Par Yassine SLIMANI et Julie BENROUBI

Selon un rapport publié en 2009 des députés Delphine Batho et Jacques-Alain Bénisti, il existe en France 58 fichiers de police auxquels s'ajoute également de nombreux fichiers européens. La loi informatique et libertés de 1978 a institué la CNIL, Commission nationale de l'informatique et des libertés, pour contrôler essentiellement l'usage et l'application de ces fichiers.

Le droit pénal a subi d'importantes transformations justifiées par une logique de surveillance de plus en plus axée sur la dangerosité. Les fichiers de police, au sens large, permettent de faciliter les investigations mais également d'évaluer la peine lors d'un procès, en conservant les informations relatives à toute personne impliquée ou condamnée dans une affaire.

La CNIL a toujours refusé l'élaboration d'un fichier en interconnectant les données personnelles par peur d'entrainer la confusion entre les différentes personnes et les différentes finalités sans tenir compte des dispositions légales.

Conformément à la loi informatique et liberté du 6 Janvier 1978, modifiée par la loi du 6 août 2004, toute personne dispose d'un droit d'accès, de modification, de rectification et de suppression des données personnelles qui la concerne.

Or cette loi a posé une exception importante, aucun fichier de police ne permet l'exercice du droit d'opposition. Seuls des recours devant les tribunaux ou par le biais de la CNIL permettent de modifier ou supprimer les données personnelles contenues dans les fichiers.

Au cours des années 90, deux fichiers vont être mis en place par la Police et la Gendarmerie. Le STIC, système de traitement des infractions constatées, ainsi que le JUDEX, système judiciaire de documentation et d'exploitation.

Ces gigantesques bases de données recensent toutes les informations des personnes mises en cause dans des procédures judiciaires, qu'elles soient en cours ou même amnistiées, contrairement au casier judiciaire qui ne fait que rendre compte des condamnations. Ces fichiers contiennent également les informations concernant les victimes. Ils visent les enquêtes ouvertes pour les crimes, les délits et les six catégories de contraventions de 5° classe. En plus de l'identité (nom, adresse, filiation, nationalité), les fichiers disposent du signalement et d'une photographie, des faits et des modes opératoires observés pendant la procédure.

Les personnes morales mises en cause peuvent également être inscrites dans le STIC et le JUDEX.

Ces sortes d'outils judiciaires facilitent donc la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs. Il permet également d'élaborer des statistiques.

En 2013, après une étude faite par la CNIL, 6,8 millions de personnes physiques mises en cause étaient répertoriées dans le STIC. 100 000 policiers ont accès à ces fichiers et on enregistre 11 millions de consultations.

Concernant le JUDEX, il existe 2,6 millions de fiches, 79 000 gendarmes y ont accès et les ont consulté 15 millions de fois.

Seulement la CNIL, relayée par les médias, n'ont fait qu'accroître la croyance légitime que de nombreux dysfonctionnements frappent le STIC et me JUDEX. Ils apparaissent à tous les niveaux, des personnes relaxées ou blanchies sont toujours enregistrées dans les fichiers, des faits incorrects sont conservés, ou encore des personnes devant être légalement retirés (après un délai de 20 ans) voient leurs données personnelles archivées. Des consultations illégales ont été constatées à plusieurs reprises.

Le STIC et le JUDEX peuvent être consultés, depuis la loi du 15 Novembre 2001 relative à la Sécurité quotidienne, confortée par la loi du 15 Mars 2003 sur la sécurité intérieure, pour le recrutement ou l'agrément de personnes qui veulent postuler pour des emplois liés à la sécurité. La CNIL a estimé que cette utilisation est venue modifier la nature même de ces fichiers. Une vigilance particulière sur la fiabilité des données est de ce fait primordiale.

Ces fichiers incertains font, de ce fait naitre, une angoisse collective de voir son nom apparaître dans une affaire réglée en des termes différents que ceux inscrits dans le STIC ou le JUDEX.

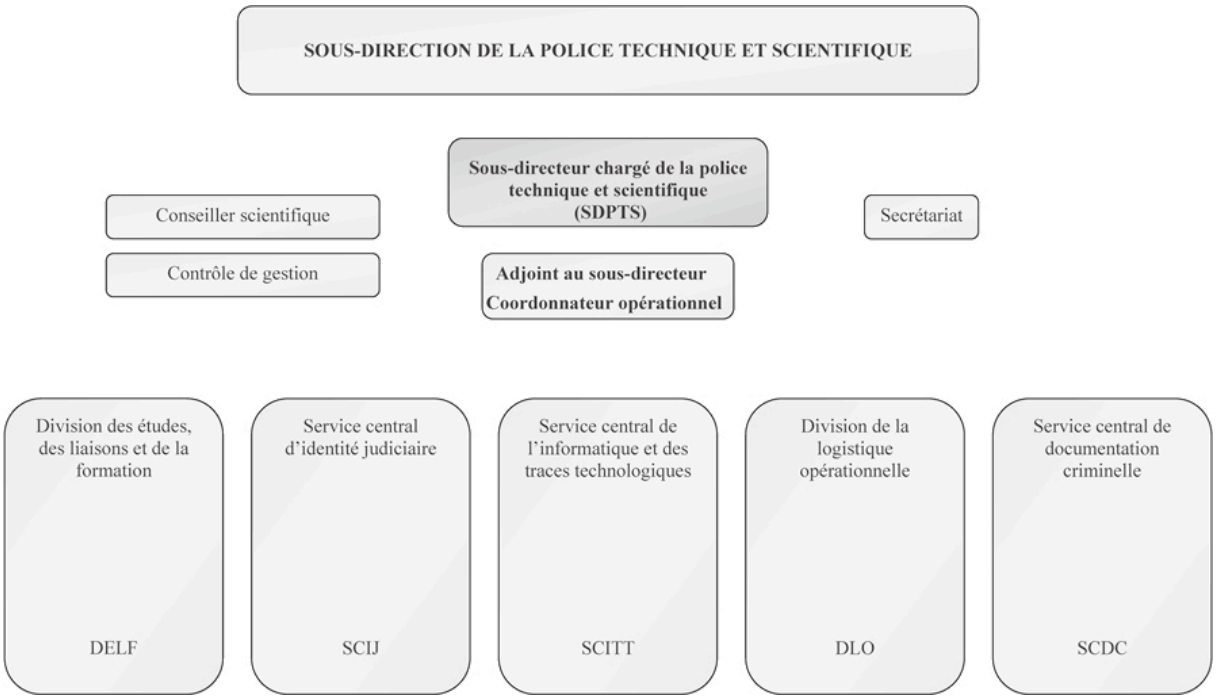
La création même de ces fichiers laissait présager de nombreuses contestations quant à leur légitimité. En effet, le STIC a été créée par la loi 95-73 du 21 Janvier 1995. Mais il entre en activité officielle sans un décret d'application. Au 1er Janvier 1997, il comportait les noms de 2,5 millions de prévenus, 2,7 millions de victimes portant sur 5 millions de procédures et 6,3 millions d'infractions. Le STIC a donc fonctionné en toute illégalité pendant pas moins de 6 ans. Il a été légalisé confidentiellement par un décret du 5 juillet 2001. Pendant sa clandestinité, les personnes concernées ne disposaient d'aucun moyen d'exercer leur droit d'accès et de rectification. Et ce n'était que le début d'une longue série de scandales entourant ces fichiers d'antécédents judiciaire.

Comment de ce fait, peut-on pallier les importantes lacunes dont souffrent le STIC et le JUDEX ? Peut-on croire valablement qu'un jour ces fichiers seront indiscutablement fiables ?

Cet historique judiciaire vulnérable (I) a fait l'objet de nombreuses tentatives d'amélioration pour permettre une meilleure garantie des données personnelles (II). En ce qui concerne ces données personnelles, la situation de Cuba est différente (II bis).

I) Un historique judicaire vulnérable.

A) Une existence nécessaire au bon fonctionnement de la justice.



LES FICHIERS D'ANTÉCÉDENTS EN CHIFFRES	
Fichier STIC	
Nombre de fiches de personnes physiques mises en cause	**6,8 millions**
Nombre de policiers ayant accès au fichier	**100.000 accès**
Nombre de consultations (en 2012)	**11 millions**
Fichier JUDEX	
Nombre de fiches de personnes physiques mises en cause	**2,6 millions**
Nombre de gendarmes ayant accès au fichier	**79.000 accès**
Nombre de consultations (en 2012)	**15 millions**
Fichier TAJ* * Déploiement avancé mais toujours en cours	
Nombre de fiches de personnes physiques mises en cause	**12,2 millions****
Nombre de policiers et gendarmes ayant accès au fichier	**179.000** (à terme)
** Le ministère de l'intérieur a précisé que ce nombre de fiches est à distinguer du nombre de personnes concernées dès lors que le versement des données STIC-JUDEX dans TAJ a parfois occasionné la création de plusieurs fiches pour une même personne lorsque celle-ci avait plusieurs antécédents. Le ministère a indiqué qu'il sera procédé à la fusion des fiches concernées.	

- A quoi sert ce fichier ?

Comme il l'a été précisé précédemment, ces fichiers répertorient des informations provenant des comptes rendus d'enquêtes effectuées après l'ouverture d'une procédure pénale. Ils recensent les personnes mises en cause mais également les victimes des infractions concernées.

Depuis la loi du 15 Novembre 2001 pour la sécurité quotidienne, et ce malgré les réticences de la CNIL, le STIC et le JUDEX peuvent être consultés dans le cadre d'enquêtes administratives qui précèdent les décisions d'habilitation des personnes en ce qui concerne l'exercice de missions de sécurité et de défense. Egalement les autorisations d'accès à des zones protégées en raison de l'activité qui s'y exerce et les autorisations concernant les matériels ou produits présentant un caractère dangereux.

Cette possibilité a été étendue par la loi du 18 Mars 2003 pour l'instruction des demandes d'acquisition de nationalité française, la délivrance ou le

renouvellement des titres relatifs à l'entrée et au séjour des étrangers, et la nomination ou la promotion dans les ordres nationaux.

-Qui est responsable de ces fichiers ?

Pour le STIC, c'est la direction générale de la police nationale, sous le contrôle du procureur de la République territorialement compétent qui est responsable.

Pour le JUDEX, c'est la direction générale de la Gendarmerie nationale.

-Que contiennent ces fichiers ?

- Concernant les personnes mises en cause : identité (nom, nom marital, nom d'emprunt officiel, prénoms, sexe), surnom, alias, date et lieu de naissance, situation familiale, filiation, nationalité, adresse(s), profession(s), état de la personne, signalement, photographie.

- Concernant les victimes : identité (nom, nom marital, nom d'emprunt officiel, prénoms, sexe), date et lieu de naissance, situation familiale, nationalité, adresse, profession, état de la personne, signalement (personnes disparues et corps non identifiés), photographie (personnes disparues et corps non identifiés).

Les victimes sont inscrites dans les fichiers pour permettre à la police d'entre en contact avec elles lors de l'arrestation de l'auteur de l'infraction. De plus, déterminer un profil victime permet également d'identifier un profil criminel ou relier entre elles plusieurs infractions commises par la même personne.

- Informations concernant les faits objet de l'enquête, les lieux, dates de l'infraction et modes opératoires, ainsi que les informations relatives aux objets, y compris celles qui sont indirectement nominatives.

-Quels sont les critères d'inscription dans ces fichiers ?

Pour apparaître dans le STIC ou le JUDEX, il faut qu'une procédure pénale soit ouverte à l'encontre d'une personne dont, au cours de la phase d'enquête, des indices ou des éléments graves et concordants attestant sa participation à la commission d'un crime, d'un délit ou d'une contravention de 5e classe visées à l'article 2 du décret du 5 Juillet 200, sont réunis.

Les conditions d'inscription sont extrêmement strictes. En aucun cas un simple témoin entendu par la police ou une personne ayant fait l'objet de suspicion ou d'une dénonciation non approfondie ne pourra apparaître dans le STIC ou le JUDEX.

- Qui peut procéder à une inscription ?

Seul le personnel habilité des services de police nationale et de la gendarmerie qui participent à une mission de police judiciaire peuvent inscrire le nom d'une personne dans l'un des deux fichiers.

- Combien de temps sont conservées les informations ?

Concernant les majeurs, les informations sont conservées pendant 20 ans. Par dérogation, elles peuvent n'être conservées que cinq ans. Mais le décret du 5 juillet 2001a dressé une liste d'infraction pour lesquelles l'inscription peut être prolongée à 40 ans. Prenons un exemple assez choquant et qui s'est vérifié en pratique avec une de mes connaissances : une personne arrêté pour port d'arme prohibée de sixième catégorie verra son ADN conservé pendant 40 longues années. Qu'à cela ne tienne, la personne refuse. Dans ce cas elle s'expose à une amende de 15 000 euros et à une année de prison. La seule possibilité pour elle d'éliminer ce types de données génétiques est d'écrire au procureur de la République. En d'autres thermes, si vous êtes illettré et que vous ne connaissez pas la procédure en la matière, vous subissez cette soustraction légale de l'ADN d'autrui.

Si l'intéressé est à nouveau mis en cause avant l'expiration de ces durées de conservation, le délai de conservation restant le plus long s'applique aux données concernant l'ensemble des infractions pour lesquelles la personne a été mise en cause.

L'inscription des mineurs ne peut excéder 5 ans.

Concernant les victimes, la durée de conservation des informations est au maximum de quinze ans.

- Qui peut consulter ces fichiers ?

Au sein de la police nationale et de la gendarmerie nationale, du personnel est individuellement désigné et habilité pour pouvoir consulter les fichiers. Dans certains cas, notamment lorsque qu'ils effectuent des missions de police, les agents de douane peuvent accéder aux fichiers.

Les magistrats du parquet et instructeur peuvent également les consulter.

Enfin, sous certaines conditions, les personnels investis de mission de police administrative, désignées par le préfet peuvent également regarder le STIC et le JUDEX.

Il est interdit en France de consulter les fichiers à l'occasion d'enquêtes administratives dites « de moralité », c'est-à-dire pour des candidatures à certains emplois publics notamment.

Seul le bulletin numéro 2 du casier judiciaire d'après le code de procédure pénal peut être obtenu par l'administration.

- Comment obtenir communication, et/ou rectification des données ?

La CNIL effectue elle-même les vérifications des fichiers. Il faut de ce fait adresser au Président de la CNIL un courrier et y joindre une copie d'un papier d'identité.

La CNIL doit d'abord constater, en accord avec le ministre de l'Intérieur, que mes informations communiquées ne mettent pas en cause la sûreté de l'Etat, la défense ou la sécurité publique. La procédure doit être de plus, judiciairement close. Enfin, la communication des informations ne peut être rendue possible que si le Procureur de la République donne son accord.

Mais de toutes les façons, les informations directement ou indirectement nominatives relatives aux personnes mises en cause doivent être supprimées en cas de décision de relaxe ou d'acquittement.

Les informations relatives aux personnes ayant bénéficié d'un non-lieu font l'objet d'une mise à jour sauf si le procureur de la République en ordonne l'effacement.

Les personnes mises en cause peuvent exiger que la qualification des faits finalement retenue par l'autorité judiciaire soit substituée à la qualification initialement enregistrée dans le fichier.

Enfin, en cas de décisions de classement sans suite, de non-lieu, de relaxe ou d'acquittement définitif, les personnes peuvent demander au procureur de la République directement, soit par l'intermédiaire de la CNIL que le fichier soit mis à jour, conformément à l'exercice de leur droit d'accès.

La CNIL a été énormément sollicitée par des demandes de droit d'accès. Elle est saisie généralement à la suite d'un refus d'embauche, d'une délivrance de visa ou de titre de séjour.

Le STIC et le JUDEX étaient autrefois totalement séparés. Le 19 Janvier 2005, une instruction conjointe de la DGPN et de la DGGN a permis l'échange des informations entre les services en interconnectant les fichiers.

Ils sont de véritables outils pour la modernisation de la police. Ils permettent d'orienter et de faciliter les enquêtes. En effet, les gendarmes ou les policiers ont la possibilité de relier entre elles plusieurs affaires présentant des points communs.

http://ldhcibp.wordpress.com/2013/03/28/fichier-adn-celui-qui-refuse-le-prelevement-est-suspect/

B) Une confidentialité relative.

Le STIC comme le JUDEX sont censés être confidentiels. En effet, l'article 230-6 du code de procédure pénal en lien direct avec le stockage de données personnelles dispose qu' « afin de faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs, les services de la police nationale et de la gendarmerie nationale peuvent mettre en œuvre des traitements automatisés de données à caractère personnel recueillies ».

Il est très clair que seuls les services de polices nationale et de la gendarmerie nationale peuvent mettre en œuvre ces fichiers, une utilisation par une personne lambda est donc inenvisageable. Et pourtant ! Cette théorie ne se vérifie

absolument pas en pratique. En témoigne les différentes affaires surprenantes qui vont suivre.

Dans le milieu artistique et plus précisément dans l'univers musicale, les données personnelles s'émancipent, elles deviennent de libre parcours. Prenons une affaire qui a fait grand bruit, celle de Booba, de La Fouine et de Rhoff. Un article paru dans Voici, un magazine intellectuel de renom, publie un article le 4 janvier 2013 intitulé « Les fiches de police de Booba, Rohff et La Fouine sont en ligne » avec en sous-titre « le grand déballage du rap français ». Un site internet, www.ViolVocal.com, a réussi à se procurer les fichiers STIC de Booba, Morsay, Cortex, Rhoff ou encore Joeystarr en passant un coup de fil, tout simplement. Un véritable gouffre dans le paysage sécuritaire de ce fichier qui est censé être confidentiel.

On apprend ainsi avec amusement que Rohff a une fiche STIC fournie. Son rival Booba est un peu plus sage. Certes, il y a une mention de « meurtre », mais sans qu'on sache en quoi il est concerné. La Fouine s'est a priori illustré pour ses liens avec le business illégal. Depuis 2006, le rappeur n'a plus eu aucune raison de figurer dans le fichier. En ce qui concerne JoeyStarr, rien de nouveau n'est ressorti : juste les habituelles violences volontaires, dégradations, et l'affaire du singe violenté.

Moins connus du grand public, Morsay et Cortex ont eux aussi une fiche STIC, moins chargée que les autres. Pour l'heure, seul Cortex a réagi, en prenant plutôt bien la chose : « Viol vocal ils sont très forts. (…) Bien les mecs, t'as vu. Mon casier judiciaire, il me suivra toute ma vie. J'en ai rien à fo*tre. » C'est là où Cortex comment une nouvelle fois l'irréparable en confondant le fichier STIC avec le casier judiciaire, distinction que nous avons déjà effectuées en amont de cette présentation.

Du côté de la police l'agent piégé explique que des mises en cause, « il y en a énormément ». L'inspection Générale des Services a été saisie pour éclaircir les faits. « On prend cette affaire très au sérieux », a déclaré la Préfecture de police de Paris au Monde. Avec une faille aussi énorme dans le système, on comprend leur inquiétude et celle de la CNIL exprimée à plusieurs reprises dans différents rapports précités en 2008, 2009, 2011 et 2013.

Et en ce qui concerne plus spécifiquement le JUDEX, vous savez le fichier rattaché à la gendarmerie nationale ? Aucun fait à répertorier à ce sujet, rien. On ne peut que constater avec effroi que la gendarmerie est plus disciplinée que la police nationale, ceci n'est donc pas une légende. Ou alors la grande muette a encore une fois su tenir sa langue dans une affaire somme toute faite assez délicate.

Après un bref passage dans le commissariat de Rueil Malmaison, on m'a clairement indiqué que le STIC est placé sous la responsabilité du directeur général de la police nationale. Il est par conséquent interdit de communiquer toutes informations contenues dans ce dernier par téléphone sans vérifier scrupuleusement l'identité de destinataire.

Par conséquent, un véritable problème de confidentialité existe. La Commission nationale informatique et liberté pointe également du doigt ces règles de confidentialité qui laissent à désirer. En 2009, la Cnil avait constaté de graves dysfonctionnements dans la transmission des données. Quatre ans plus tard et un nouveau contrôle d'envergure, la situation semble tout aussi inquiétante. Le rapport révèle que "des données STIC sont régulièrement transmises par téléphone sans qu'une traçabilité de ces échanges ne soit mise en œuvre". Il pointe aussi des "conditions de sécurité insuffisantes", telles l'absence d'e-mails sécurisés ou de données cryptées.

En matière de confidentialité, le cryptage est une arme de choix. Il s'agit du moyen de transformer une information afin qu'elle ne soit pas comprise par des personnes non autorisées. La cryptologie, littéralement science du secret, est la science qui regroupe l'ensemble des techniques de cryptage. Elle a pour objectif fondamental de permettre à deux personnes ou systèmes de communiquer des informations secrètes dans un environnement public. Par exemple, transmettre un message par téléphone à un ami, alors que la ligne est écoutée par un intrus, ou envoyer un message par Internet, alors qu'il peut être aisément intercepté. Contrairement à certaines idées reçues, les premières techniques de cryptage datent de plus de 2000 ans, en particulier auprès des anciennes civilisations comme l'Egypte ou la Grèce. Ce code de chiffrement est un des plus anciens, dans la mesure où Jules César l'aurait utilisé.

Le principe de codage repose sur l'ajout d'une valeur constante à l'ensemble des caractères du message, ou plus exactement à leur code ASCII. Il s'agit donc simplement de décaler l'ensemble des valeurs des caractères du message d'un certain nombre de positions, c'est-à-dire en quelque sorte de substituer chaque lettre par une autre. Par exemple, en décalant le message "COMMENT CA MARCHE" de 3 positions, on obtient "FRPPHQW FD PDUFKH". Lorsque l'ajout de la valeur donne une lettre dépassant la lettre Z, il suffit de continuer en partant de A. A titre d'exemple, dans le film L'odyssée de l'espace, l'ordinateur porte le nom de HAL. Ce surnom est en fait IBM décalé de 1 position vers le bas.

Pour quelle raison le cryptage n'est pas utilisé pour un fichier qui répertorie des informations personnelles provenant des comptes rendus d'enquêtes effectuées après l'ouverture d'une procédure pénale ? Il s'agit de données personnelles qui

font partie de l'intimité de la personne et dont le détournement pourrait avoir de terribles conséquences.

Manuel Valls déclarait au Grand Journal de Canal Plus après les affaires de publication des STIC de certains artistes : « Comme ministre de l'Intérieur, j'en apprends tous les jours sur, parfois, la faiblesse de l'accueil (dans les commissariats, NDLR) ». Sans attendre les résultats de l'enquête ou de la procédure, il admet sans mal « quelques dysfonctionnements » : « tout citoyen, quel qu'il soit, ne peut pas voir son nom jeté ainsi en pâture sur Internet. »

La CNIL dans son quatrième considérant du rapport de 2009 constate des pratiques peu sécurisées telles des mots de passe inscrits sur des papiers à côté de l'ordinateur, la transmission des mots de passe par écrit dans des plis non cachetés, l'absence de tenue de registre des changements de mot de passe au sein des commissariats ou des SRPJ. (service régional de police judiciaire).

Dans son sixième considérant cette fois-ci concernant la confidentialité des données adminitratives, la CNIL constate que les consultations du STIC à des fins administratives sont systématiquement effectuées à partir du module de police judiciaire. Cela signifie que les mesures adoptées par le ministère de l'intérieur pour encadrer les consultations du STIC à des fins administratives ne sont pas appliquées au sein des services de police. Le non respect des profils d'accès au STIC conduit ainsi à donner accès de façon indue à certaines informations, dont les conséquences peuvent s'avérer très préjudiciables pour les personnes concernées, en particulier quand le résultat de la consultation du STIC conditionne l'accès à un emploi. En effet, le profil judiciaire permet d'accéder, si la personne est connue, à l'ensemble des informations enregistrées dans le STIC. En revanche, le profil administratif ne permet d'avoir accès qu'aux seules affaires auxquelles aucune suite judiciaire favorable à l'intéressé (telles que classement sans suite pour insuffisance de charges, relaxe, acquittement, non-lieu) n'a été donnée par l'autorité judiciaire.

La confidentialité des fichiers de police est donc une utopie. Pourquoi crier au bunker informationnel ?. En effet, le gouvernement parle de sécurité optimale depuis plus de 10 ans mais les failles sont tellement imposantes qu'on ne peut que les constater. Aujourd'hui le STIC peut être dévoilé par téléphone. Demain, ce sera votre casier judiciaire ? La question est légitime. Dans cette histoire, le citoyen est littéralement pris en otage.

II) Vers un encadrement des dérives de cet historique.

A) Un mirador informatique aux données incertaines.

On peut en effet considérer que ces fichiers représentent de véritable mirador informatique, termes employés par le site bigbrotherawards.eu.org.

De plus, on peut considérer que le STIC et le JUDEX violent de nombreux droit et libertés fondamentaux garantis par la Constitution et les textes européens.

D'une part, la présomption d'innocence est véritablement remise en question. Les lois d'amnistie sont violées. L'obligation de mise à jour n'est pas respectée et de ce fait le droit à l'oubli est anéanti. Les chances de réinsertion pour les personnes figurant dans ces historiques judiciaires sont considérablement amenuisées. On peut également considérer que ces fichiers portent atteinte à la vie privée.

D'autre part, la notion de « mis en cause » est policière et non judiciaire. De ce fait, les auteurs ou les victimes d'une infraction sont confondus dans une même catégorie policière. Le nom des victimes figurent dans les fichiers pour mieux assurer leurs droits. Seulement en pratique il est très facile d'apparaître dans les STIC et JUDEX, en témoignent les chiffres très élevés apportés par la CNIL. Il s'agirait donc d'historiques judiciaires qui iraient bien au-delà que la simple investigation.

De nombreux cas ont prouvé que les informations contenus dans le STIC ou le JUDEX perdurent en dépit du délai légal. Par exemple, un site en 2008 avait publié le STIC de Jamel Debbouze et Johnny Hallyday qui prouvaient que ces fichiers n'était pas régulièrement mis à jour. Concernant celui de Johnny Hallyday, des faits remontaient à 41 ans, bien au-delà du délai autorisé. Les antécédents judiciaires de ces personnalités avaient été communiqués au public par un commandant de police qui souhaitait par ce biais dénoncer le fonctionnement illégal et les irrégularités du STIC. Il avait été pour cela mise en examen pour « détournement de données confidentielles », et « violation du secret professionnel ». Il a été condamné le 22 Octobre 2013 à une peine symbolique de 1500 euros avec sursis, le tribunal avait en effet retenu que « les faits qui lui sont reprochés sont partiellement motivés par les convictions d'intérêt public » sans prononcer de peine d'interdiction professionnelle.

D'autres irrégularités ont été remarquées, en effet concernant une fois de plus les mises à jour. Dans certaines affaires classées sans suite ou soldées par un non-lieu figurent toujours dans les historiques policiers. Cela va même encore plus loin, des personnes qui s'étaient vu écartées de l'affaire restent visibles. De quoi faire naitre une psychose généralisée.

La mise à jour doit normalement être faite sous le contrôle du procureur de la république au sein des services de police, mais cela ne semble pas vraisemblablement relever de leur priorité.

La CNIL avait d'ailleurs rappelé à l'ordre les procureurs de la République qui avait constaté qu'ils ne respectaient pas leur obligation de transmettre au ministère de l'Intérieur les mesures favorables aux personnes mises en cause.

De surcroît, il n'existe pas de procédure d'effacement prévue avant les délais légaux, les personnes figurent toujours dans les fichiers, c'est pour cela qu'il est nécessaire que la mention qui figurent à coté de leur nom soit modifiée, de coupable, il doit passer à « innocent ». Mais ce n'est malheureusement pas toujours le cas.

Selon la CNIL, seuls 47% des fichiers sont exacts. Sur 12 millions de fiches (STIC+JUDEX), ce chiffre est extrêmement alarmant.

En février 2013, quatre vigiles de la centrale nucléaire EDF à Flamanville s'étaient vus refuser l'agrément nécessaire à l'exercice de leur fonction par le préfet de la Manche. Cette affaire avait vivement relancé le débat sur les problèmes générés par le STIC. La direction de l'entreprise avait dû licencier ces quatre personnes. Elles avaient alors saisi leur syndical.

Comme nous l'avions vu précédemment, en vertu d'un décret du 28 Mars 2002, les professionnels de sécurité, tels que les agents de surveillance de sites sensibles, notamment s'ils doivent porter une arme, doivent obtenir un agrément des pouvoir publics. L'administration mène alors une enquête administrative préalable qui passe nécessairement par la vérification du STIC ou du JUDEX du demandeur.

Mais le problème majeur de cette affaire est logé dans le fichier même de l'un des quatre vigiles. En effet, l'un d'entre eux listé pour une affaire de divorce était allé récupérer son téléviseur chez son ex-femme absente au moment des faits à son domicile. Elle avait de ce fait porté plainte pour vol. Mais dans le fichier STIC du vigile, il y avait la mention « connu des services de gendarmerie pour vol avec violence ». La différence est colossale dans cette affaire.

Le préfet avait finalement décidé de revenir sur sa décision et trois employés avaient obtenus l'agrément nécessaire. Il s'était justifié en affirmant qu'il s'agissait « d'une erreur d'appréciation au regard de mentions peu claires inscrites dans le fichier » et avait reconnu lui-même qu'il devait « garder à l'esprit que les informations du STIC sont incomplètes ».

La CNIL s'est saisie de cette affaire pour réaffirmer une nouvelle fois ses craintes concernant les historiques judiciaire. Alex Türk, président de la CNIL

avait dans un communiqué insisté sur « la nécessité pour les autorités responsables des fichiers de police concernés, de faire preuve de la plus grand vigilance dans l'enregistrement des données et de la plus grande célérité dans leur mise à jour ».

En 2009, dans un rapport déjà cité, la CNIL avait pour la première fois contrôlée le fonctionnement du STIC. Elle s'était intéressée à la manière dont les services de police utilisaient le STIC mais également le retour des suites judiciaires pour permettre les mises à jour voire l'effacement des données contenues dans les fichiers. C'est au cours de ce contrôle que la CNIL s'était rendu compte de l'ampleur des dysfonctionnements du STIC. Elle avait de ce fait formulé 11 propositions pour qu'il soit mieux contrôlé et sécurisé et que les informations qu'il contient soit mises à jour et rectifiée de manière à ce qu'elle reflète exactement la vérité juridique.

Les principales propositions étaient celles-ci trouvées sur le site même de la CNIL :

- Mettre en œuvre une procédure pour sécuriser les opérations de saisie

- Harmoniser les conditions d'enregistrement qui diffèrent d'une SRDC (services régionaux de documentation criminelle) à l'autre et engager une réflexion sur les conditions d'enregistrement des enfants de moins de 10 ans et les personnes âgées.

- Respecter les durées de conservation des informations au niveau des bases locales

- Définir une politique de gestion des habilitations et des mots de passe plus stricte

- Exploiter la traçabilité des accès au STIC pour mieux le sécuriser

- Respecter les profils d'interrogation du fichier, en particulier en utilisant uniquement le profil administratif dans le cadre des enquêtes administratives.

- Rendre obligatoire la vérification, par le préfet, qu'aucune décision judiciaire n'est intervenue devant conclure à l'effacement ou la mise à jour de la fiche de la personne faisant l'objet d'une enquête administrative

- Assurer la transmission des suites judiciaire au ministère de l'intérieur en faisant de l'application à venir « cassiopée » (application du ministère de la justice permettant la gestion de l'ensemble de la chaîne pénale et l'échange d'informations avec le ministère de l'intérieur) une priorité et en accordant aux greffes des moyens nécessaires pour la mise à jour du fichier. Cependant,

Cassiopée ne résoudra pas les problèmes des stocks des enregistrements inexacts ou incomplets déjà dans le STIC.

La CNIL dans ses conclusions reconnaissait également que ce n'était pas la conception même du fichier qui était mise en cause. Mais l'inadéquation entre les moyens mis en œuvre par les Ministères et les objectifs assignés à ce fichier.

Dans la pratique quotidienne, elle constate un manque de rigueur dans la gestion du STIC ainsi qu'une absence de prise en compte des conséquences graves qui en découle pour les personnes.

Elle remarque également que la possibilité de consulter ces fiches à des fins administratives est un enjeu majeur pour les citoyens et peut entrainer des « conséquences désastreuses en termes d'emplois ». Elle précise aussi que « la procédure du droit d'accès indirect ouverte à tout citoyen, en raison de sa complexité juridique et de sa durée, n'est pas adaptée aux exigences du marché de l'emploi qui requiert une réponse extrêmement rapide. »

Après ce contrôle, la CNIL s'était engagée à effectuer un contrôle à nouveau le 31 Décembre 2011. Laissant de ce fait entendre que les énormes lacunes et erreurs contenues dans les STIC devaient être rectifiées. L'affaire citée ci-dessus montre que cette exigence n'a pas été respectée.

La CNIL l'a d'ailleurs reconnue elle-même « la situation demeure non satisfaisante. Nous n'avons pas constaté d'avancées significatives. Malgré toutes les améliorations imaginées par la LOPPSI 2, des anomalies constatées en 2009 et des défaillances persistent ».

D'autres affaires sont venues confirmer ces problèmes, une policière a été par exemple placée en garde à vue pour détournement présumé d'informations contenues dans le STIC de personnes connues. Ou encore un policier aurait revendu des informations issues de STIC.

Elle a proposé à nouveau en 2013 10 nouvelles propositions qui devraient être respectées dans le tout récent fichier mis en place, le TAJ.

La question que l'on peut légitimement se poser est pourquoi a-t-il fallu plus de 10 ans pour que la CNIL et l'opinion publique se penchent sur les dysfonctionnements criants du STIC ?

Si le problème des mises à jour inexistantes avait été révélé au grand jour et contrôlé de manière plus systématique depuis la création du STIC, on ne se retrouverait pas aujourd'hui dans l'incapacité évidente de purger des millions et des millions de fichiers. Il semble impossible d'y remédier « le mal est fait », pourrions-nous nous dire nous étions quelque peu pessimistes.

Bien sûr, on comprend parfaitement pourquoi le STIC existe, quelle en est la nécessité. La facilité judiciaire qu'il procure est évidente. Pourtant les énormes erreurs qu'il contient peuvent totalement ruiner l'existence d'une personne et cela remet considérablement en cause celle du STIC. On imagine parfaitement les conséquences désastreuses que peuvent avoir ces informations erronées. L'image sociale, professionnelle, la réputation d'une personne peuvent être totalement détruites par ce genre d'erreurs. De plus, on a vu à quel point il était aisé d'accéder aux données personnelles contenues dans le STIC. De surcroît, avec les nouvelles technologies de plus en plus performantes, on peut tout à fait imaginer comment en un claquement de doigts les bases de données policières peuvent être piratées.

Comment est-il possible qu'on en soit arrivé là ? Ces historiques remettent en cause la légitimité et la crédibilité même des services de police et de l'ordre judiciaire. Depuis des années on souhaite des améliorations, on a mis en place le fichier ARIANE devenu TAJ (dont nous parlerons plus en détail dans le b) II) pour rectifier ces erreurs gravissimes, mais rien ne change. Il semble totalement impossible de sortir de ce marasme accentué par la multiplication continuelle des fichiers de police.

Ne faudrait-il pas alors tout supprimer ? Faire table rase ? Le nombre de données erronées dépasse quasiment celui des données estimées exactes, cela devient extrêmement inquiétant et dangereux dans une société démocratique ou la préservation et la sécurité des données personnelles est tant mise en avant.

Cinq ans que les problèmes persistent, pourquoi somme nous si longs et incompétents ?

B) Une prise d'O-TAJ

On l'a vu, la sécurité, la confidentialité et les mises à jour laissent à désirer concernant et le STIC et le JUDEX. Faisons un bref historique des différents rapports rendus par la CNIL en 2009 et 2012.
D'une part, le nombre de rapports rendus par la commission informatique et liberté témoigne des lacunes et des dangers potentiels pour les données personnelles que peut représenter l'utilisation de ces fichiers de police et de gendarmerie. Dans tous ces rapports et en résumé, des problèmes de sécurité, de confidentialité et de mise à jour ont été mis en avant par la commission. En ce qui concerne le dernier contrôle fin 2012 et début 2013, il concernait le STIC, le JUDEX et le dernier le TAJ. Les objectifs étaient les suivants :

- Faire le bilan des mesures prises par les ministères de l'intérieur et de la justice au regard des propositions avancées par la CNIL en 2009 ;
- Anticiper les difficultés nouvelles résultant du versement des fiches du STIC et de JUDEX dans la base TAJ
- Le cas échéant, formuler des propositions concrètes susceptibles de permettre une utilisation efficace des données d'antécédents par les services du ministère de l'intérieur, dans le respect des droits des personnes et des libertés individuelles.

Concernant ce fameux TAJ, de quoi s'agit-il ?

Il s'agit de nouveau né des fichiers automatisés destiné à conserver certaines de vos informations personnelles que vous avez été mis en cause dans une affaire pénale. Son ancêtre portait le nom d'ARIANE.

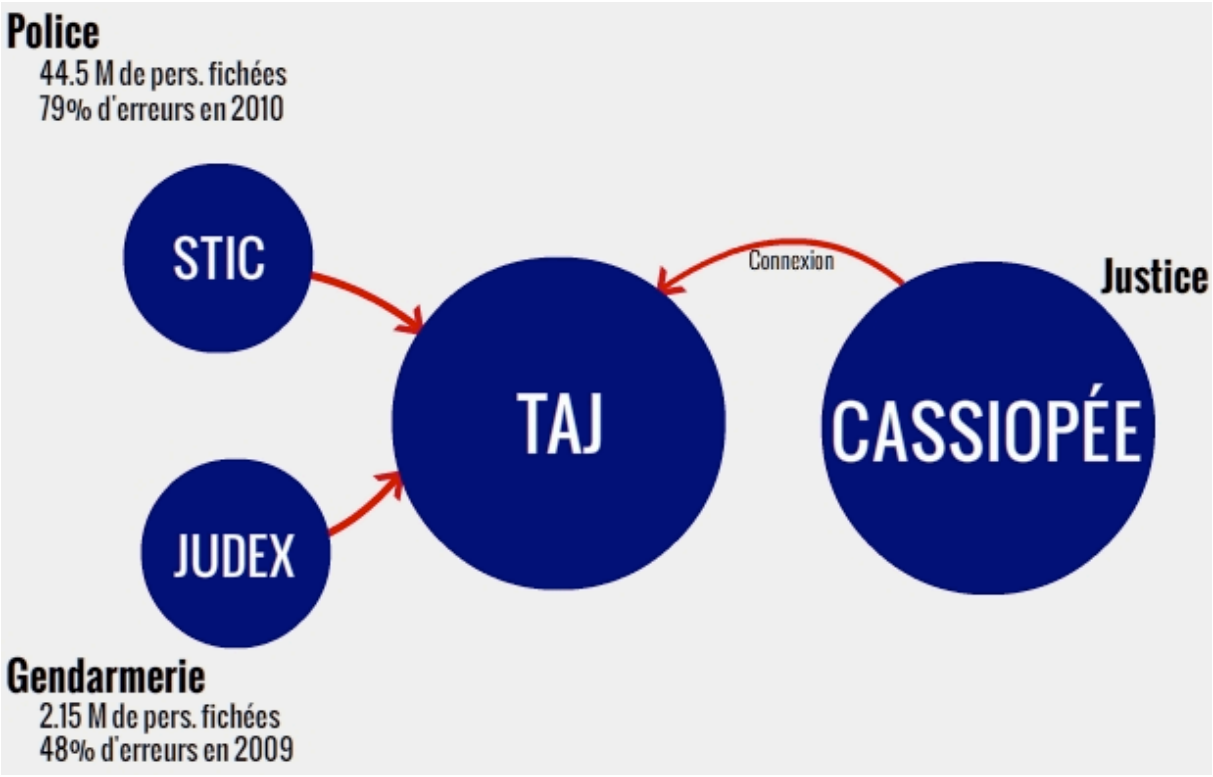
L'appétit de Nicolas Sarkozy pour les fichiers de police s'est traduit par une inflation de ces bases de données durant son mandat. Rien qu'entre 2009 et 2011, leur nombre a été porté de 58 à 80 (dont une partie n'a toujours pas de base légale). Le dernier fichier du quinquennat s'appellera TAJ. Il a fait l'objet d'un décret d'application signé in extremis par Claude Guéant le 4 mai 2012.

En effet, le décret n° 2012-652 du 4 mai 2012, pris après l'avis de la CNIL du 7 juillet 2011, a créé le traitement d'antécédents judiciaires (TAJ), en remplacement du STIC et du JUDEX. Ce traitement a pour finalité de faciliter la

constatation d'infractions, le rassemblement de preuves et la recherche des auteurs d'infractions. Il constitue le plus important fichier utilisé par les forces de police et de gendarmerie. Le TAJ apporte de nouvelles garanties aux personnes fichées (mise à jour des suites judiciaires), mais suscite également de nouvelles réserves de la part de la CNIL notamment à cause de la nouvelle technique utilisée : la reconnaissance faciale des individus.

Fini les soucis de sécurité, fini les ennuies de confidentialité et les problèmes de mise à jour. Le TAJ garantie promet des améliorations. Alors, véritable révolution en matière de traitement automatisé des données personnelles ou simple leurre ?

Les conditions de mise à jour des données qui y sont enregistrées présentent tout d'abord des garanties importantes. En effet, les suites décidées par l'autorité judiciaire seront renseignées automatiquement dans TAJ grâce à une interconnexion avec le traitement CASSIOPEE utilisé par les juridictions. Ce traitement, mis en œuvre dans les tribunaux de grande instance, permet l'enregistrement d'informations relatives aux plaintes et dénonciations reçues par les magistrats, dans le cadre de procédures judiciaires, afin d'améliorer le délai de traitement des procédures, et d'assurer l'information des victimes. Cette articulation entre le TAJ et CASSIOPEE qui joue le rôle d'un genre de garde de fou du citoyen mis en cause laisse planer un sentiment de sécurité.



Cette évolution permettra d'éviter l'absence de mise à jour à la suite de la procédure judiciaire (classement sans suite, acquittement, non lieu). Ce problème essentiel du fichier STIC, avait été révélé par les contrôles de la CNIL en 2007 et 2008 dont le rapport a été remis au Premier ministre en janvier 2009. En outre, la mise en œuvre de ce fichier est entourée des nouvelles garanties prévues par la LOPPSI (Article 11 de la Loi d'orientation et de programmation pour la performance de la sécurité intérieure) à la suite des recommandations de la CNIL :

- Toutes les décisions de classement sans suite seront dorénavant mentionnées
- Il sera impossible de consulter les données relatives aux personnes ayant fait l'objet d'une mention dans le cadre des enquêtes administratives
- Les procureurs transmettront directement au ministère de l'intérieur les décisions de rectification ou d'effacement.

Pour parfaire la sécurité et la fiabilité du TAJ, un triple contrôle de ce dernier est prévu par le décret. Cela permettra de limiter les risques de données erronées. En effet, rappelons le chiffre ahurissant de 43% de données considérées comme fausses sur le STIC en 2009. Outre les futurs contrôles de la CNIL, les procureurs de la République sont chargés de demander que les données soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire. Ils sont également en charge de contrôler la qualification pénale des faits, laquelle détermine la durée de conservation des données enregistrées dans TAJ, pouvant aller, dans certains cas, jusqu'à quarante ans. Ce traitement est ensuite contrôlé par un magistrat dit "référent", chargé de contrôler la mise en œuvre et la mise à jour du fichier.

D'un point de vue critique, la création de ce TAJ suscite de nombreuses réactions notamment de la CNIL. La reconnaissance faciale prévue par ce « fichier récipient » pose des problèmes d'éthique. En effet, pour la première fois dans un fichier de police seront mis en œuvre des procédés de reconnaissance faciale des personnes à partir de la photographie de leur visage. Ainsi, les personnes impliquées dans une infraction, et dont le visage aura été filmé par une caméra de vidéoprotection, pourront être automatiquement identifiées si elles sont déjà connues par les services de police et de gendarmerie. La CNIL a considéré que cette fonctionnalité d'identification voire de localisation des personnes, à partir de l'analyse biométrique de la morphologie de leur visage, présente des risques importants pour les libertés individuelles, notamment dans le contexte actuel de multiplication du nombre des systèmes de vidéoprotection. Cette pratique pourrait être utile pour identifier de hauts criminels, mais pour une simple personne enregistrée à cause d'un couteau suisse qu'elle portait sur elle, est-ce bien raisonnable ? Est-ce que le recueil des données personnelles n'est pas poussé à son extrême?

À noter que le TAJ est opérationnel pour le JUDEX (le fichier de la gendarmerie nationale) mais pas encore pour le STIC. Son utilisation a en effet été reportée au 1er janvier 2015. Le ministère de l'intérieur a décidé de se laisser un sursis pour remédier aux nombreux problèmes liées à l'utilisation et la mise en œuvre du STIC.

II/ bis Des éventuels STIC et JUDEX à Cuba.

En France et on l'a vu, le nombre de fichiers de police qui répertorient vos données personnelles est impressionnant. Lorsqu'on parle de Cuba on ne doit jamais oublier qu'il s'agit d'un pays très singulier par son système politique. On trouve en fait un régime autoritaire qui exerce un contrôle absolu sur les citoyens, et pas seulement sur ceux qui ont eu affaire à la justice ou à la police, mais aussi sur ceux qui manifestent une opposition idéologique au régime actuel. Cependant, on ne parvient pas à se faire une idée précise de l'existence de ces fichiers ou de qui peut y accéder.
A Cuba, il existe un Registre Central des Sanctionnés, subordonné au Ministère de la Justice, mais qui est accessible aussi à la police nationale. Dans celui-ci on enregistre les sanctions imposées par les tribunaux civiles et par les tribunaux militaires par des délits non militaires et des sanctions par des délits militaires quand le verdict du tribunal le détermine de cette manière.
On peut trouver dans ces fichiers toutes les données concernant les personnes misent en cause dans des procédures pénales, mais aussi leur adresse, alias, date et lieu de naissance, occupation, âge, situation de famille et si la personne est récidiviste et de quel type est sa récidive (générique ou spécifique).

Lorsqu'une de ces personnes souhaite déménager, elle doit communiquer sa nouvelle adresse de résidence et demander une nouvelle carte d'identité dans le bureau de la police nationale de sa nouvelle zone de résidence, qui lui délivre les nouveaux documents d'identité. Il faut souligner que ce contrôle n'est pas exclusif des personnes qui ont eu à faire à la justice, il s'agit en effet d'une obligation pour chaque personne de se présenter dans les bureaux de police afin d'actualiser ses nouvelles cordonnées concernant l'adresse ou encore le métier (et cela pour chaque membre de sa famille concerné par ces changements).
Normalement lorsque la police effectue des contrôles d'identité dans la rue, elle a accès a ces archives peut vérifier vos antécédents judiciaires, même si ceux-ci sont déjà supprimés. Dans la pratique, il est presque impossible de savoir quelles données vous concernent dans ces fichiers et qui peut y accéder ou les modifier.
Les fichiers du STIC et du JUDEX ont posés et posent encore actuellement beaucoup de problèmes en France. Mais les citoyens français en connaissent l'existence et peuvent agir en justice en cas de violation du secret qui entoure ces fichiers. Dans un pays sous régime dictatorial comme Cuba, il est tout simplement impossible de connaître leurs modes de fonctionnement, le nombre de données répertoriées ou encore la confidentialité éventuelle qui les accompagnerait.