DU SIMPLE FICHAGE

A L'INTERCONNEXION DES FICHIERS

Si tous les instruments utiles avaient existé, nul doute que la pratique du fichage remonterait à la nuit des temps.

En effet, les hommes ont de tout temps ressenti le besoin de constituer en toutes matières des fichiers. Quelques affaires célèbres le rappellent :

Dès le XVII^{ème} siècle, le roi Louis XIV a créé ce que l'on appellerait aujourd'hui un fichier pour surveiller les artisans qui ne pouvaient sortir du royaume afin de protéger les secrets de fabrication français. Il s'agissait alors de « papiers », précurseurs des passeports actuels, d'où sans doute l'expression toujours utilisée aujourd'hui par les forces de police lors des contrôles : « vos papiers, s'il vous plait ».

Il en ira de même en 1803 lorsque Napoléon instituera le livret ouvrier afin de restreindre la circulation des ouvriers en France. A défaut de le présenter, la personne contrôlée était considérée comme vagabond.

Au début du XX^{ème} siècle, « l'affaire des fiches », plus connue sous le nom « d'affaire des casseroles », visera à républicaniser l'armée en faisant appel à toutes les « associations républicaines, de la franc-maçonnerie comme des autres » pour connaître les opinions politiques des officiers. L'objectif était de faciliter la promotion des officiers républicains qui, pensait-on, avaient été défavorisés dans leur avancement et qui hésitaient à faire connaître leurs opinions par crainte pour leur carrière. Ce scandale sera dénoncé à la Chambre des députés en octobre 1904. Il est indissociable de l'affaire Dreyfus. C'est en effet la condamnation du capitaine en décembre 1894 qui va amener l'intervention des mouvements républicains.

Comme on le voit, les « fiches » ont succédé aux « papiers ».

Le « carnet B » aura pour but de repérer les suspects d'espionnage et d'antimilitarisme. En 1914, à la veille de la première guerre mondiale, 2 500 personnes seront ainsi fichées pour leur militantisme politique ou syndical.

A partir de 1933, l'utilisation des cartes perforées, inventées en 1887 par l'américain Herman Hollerith, fondateur d'IBM, pour faciliter le recensement de la population aux Etats-Unis d'Amérique, va permettre au régime nazi allemand de recenser … les juifs et d'organiser la déportation. En France, c'est le « fichier Tulard », du nom d'un policier qui après avoir fiché les communistes sous la Troisième République, s'emploiera à faire de même avec les juifs, sous le régime de Vichy, ce qui sera transmis aux responsables de la gestapo à PARIS.

Cette méthode de mécanographie par cartes perforées débouchera, sous l'impulsion du contrôleur général des armées René Camille qui avait pour mission de préparer la remobilisation après la dissolution de l'armée en 1940, sur le numéro actuel de sécurité sociale, également connu sous l'appellation de numéro INSEE, du nom du service français chargé de la statistique. Ce numéro à treize chiffres, auxquels il faut ajouter une clé composée de deux chiffres, trouve son origine dans le « numéro d'inscription au répertoire national d'identification des personnes physiques », le NIR. Il a débouché sur une

interconnexion utile à plusieurs organismes (sécurité sociale - établissements de santé - ceux spécialisés dans la lutte contre le chômage et pour la recherche d'emploi - administration fiscale…).

Ce bref rappel historique démontre que depuis les premiers fichiers « papier », le recours à des méthodes mécanisées (cartes perforées) et l'interconnexion des fichiers se sont vite imposés.

Mais c'est l'apparition de la bureautique (I-) qui a vraiment permis « l'explosion » du fichage avant qu'internet (II-) ne vienne faciliter l'interconnexion des fichiers.

I- L'influence de la bureautique sur le développement de la pratique du fichage :

Le développement de la bureautique a eu pour effet de vulgariser l'activité de fichage. En effet, tous les logiciels permettent la création de bases de données, qu'il s'agisse des logiciels de traitement de texte, des tableurs ou des logiciels spécialisés dans de telles bases. Dès lors, la création d'un fichier devient à la portée de tous que ce soit à titre privé ou à titre professionnel.

I-1 La multiplication des fichiers :

Dans un premier rapport rédigé en décembre 2006[1] à la demande du ministre de l'intérieur, Alain BAUER[2] qui présidait le groupe de travail écrivait en introduction :

« Il existe en France de nombreux fichiers tenus par l'administration en vue de recenser des personnes en fonction de leur statut (nationaux ou étrangers, par exemple), de comptabiliser les propriétaires de véhicules ou les titulaires de permis de conduire, de dénombrer les personnes condamnées (Fichier du casier judiciaire national) ou encore contribuant à prévenir ou à réprimer les crimes, délits et contraventions.

Ces derniers fichiers sont principalement gérés par les services de police et de gendarmerie. Ce sont essentiellement des fichiers à vocation opérationnelle, c'est-à-dire des systèmes automatisés de données regroupant des informations sur des procédures en cours, des personnes mises en cause, des individus surveillés. Il peut aussi s'agir de fichiers contenant des traces et indices (empreintes digitales, par exemple). Ces fichiers, dits de police, jusqu'alors principalement manuels, ont progressivement été automatisés et se sont considérablement développés au cours des dix dernières années, suivant en cela l'évolution des techniques, de l'informatique et de la science tout en répondant à l'évolution parallèle des phénomènes criminels ou terroristes ».

Il recensait ensuite un nombre impressionnant de fichiers ; il serait fastidieux pour le lecteur de les décrire tous. On citera seulement :

- Les fichiers de la police nationale (sous CHEOPS) : le Système de traitement des infractions constatées (STIC) - le Fichier des véhicules volés (FVV) - le Fichier des personnes recherchées (FPR) - le Fichier des renseignements généraux (FRG) - le Fichier national transfrontières (FNT) - le Fichier des brigades spécialisées (FBS) - le

[1] « Fichiers de police et de gendarmerie - Comment améliorer leur contrôle et leur gestion ? » (La documentation française)

[2] Alain BAUER est professeur de criminologie, Président du Conseil National des Activités Privées de Sécurité (CNAPS) - A l'époque du rapport, il était également président du conseil d'orientation de l'Observatoire national de la délinquance, membre du Collège de la Haute Autorité de lutte contre les discriminations et pour l'égalité (HALDE).

Fichier informatisé du terrorisme (FIT) - le Fichier national du faux monnayage (FNFM) - le Fichier national automatisé des empreintes génétiques (FNAEG),
- Le fichier de la Direction de la surveillance du territoire (DST),
- Le Système d'analyse et de liens de la violence associée au crime (SALVAC),
- Le fichier de travail de la police judiciaire (FTPJ),
- Le Fichier automatisé des empreintes digitales (FAED),
- Les fichiers de la gendarmerie nationale : Le Système d'information judiciaire de la gendarmerie nationale JUDEX (acronyme pour système JUdiciaire de Documentation et d'EXploitation) - Le Fichier des objets signalés (FOS) - Le fichier de traitement des images des véhicules volés (FTIVV) - Le logiciel d'analyse criminelle (ANACRIM) - Le Service central de préservation des prélèvements biologiques (SCPPB) - Le Fichier des avis de condamnations pénales (FAC) – Puls@r qui permet aux unités territoriales de la gendarmerie nationale de gérer sur le plan administratif le service et les registres (courrier et procès-verbaux) - La Bureautique brigade 2000 (BB2000) - Le Fichier alphabétique de renseignements (FAR) - Le Fichier des personnes nées à l'étranger (FPNE) - Le fichier ARAMIS de traitement des informations présentant un caractère opérationnel - Le Fichier de suivi des titres de circulation délivrés aux personnes sans domicile ni résidence fixe (SDRF) - Le Fichier de suivi des personnes étrangères faisant l'objet d'une rétention administrative - Le Fichier de la batellerie
- Le fichier Ariane qui était destiné à regrouper les fichiers STIC et JUDEX ci-dessus évoqués,
- Le Fichier judiciaire national automatisé des auteurs d'infractions sexuelles (FIJAIS),
- Le Fichier national des permis de conduire (FNPC)
- Le Fichier AGRIPPA de gestion des armes soumises à autorisation ou déclaration.

Cette liste impressionnante de fichiers ne concerne que les services de police et de gendarmerie. On imagine ce qu'elle serait si ce rapport avait recensé les fichiers utilisés dans l'ensemble du secteur public ainsi que ceux qui ont été créés dans le secteur privé.

Dans un second rapport rédigé en décembre 2008[3], Alain BAUER qui présidait le même groupe de travail ajoutait 11 fichiers aux 34 qu'il avait recensés deux ans auparavant. Dans l'un et l'autre cas, il faisait un certain nombre de recommandations au ministre de l'intérieur.

La liste est encore plus impressionnante si l'on détaille les fichiers qui n'ont pas été pris en compte par ces rapports, à savoir :

- les fichiers de la Défense nationale ;
- le fichier réseau mondial visas 2 (RMV 2) ;
- l'application de gestion des dossiers des ressortissants étrangers en France (AGDREF) ;
- le fichier ELOI (acronyme d'ELOIgnement) des étrangers faisant l'objet d'une mesure d'éloignement ;
- le fichier national des personnes incarcérées ;
- le casier judiciaire national ;
- le fichier des naturalisations ;
- les fichiers de l'Office français de protection des réfugiés et apatrides ;
- le répertoire national d'identification des personnes physiques ;
- le fichier du recensement ;
- les fichiers d'état civil ;
- le fichier national des comptes bancaires (FICOBA) ;
- le fichier national des chèques irréguliers (FNCI) ;
- le fichier central des chèques (FCC) ;
- le fichier national des incidents de remboursement des crédits aux particuliers.

[3] « Mieux contrôler les fichiers de police pour protéger les libertés » (La documentation française)

Cette situation ne pouvait qu'engendrer la création de procédures spécifiques afin de maîtriser la situation, pour ne pas dire cette dérive.

I-2 La maîtrise de la situation :

Dès 1974, une prise de conscience s'est produite en France à l'occasion du projet SAFARI qui avait pour but d'identifier chaque citoyen par un numéro et d'interconnecter tous les fichiers de l'administration. En raison de l'émotion suscitée, elle déboucha quelques années plus tard sur la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés[4] et la création de la Commission Nationale de l'Informatique et des Libertés (CNIL). On ne peut que saluer cette anticipation devant un phénomène qui aurait sans doute été difficile à maîtriser par la suite.

La CNIL exerce un contrôle mais l'influence du droit développé par le Conseil de l'Europe à travers la Cour européenne des droits de l'homme (CEDH) ne doit pas être oubliée.

I-2-a- Le contrôle par la CNIL :

La CNIL a pour mission de veiller à ce que la collecte et le traitement des données à caractère personnel ne portent atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Elle a un rôle de conseil et d'information ainsi qu'un pouvoir de contrôle de conformité des fichiers à la loi. Elle peut prononcer des sanctions et se doit de dénoncer au parquet les infractions qu'elle constate.

Son rôle régulateur est d'autant plus important que la création de fichiers en tous genres est devenue d'une grande simplicité, ce qui est le côté négatif des nouvelles technologies. Par contre, celles-ci permettent, et c'est leur côté positif, la mise à jour des fichiers, ce que ne permettait pas, ou alors de façon très imparfaite, le traitement exclusivement manuel de la plupart d'entre eux. C'est la raison pour laquelle ceux-ci sont désormais abandonnés, tels pour la gendarmerie, le fichier alphabétique de renseignements (FAR) composé de fiches manuscrites individuelles, le fichier des personnes nées à l'étranger (FNPE) ou encore le fichier des avis de condamnation (FAC).

Le droit à la protection des données et à la vie privée est inscrit dans la charte des droits fondamentaux de l'Union européenne du 7 décembre 2000, puis il a été repris dans le traité de l'Union européenne de Lisbonne du 13 décembre 2007, ce qui lui donne une dimension européenne.

Cette dimension doit être rapprochée de celle initiée par le Conseil de l'Europe.

I-2-b- L'influence du Conseil de l'Europe :

On doit se référer à plusieurs recommandations du Conseil de l'Europe :

- La recommandation Rec (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police (adoptée le 17 septembre 1987) dispose dans son article 2.1 que la collecte de données à caractère personnel doit, sauf exception légale, se limiter à ce qui est nécessaire à la prévention d'un danger concret ou à la répression d'infraction pénale déterminée.

- Dédiée à l'utilisation des analyses de l'ADN dans le cadre de la justice pénale, la recommandation Rec (92) 1 (adoptée le 10 février 1992) énonce pour sa part que les

[4] modifiée par une loi du 6 août 2004 qui a transposé en France une directive européenne n° 95/46/CE du 24 octobre 1995 relative à la protection des personnes à l'égard des données à caractère personnel

prélèvements d'échantillons aux fins d'analyse de l'ADN ne doivent être effectués que dans des circonstances déterminées par le droit interne, et sur autorisation, le cas échéant, de l'autorité judiciaire (art.3). L'article 8 de la recommandation (explicité par un mémorandum) traite de la conservation des prélèvements en considérant que les données doivent être supprimées dès lors qu'elles se rapportent à une personne innocentée.

Il en résulte que le traitement automatisé de traces et empreintes digitales et palmaires en vue de faciliter la recherche et l'identification des auteurs de crimes et de délits a pour seul but de faciliter la poursuite, l'instruction et le jugement des affaires dont l'autorité judiciaire est saisie. C'est ce qui a déterminé la CEDH dans un arrêt récent du 18 avril 2013 (Affaire M. K. c. France -Requête n° 19522/09), à condamner la France pour violation de l'article 8 de la Convention européenne des droits de l'homme.

Dans cette affaire, M. K., avait été inquiété dans deux affaires de vols de livres. Dans l'une, il avait été relaxé par le tribunal correctionnel ; dans l'autre, il avait bénéficié d'un classement sans suite. Il avait en conséquence demandé au procureur de la République l'effacement de ses empreintes digitales du fichier automatisé des empreintes digitales (FAED - ci-dessus répertorié), ce qui lui avait été refusé, tous ses recours contre cette décision ayant été rejetés (juge des libertés et de la détention - chambre de l'instruction - arrêt de la Cour de cassation en date du 1er octobre 2008).

Dans sa décision, la CEDH a rappelé que la conservation, dans un fichier des autorités nationales, des empreintes digitales d'un individu identifié ou identifiable constitue une ingérence dans le droit au respect de la vie privée (En ce sens, CEDH, Marper c/ Royaume-Uni, 4 décembre 2008). Une telle ingérence doit donc être prévue par la loi, ce qui suppose l'existence d'une base en droit interne, qui soit compatible avec la prééminence du droit. La loi doit ainsi être suffisamment accessible et prévisible, c'est-à-dire énoncée avec assez de précision pour permettre à l'individu - en s'entourant au besoin de conseils éclairés - de régler sa conduite. Pour que l'on puisse la juger conforme à ces exigences, elle doit fournir une protection adéquate contre l'arbitraire et, en conséquence, définir avec une netteté suffisante l'étendue et les modalités d'exercice du pouvoir conféré aux autorités compétentes. En l'espèce, la Cour a constaté que l'ingérence est prévue par la loi, à savoir l'article 55-1 du Code de procédure pénale et le décret n° 87-249 du 8 avril 1987 modifié. Quant à la question de savoir si la législation en cause est suffisamment claire et précise s'agissant des conditions de mémorisation, d'utilisation et d'effacement des données personnelles, la Cour a estimé que ces aspects sont en l'espèce étroitement liés à la question plus large de la nécessité de l'ingérence dans une société démocratique. Si les modalités de consultation sont suffisamment encadrées, qu'il s'agisse des personnes habilitées à consulter le fichier ou du régime d'autorisation auxquelles sont soumises les opérations d'identification qui correspondent à la finalité du fichier, la Cour a observé qu'il en va différemment du régime de collecte et de conservation des données. En effet, elle a noté que la finalité du fichier, nonobstant le but légitime poursuivi, qui a nécessairement pour résultat l'ajout et la conservation du plus grand nombre de noms possibles, n'opère aucune distinction fondée sur l'existence ou non d'une condamnation par un tribunal, voire même d'une poursuite par le ministère public. Or, dans son arrêt Marper, la Cour a souligné le risque de stigmatisation qui découle du fait que les personnes qui avaient respectivement bénéficié d'un acquittement et d'une décision de classement sans suite - et étaient donc en droit de bénéficier de la présomption d'innocence - étaient traitées de la même manière que des condamnés.

Selon la Cour, les dispositions de la législation française relative aux modalités de conservation des données n'offrent pas une protection suffisante aux intéressés. S'agissant de la possibilité d'effacement de ces données, elle considère que le droit de présenter à tout moment une demande en ce sens au juge risque de se heurter à l'intérêt des services d'enquête qui doivent disposer d'un fichier ayant le plus de références possibles. Partant, les

intérêts en présence étant - ne serait ce que partiellement - contradictoires, l'effacement, qui n'est au demeurant pas un droit, constitue une garantie « théorique et illusoire » et non « concrète et effective ».

La Cour a constaté que si la conservation des informations insérées dans le fichier est limitée dans le temps, cette période d'archivage est de vingt-cinq ans. Compte tenu de son précédent constat selon lequel les chances de succès des demandes d'effacement sont pour le moins hypothétiques, une telle durée est en pratique assimilable à une conservation indéfinie ou du moins à une norme plutôt qu'à un maximum.

En conclusion, la CEDH a estimé que la France a outrepassé sa marge d'appréciation en la matière, le régime de conservation dans le fichier litigieux des empreintes digitales de personnes soupçonnées d'avoir commis des infractions mais non condamnées, ne traduisant pas un juste équilibre entre les intérêts publics et privés concurrents en jeu. Dès lors, la conservation litigieuse s'analyse en une atteinte disproportionnée au droit du requérant au respect de sa vie privée et ne peut passer pour nécessaire dans une société démocratique.

Cette analyse pourra sans doute paraître un peu longue mais elle a le mérite de définir le cadre légal et jurisprudentiel dans lequel le fichage doit s'insérer, d'autant plus que l'interconnexion des fichiers par suite du développement des technologies liées à la communication, ne peut qu'aggraver la situation et inciter à une grande vigilance.

II- L'influence du développement d'internet sur la connexion des fichiers :

Dans son deuxième rapport ci-dessus évoqué, Alain BAUER explique que celui-ci avait été justifié par l'émotion suscitée dans l'opinion publique par la présentation du fichier EDVIGE, acronyme de « Exploitation documentaire et valorisation de l'information générale ». Créé par un décret du 1er juillet 2008, cette nouvelle base de données devait permettre de rassembler toute une série d'informations sur certaines personnes publiques (politiques, syndicales, religieuses) ou encore sur certains individus ou groupes « susceptibles de porter atteinte à l'ordre public ». Selon la CNIL, dans un avis du 15 juillet 2008, aucune interconnexion de ce fichier avec d'autres fichiers ne pouvait notamment être envisagée ; elle exprimait des réserves sur la collecte d'informations relatives aux mineurs et regrettait également que la possibilité de collecter des informations relatives aux origines ethniques, à la santé ou à la vie sexuelle des personnes ne soit pas assortie de garanties suffisantes. Enfin, elle notait l'absence d'une procédure formalisée de mise à jour et d'apurement du fichier.

Finalement, ce fichier n'a jamais vu le jour mais le vif débat qu'il a suscité a eu pour avantage d'appeler l'attention sur l'interconnexion des fichiers qu'il convient tout d'abord de définir avant d'analyser ses aspects néanmoins bénéfiques ou néfastes à travers l'évolution des fichiers STIC et JUDEX ci-dessus évoqués mais aussi de certains fichiers privés.

II-1 La notion d'interconnexion :

Selon la CNIL[5], l'interconnexion se définit comme la mise en relation automatisée d'informations provenant de fichiers ou de traitements qui étaient au préalable distincts.

Trois critères cumulatifs permettent de qualifier l'existence d'une interconnexion entre des fichiers :

[5] Cf. fiche pratique du 5 avril 2011

- L'objet de l'interconnexion doit être la mise en relation de fichiers ou de traitements de données à caractère personnel : les moteurs de recherche généraux sur Internet permettent de mettre en relation des pages web, indépendamment du fait qu'il s'agisse, ou non, de fichiers de données à caractère personnel. Les moteurs de recherche généraux (comme Google ou Bing) ne constituent donc pas des interconnexions.

- Cette mise en relation concerne au moins deux fichiers ou traitements distincts : l'ajout d'informations dans un fichier existant ou la modification des finalités d'un traitement ne constituent pas à eux seuls des formes d'interconnexion, quand bien même ces ajouts nécessitent des moyens techniques nouveaux. La notion d'interconnexion peut s'appliquer aux fichiers d'un même responsable de traitement.

- Il s'agit d'un processus automatisé ayant pour objet de mettre en relation des informations issues de ces fichiers ou de ces traitements : si deux fichiers distincts ont des destinataires communs, le fait pour ces destinataires de consulter simultanément ces deux fichiers ne constitue pas, à lui seul une interconnexion. L'ajout de nouveaux destinataires à un traitement existant ne constitue pas, à lui seul, une interconnexion. La comparaison visuelle du contenu de deux fichiers ne constitue pas une interconnexion mais un rapprochement.

Une interconnexion peut prendre des formes diverses :

- Elle peut être à sens unique : un fichier peut servir à enrichir les informations contenues dans un deuxième fichier. On parle alors « d'alimentation ».

- Elle peut être bidirectionnelle : des échanges peuvent s'effectuer dans les deux sens, lorsque des Informations issues d'un traitement sont envoyées vers un deuxième traitement, pour obtenir en retour une Information nouvelle ou sa confirmation. On parle généralement de « fichier d'appel » et de « fichier réponse » pour décrire ces échanges.

- Elle peut aboutir à la création de nouveaux flux : des fichiers issus de deux traitements distincts peuvent être rapprochés ou comparés pour obtenir une information nouvelle ou la consolidation d'informations existantes.

- Elle peut être ponctuelle : une interconnexion peut être effectuée de manière automatisée mais ponctuelle, pour un besoin particulier : une fois lors de la création du traitement, ou de manière périodique (par exemple une fois par mois).

- Elle peut être permanente : l'interconnexion peut nécessiter la mise en œuvre de moyens de communication permanents entre les différents fichiers qui la composent, par exemple pour réaliser des traitements en temps réel.

Ces interconnexions sont soumises à un régime d'autorisation de la CNIL. Les fichiers peuvent correspondre à des intérêts publics différents (traitements relevant d'une ou de plusieurs personnes morales gérant un service public) ou avoir des finalités principales différentes.

On peut citer deux exemples d'interconnexions qui ont été soumises à autorisation de la CNIL :

- Pour permettre l'application du tarif social de l'électricité, la Caisse Nationale d'Assurance Maladie des Travailleurs Salariés (CNAMTS) transmet à Electricité De France (EDF) des informations relatives aux personnes dont le foyer dispose de ressources annuelles inférieures à un plafond déterminé (comme prévu par loi n°

2000-108, précisée dans le décret 2004-325). Cette transmission est mensuelle et à sens unique. Les 4 critères précédemment cités sont tous satisfaits : cette transmission a été soumise à autorisation de la CNIL car il s'agit bien en effet d'une interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents.

- Tout opérateur de jeux en ligne a l'obligation légale d'empêcher ses salariés d'engager des mises sur des jeux ou des paris qu'il propose. Pour ce faire, il a la possibilité d'extraire de son fichier de ressources humaines le nom, prénom et la date de naissance de chacun de ses salariés et extraire de son fichier clients le nom, le prénom et la date de naissance de chaque joueur ayant ouvert un compte sur son site. Il peut ensuite croiser ces deux extractions à l'aide d'un logiciel pour éditer la liste des salariés disposant d'un compte sur son site. Le croisement de ces extractions est une interconnexion soumise à autorisation de la CNIL.

Un autre exemple d'interconnexion sera dans le secteur public (II-3) celui qui concerne les fichiers d'antécédents du ministère de l'intérieur avec celui des juridictions judiciaires actuellement en cours de déploiement, connu sous le nom de CASSIOPEE. Toutefois le secteur privé (II-2) ne doit pas être ignoré.

II-2 L'interconnexion des fichiers dans le secteur privé :

Dans un rapport publié depuis maintenant dix ans[6], la CNIL a traité du cas des « listes noires » qui constituent un exemple pertinent des dérives qui peuvent se produire dans le secteur privé en raison de la prolifération des fichiers beaucoup plus importante que dans le secteur public.

Selon elle, une « liste noire » est dans le langage courant un fichier recensant des personnes indésirables. Si aucune disposition légale ou réglementaire n'interdit la constitution de telles listes, en revanche, le risque d'exclusion et de marginalisation des personnes fichées est réel. Ces fichiers sont très largement dérogatoires aux principes généraux de la protection des données personnelles : loin de demeurer confidentielles, les informations en cause sont partagées, c'est-à-dire portées à la connaissance des acteurs professionnels concernés. Par leur fonctionnement même, ces fichiers paraissent contraires à la philosophie du « droit à l'oubli » puisque va être attaché à une personne un de ses comportements passés afin d'alerter l'ensemble d'un secteur professionnel. Un équilibre doit donc être trouvé pour garantir le respect des droits des particuliers d'une part et la protection des intérêts des professionnels d'autre part. Le rôle de la CNIL est donc essentiel mais la généralisation et le développement exponentiel du fichage des « mauvais payeurs » ou des « fraudeurs » par des acteurs privés, quel que soit le secteur d'activité concerné, rend son action très difficile.

Elle l'est d'autant plus qu'elle ne dispose pas, sur le fondement de la loi du 6 janvier 1978, du droit de s'opposer à la mise en œuvre de fichiers constitués par le secteur privé. L'existence de tels fichiers n'est en effet pas subordonnée à son examen préalable, comme c'est le cas pour les fichiers relevant du secteur public, mais à une simple déclaration à la CNIL contre délivrance d'un récépissé qui ne constitue en aucun cas un agrément et n'exonère le déclarant d'aucune de ses responsabilités.

L'absence de déclaration peut néanmoins avoir d'importantes conséquences juridiques. Ainsi, dans un arrêt rendu le 25 juin 2013, la Cour de cassation a cassé l'arrêt d'une cour d'appel au motif que tout fichier informatisé contenant des données à caractère personnel doit faire l'objet d'une déclaration auprès de la CNIL ; qu'en conséquence, la vente d'un tel

[6] Les listes noires : le fichage des "mauvais payeurs" et des "fraudeurs" au regard de la protection des données personnelles - La Documentation française - 2003

fichier qui, n'ayant pas été déclaré, a un objet illicite et n'est pas dans le commerce (chambre commerciale - Pourvoi n° S12-17.037 - en cours de p ublication).

S'agissant de la mise en œuvre de fichiers dans le secteur privé, la CNIL a vu ses pouvoirs renforcés par la directive européenne du 24 octobre 1995 relative à la protection des données, transposée dans le droit français par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés). Dans son article 25, il est prévu que *« sont mis en œuvre après autorisation de la CNIL…5° Les traitements automatisés ayant pou r objet :*
- l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents ;
- l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes ».

Ces fichiers concernent aussi bien des « auteurs d'obtentions irrégulières de crédit ou tentatives de telles obtentions », que des « clients douteux », des « personnes présentant des risques aggravés », des « auteurs d'actes répréhensibles », des personnes pour lesquelles des « anomalies » ou « incohérences » sont détectées, ainsi que des « personnes indésirables ».

Ils ont pour objet le partage d'informations entre sociétés relevant d'un même secteur d'activité afin d'écarter les « mauvais payeurs » et « les clients à risques » .

Cette mutualisation concerne les fichiers mis en œuvre par de petites structures, des regroupements ad hoc de commerçants ou de certains professionnels ou encore certaines applications de sociétés de recouvrement de créances ; elle concerne aussi les secteurs de la banque, du crédit, des assurances, de la téléphonie et des télécommunications, des transports de voyageurs (notamment en région parisienne) ou encore de la grande distribution. Elle se heurte à l'interdiction posée par l'article 30 de la loi du 6 janvier 1978 aux termes duquel : *« Sauf dispositions législatives contraires, les juridictions et autorités publiques agissant dans le cadre de leurs attributions légales ainsi que, sur avis conforme de la [CNIL], les personnes morales gérant un service public peuvent seules procéder au traitement automatisé des informations nominatives concernant les infractions, condamnations ou mesures de sûreté ».*

Il s'agit là de la création de véritables fichiers centraux, ce qui amène à traiter de l'interconnexion des fichiers dans le secteur public.

II-3 L'interconnexion des fichiers dans le secteur public :

Le STIC[7] est le système de traitement des infractions constatées et le JUDEX, le système judiciaire de documentation et d'exploitation. Ils sont respectivement mis en œuvre par les services de police et par les unités de gendarmerie. Ces fichiers collectent certaines informations extraites des procédures de police judiciaire réalisées par les enquêteurs. Leur finalité première est de faciliter la constatation des infractions pénales, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs. Ils permettent notamment mais de façon très limitative de faire des rapprochements entre différentes affaires présentant des similitudes mais surtout de matérialiser, dès la phase d'enquête, l'état de récidive de certains auteurs de crimes ou délits.

[7] Son existence a été consacrée par le décret n° 200 1-583 du 5 juillet 2001 pris en application de la loi susvisée du 6 janvier 1978. Son utilisation est détaillée dans la circulaire de la direction des affaires criminelles et des grâces de la chancellerie en date du 6 juillet 2001.

STIC et JUDEX, s'ils sont également utilisés dans des conditions et dans le cadre d'enquêtes administratives strictement autorisées par la loi, demeurent à ce jour les principaux outils d'orientation des enquêtes, alors que les fichiers d'empreintes digitales et génétiques sont aujourd'hui les principaux outils permettant l'identification formelle des auteurs.

Le rapprochement au sein du ministère de l'intérieur des services de police et de gendarmerie sous une direction opérationnelle commune a imposé la fusion de ces deux fichiers en un seul : le Traitement d'Antécédents Judiciaires (TAJ) créé par décret du 4 mai 2012. Leur suppression est en conséquence prévue à compter du 31 décembre 2013.

Le TAJ a pour finalité de faciliter la constatation d'infractions, le rassemblement de preuves et la recherche des auteurs d'infractions. Il constitue le plus important fichier utilisé par les forces de police et de gendarmerie. Il apporte de nouvelles garanties aux personnes fichées par la mise à jour des suites judiciaires.

En effet, à la suite de contrôles assortis de recommandations, effectués par la CNIL en 2009 puis en 2012[8], l'une des critiques qui était faite de façon récurrente aux fichiers STIC et JUDEX était la défaillance des mises à jour. Il faut savoir qu'en raison de cette anomalie, le STIC compte plus de 6 800 000 fiches, pendant que le JUDEX en compte 2 600 000, étant en outre observé qu'ils recensent également les personnes entendues comme témoins ou victimes. Le dommage peut être considérable si l'on sait que le STIC a été consulté 11 millions de fois au 31 décembre 2012 par 100 000 utilisateurs habilités, pendant que le JUDEX était consulté pendant le même laps de temps, 15 millions de fois par 79 000 utilisateurs habilités. Or, La tenue des fichiers d'antécédents doit respecter un équilibre entre deux impératifs : l'efficacité de l'action judicaire et administrative et la protection des libertés individuelles.

Actuellement les mises à jour se font par l'envoi à la diligence des parquets des tribunaux de grande instance de fiches navette. Autant dire que ce système fonctionne mal au détriment de la crédibilité des deux fichiers et des libertés individuelles, les décisions de classement sans suite prises par les procureurs de la République, ou celles de non-lieu, de relaxe ou d'acquittement prononcées par les juridictions pénales ne faisant pas l'objet de mises à jour systématiques des fichiers d'antécédents. De plus, les qualifications pénales qui évoluent au fil des procédures sont souvent erronées.

Il convenait donc de trouver une solution définitive à ce problème dont la CNIL regrette qu'elle ne purgera pas le passé : l'interconnexion du TAJ avec le fichier judiciaire CASSIOPEE selon une architecture connue sous le nom de Nouveau Système d'Information lié à l'Investigation » (NS2i). Elle se fonde sur un lien inter-applicatif permettant une circulation de l'information entre le fichier CASSIOPEE du ministère de la Justice et le fichier d'antécédents TAJ du ministère de l'intérieur au moyen des logiciels de rédaction. Ainsi, une fois finalisée, cette interconnexion entre TAJ et CASSIOPEE permettra une transmission automatisée et instantanée des suites judiciaires ouvrant droit à la mise à jour des fichiers d'antécédents.

CASSIOPEE est l'acronyme de « Chaine Applicative Supportant le Système d'Information Oriente Procédure pénale Et Enfants ».

Cette application a permis de doter les juridictions d'un système informatique permettant la mise en œuvre du bureau d'ordre national automatisé des procédures judiciaires

[8] Cf. rapports de la CNIL des 20 janvier 2009 et 13 juin 2013, consultables sur son site internet : www.cnil.fr

(procédures pénales, procédures d'assistance éducative, procédures civiles et commerciales enregistrées par les parquets).

Mis en œuvre dans les tribunaux de grande instance, il permet l'enregistrement d'informations relatives aux plaintes et dénonciations reçues par les magistrats, dans le cadre de procédures judiciaires (gestion des audiences, élaboration des décisions des juridictions de jugement, gestion des voies de recours et des recours en grâce, gestion des requêtes, gestion des scellés et des objets en gardiennage, gestion de l'exécution des peines, gestion des agendas, archivage électronique..), afin d'améliorer le délai de traitement des procédures et d'assurer l'information des victimes.

Pour figurer dans CASSIOPEE, il convient d'être engagé dans l'une des procédures concernées en tant que : témoin, personne mise en examen ou témoin assisté, prévenu, accusé, victime, partie civile, mineur, avocat, personnel du ministère de la justice.

Les informations enregistrées dans le cadre d'une procédure pénale sont conservées selon les cas pendant une durée de dix à trente ans. Aucune modalité d'information des personnes n'est prévue car le traitement bénéficie de la dispense de l'obligation d'information. Il est en effet mis en œuvre pour le compte de l'Etat et a pour objet la poursuite d'infractions pénales ainsi que l'exécution de condamnations pénales ou de mesures de sûreté. Le droit d'accès et de rectification s'exerce auprès du procureur de la République.

CASSIOPEE est en lui-même un exemple d'interconnexion de fichiers puisqu'il est le pivot des Echanges Inter-Applicatifs (EIA) entre l'ensemble des applications informatiques participant au fonctionnement de la chaîne pénale. Ces échanges sont susceptibles de concerner, au-delà du seul ministère de l'intérieur, l'ensemble des ministères et des services traitant de procédures pénales (comme par exemple le trésor public, le fichier des permis de conduire…). En interne au ministère, CASSIOPEE sera en mesure de communiquer avec le casier judiciaire national. Les procédures saisies avec le Logiciel de Rédaction de Procédures de la Gendarmerie Nationale (LRPGN) sont déjà transmises par cette voie aux parquets.

S'agissant plus spécialement des fichiers de police et de gendarmerie, les données d'antécédents retenues par les services enquêteurs seront ainsi mises à jour instantanément, par effacement ou ajout d'une mention selon la suite judiciaire « favorable » décidée par le procureur de la République (classement sans suite), le juge d'instruction (non-lieu), le tribunal correctionnel ou de police (relaxe), ou encore la cour d'assises (acquittement). Il restera à étendre ces applications aux cours d'appel et à la Cour de cassation.

Dès lors, il ne sera plus nécessaire pour les services des greffes judiciaires de traiter manuellement les « fiches navette » jointes aux procédures, ce qui était l'un des points faibles du système antérieur.

Il résulte de cette brève étude que l'interconnexion des fichiers peut être « la meilleure comme la pire des choses ». Elle peut en effet être attentatoire à la liberté individuelle comme elle peut concourir tout aussi bien à sa protection.

Saisie depuis le 29 mars 2010 (requête n° 21010/10) en ce qui concerne le fichier STIC, la Cour européenne des droits de l'homme aura l'occasion de dire où se situe le curseur entre ces deux exigences, en application des recommandations du Conseil de l'Europe et de l'arrêt qu'elle a rendu sur le fichier des empreintes digitales, tous deux ci-dessus évoqués.

Nous connaissons peut-être actuellement le meilleur dans un monde où le traçage des individus (géolocalisation, vidéosurveillance, balises RFID de récupération de données à distance, cartes de paiement, cartes de transport…) permet d'accéder à un service adapté à leurs exigences, la compréhension dont il fait l'objet n'étant pas propice à la vigilance. *« Tant que « tout va bien », la connaissance des données par le système rend les transactions plus faciles et fluides. Mais des données recueillies dans un contexte et un but précis peuvent être croisées avec d'autres et réutilisées dans un autre but et un autre contexte à notre insu ou à nos dépens »*[9] pour aboutir à un véritable traçage électronique[10].

Mais le pire est peut-être à venir.

Dans l'un de ses ouvrages, Jacques ATTALI[11] décrit ces « surveilleurs » qui, demain, enregistreront et analyseront toutes nos activités. Ils surveilleront la maison et éviteront que celle-ci ne soit cambriolée ; ils surveilleront la qualité des aliments que nous avons dans nos réfrigérateurs… On peut même imaginer que ces « surveilleurs » seront implantés dans chacun de nous et qu'ils agiront sur notre santé (en prévention ou en réparation des cellules malades), comme sur notre éducation et notre bien-être.

S'ils sont utilisés pour améliorer la qualité de nos vies, on ne pourra que s'en féliciter. Mais ils pourraient devenir dangereux s'ils étaient utilisés à des fins totalitaires. Selon Jacques ATTALI, nous entrons dans une société où la transparence[12] est partout revendiquée. La transparence, cela veut aussi dire que plus rien ou presque ne pourra plus être caché.

Alors, le luxe ne sera plus comme aujourd'hui d'être célèbre mais au contraire d'être inconnu.

C'est ce à quoi risque d'aboutir l'interconnexion des fichiers publics mais surtout privés si nous n'y prenons garde… Il se dit qu'un citoyen français figurerait déjà aujourd'hui dans 400 à 600 fichiers…

[9] Selon Saadi Lahlou, membre du Centre Edgar Morin - Institut interdisciplinaire d'anthropologie du Contemporain (CNRS / EHESS (IIAC) et chef du Laboratoire de design cognitif d'EDF R&D,).
[10] « Traçage électronique et libertés » - La Documentation française, n°925, juin 2006
[11] Cf. son livre « Une brève histoire de l'avenir » - Fayard - 2006
[12] Cf. sur cette notion les rapports annuels de la Cour de cassation 2010 (Le droit de savoir) et 2012 (La preuve)