L'INTEROPERABILITE ET L'INTERCONNEXION DES FICHIERS DE POLICE : ENJEUX ET AMBIGÜITE DU RAPPORT DIALECTIQUE ENTRE PRINCIPE D'EFFICACITE ET PROTECTION DES LIBERTES

par **Jean-Jacques LAVENUE**, Professeur à l'Université de Lille 2, CERAPS (UMR 8026).

La réflexion sur le développement et l'interconnexion des fichiers ne se présente plus, en 2013, sous le même angle qu'il y a vingt ans. Les événements du 11 septembre 2001, la prise de conscience du caractère dissymétrique des conflits potentiels, et la priorité qu'a pris pour les États l'objectif de sécurité, ont fait que l'interrogation n'est plus formulée comme elle pouvait l'être, par exemple en France en 1978 : celle de la création, ou non, de tel ou tel fichier et de son contrôle préalable. Qu'on le déplore ou qu'on s'en félicite, la multiplication des fichiers administratifs ou de police, le développement de leur interopérabilité, de leurs interconnexions, voire de leurs agglomérations sont devenus des faits qu'il n'est plus possible d'ignorer.

Qui plus est la possibilité qu'ont les autorités étatiques d'avoir recours aux compléments d'informations fournis par les systèmes de type OSINT (Open Source Intelligence)[1], fait du risque d'intrusion dans la vie privée des individus une réalité qui fait partie de la « boîte à outils » de la gouvernance sociale. Pour peu qu'un État décide de s'en donner les moyens, rien dans la vie des autres n'échappera à l'œil de Sauron[2] et, au nom de la sécurité collective nécessaire, à ce que certains appelleront la dictature de la transparence[3].

Pour autant que ces faits existent, et que les différences de positionnements sur leurs finalités soient envisageables, faut-il que le droit renonce à son empire ? Retournant l'adage de Cicéron[4] doit-on se résoudre à ce que « *toga cedat armis* » ? Si les circonstances et l'évocation d'une certaine nécessité ont fait que le droit a vu sa fonction préventive de moins en moins jouer « *ab initio* »[5], au moyen d'autorités administratives indépendantes, c'est

[1] http://en.wikipedia.org/wiki/Open-source_intelligence.

[2] Cf. Jean-Jacques Lavenue » *La structure de l'œil de Sauron*« , colloque : Les libertés à l'épreuve de l'informatique, Revue Terminal, n°108-109, pp.153-173.

[3] http://www.lenouveleconomiste.fr/la-dictature-de-la-transparence-9882/#.UR3oIfJTeTY.

[4] Cicéron, « *Arma cedant togae* » - que les armes le cèdent à la toge, De officiis (Des devoirs), XXII.

[5]. Cf. en France l'évolution du contrôle de la CNIL passant d'un contrôle a priori à un contrôle a posteriori http://www.cnil.fr/la-cnil/missions/controler.

désormais sur l'intervention du juge que devra reposer de plus en plus le contrôle de la protection des libertés définies par la loi. L'interprétation qu'il pourra être amené, par exemple, à donner des termes de « Sûreté » et de « Sécurité » sera un véritable enjeu de gouvernance démocratique[6] et aura une incidence sur la gestion quotidienne de la vie publique. Et l'interprétation ne sera pas simple. La confrontation des concepts et des philosophies n'échapperont pas aux ressentis irrationnels, des populations et aux propos, parfois démagogiques, des politiques qui borderont d'écueils le cheminement de la prise de décision judiciaire. Il suffit d'en donner un exemple.

Lors de l'élection présidentielle de 2012 en France, la sécurité a été au centre du débat public. Qu'ils soient de droite, du centre ou de gauche, les candidats ont été confrontés à l'interrogation sur les finalités et les moyens qui pouvaient être envisagés pour répondre à ce qui paraissait être la question dont le caractère était perçu comme prioritaire. Sécurité, sûreté, tentations sécuritaires, vidéo surveillance ou vidéo protection, interconnexion des fichiers, croisement des données, est alors apparue dans les discours comme des concepts polysémiques. Et l'usage que l'on en a fait a bien souvent servi à justifier des choses extrêmement différentes, voire opposées. Ainsi l'interpellation « que fait la police », selon que lui est associé un point d'interrogation ou un point d'exclamation, peut traduire, à la fois, l'extrême ampleur de ces nuances, mais aussi la complexité de ce que nous envisageons d'étudier ici.

« Que fait la police ? », interroge le public, lorsque l'on arrête l'auteur d'un crime sexuel et que l'on découvre que celui-ci, répertorié dans différents fichiers, était multirécidiviste et aurait dû être suivi sur le plan médico-social[7].

« Que fait la police ! » s'indignera le citoyen qui n'aura pas été recruté par un employeur parce que, ayant été témoins d'un incident pénal, il aura été inscrit dans le Système de traitement informatique des infractions constatées (STIC) ou dans celui des empreintes génétiques (FNAGE) et qu'une enquête administrative aura révélé qu'il avait été « impliqué dans une affaire »[8]. Il aura pu suffire en effet qu'il ait été témoin d'une infraction, qu'il soit « passé par là » au mauvais moment, pour que son nom et ses caractéristiques génétiques s'y retrouvent collectés[9]. Les lourdeurs administratives, le manque de mise à jour de ces fichiers (Cf. CNIL et STIC)[10] pourront ainsi suffire à faire d'un individu un paria et à obérer ses possibilités professionnelles.

[6] Cf. M. Delmas-Marty, Libertés et sureté dans un monde dangereux, Seuil 2009.
[7] http://www.publications-justice.fr/accueil/un-multirecidiviste-suspecte-de-viol-pourquoi-etait-il-libre.
[8] http://www.franceinfo.fr/justice/affaire-ikea-d-autres-entreprises-puisent-abondamment-leurs-informations-dans-542613-2012-02-29.
[9] L'article 706-56 du code de procédure pénale prévoit une amende de 15000 euros en cas de refus de prélèvement d'empreintes génétiques.
[10] http://www.cnil.fr/la-cnil/actualite/article/article/nouveau-controle-du-fichier-stic.

En France la Commission Informatique et libertés a relevé en 2009 un taux d'erreur de 83 % dans le STIC[11].

Ces deux exemples nous permettront de situer les deux pôles entre lesquels se déploieront les différentes options liées à la problématique de la sécurité, des fichiers de polices, et de la sûreté des citoyens, dans un monde où les technologies informatiques sont susceptibles de faciliter la surveillance, l'intrusion, le fichage, la transparence, la traçabilité des individus.

L'utilisation de bracelets de géolocalisation dans le cadre de procédures judiciaires, l'implantation des puces électroniques contenant des données biométriques, médicales, bancaires, l'usage des techniques RFID[12] permettant les vérifications sans contact, et les fichiers correspondants, peuvent voir justifier leur consultation à des fins de lutte contre le terrorisme, de protection sanitaire, de surveillance sociale des citoyens, des migrants, des clandestins, etc. Mais une telle justification est-elle suffisante ? La sécurité et la sûreté, comme nous l'avons évoqué, sont-elles une même chose ? La sécurité doit-elle conduire à une dictature de la transparence ? On connaît la célèbre citation de Benjamin Franklin selon laquelle : « un peuple prêt à sacrifier un peu de liberté pour un peu de sécurité ne mérite ni l'une ni l'autre, et finit par perdre les deux »[13].

L'évolution que l'on constate justifie, à la fois, la nécessité de la réflexion sur le développement et les usages des fichiers, mais aussi sur le fait que ce débat est peut-être déjà dépassé. Raison pour laquelle il sera plus que jamais important, à l'occasion de la mise en place des mécanismes de recherche, de réfléchir également sur le droit à l'oubli, voire à l'obscurité, face aux mégas moteurs de recherche. Car si tous les fichiers publics ne peuvent être considérés comme fichier de police, tous les fichiers, y compris privés, peuvent être accessibles à la police grâce aux métas moteurs, aux brokers d'informations et aux différentes utilisations du Data Mining[14].

Les données techniques de la problématique de la mise en place et de l'usage des fichiers de police en France et dans le cadre de l'Union européenne reposent sur deux notions et l'usage que l'on en fait : la notion d'interopérabilité et la notion d'interconnexion des fichiers. Et c'est l'évolution du niveau de combinaison de celles-ci qui déterminera le rapport dialectique entre l'efficacité politique et le degré de liberté, d'autonomie, des individus[15]. Dans

[11] http://www.lefigaro.fr/actualite-france/2009/01/22/01016-20090122ARTFIG00687-un-taux-d-erreurs-siderant-dans-le-fichier-policier-stic-.php.

[12] http://www.wikistrike.com/article-la-puce-rfid-obligatoire-pour-tous-les-americains-en-2013-76382661.html

[13] 1755, lettre à l'Assemblée de Pennsylvanie.

[14]. http://www.lemonde.fr/technologies/article/2013/02/11/une-societe-de-defense-cree-un-outil-de-traque-sur-les-reseaux-sociaux_1830288_651865.html.

[15] Je ne dis pas « citoyens » dans la mesure où sur le territoire d'un Etat, il y a aussi des non nationaux, résidents ou non, et où la gestion de ceux-ci induit dans le cadre français et européen la constitution de nombreux fichiers (ex : SIS I &SISII, VISA, PARAFES-PEGASE, OSCAR-OFII), cf. Jean-Jacques Lavenue, « *La structure de l'œil de Sauron* ,« Terminal n ,109 108°été ,2011 pp.153-173.

leur dimension politique, elles seront liées aux ambiguïtés entretenues autour des notions de sûreté et de sécurité, de sécurité et de liberté. En France, par exemple, une illustration saisissante de ce phénomène peut être trouvée dans le passage, au sein du discours officiel, de la notion de « vidéo surveillance » à celle de « vidéo protection ».

Mireille Delmas-Marty, dans son ouvrage « Libertés et sûreté dans un monde dangereux », a très utilement su rappeler le sens juridique du concept de sûreté. Elle fournit un instrument efficace pour la déconstruction des discours, qu'ils soient politiques ou médiatiques, sur les transformations du contrôle et les effets de brouillage terminologique. Ainsi qu'elle le rappelle, en faisant référence à la Déclaration des droits de l'homme de 1789[16], le droit à la sûreté du citoyen est d'abord de vivre en paix chez lui, y compris face à l'État, tant qu'il n'est pas déclaré coupable d'avoir violé la loi. Elle y voit une sorte d'habeas corpus, synonyme de garantie des droits : parmi les libertés les droits « naturels et imprescriptibles de l'homme », l'article 2 vise la liberté, la propriété, la sûreté et la résistance à l'oppression[17]. L'ambiguïté du discours sera, sous prétexte d'assurer la sûreté du citoyen, d'empiéter sur ses libertés au nom de la sécurité. Depuis le 11 septembre 2001, la lutte contre le terrorisme fournit aux différents pouvoirs un argument supplémentaire, selon une démarche proactive ou préventive, pour développer des actions au caractère intrusif de plus en plus marqué que ce soit aux États-Unis (PNR, NEXUS, TIA[18]) en France ou dans l'UE (PNR, PARAFE, GESTEREXT).

Dans ce contexte l'informatique et le développement des technologies de l'information et de la communication ont donné aux exécutifs les moyens de réaliser le rêve de tous les ministres de l'Intérieur dans tous les psys et à toutes les périodes de l'histoire. Celui de tout savoir sur tous, celui du numéro de référence unique, du grand livre, du méga fichier. Chaque époque et chaque pays a son Joseph Fouché[19], ou son J.Edgard Hoover[20]. Ce rêve du pouvoir peut, on le sait devenir le cauchemar des citoyens. La littérature nous en a présenté bien des modèles. Ils

[16] http://www.diplomatie.gouv.fr/fr/la-france/institutions-vie-politique/symboles-de-la-republique-et-14/article/la-declaration-des-droits-de-l.

[17] Ainsi que l'a écrit Georges Burdeau » : De toutes les conditions de la liberté ,la sureté est une des plus évidentes puisque si elle manque, c'est l'apparence même de la liberté qui disparaît .Aussi compte-t-elle parmi celles qui furent comprises les première sous forme d'une organisation impartiale de la procédure pénale.Mais cette primauté de la sureté, si naturelle semble-t-il n'a pas échappé aux offensives modernes de l'arbitraire…Nous savons aujourd'hui, par expérience directe, que ce qu'il convient d'entendre par sureté individuelle c'est, à la fois, l'assurance d'une certaine sécurité morale grace à laquelle l'individu, sur la foi de l'ordre juridique existant, peut organiser sa vie, courir sa chance et aménager son avenir, et la garantie d'une sécurité physique qui écarte le danger des pénalités arbitraires. La sureté c'est le bienfait du règne du droit ».in *Les libertés publiques*, LGDJ, 1966, p.119.

[18] Cf. Jean-Jacques Lavenue, *La lutte contre le terrorisme et la protection des libertés,* in La sécurité aujourd'hui dans la société de l'information, L'Harmattan CNRS, 2007, pp.117-140.

[19] http://fr.wikipedia.org/wiki/Joseph_Fouch%C3%A9.

[20] http://fr.wikipedia.org/wiki/J._Edgar_Hoover.

relèvent du champ de la civilisation, de la démocratie et des libertés. Quand la technique informatique étend son emprise sur la prise en charge de l'ordre social, le questionnement doit alors se faire sur les finalités d'une société numérisée et l'on n'est plus très loin d'Orwell[21] ou d'Huxley[22].
Au cours des dernières années, s'est indubitablement manifesté en France et dans le cadre de l'Union européenne ce que d'aucuns ont pu qualifier de dérive sécuritaire[23]. La résurgence des menaces terroriste la rend récurrente. Elle apparaît dans l'évolution des ordonnancements juridiques, le développement de ce que l'on appellera des « zones grises ». Elle pourra justifier une réflexion sur ce que l'on pourrait qualifier de rapport dialectique entre ces phénomènes et le plaidoyer pour le droit à l'oubli, voire à l'opacité numérique.

§ 1 – LA MULTIPLICATION DES FICHIERS : SYNDROME OU ÉPIPHÉNOMÈNE D'UNE SOCIÉTÉ NUMÉRISÉE ?

La multiplication des fichiers de police est associée à l'idée de dérive sécuritaire. Le phénomène a, en France, une histoire et repose sur une philosophie. À l'origine chaque fichier devant répondre à une finalité spécifique[24], et ne pouvant être interconnecté, se sont démultipliés de façons plus ou moins légales les fichiers en fonction de chaque spécificité particulière. Le temps passant, le développement de l'interopérabilité et de l'interconnexion a fait que la puissance d'intervention policière et son efficacité se sont particulièrement étendues. Il en est découlé un changement d'approche de la conception de l'action policière préventive qui peut être perçue, à tort ou à raison, comme un risque de dérive sécuritaire.
Juridiquement on pourra analyser ce phénomène de dérive sécuritaire comme le passage, dans la mise en place de la surveillance, de la constitution des fichiers de police sur la base d'actes ayant donné lieux à sanctions, et sur la notion de culpabilité constatée (fichier des condamnations, des délinquants sexuels), à la prise en compte pour la constitution des fichiers d'une notion de dangerosité[25] en dehors de toute violation de la loi. Vont alors être mis sous surveillance et inscrits dans un fichier, même s'ils n'ont pas été condamnés, des individus dont on estimera qu'ils peuvent présenter un risque, une dangerosité. Ce glissement met en cause la notion même d'État de droit. Et la notion de « dangerosité » est tout à fait susceptible, dans son contenu, de mutations politiques conjoncturelles. L'immigré

[21] http://fr.wikipedia.org/wiki/Le_Meilleur_des_mondes.
[22] http://fr.wikipedia.org/wiki/Le_Meilleur_des_mondes.
[23] Cf. David Martin, *Les fichiers de police en France: dérive sécuritaire ou sécurité à la dérive ?*;1996.
[24] Cf ; loi informatique et libertés de 1978 ,http://www.cnil.fr/en-savoir-plus/textes-fondateurs/loi78-17.
[25] Qui pourra être définie aussi bien en raison des fantasmes d'une société donnée, ou de manœuvres populistes désignant par exemple des boucs émissaires.

irrégulier, le heimatlos, le tzigane, le roumain, le noir, le jaune, le blanc, présentent-ils par nature, un caractère de dangerosité ? Peuvent-ils dissimuler des terroristes potentiels ? Le « Si ce n'est toi, c'est donc ton frère »[26], évoqué par le fabuliste, peut-il être considéré comme un mode d'organisation de l'ordre public ? Le fameux « délit de sale gueule » doit-il constituer un chef d'inculpation ? Avons-nous encore nos Hilotes dont il serait prudent de se méfier ? Thucydide écrivait, vers 430 avant notre ère, dans l'Histoire de la guerre du Péloponnèse : « car le principe essentiel de la politique des Lacédémoniens à l'égard des Hilotes a toujours été d'être principalement dicté par les soucis de s'en protéger »[27]. L'histoire ne fait-elle que bégayer ? Ces références historiques nous montrent au fond que nous touchons là à des interrogations qui ne sont pas nouvelles et dépassent l'interrogation de technique policière.

Dans le contexte d'une société informatisée, à côté des fichiers classiques, déjà nombreux, se sont multipliés des fichiers « informatifs », spécialisés, de traçages, et assez rapidement, de manière insidieuse au nom de l'efficacité, l'idée de leur interconnexion est apparue. Sur le plan national d'abord, puis au niveau européen et, dans le cadre de la lutte contre le terrorisme, avec les États-Unis, le Canada et les Etats concernés. Croissance ou métastases ? Dans la galaxie des fichiers est-il encore possible d'avoir une idée exacte du nombre d'étoiles dont on découvre chaque jour de nouvelles unités ? Pour la France, les rapports Bauer[28] de 2006, Batho et Bénisti de 2009[29] et 2011[30], peuvent nous laisser croire que les chiffres avancés ne correspondent pas nécessairement à l'exact décompte de leur nombre.

A) La multiplication en France des fichiers de police.

En décembre 2011, en France il y avait 80 bases de données de sécurité publique, parmi lesquels 62 fichiers de police, dont 45 % n'avaient aucune base légale. Dix fichiers étaient également en construction[31]. Nous en citerons ici que quelques exemples pour mémoire en distinguant entrent fichiers internes et systèmes rattachés à la surveillance aux frontières.

[26] Cf. Jean de La Fontaine, « *Le loup et l'agneau* », vers 22.
[27] Histoire de la guerre du Péloponnèse, Livre IV, ch. LXXX, 3. Traduction Jean Ducat.
[28] http://www.ladocumentationfrancaise.fr/rapports-publics/064000885/index.shtml.
[29] http://www.assemblee-nationale.fr/13/rap-info/i1548.asp.
[30] http://www.assemblee-nationale.fr/13/rap-info/i4113.asp.
[31] http://www.assemblee-nationale.fr/13/rap-info/i4113.asp#P1171_341533.

1) Les fichiers de police internes

Le Système de traitement des infractions constatées (STIC).

Après avoir existé dans l'illégalité pendant 6 ans, créé officiellement en 2001 ce fichier contient des renseignements issus des procès-verbaux sur les auteurs d'infraction et leurs circonstances, les personnes mises en causes et les victimes, les objets volés. Il répertorie des informations provenant des comptes rendus d'enquêtes effectuées après l'ouverture d'une procédure pénale. Il recense à la fois les personnes mises en cause et les victimes des infractions. Il contient l'identité, la situation familiale, la nationalité, la profession et la photographie des personnes mises en cause et des victimes. Au 1er novembre 2011, 6,5 millions de mis en cause et 38 millions de victimes. Selon le rapport de la CNIL publié en 2009, seules 17 % des fiches des personnes mises en cause étaient exactes[32] et en 2010 celui-ci contenait encore 79 % d'erreurs[33].

Le Système judiciaire de documentation et d'exploitation (JUDEX)

Créé en 1986, étendue en 1993, ce fichier est resté 21 ans dans la plus complète illégalité. Il contient des données sur les personnes, recueillies dans les procédures établies par les gendarmes. En 2007 ce fichier a été consulté 12 millions de fois. En 2010 la CNIL constatait qu'il contenait 48 % d'erreurs. Sa fusion avec le STIC avait été prévue sous le nom d'*ARIANE* en avril 2008. Dans l'attente de la création de la base commune, 9 accès réciproques furent ouverts au niveau des principaux centres de renseignement judiciaires des forces de police et de gendarmerie. Ce projet a évolué et a été absorbé en 2011 dans un projet TPJ (Traitement des procédures judiciaires)[34] qui devait absorber également le système de traitement CASSIOPPEE[35]. Reformulé en 2012 en projet TAJ (Traitement d'antécédents judiciaires)[36] qui sera géré par un Nouveau système d'information dédié à l'investigation (NS2I)[37], qui succède au système ARDOISE (Application de recueil de la documentation opérationnelle et d'information statistique sur enquête), expérimenté en 2008 et

[32] Pour les erreurs relevées, dans la majorité des cas, il s'agit de personnes dont le nom figure toujours au fichier alors qu'il aurait dû être effacé à la suite, par exemple, d'une affaire classée. Les conséquences peuvent être graves. Ainsi des chômeurs se voient écartés de certains emplois sensibles parce que leur nom apparaît à tort sur un fichier.
[33] http://owni.fr/2012/05/18/le-gros-bug-des-fichiers-policiers
[34] http://www.lexpress.fr/actualites/1/societe/deux-fichiers-de-police-et-gendarmerie-controverses-remplaces-en-2012_1004360.html
[35] Le traitement CASSIOPEE, 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.
[36] Décret n 652 2012°du 4 mai 2012. JORF n 0107°du 6 mai 2012, p.8047.
[37] http://owni.fr/2012/05/18/le-gros-bug-des-fichiers-policiers

suspendu à la suite des protestations entraînées par l'annonce de sa création[38], il doit entrer en service en décembre 2013.

Le Fichier judiciaire des auteurs d'infractions sexuelles ou violentes (FIJAISV)

Créé par la loi n° 2004-204 du 9 mars 2004 et aménagé par la loi du 10 mars 2010 est un fichier géré par la police, mais administré par la justice. Il tend à prévenir la récidive des auteurs d'infractions sexuelles ou violentes déjà condamnés et à faciliter l'identification de ces infractions. Y sont inscrites les personnes condamnées, même non définitivement, mais aussi les personnes mises en examen par une juridiction d'instruction ayant fait l'objet d'un non-lieu, d'une relaxe, ou d'un acquittement fondé sur des motifs tenant à l'abolition des facultés de discernement. Il recense également les ressortissants français condamnés à l'étranger pour de telles infractions. Il compte aujourd'hui environ 55 000 personnes. On reproche à ce fichier de n'être pas à jour. Environ 110 jours entre la décision judiciaire et l'inscription.
On insistera sur ces changements de sigles pour faire comprendre la complexité de la tâche de restructuration entreprise en France des fichiers de police. On peut y voir un effort de démarche vertueuse. D'autres seront tentés d'évoquer un véritable jeu de bonneteau auquel se livrent les ministères de l'intérieur successifs pour faire réapparaître, ici, ce qu'ils ont dû retirer là, sous la pression des parlementaires, des associations ou/et des médias. Cela explique aussi la difficulté qu'aura l'observateur à ne pas se perdre parmi tous ces fichiers reprenant les prénoms di calendrier : AGGRIPPA, ARAMIS, ARIANE, CRISTINA, DELPHINE, EDVIGE, ELOI, GREGOIRE, OSCAR.

Le fichier d'Exploitation documentaire et de la valorisation de l'information relative à la sécurité publique (EDVIRP)

Ce fichier a été présenté comme un avatar allégé d'EDVIGE. Mais le projet de décret transmis à la CNIL en septembre 2008 a prévu que contrairement à Edvige EDVIRSP seront autorisées à collecter des données relatives aux « origines raciales ou ethniques » - dans la mesure où elles « ne sont pas relatives à la santé ou à la vie sexuelle des personnes. » D'autre part, le fichage des jeunes à partir de 13 ans est maintenu. Le projet de décret précis toutefois que les informations « ne peuvent être conservées au-delà du 18e anniversaire » sauf « si un élément nouveau justifiant un enregistrement au même titre est intervenu durant les deux années précédentes », soit entre 16 et 18 ans ; dans ce cas, les données « peuvent être conservées jusqu'au 21e anniversaire ». Ce

[38] http://www.lexpress.fr/actualite/politique/fichier-ardoise-les-associations-soulagees-apres-le-retrait_472300.html

fichier est devenu en 2009 le Fichier de prévention des atteintes à la sécurité publique (PASP).

Le Fichier National Automatisé des Empreintes Génétiques (FNAEGE)

À raison de 25 000 entrées nouvelles par mois, le Fichier National Automatique des Empreintes Génétiques (FNAEG) a dépassé en 2011 le nombre de 1 800 000 de profils ADN. Ceux-ci correspondent à 280 339 condamnés et 934 112 « mis en cause ». Depuis la loi du 18 mars 2003 sur la sécurité intérieure, ce fichier a été étendu à tous types de délits.

Le Fichier automatisé des empreintes digitales (FAED)

Créé en 1987. Il contient des empreintes digitales et palmaires. En 2007 il a été consulté 21 000 fois. Le taux d'élucidation des traces était de 16 %. Au 1er novembre 2011, le FAED comptait : 4 060 000 individus enregistrés et 200 000 traces non identifiées.

Le Fichier des personnes recherchées (FPR)

Créé en 1996, modifié en 2010 pour permettre des connexions avec le système européen Schengen (SIS). Il contient des renseignements sur les personnes sous le coup d'un mandat d'arrêt ou de justice, en fuite, faisant l'objet de recherches de police judiciaire, ou de personnes interdites d'entrée sur le territoire. En 2011 il contenait 416 000 fiches et était consulté 10 millions de fois par an par les forces de police et de gendarmerie.

Le Fichier administratif de suivi des titres de circulation délivrés aux personnes sans domicile ni résidence fixe (SDRF)

Créé en 1994, modifié en 2005. Les informations nominatives sur les SDF sont conservées 6 mois après leur sédentarisation ou jusqu'à ce qu'ils atteignent l'âge de 80 ans. Le SDRF peut être consulté par la police, les services préfectoraux, le trésor et le ministère de la Santé. En 2007, il a été consulté 155 000 fois.

Le Fichier des véhicules volés et signalés (FVVS)[39]

Depuis un arrêté du 18 août 2011 qui modifie sensiblement l'arrêté du 15 mai 1996 relatif au fichier des véhicules volés, géré par le ministère de l'Intérieur et le ministère de la Défense, « les policiers municipaux sont destinataires des données à caractère personnel et informations enregistrées dans le fichier, dans le

[39] http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000024531387&dateTexte=&categorieLien=id.

cadre de leurs attributions légales et pour les besoins exclusifs des missions qui leur sont confiées, dans la limite du besoin d'en connaître ». En France environ 3 500 maires ont mis en place des postes de police municipale.

Le Système d'analyse des liens de la violence associée aux crimes (SALVAC)

Créé en 2003. Il tend à mettre en évidence le caractère sériel des crimes et contient des renseignements sur des infractions graves, meurtres, assassinats, empoisonnements, actes de torture et de barbarie, enlèvements, viols, agressions sexuelles sur mineurs, entraînant un délit puni de plus de cinq ans d'emprisonnements.

La Base Caliope sur les images à caractère pédopornographique.

Ce fichier de la Gendarmerie nationale, créé par un arrêté du 30 mars 2009 est un logiciel de rapprochement des images pédopornographiques conservées par le centre national d'analyse des images mis en place en 2003.
Dans leur ensemble, ces fichiers reposent pour leur constitution sur des entrées opérées sur les bases d'infractions commises, de condamnations, ou de mises en cause dans des affaires spécifiques impliquant une violation de la loi. Mais allant plus loin, la préoccupation de maintien de l'ordre public a conduit le gouvernement français précédent à envisager de pousser les soucis de la sécurité jusqu'à envisager ce que l'on a appelé le « fichage des honnêtes gens ». Une telle évolution pouvait-elle être considérée comme l'acmé de la dérive sécuritaire ? Nous y reviendrons dans notre B).

Un certain nombre de fichiers ne sont plus censés exister.

Certains fichiers de police ont été détruits, d'autres se sont fondus dans d'autres fichiers. La déclaration de cessation d'existence n'implique pas nécessairement, pour ceux qui ont officiellement disparu, que leur contenu ait lui-même disparu[40]. De fusions en reconfigurations certains participent vraisemblablement toujours d'une manière ou d'une autre au Police Data Mining des services régaliens.

[40] On pourra faire référence à l'histoire du « Fichier Tulard ,« pour souligner la sensibilité des interrogations sur les possibles réapparitions de fichiers censés être détruits.http://fr.wikipedia.org/wiki/Andr%C3%A9_Tulard

Le Fichier alphabétique de renseignement (FAR)

Considéré comme obsolète a été détruit le 3 mars 2011, ce fichier mécanographique de la gendarmerie, créé en 1971, reposant sur la connaissance des populations locales, permettait de vérifier avant toute intervention si la personne concernée était connue pour des faits de violence ou pour tout autre fait susceptible de rendre l'intervention plus complexe (armes, chien dangereux, personne suicidaire, etc.). Certains fonds de brigades ont été conservés à des fins historiques.

FPNE (Fichier des personnes nées à l'étranger) de la gendarmerie nationale[41]

Créé en 1975, le fichier des personnes nées à l'étranger est un fichier mécanographique. Ce fichier a été détruit au cours de l'été 2011 à l'exception des fiches de la lettre B conservées à des fins historiques. À l'instar du fichier alphabétique de renseignements (FAR), il était constitué de fiches cartonnées individuelles. Il comportait environ 7 millions de fiches).

Le Fichier de suivi des personnes faisant l'objet d'une rétention administrative (SUICRA)

Créé en 1994, ce fichier a été supprimé par un arrêté du 4 avril 2011. La procédure de rétention administrative n'ayant pas été supprimée, on peut considérer logiquement que le suivi des personnes concernées a dû être confié à un autre fichier de police. On peut penser qu'il s'est fondu dans le fichier ElOI qui s'est lui-même dissous dans AGDREF2.

Le Traitement automatisé de données à caractère personnel relatives aux étrangers faisant l'objet d'une mesure d'éloignement (ELOI)

Créé par le décret du 26 décembre 2007 Le décret édicté par le ministère de l'Immigration créait une base de « données à caractère personnel relatives aux étrangers faisant l'objet d'une mesure d'éloignement » afin « d'établir des statistiques relatives à ces mesures et à leur exécution ». État civil avec photographie, identité des parents et des enfants, langues parlées, éventuelle « nécessité d'une surveillance particulière au regard de l'ordre public. » La multitude de données informatisées pouvait être conservée trois mois à compter de la date de l'éloignement effectif, sauf celles concernant l'état civil et la filiation qui pourront être conservées trois ans. Invalidé partiellement par le

[41] Sa destruction était prévue avant l'échéance du 24 octobre 2010 au titre de l'article 21 de la loi du 6 août 2004..

Conseil d'État le 30 décembre 2009, ce fichier n'est plus censé avoir d'existence comme tel. Abrogé par le décret n° 2011-638 du 8 juin 2011, il est remplacé par le fichier AGDREF2 dont nous parlerons plus bas.

Le Fichier de la Direction de la surveillance du territoire (DST)

Il contient des informations sur les personnes physiques, les entreprises, des données documentaires et reçoit des informations classifiées des services étrangers. Protégé par le secret défense il n'est pas soumis au même régime juridique que les autres. Aucune donnée n'est communiquée. Sa fusion avec le fichier des RG était prévu en juillet 2008. Il devait servir à alimenter CRISTINA.

Le Fichier des Renseignements généraux (RG)

Un décret de 1991 avait autorisé les RG à collecter des données nominatives (physiques, activités politiques, philosophiques, religieuses ou syndicales) si les personnes peuvent porter « atteintes à la sûreté de l'État ou à la sécurité publique » ou « jouent un rôle politique, économique, social ou religieux significatif » et que ces informations sont « nécessaires pour donner au gouvernement ou à ses représentants les moyens d'apprécier la situation politique, économique et sociale et prévoir son évolution ». Ce fichier a été gelé à compter du 1er juillet 2008, mais le transfert des données vers d'autres fichiers continuait, selon la mission Batho-Batisti, encore en 2011[42].

2) La mise en place des systèmes de surveillance aux frontières

L'organisation de la surveillance aux frontières va reposer sur un double niveau de coopération policière : dans l'espace Schengen, d'une part, et dans les relations entre cet espace et certains États tiers, d'autre part. Dans la mise en place de ces procédures, les liens spécifiques avec les États-Unis et le Canada peuvent permettre d'envisager l'adoption de certaines de ces techniques comme le résultat d'une sorte de benchmarking sécuritaire. Nous évoquerons ici spécifiquement les systèmes de surveillance dans l'espace Schengen. Ceux-ci s'appuient également sur des systèmes de coopérations institutionnels dont nous ne parlerons pas ici (Agence Frontex, Eurosur).
La surveillance aux frontières va reposer sur la création de fichiers ainsi que sur la mise en place d'une coopération fonctionnelle. Dans les deux cas, une différence devra être faite entre ce que l'on pourra qualifier de régime de droit commun et les traitements spécifiques relevant de la lutte contre le terrorisme. La constitution de fichiers répondra à trois finalités de contrôle : à

[42] Cf. op. cit. p.158.

l'entrée, au suivi une fois entré et à la sortie de la zone à protéger. En cas de sortie il est concevable d'imaginer des possibilités de communications de zones à zones voire d'interconnexion, dans le cadre de coopération dans la lutte contre le terrorisme par exemple. Un croisement de vérification avec le système PNR et les possibilités de traçage qu'il implique est à cet égard concevable.

a) Surveillance à l'entrée

Ainsi que l'explique le Rapport des députés Delphine Batho et Jacques Alain Bénisti :

> « L'échange d'informations étant à la base du renforcement de la coopération policière, douanière et judiciaire, la « clef de voûte » de ces accords (de Schengen) a été la création du Système d'information Schengen (SIS), fichier de police, comportant des signalements, notamment d'étrangers. L'importance du SIS se reflète en outre dans la place qu'il occupe dans la convention d'application[43] de l'accord de Schengen »[44]. Il a été complété en 2004 par la mise en place d'un système d'information sur les visas (VIS)[45].

Les Systèmes d'information Schengen (SIS I & SIS II)

Le Système d'information Schengen est un réseau informatique contenant des informations sur les personnes recherchées ainsi que dur les objets et véhicules volés. À partir des milliers de terminaux installés en Europe, connectés à l'ordinateur central de Strasbourg, les autorités habilitées[46] peuvent à tout instant vérifier si un étranger entrant ou sortant de l'espace est inscrit au SIS[47]. Conçu à l'origine[48] comme un accompagnement de la mise en place de la liberté de circulation à l'intérieur de l'Espace Schengen, il a organisé des mécanismes d'assistance mutuelle d'informations entre les forces de police, la surveillance transfrontalière, la poursuite de suspects, ainsi qu'un renforcement des moyens de communication et d'échanges d'informations via les autorités répressives à l'échelon central.

---

[43] Son titre IV lui est consacré, il se compose de 28 articles sur un total de 142. http://www.senat.fr/europe/acquis_schengen_1999.pdf ; p.42 et ss.

[44] Cf. "*Rapport d'information sur les fichiers de police",* n° 1548, Assemblée nationale, remis le 24 mars 2009, p.28.

[45] Décision 2004/512/CE du Conseil, du 8 juin 2004,

[46] Police, gendarmerie, douane, autorités judiciaires.

[47] Il s'agit : des données concernant des personnes recherchées ou placées sous surveillance (nom, prénom, alias, date et lieu de naissance, sexe, nationalité, signes physiques particuliers, objectifs et inaltérables, indication que la personne est armée ou violente, motif du signalement, conduite à tenir) ; des données concernant des véhicules ou des objets recherchés (ex : pour les véhicules : motif de la recherche, caractéristiques : couleur, catégorie, marque, numéros de série et d'immatriculation, dangerosité, conduite à tenir ; pour les documents d'identité délivrés : nom et prénom du titulaire, date de naissance, motif de recherche, conduite à tenir).Au 1er février 2009, le N-SIS contenait 1.223.871 signalements concernant des personnes. http://www.cnil.fr/dossiers/police-justice/les-grands-fichiers/article/34/sis-systeme-dinformation-schengen/

[48] Accord signé le 14 juin 1985.signé par 5 Etats membres. Opérationnel depuis 1995.

Sous couvert d'une mise à niveau (SIS II) le système a pu être suspecté de changer de finalité et d'évoluer vers une base de données de surveillances et d'enquêtes. Cette évolution ressort de la présentation même de ces accords. Alors, par exemple que la convention d'application des accords de 1985 notait : « Ayant décidé d'accomplir la volonté exprimée dans cet accord de parvenir à la suppression des contrôles aux frontières communes dans la circulation des personnes et d'y faciliter le transport et la circulation des marchandises, etc. »[49], le texte de l'article 1 § 2 du Règlement (CE) n° 1987/2006 du Parlement Européen et du Conseil sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II) dispose : "L'objet du SIS II… est d'assurer un niveau élevé de sécurité dans l'espace de liberté, de sécurité et de justice de l'Union européenne, y compris la préservation de la sécurité publique et de l'ordre public et la sauvegarde de la sécurité sur les territoires des États membres, ainsi que d'appliquer les dispositions du titre IV, chapitre 3, du traité relatives à la libre circulation des personnes sur les territoires des États membres"[50]. Pourront être ajoutés les fichiers des Cartes d'identité, des passeports, des cartes de séjour, des cartes grises, des impôts, taxes en tous genres, du cadastre, de la sécurité sociale, des allocations familiales, des dossiers de santés, etc. Le SIS II, lancé en janvier 2013 devrait être opérationnel en avril 2013.

Le Système d'Information des Visas (VIS)

Le Système d'Information des Visas (VIS) a été créé par la décision 2004/512/CE du Conseil, du 8 juin 2004[51]. Le règlement CE n° 767/2008 du Parlement européen et du Conseil, du 9 juillet 2008[52] en a défini l'objet, les fonctionnalités et les procédures d'échange des données sur les visas entre les États membres. Il était précisé dans ses considérants qu'il « devrait avoir pour objet d'améliorer la mise en œuvre de la politique commune en matière de visas, la coopération consulaire et la consultation des autorités centrales chargées des visas en facilitant l'échange de données entre les États membres… ainsi que contribuer à la prévention des menaces pesant sur la sécurité intérieure de l'un des États membres ».[53] Cet objet trouve sa confirmation à l'art.2 g) et 3 du règlement. Sont enregistrées dans le VIS les données alphanumériques sur le demandeur et les visas demandés, les photographies, les empreintes digitales, les liens avec les demandes de visa antérieures et avec les dossiers de demande des

[49] 19 juin 1990 : http://www.ena.lu/convention_application_accord_schengen_19_juin_1990-010302464.html
[50] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:381:0004:0023:FR:PDF
[51] JOUE n°L213, du 15/06/2004, p. 5.
[52] JOUE n°L218, du 13/08/2008, pp. 60-81.
[53] 5ème considérant du Règlement n°767/2008, JOUE n°L218, du 13/08//2008, p. 60.

personnes qui voyagent ensembles. L'ensemble instaure une interopérabilité entre les bases de données européennes, créé une synergie entre les systèmes SIS II, VIS et Eurodac.

b) Suivi une fois entré et à la sortie

L'entrée dans l'espace de liberté de circulation Schengen n'offrira pas l'assurance d'un incognito au bénéficiaire du visa. Sa sortie ne garantira pas non plus un retour à l'oubli des traces multiples qu'il aura pu laisser. Il existe en effet toute une série de fichiers qui sous des angles divers auront enregistré, classé, répertorié l'activité de l'individu cosmopolite numérisé. Il est possible d'en évoquer brièvement un certain nombre.

PARAFES-PEGASE, (Passage Automatisé Rapide aux Frontières Extérieures Schengen)

Le dispositif PARAFES créé par décret le 3 août 2007 [54] est un héritier du projet expérimental PEGASE d'identification biométrique lancé en juin 2005 par Air France au terminal 2F de l'aéroport Roissy-Charles-de-Gaulle. Il peut apparaître comme un élément complémentaire du système Schengen applicable aux ressortissants de l'Union européenne, mais aussi comme un moyen d'alimenter une véritable base de données à l'échelle européenne. Pour peu que l'on imagine la possibilité d'additionner fichiers SIS, VIS, PARAFES, on pourra s'interroger sur la possibilité pour un individu circulant en Europe d'échapper à la surveillance policière. L'article 4 § 2 du décret prévoit en effet que les données alphanumériques du fichier PARAFES feront l'objet d'une interconnexion avec le fichier des personnes recherchées (FPR) et avec le système d'information Schengen (SIS)[55].

[54]. Décret n°2007-1182 du 3 aàut 2007 portant création d'un traitement de donnéees à caractère personnel relatives à des passagers des aéroports francais franchissant les frontières extérieures des Etats parties à la convention signée à Schengen le 19 juin 1990; JO n° 181 du 7 août 2007 p 13203

[55] La Cnil dans sa délibération n°2007-094 du 3 mai 2007, J0n°181 du 7 août 1007, texte 142, avait souhaité "*que le projet de décret devrait être complété pour mieux définir et limiter les modalités d'interconnexion de ces fichiers. Elle propos(ait) de reformuler la première phrase du paragraphe 2 de l'article 4, par exemple sous la forme suivante: 'Des dispositions techniques sont prises pour que le traitement PARAFES nterroge systématiquement le fichier des personnes recherchées et le systéme d'information Schengen, dans ce seul sens, sur la base des seules données alphanumériques, afin de ne connaitre que le statut 'connu, inconnu ou signalé de la personne en cause'*". Le fait que la rédaction définitive du décret n'ai pas retenu cette précision essentielle, ne contribue pas à lever les suspicions pouvant être formulées sur les possibilités d'évolutions pathologiques du système mis en place.

OSCAR-OFII, (Outil de statistique et de contrôle de l'aide au retour[56] relevant de l'Office français de l'immigration et de l'intégration)

Le dispositif OSCAR-OFII, créé par décret le 26 octobre 2009[57], introduit dans la partie réglementaire du code de l'entrée et du séjour des étrangers et du droit d'asile une série d'articles[58] ainsi qu'une annexe présentant la liste des 23 données à caractère personnel enregistrées par ce traitement. Selon l'art R. 611-35 le traitement OSCAR a pour finalité de liquider l'aide au retour en permettant de déceler une nouvelle demande présentée par une personne ayant déjà bénéficié de cette aide, le cas échéant sous une autre identité, de permettre un suivi administratif, budgétaire et comptable des procédures d'aides au retour et d'établir des statistiques relatives à celles-ci. À ces fins, outre les données à caractère personnel que nous avons évoqué, l'art. R611-36 prévoit que les données enregistrées dans le traitement sont :

> « 1 ° Les images numérisées des empreintes des dix doigts du bénéficiaire et de ses enfants mineurs âgés d'au moins douze ans, ou la mention de l'impossibilité de collecte totale ou partielle de ces empreintes ;
> 2 ° Les données à caractère personnel relatives aux bénéficiaires énumérées à l'annexe 6-8. »

Bien que le texte du décret précise : « Le traitement ne comporte pas de dispositif d'identification nominative à partir des empreintes ni de dispositif de reconnaissance faciale à partir de la photographie. ", le fait que l'on puisse rechercher la possibilité d'une attribution antérieure de l'aide sous une autre identité montre que dans un deuxième temps il sera toujours possible d'établir un lien entre le nom, les empreintes et le fichier. La possibilité technique d'interconnexion avec les fichiers SIS, VIS, FPR, ELOI, FNAED, ne paraît pas non plus relever d'une imagination excessive.

En l'état actuel des choses le texte prévoit que les données seront effacées en cas de refus d'aide au retour ou au plus tard 5 ans après attribution de cette aide... Quid des demandes imaginables de 'resquilleurs' postulant à 5+ 1, les empreintes, les photos étant censées avoir été effacées ? En dehors même d'une diligence, souvent mise en cause, faute de moyens des services, peut-on raisonnablement imaginer une administration prête à se priver de cet exceptionnel moyen de contrôle et de suivi dans le temps ?

AGDREF (Application de gestion des dossiers de ressortissants étrangers en France) et AGDREF2. L'application de gestion des

[56] 10 072 aides au retour ont été délivrées en 2008, contre 3311 en 2007, soit une croissance de 200%, cf? Libération 29 octobre 2009. En 2011 environ 12 000.

[57] Décret n°2009-1310 du 26 octobre 2009 portant création d'un traitemenet autmatisé de données à caractère personnel relatives aux étrangers bénéficiaires du dispositif d'aide au retour géré par l'Office français de l'immigration, JORF n°0250 du 28 octobre 2009, page 18252, texte n°3.
http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=BD5AD165804F461AC55A6D7F5B3D3BE3.tpdjo13v_1?cidTexte=JORFTEXT000021204848&categorieLien=id

[58] De l'art. R 611-35 à R 611-41.

dossiers des ressortissants étrangers en France (AGDREF) a été créée par décret du 29 mars 1993[59]. Il a été abrogé par décret le 6 juin 2011.

Ses finalités qui ont été reprises par ADGREF2 consistaient à : d'une part, à enregistrer toutes les données relatives à la situation administrative d'un ressortissant étranger en France (demande de titre de séjour ou d'autorisation provisoire de séjour, demande de regroupement familial, demande d'asile, demande de documents de circulation pour un enfant étranger mineur, mise en place et exécution d'une procédure d'éloignement, demande de naturalisation, demande d'aide au retour, demande de visa de retour) ; d'autre part, à assurer un mode de fabrication des titres de séjour et des récépissés de demande de délivrance ou de renouvellement de ces titres qui évite les risques de falsification ; en outre à permettre la vérification par les agents de l'autorité du séjour d'un ressortissant étranger en France ; enfin à alimenter une base dérivée dédiée permettant l'établissement de statistiques.

Les catégories d'informations enregistrées dans le fichier sont : état civil complet, numéro national d'identification unique, adresse, filiation, situation familiale, données relatives à la gestion du dossier, conditions d'entrée en France, visas obtenus, catégorie socioprofessionnelle, données relatives à l'autorisation de séjour détenue, autres données relatives à la situation administrative de l'étranger.

Le Projet AGDREF2, qui a été lancé en juin 2011 a procédé à une refonte d'AGDREF qu'il remplace ainsi que l'application ELOI qui traite de l'éloignement des étrangers se maintenant de manière irrégulière sur le territoire français. Il devrait prévenir les fraudes documentaires et les usurpations d'identités grâce à l'introduction pour sa mise en œuvre des techniques biométrique[60].

AGDREF2 est aussi interconnecté avec certaines catégories du fichier des personnes recherchées (FPR). Le FPR est en particulier systématiquement consulté avant délivrance du récépissé de demande de titre de séjour. Le fait que le décret portant création du fichier Eloi prévoyait l'enregistrement dans celui-ci du numéro AGDREF conduira le Conseil d'État à annuler cette disposition dans un arrêt du 30 décembre 2009[61].

[59] Décret du 29 mars 1993, JORF n°75 du 29 mars 1993, p.5577; http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=015C00FEE1EA6BE5A0A710FFB0AF00BF.tpdjo09v_1?cidTexte=JORFTEXT000000177727&categorieLien=id

[60] Le fichier biométrique des étrangers AGDREF2 a été validé par le Conseil d'État qui a rejeté le 7 mai 2012 la demande d'annulation du décret n°2011-638 déposée par le GISTI, la CIMADE et la LDH

[61] http://www.conseil-etat.fr/cde/fr/communiques-de-presse/le-fichier-%C2%AB-eloi-%C2%BB-des-etrangers-faisant-lobjet-dune-mesure.html

b) La prise en compte de la lutte contre le terrorisme

Le FNT (Fichier National Transfrontière)

Ainsi que le rappelle la Documentation Française :

> **« Pour les services de police chargés de la lutte antiterroriste, il est déterminant d'avoir accès à des informations sur les voyageurs se rendant de manière régulière ou prolongée dans des pays connus pour abriter des lieux de radicalisation, ainsi que sur les déplacements des individus déjà repérés. »** [62]

Afin d'améliorer le contrôle aux frontières et de lutter contre l'immigration clandestine, la loi du 23 janvier 2006[63] **a autorisé le ministre de l'Intérieur à procéder à la mise en œuvre de traitements automatisés de données à caractère personnel recueillies à l'occasion des déplacements internationaux en provenance ou à destination d'États n'appartenant pas à l'Union européenne**[64]**. Ces traitements peuvent être mis en œuvre pour prévenir et réprimer les actes de terrorisme. Ils peuvent faire l'objet d'une interconnexion avec le Fichier des personnes recherchées et le SIS. En autorisant l'alimentation automatique du FNT à partir de la bande MRZ pour la lecture optique des documents de voyage et des visas au moment du contrôle transfrontalier** les services de surveillance gagnent une efficacité qui sera encore accentuée par l'accès aux données de réservation, de contrôle des départs des compagnies aériennes.

CRISTINA (Centralisation du renseignement intérieur pour la sécurité du territoire et les intérêts nationaux)

Le fichier de Centralisation du renseignement intérieur pour la sécurité du territoire et les intérêts nationaux (CRISTINA)[65]. Après l'abandon du projet EDVIGE (Exploitation documentaire

---

[62] http://www.ladocumentationfrancaise.fr/dossiers/renseignement-terrorisme/renseignement-lutte-anti-terroriste.shtml

[63] Loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers. JORF n°20 du 24 janvier 2006 page 1129 texte n° 1 : http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=C597CD76FD8A182A0BB37F5E9BA7A535.tpdjo04v_2?cidTexte=JORFTEXT000000454124&dateTexte=20100322.

[64] Il s'agit des données "1° Figurant sur les cartes de débarquement et d'embarquement des passagers de transporteurs aériens ; 2° Collectées à partir de la bande de lecture optique des documents de voyage, de la carte nationale d'identité et des visas des passagers de transporteurs aériens, maritimes ou ferroviaires ; 3° Relatives aux passagers et enregistrées dans les systèmes de réservation et de contrôle des départs lorsqu'elles sont détenues par les transporteurs aériens, maritimes ou ferroviaires. Les traitements mentionnés au premier alinéa sont soumis aux dispositions de la loi n° 78-17 du 6 janvier 1978 précitée.

[65] www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&sqi=2&ved=0CDsQFjAC&url=http%3A%2F%2Fwww.nonfiction.fr%2Farticle3320le_conseil_detat_valide_le_fichier_cristina_et_le_dispense_de_publication_au_journal_officiel.htm&ei=rHMXUf_dO6uR0QWY84GgBA&usg=AFQjCNHwdlnflnwBBhtBoawhHzJ_tvoz2w/.

et valorisation de l'information générale)[66], proche à les confondre du fichier PASP[67] (Prévention des atteintes à la sécurité publique), CRISTINA traduit un peu ce paradigme du bonneteau dont nous avons évoqué l'existence. La réforme des services de renseignement a conduit à la création, le 1er juillet 2008, d'un service de renseignement intérieur unique, la direction centrale du renseignement intérieur (DCRI), obtenu comme par la fusion de la DST (direction de la surveillance du territoire) et des RG (Renseignements généraux). Mais il faut noter que, si les effectifs de la DST tournaient autour de 2000 personnes, la DCRI disposera du double ! Le décret portant création de la DCRI précise qu'« elle contribue à la surveillance des communications électroniques et radioélectriques susceptibles de porter atteinte à la sûreté de l'État ».

Selon le rapport Bauer :

> « La réorganisation des services de renseignement du ministère de l'Intérieur, survenue le 1er juillet 2008, a permis de constituer un service de renseignement intérieur unique, chargé des missions de l'ancienne DST et d'une partie de celles de l'ancienne DCRG. CRISTINA est le fichier de renseignements de cette nouvelle direction centrale du renseignement intérieur (DCRI). Ce traitement, comme le fichier de la DST (qui datait de 1986), est soumis au régime juridique des fichiers "de souveraineté", défini par l'article 26 (III) de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et par le décret no 2007-914 du 15 mai 2007 : CRISTINA ne peut faire l'objet d'un contrôle sur place de la CNIL et le décret en portant création n'est pas publié. »[68]

CRISTINA n'est interconnecté avec aucun autre fichier et n'est consultable que par les fonctionnaires spécialement habilités par le directeur central du renseignement intérieur. Cristina pourra garder traces des données provenant des écoutes (téléphoniques et internet) de ceux que les autorités voudront surveiller.

Le fichier GESTEREXT (Gestion du terrorisme et des extrémismes à potentialité violente)

Ce fichier mis en œuvre par la sous-direction chargée de la lutte contre le terrorisme et les extrémismes à potentialité violente de la Direction du Renseignement de la Préfecture de Police de Paris pour exercer ces missions qui sont couvertes par le secret. Aucun texte de référence initial ne peut être mentionné. Ce traitement, comme le fichier CRISTINA de la DCRI, est soumis au régime juridique des fichiers « de souveraineté », défini par l'article 26 (III) de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Selon le rapport Bauer qui a en quelque sorte « mis à jour » ce fichier à l'occasion de son rapport,

---

[66] http://fr.wikipedia.org/wiki/Exploitation_documentaire_et_valorisation_de_l%27information_g%C3%A9n%C3%A9rae.

[67] http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=?cidTexte=JORFTEXT000021163879&dateTexte=&oldAction=rechJO&categorieLien=id.

[68] Op. cit. p.46.
http://lesrapports.ladocumentationfrancaise.fr/BRP/084000748/0000.pdf

> « GESTEREXT, qui n'est interconnecté avec aucun autre fichier, n'est alimenté et n'est consultable que par les fonctionnaires spécialement habilités par le préfet de police de la sous-direction chargée de la lutte contre le terrorisme et les extrémismes à potentialité violente de la DR-PP. Le fichier est soumis au droit d'accès et de rectification garanti à chaque citoyen par l'article 41[69] de la loi de 1978. Ce droit s'exerce, comme pour presque tous les fichiers de police, par l'intermédiaire de la CNIL. »[70]

Révélatrice de la vigilance accrue, tant au niveau européen que national[71] à l'égard de l'étranger perçu comme menace, la multiplication de ces fichiers va trouver une forme de consolidation et de coordination dans la mise en place de coopérations structurelles et conventionnelles au niveau européen.

B) L'interconnexion des fichiers de police et l'extension des sources du contrôle

Le développement des fichiers de police et leur interconnexion sont à l'origine de questionnements qui mettent en opposition l'efficacité administrative et policière et la protection des libertés. Mais, paradoxalement, alors même que depuis l'expérience, en France, du projet Safari[72], l'attention se fixe sur l'intégration ou l'agrégation des multiples fichiers dans un Méga fichier, le problème s'est déjà déplacé vers d'autres niveaux technologiques : celui de l'utilisation par la police de méta fichiers et de l'utilisation des données de l'open Data. Cette extension de la possibilité

---

[69]. Article 41 de la loi du 6 janvier 1978 :

> « Par dérogation aux articles 39 et 40, lorsqu'un traitement intéresse la sûreté de l'Etat, la défense ou la sécurité publique, le droit d'accès s'exerce dans les conditions prévues par le présent article pour l'ensemble des informations qu'il contient.La demande est adressée à la commission qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'Etat, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de la commission. Il est notifié au requérant qu'il a été procédé aux vérifications.
>
> Lorsque la commission constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'État, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant.
>
> Lorsque le traitement est susceptible de comprendre des informations dont la communication ne mettrait pas en cause les fins qui lui sont assignées, l'acte réglementaire portant création du fichier peut prévoir que ces informations peuvent être communiquées au requérant par le gestionnaire du fichier directement saisi. »

Article 42 de la loi du 6 janvier 1978 :

> « Les dispositions de l'article 41 sont applicables aux 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, si un tel droit a été prévu par l'autorisation mentionnée aux articles 25, 26 ou 27 ».

[70] op. cit. pp.49-50
http://lesrapports.ladocumentationfrancaise.fr/BRP/084000748/0000.pdf

[71] Nous pourrions trouver des correspondances à l'étranger de la multiplication de ces fichiers.

[72] http://www.cnil.fr/vos-libertes/histoire.

d'accumuler et d'entrecroiser les données relatives aux individus qu'elles soient fournies par les fichiers de polices, ceux des sociétés utilisant les réseaux sociaux, ou des brokers d'information montre que le problème n'est peut être plus celui de la mise en place de ces fichiers que celui du contrôle qui devra être exercé sur l'élaboration de leur contenu, le contrôle de leur utilisation et notamment de l'habilitation qui sera délivrée à ceux qui y auront recours. En cela le rôle du magistrat sera essentiel pour la protection des individus contre les procédures inutilement intrusives, la protection des libertés et en particulier de la vie privée, et de la protection du droit à l'oubli dans un monde soumis à la dictature de la transparence.

1) Du méga fichier aux métafichiers et utilisation des OSINT

Après l'abandon du projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus), en 1974 dont l'objet était d'organiser une interconnexion des fichiers nominatifs de l'administration française, notamment par le biais du numéro INSEE ; la proposition de créer un « Fichier des honnêtes gens », est apparu comme une tentative de revenir au projet de Méga fichier envisage sous la présidence de Georges Pompidou.

a) La création du « Fichier des honnêtes gens »

En mars 2012, l'annonce de la mise en place de deux nouveaux fichiers peut être perçue comme le point culminant de la mutation observée par Mireille Delmas-Marty. Au-delà du fichier administratif classique ou du fichier de police à vocation de contrôle, de prévention ou de poursuite, est apparu le projet de « Fichier des honnêtes gens ». Le 7 mai était publié le décret emportant la création du « Fichier d'analyse sérielle »[73]. Lié à la mise en place de la nouvelle carte d'identité électronique, censée être en mesure d'apporter une réponse définitive au phénomène de l'usurpation d'identité, le fichier des « honnêtes gens » a soulevé de véhémentes protestations, un avis défavorable de la CNIL[74] et une décision du Conseil Constitutionnel déclarant non conformes au texte fondamental un certain nombre de points de la proposition de loi relative à la protection de l'identité du 6 mars 2012[75]. Après suppression de ses dispositions non conforme, la loi du 27 mars 2012[76] a instauré un système de protection de l'identité plus adapté à sa finalité immédiate.

[73] http://www.legifrance.gouv.fr/affichTexte.do ;jsessionid= ?cidTexte=JORFTEXT000025823014&dateTexte=&oldAction=rechJO&categorieLien=id
[74] http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025804936
[75] http://www.assemblee-nationale.fr/13/ta/ta0883.asp
[76] http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025582411&dateTexte=&categorieLien=id

Le projet initialement envisagé consistait en la mise en place d'un double système de puces électroniques séparées. L'une de ces puces, que l'on qualifiera de régalienne, contenant les informations d'état civil et des données biométriques (taille, sexe, empreintes digitales, photographie) concernant le titulaire (art. 2). Ces données devant être rassemblée dans un méga fichier national, la base centrale TES (Titre Électronique Sécurisé) géré par le ministère de l'Intérieur (art.5), dont les modalités d'utilisation et les finalités, ont été au centre même du débat. Une seconde puce, facultative (art.3) permettrait au titulaire du titre sécurisé d'apposer une signature électronique dans le cadre d'opérations de commerce électronique ou de démarches administratives en ligne. Ces fonctionnalités de la carte furent fortement encouragées par les industriels membres du GIXEL[77], n° 1 mondial des empreintes digitales et des papiers d'identité biométriques, dont 14 des 31 personnes auditionnées au Sénat étaient membres[78].

Nous aurons l'occasion de revenir, dans notre deuxième partie, sur la manière dont le Conseil Constitutionnel, le 12 mars 2012 en se fondant sur la réaffirmation des principes de finalité et de proportionnalité, notamment, opéra un remodelage de ce projet de loi.

La décision du Conseil constitutionnel fut présentée par la presse[79] comme un échec pour le ministre de l'Intérieur Claude Guéant. Fallait-il, dès lors, considérer, ainsi que le firent les médias, la parution le 7 mai[80], au lendemain de l'élection du nouveau président de la République, du décret créant le « Fichier d'analyse sérielle »[81], comme une ultime tentative du ministère de l'Intérieur de se doter de l'instrument lui permettant de mobiliser l'ensemble des données à la disposition de l'État ? La réaction des opposants à ces fichiers paraîtra d'autant plus disproportionnée que, d'une part, leur mise en place est rigoureusement encadrée, mais surtout en ce que, dans la crainte des atteintes aux libertés, leur combat les détourne de ce qui techniquement peut représenter un risque plus immédiat : l'existence et la mise en œuvre effective depuis 2002 des métas moteurs, voire du moteur de requête unique. Aujourd'hui le logiciel « CHEOPS »[82], bientôt « PASSAGE »[83].

---

77. http://www.gixel.fr/rubrique/secteurs_activite/136/index.htm

78 Cf. Ladepeche. fr, 6 février 2011 : http://www.ladepeche.fr/article/2012/02/03/1276874-bientot-en-vigueur-le-fichier-des-gens-honnetes.html

79 Cf. « Le Monde » du 24 mars 2012, p. 10 sous la signature de Laurent Borredon.

80 http://www.lepoint.fr/chroniqueurs-du-point/guerric-poncet/fichier-geant-le-cadeau-de-depart-de-claude-gueant-10-05-2012-1460063_506.php

81 D'aucuns iront jusqu'à parler de « bombe atomique contre la vie privée » (Valérie Dagrain via Creis terminal 12/05/2012).

82 http://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&ved=0CGgQFjAG&url=http%3A%2F%2Fwww.interieur.gouv.fr%2Fsections%2Fa_votre_service%2Fpublications%2Fcirculaires%2F2002%2FINTA0200210C.pdf%2FdownloadFile%2Ffile%2FINTA0200210C.pdf%3Fnocache%3D1161765346.82&ei=_2vUT8-KCsHJ0QWhrK33Aw&usg=AFQjCNF0QIhzcu55fmoVdbnb-OsBqwfZOg

83 Évoqué par la délibération CNIL n° 2011-204 :

b) Méga fichier ou méta moteur : le risque réel

Un dernier exemple doit permettre à la fois de distinguer ce qui relève du fantasme et, techniquement, d'une confusion des concepts. Le problème de l'accès aux données ne se résume pas à la question de l'existence d'un méga fichier unique, voire de fichiers interconnectés. L'existence d'un logiciel, d'une « application », permettant à une autorité de contrôle, policière ou administrative, d'accéder aux données de multiples fichiers, fussent-ils séparés sur le plan matériel les uns des autres, est en soit largement suffisant et tout aussi menaçant. L'étude du projet « CHEOPS » et du NS2I est à cet égard particulièrement éclairante de ces sortes de contorsions de l'exécutif, et en particulier du ministère de l'Intérieur dans la recherche des voies et moyens d'accès aux informations considérées comme nécessaires à la recherche de ce que l'on considérera comme l'ordre public. Notion éminemment politique et donc susceptible de contenus évolutifs.
On comprendra aisément qu'il ne sera plus nécessaire de parler d'interconnexion ou de fichier universe l[84]à partir du moment où est mis en place un véritable « Google de la police » (méta moteur de recherche unique) permettant d'arriver au même résultat. Quand le médiologue s'inquiète de la fusion, en mai 2012, des fichiers du « STIC » et « Judex », le citoyen ferait mieux d'avoir conscience des effets de l'application « CHEOPS » qui est opérationnelle depuis janvier 1999.

Le Projet CHEOPS (Circulation Hiérarchisée des Enregistrements Opérationnels de Police Sécurisés)

L'un des objectifs principaux du projet « CHEOPS » a été de mettre en place une architecture logicielle et matérielle homogène, sécurisée et commune à l'ensemble des applications. Les applications accessibles via « CHEOPS » étaient, selon une littérature grise du ministère de l'Intérieur, que l'on pourra, mutatis mutandis, actualiser en tenant compte des changements de sigles et des aléas politiques (cf. Edvige, Cristina, Eloi, Ariane, Ardoise, Anacrim) :

> Fichier d'antécédents judiciaires (FAJ) (= mutualisation du STIC[85] et de JUDEX[86]

http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025804888&dateTexte=&categorieLien=id

[84] Avec plus ou moins de cynisme, on pourra même, politiquement, critiquer les méga fichiers et s'en indigner sans conséquence.

[85] Système de traitement des infractions constatées de la police nationale. http://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CFoQFjAA&url=http%3A%2F%2Fwww.cnil.fr%2Ffileadmin%2Fdocuments%2Fapprofondir%2Fdossier%2FControles_Sanctions%2FConclusions%2520des%2520controles%2520STIC%2520CNIL%25202009.pdf&ei=sV_HT5_4BILOhAe4spD9Cg&usg=AFQjCNHrXGAZQ16acLBEbr6IpaagYp7ym

Fichier des personnes recherchées (FPR)
Fichier des véhicules volés (FVV)[87]
Fichiers des brigades spécialisées (FBS)
L'application des visas (VISA) ; (RMV2)[88]
Fichier des renseignements généraux (FRG) ;
Fichier informatique du terrorisme (FIT) GESTEREXT[89]
Fichier national transfrontière (FNT)[90]
Fichier national des immatriculations (FNI)[91]
Fichier national des permis de conduire (FNPC)[92]
Application de gestion des dossiers des ressortissants étrangers en France [AGDREP)[93] ; GREGOIRE – AGDREF2[94]

Sans doute est-il précisé pour la plupart, de ces fichiers qu'ils ne peuvent donner lieu à aucune utilisation administrative. Néanmoins certains le resteront (STIC) et l'on peut dès lors considérer qu'existera, de ce fait, une faille dès la conception du système.

Le système HERISSON [Habile Extraction du Renseignement d'Intérêt Stratégique à partir de Sources Ouvertes Numérisées]

HERISSON a été présenté comme un « démonstrateur technologique » de prototype dont l'objet était de tendre à la création d'une plate-forme intégrant de multiples outils de collecte de l'information, sur les réseaux ouverts, en exploitant les protocoles [HTTP, FTP, IRC, P2P, Pop3] et formats de fichiers [texte, audio, vidéo] les plus courants. L'instrument dont la création était envisagée devait accéder aux contenus diffusés sur internet, mais également aux flux TV et radio, terrestres et satellitaires. Il devait permettre la reconnaissance des langues et l'analyse des images. Dédié à l'origine du projet au ministère de la Défense son partage avec le ministère de l'Intérieur n'était ni affirmé ni dénié. Si la DGA, en son temps, a affirmé haut et fort que cet instrument n'avait pas vocation à pénétrer la sphère privée, d'aucuns n'ont pas manqué d'y voir un « système ECHELON » à la française.

[86] Système judiciaire de documentation et d'exploitation de la gendarmerie nationale. http://www.renseignementsgeneraux.net/judex.php
[87] http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000376053&categorieLien=cid
[88] http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000771780&fastPos=1&fastReqId=1064739257&categorieLien=id&oldAction=rechTexte
[89] Gestion du terrorisme et des extrémistes à potentialité violente.
[90] http://www.google.fr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&sqi=2&ved=0CGcQFjAG&url=http%3A%2F%2Fwww.assemblee-nationale.fr%2F13%2Fpdf%2Feurope%2Frap-info%2Fi3961.pdf&ei=IXvIT5a9Feyp0AXNg-W-AQ&usg=AFQjCNF-jHfUsDU0J3pR4YNfUjwlr3zsL
[91] http://www.cnil.fr/en-savoir-plus/fichiers-en-fiche/fichier/article/fni-fichier-national-des-immatriculations
[92] http://fr.wikipedia.org/wiki/Permis_de_conduire_en_France
[93] http://fr.wikipedia.org/wiki/Application_de_gestion_des_dossiers_des_ressortissants_%C3%A9trangers_en_France
[94] http://www.senat.fr/rap/a10-116-110/a10-116-11012.html.

Les renseignements de sources ouvertes : OSINT [Open Source Intelligence] ou ROSO [Renseignement d'Origine Source Ouverte]

Les renseignements de sources ouvertes constituent l'une des sources les plus exploitées en matière de recherche d'information. L'OSINT présente l'avantage de pouvoir être exploité et disséminé jusqu'aux plus bas niveaux de classification, favorisant une diffusion dans les ministères et les administrations, voire auprès du public.

§ 2 – LE RÔLE FONDAMENTAL DU JUGE ET LE DROIT À L'OUBLI

En France, la réponse donnée par le Conseil Constitutionnel à la tentative de mise en place de ce méga fichier qu'aurait pu être le « fichier des honnêtes gens, fournit une illustration intéressante d'un type de protection juridique des citoyens reposant sur le rappel par le juge constitutionnel du partage fondamental des compétences entre pouvoir législatif et pouvoir exécutif. Le rappel de la juridiction suprême française permet de souligner le rôle nécessaire du juge dans l'utilisation des fichiers et leur interconnexion.

A) Le rôle nécessaire du juge

Depuis 2009, une réelle prise de conscience semble être intervenue. Plusieurs fichiers de police utilisés au plan national par l'ensemble des forces de l'ordre ont été supprimés ou régularisés. Mais, ainsi que l'a souligné le rapport d'information parlementaire, du 21 décembre 2011, « Les dysfonctionnements et les inexactitudes dans la gestion des fichiers portent préjudice aux citoyens comme aux utilisateurs » et le rôle du juge s'avérera prépondérant. Il se manifestera notamment à deux niveaux qui traduisent deux aspects fondamentaux du respect de la loi : celui du respect de la répartition des compétences entre exécutif et législatif, d'une part, celui du contrôle des droits d'accès aux fichiers et de leurs contenus d'autre part.

1) L'intervention du juge, le respect de la constitution et de la loi

Pour ce qui est du champ de notre observation elle s'est manifestée tant au niveau du contrôle constitutionnel de la répartition des compétences entre le législatif et l'exécutif, qu'à celui du respect des lois : en particulier celle de la loi de l'informatique et des libertés de 1978.

La décision du Conseil Constitutionnel français du 22 mars 2012 relative au « Fichier des honnêtes gens »

Le fichier, que d'aucuns présentaient comme un méga fichier liberticide et d'autres comme la panacée dans la lutte contre les fraudes à l'identité, a été ramené à de plus justes proportions par la Décision du 22 mars 2012. La censure assez large de la loi a été en cela présentée par la presse comme un échec du ministre de l'Intérieur du moment[95].

La Haute juridiction a ainsi déclaré inconstitutionnels les articles 3, 5, 7, 10 du projet dans leurs totalités, ainsi qu'une partie des articles 6 et 8 d'une loi qui en comprenait 12. S'en tenant à un raisonnement reposant sur les principes fondamentaux de la constitution [art. 34) sur la répartition des compétences entre le pouvoir législatif et le pouvoir exécutif, ainsi que sur l'article 2 de la Déclaration des droits de l'homme et du citoyen, elle a validé d'une certaine manière les soupçons de détournements de finalité, ou du principe de proportionnalité, liés à la perspective de mise en œuvre du projet. Ainsi que l'observa le Conseil sa décision fut prise en :

> « Considérant que, selon les requérants, la création d'un fichier d'identité biométrique portant sur la quasi-totalité de la population française et dont les caractéristiques rendent possible l'identification d » une personne à partir de ses empreintes digitales porte une atteinte inconstitutionnelle au droit au respect de la vie privée ; qu'en outre, en permettant que les données enregistrées dans ce fichier soient consultées à des fins de police administrative ou judiciaire, le législateur aurait omis d'adopter les garanties légales contre le risque d » arbitraire ;
>
> Considérant, en premier lieu, que l'article 34 de la Constitution dispose que la loi fixe les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ainsi que la procédure pénale ; qu'il appartient au législateur, dans le cadre de sa compétence, d'assurer la conciliation entre, d'une part, la sauvegarde de l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la protection de principes et de droits de valeur constitutionnelle et, d'autre part, le respect des autres droits et libertés constitutionnellement protégés ;… en second lieu, que la liberté proclamée par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 implique le droit au respect de la vie privée ; que, par suite, la collecte, l'enregistrement, la conservation, la consultation et la communication de données à caractère personnel doivent être justifiés par un motif d'intérêt général et mis en œuvre de manière adéquate et proportionnée à cet objectif ; […]
>
> Considérant, toutefois, que, compte tenu de son objet, ce traitement de données à caractère personnel est destiné à recueillir les données relatives à la quasi-totalité de la population de nationalité française ; que les données biométriques enregistrées dans ce fichier, notamment les empreintes digitales, étant par elles-mêmes susceptibles d » être rapprochées de traces physiques laissées involontairement par la personne ou collectées à son insu, sont particulièrement sensibles ; que les caractéristiques techniques de ce fichier définies par les dispositions contestées permettent son interrogation à d'autres fins

[95] Cf. « Le Monde », 24 mars 2012, p.10.

> que la vérification de l'identité d'une personne ; 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 ;… 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 ; que, par suite, les articles 5 et 10 de la loi doivent être déclarés contraires à la Constitution ; qu'il en va de même, par voie de conséquence, du troisième alinéa de l'article 6, de l'article 7 et de la seconde phrase de l'article »[96].

C'est également sur la base de la violation de l'article 34 de la constitution que sera écarté l'article 3 de la proposition de loi, sur les dispositions facultatives relatives à la signature électronique : « considérant… que les dispositions de l'article 3 ne précisent ni la nature des "données" au moyen desquelles ces fonctions peuvent être mises en œuvre ni les garanties assurant l'intégrité et la confidentialité de ces données ; qu'elles ne définissent pas davantage les conditions dans lesquelles s'opère l'authentification des personnes mettant en œuvre ces fonctions, notamment lorsqu'elles sont mineures ou bénéficient d'une mesure de protection juridique ; que, par suite, le législateur a méconnu l'étendue de sa compétence ; qu'il en résulte que l'article 3 doit être déclaré contraire à la Constitution »[97].

Le contrôle au niveau législatif

Par ailleurs, pour ce qui est du contrôle de la légalité, le juge trouvera, par exemple, dans le contrôle du respect de l'article 6 de la loi n° 78-17, du 6 janvier 1978, qui a vocation à s'appliquer à tous les fichiers quelle qu'en soit la nature[98], selon lequel les données recueillies pour les fichiers doivent notamment être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées, et de leur traitement ultérieur », fournira une base de contrôle particulièrement pertinente.[99] Le contrôle du respect de l'article 8 de cette même loi sur le respect de l'interdiction de collecte des données sensibles, qui tend à être plus encadré, relèvera particulièrement de sa compétence.

2) Le juge garant du contrôle démocratique de l'usage des fichiers et des interconnexions

La clé de voûte de la garantie des libertés et de la protection des droits ne se situera peut-être pas tant au niveau de l'existence d'un

[96]. http://www.conseil-constitutionnel.fr/decision/2012/2012-652-dc/decision-n-2012-652-dc-du-22-mars-2012.105165.html

[97] http://www.conseil-constitutionnel.fr/decision/2012/2012-652-dc/decision-n-2012-652-dc-du-22-mars2012.105165.html

[98] Cf. Décision du Conseil constitutionnel 2003-67 du 13 mars 2003, 226 ème considérant.

[99] Ex : cf. Jugement TGI de Compiègne du 28 juin 2011, Mathieu, n° minute 562/11, pour un refus prélèvement FNAGE.

méga fichier (dont la possibilité virtuelle existe), qu'à celui de l'habilitation à l'accès au méga moteur de recherche qui existe déjà et est en train d'étendre son domaine d'exploration. Dans le triptyque « administration-police-justice », la problématique du contrôle de la norme n'est pas une question de répartition entre fichiers de police et fichiers administratifs, régaliens ou ordinaires, ni même de distinction entre exécutif et législatif, mais, plus que jamais, celle du contrôle permanent du juge indépendant pour la mise en œuvre et le suivi de l'action publique dans les champs d'activités pouvant impliquer les consultations de données personnelles ; quel que soit le procédé technique mis en place pour y avoir accès.
La réglementation européenne a ainsi déjà déterminé quelles étaient les autorités pouvant avoir accès aux fichiers mis en place dans le cadre.

Le VIS

Pour ce qui est du VIS, par exemple, le texte prévoit[100] que l'accès au VIS aux fins de consultations est exclusivement réservé au personnel dûment autorisé des autorités nationales compétentes pour les besoins prévus par les articles 15 à 22 du règlement[101]. Ainsi que le prévoit l'article 3 :

> « 1. Les autorités désignées des États membres peuvent, dans des cas spécifiques et sur la base d'une demande motivée, présentée sous forme écrite ou électronique, accéder aux données conservées dans le VIS, visées aux articles 9 à 14 (=une quarantaine de données), s'il y a des motifs valables de considérer que la consultation des données VIS contribuera substantiellement à la prévention à la détection ou à l'investigation d'infractions terroristes et autres infractions pénales graves, Europol peut accéder au VIS dans les limites de son mandat et, le cas échéant, pour l'accomplissement de sa mission. […]
> 3-Les données fournies par le VIS (...) ne peuvent être communiquées à un pays tiers ou à une organisation internationale ni être mises à leur disposition. Cependant, en cas d'urgence exceptionnelle, ces données peuvent être transférées à un pays tiers ou à une organisation internationale ou être mises à leur disposition, uniquement aux fins de prévention de détection et d'investigation d'infractions terroristes et autres infractions pénales graves et dans les conditions prévues par ladite décision ».

La question qui néanmoins se pose sera celle de l'incidence possible de l'évolution des politiques sécuritaires des États membres dans ce domaine. La notion même d'État de droit apparaîtra alors éminemment dépendante d'un environnement politique contingent. L'évolution dans le temps du contenu du concept de « sécurité frontalière », les conflits de sens et de valeur dont il peut être l'objet, nous en fournit des exemples.

[100] Art. 6 § 2 du règlement n° 767, op. Cit. p.65 ;
[101] Aux fins de l'examen et des décisions d'accorder, d'annuler, de retirer, de proroger ou de réduire la validité du visa, établissement de statistiques, vérification de l'identité du titulaire et de l'authenticité du visas et/ou conditions d'entrée sur le territoire.

L'AGDREF2

Dans le cas d'AGDREF2, autre exemple, les organismes chargés de la gestion d'un régime obligatoire de Sécurité sociale, l'ANPE et les organismes chargés de la gestion de la déclaration préalable à l'embauche peuvent légalement interroger le fichier afin de déterminer si les étrangers demandeurs ou bénéficiaires des prestations que ces organismes offrent ou distribuent sont en situation régulière. En pratique, seules les caisses d'allocations familiales ont un accès indirect à ce fichier. Par ailleurs, ont accès à ce fichier : les magistrats de l'ordre judiciaire, les préfectures pour l'application de la réglementation relative aux étrangers et les services de la police et de la gendarmerie nationales dans le seul but de vérifier la régularité du séjour des ressortissants étrangers en France. Depuis le décret du 8 décembre 2009,[102] le traitement AGDREF fait l'objet d'une interconnexion avec le fichier IMMI2 de l'office français de l'immigration et de l'intégration (OFII, ex ANAEM), auprès de qui les étrangers titulaires d'un visa de long séjour doivent déclarer leur état civil et leur domiciliation en France.

Le GESTEREX

De son côté, le GESTEREX n'est consultable que par les fonctionnaires spécialement habilités par le Préfet de Police de la sous-direction chargée de la lutte contre le terrorisme et les extrémismes à potentialité violente de la DR-PP.
Reste que sur le plan informel il est toujours possible de craindre que l'accès puisse être dévoyé. Certaines affaires en ont donné l'exemple[103]. Là encore le rôle du juge se révélera déterminant.
Ainsi que le soulignait, en 2011, le rapport des députés Batho et Batisti[104], « Une fois le fichier de police créé, le principal enjeu consiste à assurer la sécurisation de l'accès aux données et de leur utilisation. De nombreux progrès ont été accomplis dans ce domaine, au gré des avancées technologiques et de la modernisation de nombreux traitements de données à caractère personnel. Toutefois, certains services exercent encore un contrôle inadéquat de la bonne utilisation des fichiers de police ».

[102] Décret n° 2009-1516 du 8 décembre 2009 modifiant le code de l'entrée et du séjour des étrangers et du droit d'asile et relatif au système informatisé de gestion des dossiers des ressortissants étrangers en France, JORF n° 0285 du 9 décembre 2009 page 21275, texte n° 56. http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021410966&dateTexte=&categorieLien=id
[103] http://www.lepoint.fr/societe/un-policier-mis-en-examen-a-marseille-sur-fond-de-franc-maconnerie-02-09-2011-1369335_23.php
[104] Op. cit. p.79

B) Fichiers de police et droit à l'oubli.

Dans une interview de l'ancien président de la Commission Informatique et Libertés réalisée en 2011 par Grégoire Menneveux, Alex Türk déclarait :

> « Le droit à l'oubli est en réalité une espèce de mécanisme juridique qui vient, si j'ose dire s'éclipser' sur les deux libertés fondamentales que sont la liberté d'expression et la liberté d'aller et venir, et donc le droit a l'oubli, pour moi, est simplement un mécanisme qui devrait nous permettre de continuer à exercer nos libertés dans la société qui s'est numérisée entre temps. Quand je dis droit à l'oubli c'est à la fois physique et mental. Souvent les gens pensent que le droit à l'oubli c'est sur internet, mais pas seulement […] L'intimité est quelque chose qui est au cœur du patrimoine génétique de nos libertés, cette dernière peut être préservée grâce au droit à l'oubli qui fera que je n'accepterais pas qu'on nous surveille, qu'on me suive à la trace partout, qu'on me suive à la trace sur les réseaux et ainsi de suite… »[105]

La problématique de droit à l'oubli numérique est une problématique sociétale qui devra trouver une réponse au niveau législatif, voire constitutionnel. Pour ce qui concerne l'objet de notre réflexion qui est celui des fichiers de police et de ce que de manière un peu caricaturale je qualifierai de « police data mining », la question posée sera celle de la durée de la conservation des données et des mécanismes techniques de leur destruction automatisée. Selon que l'on sera d'un côté ou de l'autre de la barrière, selon que l'on optera pour la « sécurité "ou la 'sûreté', le choix que l'on mettra en avant ne sera pas le même. On se trouve alors au cœur même du choix politique et du débat démocratique. Et même à ce niveau, ainsi que le souligna le sénateur Türk, la marche peut être longue entre l'affirmation de l'intention et sa réalisation législative.

La question de la durée de conservation des données

Sans qu'il soit ici question de rentrer dans le détail d'une question particulièrement complexe, retenons que le problème se pose sur le plan interne, mais qu'il se pose aussi à propos des données qui peuvent être transférées hors de nos frontières pour la destruction desquelles notre pouvoir est inexistant[106]. Nous n'en parlerons pas ici.

Sur le plan interne, les questions relatives à la durée de conservation des données, et/ou de l'harmonisation de ces durées restent posées. Sans doute la finalité des fichiers explique-t-elle des différences qui vont faire que les durées de conservation seront différentes : FNAGE (40 ans), FIJAIS (30 ans), STIC (20

[105] Gregoire Menneveux, « *L'avènement du droit à l'oubli numérique* ,« Mémoire de Master »Droit du cyberespace ,« Université de Lille2, 2010, p.68-69.

[106] Je pense par exemple aux données PNR transférées aux États-Unis. Cf. Jean-Jacques Lavenue, *« Interopérabilité internationale, interconnexion des fichiers et protection des libertés : interrogation sur le devenir des données transférées dans le cadre de la lutte contre le terrorisme* », in Droit de l'Administration électronique, Bruylant, nov. 2011 pp. 413-436.

ans), FAED (25 ans), voire pour le FPR sans limites maximales. Mais le manque de moyen ou le manque de rigueur fera, ainsi qu'a pu le constater la CNIL et différentes commissions parlementaires que seront maintenues de données au-delà du temps nécessaire. Il est clair qu'en termes de droit à l'oubli on se trouvera alors loin du compte.

On doit noter toutefois qu'un droit à l'oubli pour les mineurs a bien été créé. L'article 5 du décret établissant un traitement relatif à la gestion de l'information et la prévention des atteintes à la sécurité publique (GIPASP)[107] prévoit : 'Ces données ne peuvent alors être conservées plus de trois ans après l » intervention du dernier événement de nature à faire apparaître un risque d » atteinte à la sécurité publique ayant donné lieu à un enregistrement.' Un décret de 2010 prévoit également qu'un magistrat de Conseil d'État sera désigné comme référent pour assurer le respect de cette mesure. Ainsi qu'en dispose l'article 5 modifié :

> « Un référent national, membre du Conseil d'État, concourt par les recommandations qu'il adresse au responsable du traitement au respect des garanties accordées aux mineurs par les dispositions du présent décret. Il est assisté d'adjoints, membres du corps des tribunaux administratifs et des cours administratives d'appel, auxquels il peut donner délégation. Le référent national et ses adjoints sont désignés par arrêté du vice-président du Conseil d'État.
>
> Le référent national s'assure de l'effacement, au terme du délai de trois ans prévu au premier alinéa, des données concernant les mineurs. Tous les douze mois à compter de l'enregistrement des données, et lorsque le mineur atteint l'âge de la majorité, il examine en outre si, compte tenu de la nature, de la gravité et de l'ancienneté des faits, la conservation des données est justifiée.
>
> Lorsqu'il constate une méconnaissance des règles applicables à la conservation des données relatives aux mineurs, le référent national en avise le responsable du traitement.
>
> Le référent national établit chaque année un rapport public.
>
> Le référent national et ses adjoints exercent leurs missions sans préjudice des compétences de la Commission nationale de l'informatique et des libertés. »[108]

Il semblerait que ce référent n'ait pas encore été désigné.

La question des mécanismes techniques de la destruction des données donne également lieu à interrogation. Ainsi que l'observait dans l'interview précitée[109], l'ancien président de la CNIL : 'est-ce que oui ou non il est possible de créer un système qui fera que si on appuie sur un bouton toutes les informations d'une personne sur le réseau où qu'elle se trouve disparaissent ? Je pense que si on le veut, si on y met les moyens, technologiquement cela doit être faisable, mais on ne fait rien pour y arriver'. L'observation est-elle transposable à l'univers technologique du maintien de l'ordre ? Fut-ce en envisageant un

[107] Décret n° 340-2011 du 29 mars 2011 :
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023781834&dateTexte=&categorieLien=id.

[108] Décret n° 2010-1540, art. 1er :
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023229606

[109] Cf. Grégoire Menneveux, op. cit. p.69.

accompagnement juridique ? L'histoire des contrôles opérés par la Commission l'Informatique et des Libertés, et leur efficacité relative, montrent que le temps de réponse reste encore souvent lent. Ainsi que le notait le dernier rapport de la mission d'information sur les fichiers de police, présenté par les députés Delphine Batho et Jacques Alain Benisti :

> « D'importants motifs d'insatisfaction demeurent. Les délais de traitement des demandes d'accès indirect sont toujours trop longs, les demandent d'effacement et de rectification particulièrement urgentes ne bénéficient d'aucun traitement particulier. L'information des personnes demeure indigente et d'importantes failles juridiques aboutissent à ce que figurent dans les fichiers des données et des personnes qui ne devraient pas y être. Aujourd'hui comme hier, la protection des libertés reste, pour vos rapporteurs, un impératif absolu. »[110]

Le développement des technologies offre aux pouvoirs publics des États de plus grandes facilités pour assurer l'ordre public et la sécurité des citoyens. Mais dans la pratique, une trop grande facilité peut conduire à certaines confusions comme celle que nous avons évoquée entre sécurité et sûreté, par exemple. Éviter ce risque fait partie des fonctions majeures de l'État et de la définition qu'il donnera, à travers la loi, de la notion de finalité des fichiers de police, de leur constitution, de leur usage et de leurs interconnexions éventuelles. La technique ne peut pas fournir une explication suffisante et qu'un fichier soit interconnectable ne suffit pas à justifier qu'il le soit. On se trouve alors face à un phénomène social qui implique un choix de civilisation sur la maîtrise et le contrôle nécessaire des technologies. Ce choix relève de la souveraineté de l'État et de l'expression que donne le pouvoir régalien de ses choix démocratiques.

Dans la conclusion de son ouvrage, *La vie privée en péril*, Alex Türk, l'ancien président de la Commission de l'informatique et des libertés écrivaient :

> « Le réalisme oblige à reconnaître que les fichiers destinés à la lutte contre la criminalité et le terrorisme sont nécessaires, que le recours à la vidéosurveillance, à la biométrie, à la géolocalisation rend, nous l'avons vu, de réels services, et qu'Internet est un formidable vecteur de progrès. Et, d'ailleurs voudrait-on enrayer le développement de cette société numérique, comment s'y prendrait-on ?
>
> En revanche, nous devrions être capables d'évaluer, en nous dotant des moyens technologiques et juridiques nécessaires l'impact des applications nouvelles… Nous devons également poursuivre les efforts pour aboutir à une prise en compte à l'échelon politique le plus élevé du pouvoir politique, et ce dans une dimension internationale, du défi ainsi lancé à notre civilisation. » [111]

[110] Rapport n° 4113, du 21 décembre 2011, p.35.
[111] Éditions Odile Jacob, avril 2011, pp. 262-263.