisations, notamment syndicales, dont la Confédération Générale du Travail (CGT), ont accusé l'objectif de simplification du RNCPS d'être un faux prétexte pour regrouper des données d'état civil et d'affiliation, ainsi que sur les montants et la nature de toutes les prestations obtenues par les bénéficiaires. Pour la CGT, la constitution d'un tel fichier constitué des données de millions de personnes non-fraudeuses a priori n'est pas tolérable dans un pays démocratique. En mars 2009, elle a réclamé l'organisation d'un débat national, qui n'a jamais eu lieu.

6. Les recours contre ces fichiers

HOPSY

- Recours administratifs, notamment suite à des refus de communication de dossier.
- Exemple : dans une affaire opposant Madame H. ayant été hospitalisée sous contrainte, à la Préfecture de Paris (représentant la DDASS de Paris), le Tribunal administratif a condamné la Préfecture. Le TA a annulé la décision de « *refus implicite* » de la Préfecture, lui a fait injonction de lui communiquer le contenu du fichier informatique HOPSY la concernant ainsi que l'acte officiel la portant à ce fichier, sous astreinte de 75 € par jour de retard. Le TA a condamné l'Etat (Préfecture de Paris) à verser à la requérante la somme de 750 Euros.

RIM-Psy

- Un groupe de patients avait entamé une action auprès de la CNIL pour faire valoir leur droit d'opposition (sans résultat puisque le droit d'opposition ne s'applique pas à ce fichier). Pour ce groupe de patients, l'absence de consentement du patient à voir ses données enregistrées est regrettable, alors même que le fichier RIM-Psy contient des données sensibles.
- Recours de l'Union syndicale de la psychiatrie le 16 juin 2011 contre l'arrêté du 20 décembre 2010, modifiant l'arrêté du 29 juin 2006, qui prévoyait la possibilité d'inscrire les caractéristiques sociales des patients afin de les utiliser à des fins statistiques (l'utilisation n'étant pas prévue légalement dans les finalités du fichier). Le Conseil d'Etat n'a toujours pas remis sa décision et, aujourd'hui, l'arrêté en question a été remplacé.

7. Points forts / points faibles / bonnes pratiques

Bonnes pratiques

DMP et DP : la CNIL a édité un Guide pour les professionnels de santé[61].

HOPSY : en 2011, le ministère chargé de la santé a effectué un recensement de tous les personnels en charge du suivi des soins sans consentement dans les ARS afin d'identifier les comptes utilisateurs du logiciel HOPSY valides ou invalides.

RIM-Psy :

- dans certains établissements, les recherches sur le fichier ne peuvent s'effectuer qu'à partir du nom du patient, et pas à partir d'autres critères (domicile, date de naissance….) ;
- certains établissements mènent des réflexions éthiques sur la question de l'information du patient, et sur le caractère nominatif du fichier.

61. http://www.Cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_professionnels_de_sante.pdf

Développements actuels et prévisible

▸ **DMP** : l'existence de ce fichier dont le projet a fait l'objet de multiples modifications du fait des critiques fondées, tant des médecins que des associations de malades, est peu connue du grand public et il est peu utilisé. La Cour des comptes a rendu, le 19 février 2013, un rapport sur le coût du dossier médical personnel. Elle déplore l'absence de suivi financier et la disproportion entre le coût et les résultats : le DMP aurait coûté de 2004 à 2011 plus d'un 210 millions d'euros. De plus, elle remarque l'inadéquation du DMP aux besoins des praticiens.

Aggravation de la situation ou améliorations ?

Du fait du manque d'informations concernant le fonctionnement et l'utilisation de certains fichiers de santé, des hésitations et des retards pris dans la mise en œuvre, il est à craindre une évolution des différents fichiers moins protectrice des données de santé.

4. LE ROLE DE L'AUTORITE DES DONNEES PERSONNELLES

Recours et arguments des citoyens, refus de fichiers autorisés

▸ La loi du 6 janvier 1978 a fait l'objet de plusieurs modifications, notamment en août 2004 lors de la transposition de la directive européenne du 24 octobre 1995 dite Directive 95/46/CE. Sous prétexte d'une mise en conformité, la loi a supprimé le régime d'autorisation préalable qui donnait, jusqu'à lors à la CNIL, la compétence pour refuser notamment la constitution de fichiers de police. Elle a libéralisé la création de fichiers portant sur des données dites sensibles (biométriques, génétiques, sociales, etc.). La loi du 23 janvier 2006, relative à la lutte contre le terrorisme, stipule que les demandes d'avis portant sur les fichiers relatifs à la sûreté de l'Etat, la défense ou la sécurité publique « *peuvent ne pas comporter tous les éléments d'information* » habituellement transmis à la CNIL. En 2011, la CNIL a vu ses compétences s'élargir au contrôle des dispositifs de vidéosurveillance (pour les lieux ouverts au public et la voie publique) afin de s'assurer qu'ils sont conformes aux obligations légales.

▸ Dans un article du 10 juillet 2012 « Les perspectives pour 2012-2013 : la régulation des données personnelles au service d'une véritable "éthique du numérique" », la CNIL souhaite une constitutionnalisation de la protection des données personnelles. « *La protection des données personnelles constitue un droit fondamental, complémentaire des droits et libertés constitutionnellement garantis que sont la protection de la vie privée, le droit de propriété, la liberté d'expression ou encore la liberté d'aller et venir. Ce droit est d'autant plus fondamental aujourd'hui à l'heure où les données personnelles constituent le "carburant" du numérique.* » Pourtant, alors même que cette protection est consacrée par la Charte des droits fondamentaux de l'Union européenne, mais aussi dans les constitutions ou normes suprêmes de 13 pays en Europe, notre Constitution est muette sur le sujet. Or, aucun des droits et libertés actuellement consacrés par notre Constitution n'épuise la question des données personnelles. La CNIL promeut donc l'objectif d'inscrire, dans la Constitution, le droit à la protection des données personnelles. Une telle reconnaissance constituerait un acte fort, moderne, au service d'une protection effective du citoyen.

▸ Le changement récent de « devise » de la CNIL indique des préoccupations et une vigilance plus orientées vers l'utilisation des données personnelles dans le cadre de l'internet et des nouvelles technologies que dans le domaine du fichage institutionnel

Forces / Faiblesses / Bonnes pratiques

▸ **Forces**

Si la question de l'indépendance de la CNIL a pu se poser pendant quelques années, lorsque son président était aussi parlementaire, la question semble réglée par la réforme de son organisation et notamment le fait que son président ne puisse plus être un parlementaire ni être membre de la formation restreinte qui est l'organe qui juge des plaintes et des sanctions applicables. La procédure de la désignation de ses membres implique à la fois le pouvoir exécutif, législatif et judiciaire ainsi que d'autres groupes organisés de la société.

La certaine transparence de ses activités est notable.

Beaucoup de documentation est accessible sur son site, ce qui démontre une réelle prise en compte de son rôle de prospective et de formation/information des citoyens.

La CNIL a un rôle important dans le G29 européen et dans un réseau international (l'association francophone des autorités de protection des données personnelles – AFAPDP). Elle y a acquis une expérience et une légitimité pour traiter de sujets qui sont de plus en plus internationaux.

Faiblesses

Le fait que la CNIL n'ait plus de pouvoirs en matière de création de fichiers relatifs à la sûreté de l'Etat, 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, a considérablement affaibli cette Autorité.

Le fait que les recommandations qu'elle avait faites en 2009, dans le cadre d'une enquête sur les fichiers de police qu'elle a le pouvoir de contrôler (STIC) n'aient pas été suivies d'effets, au point qu'en 2013, elle ait été obligée de les reprendre en grande partie, indique qu'elle a peu de pouvoir (voir recommandations de 2009 sur STIC et JUDEX non prises en compte en 2012-2013).

Par ailleurs, la durée des traitements par la CNIL des demandes d'accès indirects des fichiers tels que le STIC sont très préjudiciables aux personnes qui postulent pour certains emplois (plus d'un million d'emplois sont concernés).

Bonnes pratiques

Une étude de l'Agence des droits fondamentaux de l'UE (FRA) sur les Autorités de protection des données de l'UE[62] relève quelques bonnes pratiques de la CNIL : elle met au service des citoyens une hotline afin de répondre à leurs questions ainsi que des programmes à destination des enfants pour les sensibiliser à la protection des données personnelles.

Enfin, elle met à disposition des modèles de courriers, des conseils juridiques sur les démarches à suivre dans de nombreux cas d'infractions à la protection des données. La possibilité d'effectuer des formalités en ligne est utilisée dans 93 % de celles-ci.

62. http://fra.europa.eu/fr/publication/2012/la-protection-des-donnes-caractre-personnel-dans-lunion-europenne-le-rle-des en anglais : http://fra.europa.eu/sites/default/files/tk3109265frc_fr_web.pdf

5. DIFFICULTÉS RENCONTRÉES

▸ Il n'y a pas de travaux de recherches exhaustifs existants sur le sujet.

▸ Le site internet de la CNIL n'est pas toujours complet. Seuls certains fichiers font l'objet d'un article (fiche) publié sur son site et, si ses délibérations sont citées, il n'y a pas toujours de lien URL actif vers le site http://www.legifrance.gouv.fr/ où se trouve le texte complet et argumenté. Certains articles ne sont pas datés alors que la législation évolue sans cesse. L'accès à l'information des citoyens sur l'ensemble des fichiers institutionnels existants n'est donc pas facilité.

▸ La complexité de la législation et de ses évolutions rend le fonctionnement de certains fichiers plus obscur que d'autres. Par conséquent, il est parfois difficile de connaître la véritable portée du fichier et des traitements qui en sont faits, et donc de se rendre compte des risques qu'il peut induire.

▸ Il est difficile de trouver des informations non pas sur l'existence même des fichiers, mais sur l'usage qui en est fait et les pratiques courantes autour de ces fichiers. Or, la question de la pratique est importante. Lors de la recherche d'informations, il s'est avéré que des utilisateurs eux-mêmes des fichiers étaient désireux d'en savoir plus sur les outils qu'ils maniaient (comme les médecins et juristes de l'Etablissement public de santé mentale EPSM Lille-Métropole). Cela souligne le manque de formation et d'information des agents ayant accès aux fichiers. Or, il s'agit d'un aspect important pour que les garanties imposées aux traitements de données soient réellement appliquées.

▸ Manque de clarté sur la question des interconnexions entre fichiers, au niveau national, mais encore plus au niveau international (quelles informations d'un fichier national alimentent quels fichiers européens). Encore une fois, la législation est complexe et les textes épars : il est parfois difficile de savoir quels pays exactement peuvent avoir accès aux données, à quelles données, et par quelle procédure.

▸ Difficultés à trouver des cas de recours individuels contre les fichiers, tout comme des témoignages ou des cas concrets de préjudice.

▸ Les échanges avec les entités en charge des fichiers ou utilisant les fichiers se sont parfois révélées difficiles, voire impossible (refus de demande d'entretien de l'Institut de recherche criminelle de la gendarmerie nationale, malgré quatre relances pas d'autorisation du cabinet de la garde des sceaux pour autoriser un entretien avec le magistrat en charge du FIJAIS et du fichier des casiers judiciaires). De même, nous avons rencontré des problèmes de lenteur de l'administration pour l'obtention de certaines réponses. A noter qu'une de nos demandes a permis aux services du ministère de la Justice de constater qu'une circulaire n'avait jamais été publiée, ni au BO, ni sur le site du Premier ministre, circulaires.gouv.fr (circulaire du 21 mai 2007 présentant les dispositions relatives au fichier national automatisé des empreintes génétiques de la loi n°2007-297 du 5 mars).

6. BESOIN D'UN TRAVAIL DE SENSIBILISATION AUPRÈS DES CITOYENS ET DES ELUS

Trente cinq ans après la création de la loi informatique et libertés, il est toujours nécessaire de faire connaitre aux citoyens leurs droits en matière de protection de la vie privée et de protection des données personnelles.

Des chiffres qui démontrent si besoin la pertinence de notre étude :

- une étude Eurobaromètre de 2010[63] indiquait que seulement 30 % des Français connaissent l'existence de la CNIL (se situant dans la moyenne européenne par rapport à leur autorité publique nationale chargée de la protection de leurs droits concernant leurs données personnelles). Pourtant, selon un sondage de la CNIL en 2008, « *61 % des Français pensaient que la constitution de fichiers porte atteinte à leur vie privée* » ;
- cette même étude montre qu'en France, 93 % des sondés souhaitent des mesures de protection des données communes à tous les Européens (la moyenne dans l'Union européenne est de 90 %) ;
- la grande majorité des Européens souhaite que les données génétiques aient la même protection spéciale que les données sur la santé, la vie sexuelle, l'origine ethnique, la religion et les opinions politiques ;
- concernant les données personnelles sensibles, des règles européennes offrent une protection spéciale pour leur traitement. 88 % des Européens interrogés pensent que les données génétiques telles que les données ADN devraient également avoir la même protection, contre 7 % qui ne le souhaite pas ;
- les Européens sont plutôt prudents concernant les circonstances dans lesquelles la police devrait avoir accès aux données personnelles des individus. Alors qu'un tiers des Européens disent que la police devrait être en mesure d'accéder aux données personnelles pour toutes ses activités de prévention du crime, une plus grande proportion pense que la police devrait avoir cet accès uniquement en relation avec une enquête spécifique ;
- en outre, un quart des Européens pense que l'autorisation d'un juge devrait être nécessaire. Pour la France, les réponses concernant l'accès aux données par la police sont :
  - seulement dans le cadre d'une enquête spécifique : 29 % ;
  - pour toutes les activités de prévention des crimes : 30 % ;
  - uniquement avec l'autorisation d'un juge : 38 %.

Selon le dernier rapport CNIL, en 2012, 55 % des Français connaissent la CNIL, contre 32 % en 2004[64].

63. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf
64. Rapport d'activité 2012 de la CNIL, page 13
http://www.Cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL_RA2012_web.pdf

Bonnes pratiques existantes

Les bonnes pratiques viennent la plupart du temps des Organisations de la société civile (associations de défense des droits de l'Homme, des libertés, associations « d'usagers », de victimes, mais aussi de professionnels par secteurs : santé, services sociaux, etc.). Elles jouent un rôle d'alerte sur des projets de fichiers ou leur évolution : recours en commun au Conseil d'Etat, campagnes de mobilisation notamment contre Base élèves, contre le projet de fichier Edvige, contre TES et le passeport biométrique, etc.

L'outil juridique que constitue la possibilité de poser une « Question prioritaire de constitutionnalité » peut se révéler utile (ex : FNAEG – Voir p. 31).

Il est important que les citoyens soient persévérants et aillent au bout des procédures, y compris jusqu'à la Cour européenne des droits de l'Homme de Strasbourg car celle-ci défend le droit à la vie privée et à la protection des données personnelles et a condamné des Etats (arrêt définitif du 4 décembre 2008 S. et Marper c. Royaume-Uni et aussi l'arrêt M.K. c. France définitif depuis le 18 juillet 2013) pour violation de l'article 8 de la Convention européenne des droits de l'Homme.

Notes de fin

[i] Les données sensibles sont celles qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou sont relatives à la santé ou à la vie sexuelle de celles-ci. Par principe, la collecte et le traitement de ces données sont interdits. Cependant, dans la mesure où la finalité du traitement l'exige, ne sont pas soumis à cette interdiction :

- les traitements pour lesquels la personne concernée a donné son consentement exprès ;
- les traitements justifiés par un intérêt public après autorisation de la CNIL ou décret en Conseil d'Etat.

La collecte et le traitement de ces données doivent, dans ces hypothèses, être justifiés au cas par cas au regard des objectifs recherchés.

Autres données à risque :

- données génétiques ;
- données relatives aux infractions pénales, aux condamnations etc. ;
- données comportant des appréciations sur les difficultés sociales des personnes ;
- données biométriques ;
- données comprenant le numéro NIR.

[ii] **Exemple de plaintes instruites par la CNIL** (extrait du rapport annuel publié en 2013)

- Ajout d'une mention dans les fichiers au regard de la suite judiciaire intervenue. Monsieur L., 39 ans, travaillant dans le domaine de la sécurité depuis 2004 sans avoir jamais eu la moindre difficulté, a souhaité exercer son droit d'accès indirect, craignant que les difficultés rencontrées dans le cadre de son divorce puissent lui être professionnellement préjudiciables. Le procureur de la République s'est opposé à l'effacement des faits (« *appels téléphoniques malveillants* » et « *menaces* ») dans la mesure où les suites judiciaires intervenues n'y ouvraient pas droit (classements sans suite pour « r*appel à la loi* » et « *médiation pénale* »). Les vérifications menées par la CNIL ont néanmoins permis de s'assurer de l'ajout d'une mention dans le fichier STIC pour ces deux affaires. **Cette mention a pour effet de rendre l'affaire concernée inaccessible lors des enquêtes administratives.**

- Absence de transmission par les parquets des suites judiciaires favorables intervenues. Madame D., maire d'une commune, a saisi la CNIL au titre du droit d'accès indirect après s'être vu refuser l'accès en zone aéroportuaire pour assister à une réunion de travail dans le cadre de l'exercice de ses fonctions. A la suite des démarches de la Commission, les informations enregistrées la concernant dans le fichier STIC (« *atteinte à la liberté d'accès ou à l'égalité des candidats dans les marchés publics, usage de faux en écriture* ») ont été effacées. Le **jugement de relaxe dont elle avait bénéficié en 2006 n'avait pas été porté, en son temps, à la connaissance des services gestionnaires de ce fichier par l'autorité judiciaire**.

- Monsieur G., 30 ans, s'est vu opposer, par le Préfet de son département, un refus de délivrance de sa carte professionnelle en raison d'une plainte déposée par le père de son beau-fils pour « *violences volontaires sur personne de moins de 15 ans par personne ayant autorité* ». Ces faits avaient été classés sans suite pour insuffisance de charges mais demeuraient enregistrés dans le fichier STIC car cette décision judiciaire favorable, avec accord d'effacement du procureur de la République concerné, n'avait pas été portée à la connaissance des services gestionnaires de ce fichier. **La procédure de droit d'accès indirect qu'il a engagé a permis d'en assurer l'effacement.**

- Monsieur F., 35 ans, ingénieur dans le génie civil industriel et nucléaire, est appelé à procéder à des visites et inspections de centrales nucléaires pour sa société. Il a saisi la CNIL d'une demande de droit d'accès indirect craignant que son enregistrement dans le fichier STIC pour une affaire classée sans suite (« *violences volontaires par conjoint* ») fasse obstacle à l'obtention des habilitations nécessaires d'autant que, par le passé, il s'est vu opposé un ajournement de sa demande de naturalisation pour ces mêmes faits. Au terme des vérifications, l'affaire a fait l'objet d'une **suppression compte tenu de la décision de classement sans suite** pour insuffisance de charges intervenue et de l'accord, en ce sens, du procureur de la République.

- Mauvais enregistrement initial des faits. Monsieur C., 29 ans, travaillant dans le domaine de la maintenance aéronautique, s'est vu refuser son badge pour l'accès en zone aéroportuaire en raison de son inscription au fichier STIC. Dans le cadre des vérifications, il a été confirmé que l'intéressé était enregistré pour des faits de « *dégradations volontaires de véhicule* ». Toutefois, l'examen de la procédure établie pour ces faits a mis en évidence, comme il l'avait d'ailleurs indiqué, qu'il n'était pas mis en cause. L'affaire concernée a donc été supprimée par le service gestionnaire.

- Requalification des faits. Monsieur D., 35 ans, agent SNCF, s'est vu refuser sa mutation interne au sein du service de la surveillance générale de la SNCF en raison de son inscription au fichier STIC pour des faits de « *dégradations de biens privés* ». Les vérifications menées par la CNIL et la requalification en « *dégradations légères* » par le parquet ont conduit à la réduction du délai de conservation de 20 à 5 ans et à la suppression immédiate de cette affaire du fait de l'expiration de ce délai.

[iii] Infractions donnant lieu à inscription au FNAE (site : http://www.jcomjeune.com/sites/default/files/infractions_donnant_lieu_a_inscription_au_fnaeg.pdf - novembre 2012).

Crimes et délits contre les personnes :

- meurtre ou assassinat précédé ou accompagné d'un viol ou de tortures ou d'actes de barbarie (art. 222-23 et 222-26 du Code pénal) ;
- agression ou atteintes sexuelles (art. 222-27 à 222-29 et 227-25 à 227-27 du Code pénal) ;
- proxénétisme à l'égard d'un mineur (art. 225-7-1° du Code pénal) ;
- recours à la prostitution d'un mineur (art. 225-12-1 à 225-12-3 du Code pénal) ;
- corruption de mineur (art. 227-22 du Code pénal) ;
- propositions sexuelles à un mineur de moins de 15 ans par un majeur (art. 227-22-1 du Code pénal) ;
- fixation, enregistrement ou transmission de l'image d'un mineur à caractère pornographique (art. 227-23 du Code pénal) ;
- fabrication, transport ou diffusion d'un message violent ou pornographique susceptible d'être vu par un mineur (art. 227-24 du Code pénal) ;
- mise en péril d'un mineur (art. 227-18 à 227-21 du Code pénal) ;
- exhibition sexuelle (art. 222-32 du Code pénal) ;
- meurtres et assassinats (art. 221-1 à 221-5 du Code pénal) ;
- tortures et actes de barbarie (art. 222-1 à 222-6-2 du Code pénal) ;
- violences volontaires (art. 222-7 à 222-16-1 du Code pénal) ;
- menaces d'atteinte aux personnes (art. 222-17 et 222-18 du Code pénal) ;
- trafic de stupéfiants (art. 222-34 à 222-40 du Code pénal) ;
- atteintes aux libertés de la personne, enlèvement et séquestration et détournement d'un moyen de transport (art. 224-1 à 224-8 du Code pénal) ;
- traite des êtres humains (art. 225-4-1 à 225-4-du Code pénal) ;
- proxénétisme (art. 225-5 à 225-10 du Code pénal) ;
- exploitation de la mendicité (art. 225-12-5 à 225-12-7 du Code pénal).

Crimes et délits contre les biens :

- vols (art. 311-1 à 311-13 du Code pénal) ;
- extorsions (art. 312-1 à 312-9 du Code pénal) ;
- escroqueries (art. 313-2 du Code pénal) ;
- destructions, dégradations, détériorations et menaces d'atteintes aux biens (art. 322-1 à 322-14 du Code pénal).

Autres crimes et délits :

- atteintes aux intérêts fondamentaux de la nation (art. 410-1 à 413-12 du Code pénal) ;
- actes de terrorisme (art. 421-1 à 421-4 du Code pénal) ;
- fausse monnaie (art. 442-1 à 442-5 du Code pénal) ;
- association de malfaiteurs (art. 450-1 du Code pénal).

[iv]

http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=D1C314D7C8358239FFC1106148D2094C.tpdjo15v_3?cidTexte=LEGITEXT000019713352&dateTexte=20130923

Arrêté du 20 octobre 2008 portant création d'un traitement automatisé de données à caractère personnel relatif au pilotage et à la gestion des élèves de l'enseignement du premier degré NOR: MENE0824968A. Version consolidée au 01 février 2013.

L'arrêté du 20 octobre 2008 portant création d'un traitement automatisé de données à caractère personnel relatif au pilotage et à la gestion des élèves de l'enseignement du premier degré a été modifié.

Le Conseil d'Etat, par décision n° 317182 du 19 juillet 2010, article 5, annule l'arrêté du 20 octobre 2008 du ministre de l'Education nationale, portant création d'un traitement automatisé de données à caractère personnel relatif au pilotage et à la gestion des élèves de l'enseignement du premier degré en tant qu'il interdit expressément la possibilité pour les personnes concernées de s'opposer, pour des motifs légitimes, à l'enregistrement de données personnelles les concernant au sein de Base élèves 1er degré.

Le Conseil d'Etat, par décision n° 317182 du 19 juillet 2010, article 6, annule l'arrêté du 20 octobre 2008 du ministre de l'Education nationale, portant création d'un traitement automatisé de données à caractère personnel relatif au pilotage et à la gestion des élèves de l'enseignement du premier degré en tant qu'il met en œuvre un fichier qui permet le rapprochement et la mise en relation de données avec d'autres fichiers, sans que cette modalité d'exploitation du traitement Base élèves 1er degré ait été mentionnée dans la déclaration adressée par le ministre à la C.N.I.L., ainsi que dans cette mesure le refus de l'abroger.

NOTA :

Décision du Conseil d'Etat n° 317182, 323441, en date du 19 juillet 2010, art. 5 : « L'arrêté du 20 octobre 2008 a été annulé en tant qu'il interdit expressément la possibilité pour les personnes concernées de s'opposer, pour des motifs légitimes, à l'enregistrement de données personnelles les concernant au sein de "Base élèves 1er degré" ».

[v] Hébergement des données de santé à caractère personnel.

http://www.legifrance.gouv.fr/affichCode.do;jsessionid=ADD7EFBCDAD9D1FACE8204080B373748.tpdjo15v_2?idSectionTA=LEGISCTA000006196138&cidTexte=LEGITEXT000006072665&dateTexte=20110306

Article R1111-9 du code de santé publique.

Créé par Décret n°2006-6 du 4 janvier 2006 - art. 1 JORF 5 janvier 2006.

Toute personne physique ou morale souhaitant assurer l'hébergement de données de santé à caractère personnel, mentionné à l'article L. 1111-8, et bénéficier d'un agrément à ce titre doit remplir les conditions suivantes :

1° offrir toutes les garanties pour l'exercice de cette activité, notamment par le recours à des personnels qualifiés en matière de sécurité et d'archivage des données et par la mise en œuvre de solutions techniques, d'une organisation et de procédures de contrôle assurant la sécurité, la protection, la conservation et la restitution des données confiées, ainsi qu'un usage conforme à la loi ;

2° définir et mettre en œuvre une politique de confidentialité et de sécurité, destinée notamment à assurer le respect des exigences de confidentialité et de secret prévues par les articles L. 1110-4 et L. 1111-7, la protection contre les accès non autorisés ainsi que la pérennité des données, et dont la description doit être jointe au dossier d'agrément dans les conditions fixées par l'article R. 1111-14 ;

3° le cas échéant, identifier son représentant sur le territoire national au sens de l'article 5 de la loi du 6 janvier 1978 ;

4° individualiser dans son organisation l'activité d'hébergement et les moyens qui lui sont dédiés, ainsi que la gestion des stocks et des flux de données ;

5° définir et mettre en place des dispositifs d'information sur l'activité d'hébergement à destination des personnes à l'origine du dépôt, notamment en cas de modification substantielle des conditions de réalisation de cette activité ;

6° identifier les personnes en charge de l'activité d'hébergement, dont un médecin, en précisant le lien contractuel qui les lie à l'hébergeur.

LDH, Ligue des droits de l'Homme
www.ldh-france.org

AEDH, Association européenne
pour la défense des droits de l'Homme
www.aedh.eu

Humanistische Union
www.humanistische-union.de

HCLU, Hungarian Civil Liberties Union
www.tasz.hu/en

ALOS-LDH, Action Luxembourg Ouvert
et Solidaire - Ligue des droits de l'Homme
www.ldh.lu

MEDEL, Magistrats européens
pour la démocratie et les libertés
www.medelnet.eu

Cette publication a été éditée avec le soutien financier du programme Fundamental Rights de la Commission européenne.