LES FICHIERS DE POLICE OU LE DIFFICILE ÉQUILIBRE ENTRE ORDRE ET LIBERTÉS DANS LA SOCIÉTÉ DE L'INFORMATIQUE

Anne RAINAUD

Maître de conférences en droit public à l'Université de Nice – Sophia Antipolis, CERDACFF

L'une des réponses de sécurité et défense aux menaces sur le territoire se trouve à travers les fichiers de police, lesquels soulèvent immanquablement la question classique mais néanmoins délicate du difficile équilibre entre ordre et libertés, spécialement dans le contexte relativement récent de la société de l'informatique.

La société de l'informatique a permis des capacités de développement énormes au même titre que l'imprimerie de Gutenberg. Ce sont les militaires américains (notamment pour la fiabilité des réseaux de communication), les chercheurs dans des secteurs de pointe comme l'aéronautique et le nucléaire (impliquant des modélisations complexes) qui ont favorisé le développement de cet outil merveilleux et dangereux dont la capacité de stockage et de traitement de l'information a permis de réaliser des prouesses techniques mais dont les réalisations laissent aussi parfois perplexe. On retrouve à la charnière des 20e et 21e siècles à propos de l'informatique, la même problématique que celle soulevée dans l'antiquité sur la langue d'Esope, capable du meilleur comme du pire.

La pratique des fichiers de police qui est assez ancienne puisque antérieure à la Révolution[1], a perduré à travers les siècles et les forces de l'ordre utilisent désormais cet extraordinaire instrument que sont les bases de données qui ne semblent avoir aucune limite technique tout au moins au regard des capacités de stockage des disques durs, toujours plus petits et pourtant à même de mémoriser davantage chaque année. Les limites n'existent que là où les acteurs de la sécurité veulent bien les mettre, notamment quant à la durée, quant au(x) contenu(s), quant à l'exploitation des données collectées. Or les fichiers qui ne sont à la base qu'une pratique née pour les besoins d'un service, ou plutôt du service, n'ont été rattrapés que tardivement par le législateur, qui a cherché à poser un cadre dont la mise en place n'est toujours pas aisée. Ainsi, une pratique vieille de plus de deux siècles jamais remise en cause par l'exécutif, ni par les grandes lois libérales de la 3ème

[1] Voir notamment, Bauer A. et Soullez C., *Les fichiers de police et de gendarmerie*, 2e éd., QSJ, PUF, 2011 ; Batho D. et Bénisti J.-A., Rapport d'information déposé en application de l'article 145 du Règlement par la commission des lois constitutionnelles, de la législation et de l'administration générale de la République *sur les fichiers de police,* 24 mars 2009.

République, se heurte actuellement à des standards de protection au profit des droits de l'homme.

Sur la question des fichiers informatiques et notamment ceux de police, le législateur a donc joué un rôle très traditionnel de contre-pouvoir, notamment avec l'emblématique loi de 1978 et son prolongement institutionnel qu'est la CNIL. Il le peut toujours, mais les majorités ne sont pas toujours faciles à convaincre. L'immobilisme est en marche est une formule que les rapporteurs parlementaires de 2011 Delphine Batho et Jacques Alain Bénisti auraient pu reprendre, mais les deux députés n'ont pas mâché leurs mots en estimant que « la révolution n'a pas eu lieu »[2] au regard des propositions qu'ils avaient formulées en 2009 et que le parlement n'a toujours pas transformées !

Un des contre-poids significatif à l'heure actuelle se trouve dans le pouvoir judiciaire européen. La CEDH a ainsi sanctionné la France pour son fichier des empreintes digitales en avril 2013[3]. La conservation d'empreintes digitales d'un ressortissant non condamné constitue une atteinte disproportionnée au droit à la vie privée. La proportionnalité d'une mesure de police est un élément traditionnel du droit administratif français. La CEDH ne nous fait pas découvrir un concept nouveau avec lequel composer. Cet arrêt a surtout la valeur d'un rappel au vu et au su de tous, à des notions fondamentales de notre droit public, mais qu'il s'agit de rendre effectives dans le service public de la surveillance qui s'est structuré au-delà de la simple mesure de police administrative. Malgré les nombreuses menaces sur le territoire, la lutte contre le terrorisme, pour la sauvegarde de la sûreté de l'État et donc la tranquillité des particuliers (...), ne saurait permettre des atteintes injustifiées aux droits essentiels de la personne. Le dernier arrêt Kadi de la CJUE rendu en juillet 2013[4] montre bien cet attachement de la Cour aux droits fondamentaux de la défense que ne saurait justifier le dispositif onusien pour la lutte contre Al Qaida.

Le pouvoir judiciaire européen sanctionne les pratiques étatiques (France, Royaume uni[5]). Et la société civile, médias ou associations de saisir cette perche pour tancer le pouvoir politique et mettre en avant le spectre du *big brother* et ce, d'autant qu'en interne les alertes existent, exprimées par les canaux officiels tels que la CNIL ou les rapports parlementaires.

Un certain parfum de scandale accompagne la question des fichiers de police, créant une forme de malaise dans une société qui traverse une crise de confiance envers ses gouvernants et en aval ses serviteurs. Or cette crise de confiance est grave en ce qu'elle crée un climat délétère où les forces de l'ordre ne se sentent pas

[2] Batho D. et Bénisti J.-A., Rapport d'information déposé en application de l'article 145 du Règlement par la commission des lois constitutionnelles, de la législation et de l'administration générale de la République *sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police*, 21 décembre 2011.

[3] CEDH, affaire M. K. c. France, 18 avril 2013, Requête n° 19522/09.

[4] CJUE, affaire Commission contre Kadi, aff. jointes C-584/10 P, C-593/10 P & C-595/10 P, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62010CJ0584:FR:HTML

[5] CEDH, Grande Chambre, S. et Marper c. Royaume-Uni, 4 décembre 2008, Requêtes n° 30562/04 et 30566/04.
http://www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/S.%20AND%20MARPER%20c.%20ROYAUME%20UNI%20fr.pdf

toujours investies de la confiance sociale que devrait pourtant susciter leur mission de protection.

Certes, la surveillance du corps social participe de la pérennité et du confort de celui-ci. Le pacte social selon Hobbes doit bien s'accommoder de certaines restrictions. Si les fichiers de police sont au service de la sécurité intérieure[6], ils sont corrélativement et nécessairement au service de la sécurité des citoyens (I). Les fichiers de police se rattachent fondamentalement à un service public de la surveillance, mais qui doit en même temps rester dominé par des limites afin de ne pas évoluer vers un mécanisme d'hyper surveillance dont le pouvoir peut certes tirer parti à court terme mais qui peut être fort dangereux par une mise en cause de sa légitimité du fait de dérives possibles et qui peut s'avérer à terme peu efficace. Les fichiers de police risquent de représenter alors (si ce n'est pas déjà le cas) l'outil symbolique d'une crise de confiance entre gouvernants et gouvernés, d'autant que sous cette appellation générale se retrouvent des fichiers plus ou moins transparents. La contre productivité d'un service de l'hyper surveillance en raison des troubles qui peuvent en découler est plausible dans notre société démocratique si une réponse d'envergure n'est pas déployée par les détenteurs de la souveraineté nationale dans une optique plus conciliante avec les libertés fondamentales (II).

I. Les fichiers de police : un service public de la surveillance au profit de la sécurité des citoyens

La pratique des fichiers est une réponse traditionnelle aux menaces qui pèsent sur la sécurité publique et la sûreté de l'État. Il y a de la continuité dans la démarche des pouvoirs publics à laisser prospérer cet instrument utile. Néanmoins, le poids des menaces a pris une telle dimension surtout depuis le 11 septembre, que les objectifs sécuritaires des pouvoirs publics jettent un trouble sur cette pratique qui se déploie dans un contexte où les États cherchent à renforcer leurs moyens de renseignement au point qu'ils utilisent parfois des procédés fort contestables de surveillance. Le louable service public de la surveillance est alors éclaboussé par les transgressions facilitées par la multiplication des fichiers en tous genres, qui construisent une société de la surveillance.

A. Les fichiers de police : Une réponse traditionnelle réactivée avec force en période troublée

1. Une tradition

Les divers rapports et ouvrages sur la question des fichiers de police[7] rendent bien compte que les fichiers correspondent à une politique pragmatique développée par les services chargés de l'ordre et ce, sans support juridique officiel jusqu'à peu. La tradition n'a été légalisée que récemment, opérant ainsi une sorte de mise dans le rang plus conforme à une certaine idée de l'État de droit.

[6] Koubi G., « Les fichiers de police sont au service de la sécurité intérieure », *Sécurité intérieure, les nouveaux défis*, juin 2013, p. 235.
[7] Cf. notamment, Bauer A. et Soullez C., *op. cit.*, Batho D. et Bénisti J.A., *op. cit.*

a. Une politique ancienne développée par les services.

La constitution de fichiers remonte à loin, puisque des traces ont été trouvées depuis le 13e siècle, et a connu un développement significatif au 18e siècle. L'ouvrage d'Alain Bauer et Christophe Soullez développe pertinemment cet aspect historique dont nous citerons quelques lignes les plus significatives et riches d'enseignements :

« L'année 1724 marque un tournant » (...) avec « le premier registre centralisé à l'échelle de tout le Royaume. Tenu à l'Hôpital général des pauvres de Paris et alimenté par tous les hôpitaux de province, il recense les mendiants arrêtés et fournit des renseignements sur leur identité, leur signalement, ainsi qu'une synthèse de leurs dépositions. Ce registre est communiqué, entre autres, aux officiers de la maréchaussée. En 1752, cette mesure est généralisée à tous les « gibiers de police ». Le lieutenant général de police Berryer met en place le « livre rouge » et étend l'inscription aux registres aux individus arrêtés pour vols et autres crimes (sommiers judiciaires), aux personnes détenues par lettres de cachet et enfin aux personnes de conduite suspecte (« ceux qui n'avaient pas d'autres ressources que l'intrigue ou fréquentaient de mauvaises compagnies ») ». En 1750, « le traitement de l'information se professionnalise. Ainsi, Guillauté, officier de la maréchaussée, invente le premier système de stockage et de consultation des informations consignées sur des feuillets papiers par les officiers de police : le serre-papiers... Initialement destinés à la répression et la surveillance des criminels récidivistes, les fichiers s'étendent progressivement à d'autres populations du fait de l'apparition de nouvelles formes d'incrimination (prostitution, vagabondage, etc.). À la fin du XIXe siècle, on recense déjà plusieurs fichiers : sommiers judiciaires ; fichier des interdits de séjour ; fichier des étrangers ; registre de la prostitution ; dossiers individuels de la section politique ».

Les fichiers sont ainsi un instrument de l'ordre politique et de la tranquillité sociale. Mais ce qu'il est intéressant de noter est ce glissement du fichage vers différentes catégories de personnes : il y a une propension à l'expansion. Le 20e siècle ne sera pas en reste notamment avec la place qui sera donnée au renseignement, tel que le souligne le rapport de 2009 des députés Batho et Bénisti. Ainsi, dans le vaste ensemble des fichiers de police qui ont essayé d'être listés par les deux rapporteurs précités, on peut noter la dualité entre les fichiers judiciaires fondés sur des faits, notamment ceux, par exemple, qui ont conduit ou non à des condamnations et les fichiers administratifs dont ceux du renseignement qui permettent de collecter des données multiples et même sensibles sur des personnes qui n'ont jamais eu de démêlés avec la justice.

Si l'outil perdure ainsi, c'est qu'il est devenu une pièce importante des métiers de police et de gendarmerie. Et il est notable de relier les fichiers quant à leur potentiel réactivé avec les périodes troublées ou sur le point de l'être.

L'invention par l'officier de la maréchaussée, Guillauté, du premier système de stockage et de consultation des informations en 1752 se situe 37 ans avant la révolution ; l'année 1882 connaît à la fois des attentats significatifs (explosion d'une bombe à la dynamite du box n° 4 du café Bellecour) et la création d'un service anthropométrique puis photographique en préfecture de police.

En 1967, lorsqu'une mission procède à une inspection de la documentation policière, il en ressort que « pour la seule préfecture de police de Paris, sont recensés près de 400 fichiers différents et 130 millions de fiches »[8]. Or, la France se situe ici dans l'immédiat après guerre d'Algérie et la contestation de 1968 est imminente.

La traque du terrorisme suite aux attentats du 11 septembre alimentera elle aussi cette méthode de travail qui se situe cependant dans un cadre technique beaucoup plus avancé grâce à l'informatique.

Mais le terreau était déjà prêt : l'enrichissement du droit pénal et notamment la création du délit d'association de malfaiteurs en relation avec une entreprise terroriste, introduit par la loi du 22 juillet 1996[9], qui, habilitant les autorités à prendre des mesures préventives bien avant la commission de l'acte, favoriseront en aval la pratique du fichage.

Sans continuer davantage sur le lien entre fichier de police et menace sur la sécurité, il est apparu aux analystes de ces questions que la capacité de collecter ainsi traditionnellement mise en place souffrait d'un manque de base légale.

b. La faiblesse du support juridique des fichiers

Les députés Batho et Bénisti en 2009 s'alarmaient de ce que le Parlement était relégué à une place mineure[10] dans le vaste dispositif des fichiers créé et géré par les diverses administrations dont celles chargées de la sécurité. Ils accentuaient cette inquiétude deux ans plus tard tant le poids de la tradition est lourd.

Certes, la loi informatique et libertés a posé un cadre en 1978, et donne une définition de la notion[11]. Aucune disposition législative n'était venue jusqu'alors imposer de grands axes pour encadrer une pratique qui allait pouvoir démultiplier sa capacité avec la technologie de l'informatique. La mise en place en 1975 de la Commission « informatique et libertés » ne fait-elle pas suite à la crise provoquée par le projet d'interconnexion de fichiers de police dénommé « SAFARI » ? Cependant, si le parlement légifère assez largement sur les fichiers, il reconnaît un régime dérogatoire aux fichiers de police et la notion est fort large : sûreté, sécurité, défense, prévention des infractions pénales !

Si le parlement français est assez effacé dans ce domaine, malgré des rattrapages tardifs tels que ceux de la LOPSSI de 2011[12], ce n'est pas le cas de

[8] Bauer A. et Soullez C., *Les fichiers de police et de gendarmerie*, 2e édition 2011, PUF.

[9] Loi n° 96-647 du 22 juillet 1996 tendant à renforcer la répression du terrorisme et des atteintes aux personnes dépositaires de l'autorité publique ou chargées d'une mission de service public et comportant des dispositions relatives à la police judiciaire

[10] Les fichiers de police connaissent deux modes de création, D'une part, en vertu de l'article 26 de la loi du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, tout fichier de police peut être créé par arrêté ou décret en Conseil d'État, pris après avis motivé et publié de la CNIL, le décret en Conseil d'État étant nécessaire pour les fichiers de police qui portent sur des données sensibles. D'autre part, en marge du régime général défini par l'article 26 précité, le gouvernement peut être autorisé par le législateur à créer tel ou tel fichier de police, lorsque des lois spécifiques l'y autorisent.

[11] Au regard de l'article 26 de la loi Informatique et Libertés, les fichiers de police correspondent aux traitements de données « qui intéressent la sûreté de l'État, la défense ou la sécurité publique ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ».

[12] Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure, JORF n° 0062 du 15 mars 2011 page 4582.

l'exécutif qui domine la matière, surtout depuis que le ministre de l'Intérieur[13] en 2006, inquiet du vide juridique qui caractérise certains fichiers, commande un rapport dans le souci de clarifier une situation complexe et qui en l'état, ne coïncide pas toujours avec les valeurs de l'article 2 de la déclaration des droits de l'Homme de 1789[14]. La lettre de mission rédigée par Nicolas Sarkozy mentionne clairement l'objectif d'équilibre entre protection des personnes, lutte contre le terrorisme, banditisme et protection des libertés. Le rapport Bauer quant à lui vise bien à « améliorer le contrôle et la gestion » des fichiers de police et de gendarmerie. L'exécutif est conscient que la situation est perfectible.

Le rapport des députés en 2009 établit sans complaisance la liste des nombreux fichiers de police existants et souligne pour beaucoup l'absence de texte. Et l'exécutif de combler le vide juridique. Or le rapport effectué en 2011[15] par les deux députés sur la mise en œuvre de leurs propres recommandations, notait toujours une situation contraire à leur souhait (une autorisation législative), même si une formalisation juridique reste une marque de progrès : « C'est par la voie réglementaire qu'ont été créés les fichiers les plus récents : le fichier de prévention des atteintes à la sécurité publique, le fichier des enquêtes administratives liées à la sécurité publique , la base de données de sécurité publique, le logiciel de rédaction des procédures de la police nationale ».

Si les textes prolifèrent sous la plume de l'exécutif, c'est certes pour pallier le vide mais aussi pour donner plus de pugnacité à ces outils. Le service public de la surveillance a connu une montée en puissance avec les attentats du 11 septembre, situation qui va conduire à exploiter les différents canaux pour pister et dépister les tentatives terroristes et à solliciter alors logiquement le potentiel des fichiers de police et de gendarmerie.

2. *Le 11/09/2001, la montée en puissance du service public de la surveillance et des fichiers*

La lutte contre le terrorisme et les menaces diverses qui y sont liées vont mener au développement des moyens mis à la disposition des forces de l'ordre et à augmenter leurs pouvoirs d'investigation. Dans le prolongement des résolutions adoptées dans la suite immédiate des attentats, les États ont dû d'ailleurs faire une synthèse à l'ONU de leurs dispositifs nationaux de lutte et de nécessaires modernisations sur le plan législatif se sont ainsi produites. La France n'y a pas échappé. Depuis novembre 2001[16], plusieurs textes de loi ont ainsi été adoptés où la question des données personnelles est ciblée explicitement.

---

[13] Sarkozy N., lettre de mission, http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/064000885/0000.pdf

[14] Article 2 de la DDHC : « Le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression ».

[15] Batho D. et Bénisti J.-A., Rapport d'information déposé en application de l'article 145 du Règlement par la commission des lois constitutionnelles, de la législation et de l'administration générale de la République *sur la mise en oeuvre des conclusions de la mission d'information sur les fichiers de police,* 21 décembre 2011.

[16] Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, article 22 : « Les dispositions du présent chapitre répondent à la nécessité de disposer des moyens impérieusement nécessaires à la lutte

a. Développement des moyens et pouvoirs d'investigation en France

L'État a conscience que les nouvelles technologies de l'information et de la communication constituent des moyens qui peuvent être utilisées contre lui et plus largement l'ordre public. Les lois sécuritaires augmentent les capacités des forces de l'ordre et le fichage se retrouve comme un des moyens à développer. Il est par exemple créé un fichier national automatisé nominatif des personnes qui sont interdites d'acquisition et de détention d'armes en vertu de la loi sur la sécurité quotidienne[17]. Mais l'optique sécuritaire des textes a permis d'étendre le champ du fichage et l'exemple est particulièrement révélateur avec le fichier national automatisé des empreintes génétiques (FNAEG). Créé par la loi Guigou du 18 juin 1998, sa destination était de recueillir les empreintes génétiques des personnes impliquées dans les infractions à caractère sexuel. Or le FNAEG a été ensuite étendu par des lois successives, mais significativement par loi sur la sécurité quotidienne de novembre 2001 à de nombreux autres crimes et délits (ceux visés à l'article 706-55 du code de procédure pénale). Pour le ministère de la Justice lui-même, ce fichier « a été ainsi détourné de sa vocation initiale »[18]. Les autres textes de loi sur la lutte contre le terrorisme s'engouffreront dans la brèche et les fichiers se multiplient (Traitement automatisé de données à caractère personnel relatives aux étrangers sollicitant la délivrance d'un visa (VISABIO), Traitement automatisé de données à caractère personnel relatives aux étrangers faisant l'objet d'une mesure d'éloignement (ELOI) remplacé par le fichier AGDREF2, Traitement (expérimental) automatisé de données à caractère personnel de ressortissants étrangers qui, ayant été contrôlés à l'occasion du franchissement de frontières, ne remplissent pas les conditions d'entrée requises ou « fichier des non-admis » (FNAD), Centralisation du renseignement intérieur pour la sécurité du territoire et les intérêts nationaux (CRISTINA) ...)[19].

b. Les pressions de l'extérieur

Par ailleurs, les pressions extérieures, notamment des États-Unis pour sécuriser le transport aérien, vont conduire l'Union Européenne à répondre à la demande de transmission de données sur les voyageurs enregistrés à destination des États-Unis (Passenger name record) et lors des réservations de billets. La traçabilité des déplacements et des personnes induit une inflation du fichage (le fichier des passagers aériens (FPA)[20].

La surveillance/fichage des voyageurs amène par ailleurs à se saisir de la question des fichiers d'identité nationale, notamment avec les passeports à lecture optique d'abord et biométriques enfin. Les usurpations d'identité grâce aux anciens documents devenues trop faciles à maquiller avec les logiciels de modification d'image poussent *in fine* le législateur à adopter jusqu'à une carte nationale

contre le terrorisme alimenté notamment par le trafic de stupéfiants et les trafics d'armes et qui peut s'appuyer sur l'utilisation des nouvelles technologies de l'information et de la communication ».

[17] Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, article 8.

[18] Question écrite N° : 14826 de M. Patrice Carvalho (Gauche démocrate et républicaine - Oise), Question publiée au JO le : 01/01/2013 page : 37, Réponse publiée au JO le : 02/04/2013 page : 3613, http://questions.assemblee-nationale.fr/q14/14-14826QE.htm

[19] Batho D. et Bénisti J.-A., *op. cit.*, 2009, consulter l'annexe du rapport.

[20] Loi n° 2006-64 du 23 janvier 2006 (article 7), transposant la directive 2004/82/CE du 29 avril 2004.

d'identité électronique. La formule employée par certains est facile, mais avec une certaine once de véracité : l'Assemblée nationale vote un fichier des «gens honnêtes» ! Le fichier a vocation à toucher ainsi à terme l'ensemble de la population française. Mais on sait que cette loi[21] après des avis critiques de la part de la CNIL[22] et de la Commission nationale consultative des droits de l'homme (CNCDH)[23] a été censurée partiellement par le Conseil constitutionnel[24] et tout spécialement, à propos de la disposition créant le fichier des données relative à cette carte, en considérant qu'il y a « atteinte au droit au respect de la vie privée qui ne peut être regardée comme proportionnée au but poursuivi ». « La base de données aurait été légitime pour lutter contre l'usurpation d'identité. Or, la consultation de ce fichier aurait été possible à d'autres fins de police administrative et judiciaire »[25]. La finalité du fichier potentiellement détournée a ainsi bien été saisie par les instances de contrôle. Le risque de perméabilité du fichier a donc poussé à sa censure.

Malgré ce revers, le fichage s'est banalisé, il est rentré dans les mœurs d'autant que, outre la multiplication des fichiers publics (fichiers de police, dont les fichiers régaliens axés sur le renseignement, mais aussi fichiers relevant de diverses administrations tels que caisse d'allocation familiale, sécurité sociale, fisc...), les fichiers privés sont fort nombreux. Or des entreprises privées dans notre société actuelle disposent de réservoirs de données personnelles qui peuvent être très tentants pour les pouvoirs publics dans un contexte de mondialisation, lorsque ceux-ci tracent une stratégie sécuritaire d'un niveau élevé, pouvant être potentiellement attentatoire à la vie privée et aux libertés individuelles.

B. Le déploiement des fichiers dans une société de surveillance

Le déploiement des fichiers rend difficile le respect des libertés individuelles et des scandales ou des révélations critiques pointent des débordements dont les pouvoirs publics ont conscience cependant.

1. La conscience du difficile respect des libertés individuelles

Les objectifs sécuritaires des pouvoirs publics qui luttent sur de multiples fronts dans l'intérêt de la sécurité du citoyen ont parfois du mal à s'accorder avec le

[21] La loi n° 2012-410 du 27 mars 2012 relative à la protection de l'identité, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000025582411

[22] CNIL, Note d'observations de la Commission nationale de l'informatique et des libertés concernant la proposition de loi relative à la protection de l'identité, 25 octobre 2011, http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/CNIL-PPLidentite-Noteobservations-25-10-2011.pdf

[23] Commission nationale consultative des droits de l'homme, Avis sur l'inclusion d'éléments biométriques dans la carte d'identité : « Il y a lieu d'écarter une constitution inutile et vulnérable de fichiers ».
http://www.cncdh.fr/fr/publications/avis-sur-linclusion-delements-biometriques-dans-la-carte-didentite

[24] Conseil constitutionnel, 22 mars 2012, Décision N° 2012-652 DC, loi relative à la protection de l'identité,
http://www.legifrance.gouv.fr/affichJuriConst.do?oldAction=rechJuriConst&idTexte=CONSTEXT000025561603&fastReqId=1482310064&fastPos=1

[25] Pérégrinations juridiques, 4 avril 2013, http://peregrinationsjuridiques.wordpress.com/2013/04/04/carte-nationale-didentite-electronique-et-biometrie/

respect des libertés. C'est pourtant le défi qui a bien été compris par les États, même si le point d'équilibre est loin d'être obtenu dans certains cas de figure.

Déjà en 2007, au sein de l'Union européenne, le vice-président Franco Frattini, membre de la Commission chargé de la Justice, de liberté et de la sécurité, avait parfaitement exprimé la difficulté de protéger qui incombe à la puissance publique : « la mission de confiance que nous confient les citoyens est double: ils nous demandent de les protéger contre la criminalité et les attaques terroristes, mais aussi de protéger leurs droits fondamentaux. Je pense qu'en utilisant à bon escient la technologie, nous pouvons accroître la sécurité tout en renforçant la protection de la vie privée et des données à caractère personnel[26] ».

Si les textes encadrent les cas pour lesquels les forces de l'ordre peuvent procéder à un fichage tel que le FAED, FNAEG, il est indispensable de souligner l'extension de ces cas et un mélange des genres que le bon sens vient dénoncer. En effet au regard du dispositif juridique, il est possible de procéder au fichage de personnes qui sont éventuellement en lien autant avec des infractions fort graves (telles que le terrorisme ou un crime de guerre) qu'avec des infractions qui le sont nettement moins (le fait de tracer des inscriptions, des signes ou des dessins, sans autorisation préalable, sur les façades, les véhicules, les voies publiques ou le mobilier urbain). Il suffit désormais que la personne tombe sous le coup de l'article 706-55 du code de procédure pénale en tant que suspect. Par ailleurs, des réactions au sein de la police dénoncent un fichage excessif lié aux gardes à vue dont le chiffre a explosé, désapprouvent des pressions de leur hiérarchie pour des résultats chiffrés afin de valoriser l'efficacité des commissariats. Et d'évoquer ainsi un devoir d'information où il serait bien hasardeux pour un observateur extérieur de prendre parti, mais duquel résulte un certain climat de suspicion.

Sans chercher à polémiquer sur ce thème, un rapport de l'Inspection générale de l'administration sur l'enregistrement des plaintes par les forces de sécurité intérieure daté de juin 2013[27] laisse perplexe dans la synthèse réalisée et qui est très critique sur la qualité et donc la fiabilité des enregistrements des plaintes. En effet, est mentionnée explicitement comme cause d'explication des dérives, la politique du chiffre. Or quand de telles affirmations sont réalisées dans des rapports sérieux tel que celui mentionné, il est assez logique qu'en découle des incertitudes, une crise de confiance générale sur les procédés d'enregistrement et notamment des données personnelles. Et ce d'autant que la CNIL comme les rapports parlementaires de D. Batho et J.-A. Bénisti pointent les nombreuses erreurs qui existent dans les fichiers de police et de gendarmerie. Ainsi d'une part, les fichiers de police dont le volet est judiciaire et donc théoriquement rattachés à des faits commis ou suspectés

[26] Franco Frattini, Sécurité publique, vie privée et technologie : renforcer la protection des données à caractère personnel et assurer l'accès sécurisé et rapide aux informations, 20 novembre 2007, http://europa.eu/rapid/press-release_IP-07-1726_fr.htm?locale=FR

[27] Rapport de l'Inspection générale de l'administration sur l'enregistrement des plaintes par les forces de sécurité intérieure, juillet 2013 : « Le management par objectifs de la délinquance, connu sous la dénomination de "politique du chiffre" a largement contribué à cette absence ou ce désengagement du contrôle de l'enregistrement. Les chefs de service, placés entre l'injonction d'afficher de bons résultats et l'impératif de contrôler la bonne application du guide de méthodologie statistique, privilégiaient souvent la première option », *in* http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/134000423/0000.pdf

de l'être ont été (sont encore) alimentés avec excès[28]. D'autre part, la gestion de ceux-ci est défaillante par référence aux erreurs réalisées et par la mauvaise volonté des procureurs à expurger les fichiers alors même qu'il y a un classement sans suite ou encore un jugement de cour d'appel ordonnant un effacement mais qui reste lettre morte malgré l'autorité de la chose jugée.

En conséquence, les deux grandes catégories de fichiers de police, les fichiers administratifs liés au renseignement et les fichiers judiciaires, laissent insatisfait quant à leur potentiel d'atteintes aux libertés fondamentales. En effet, les premiers ont une finalité très large et les décrets[29] créant le PASP et le GIPASP sont révélateurs d'un champ quasi illimité : « la prévention des atteintes à la sécurité publique comme la gestion de l'information et prévention des atteintes à la sécurité publique » ont « pour finalité de recueillir, de conserver et d'analyser les informations qui concernent des personnes dont l'activité individuelle ou collective indique qu'elles peuvent porter atteinte à la sécurité publique »[30]. Les seconds sont trop souvent erronés, insuffisamment contrôlés, trop largement nourris avec un accès à la rectification ou à l'effacement qui est digne de Kafka. Le service public de la surveillance semble connaître quelques dérapages et glisse vers une société de l'hyper surveillance.

Outre ces éléments d'information donnés par les institutions publiques elles-mêmes (CNIL, rapports parlementaires), certains scandales éclatent sur les excès de la société de surveillance au sens large du terme et ceux-ci n'ont alors d'autre effet que de ternir un outil comme les fichiers de police et de gendarmerie dont les citoyens perçoivent qu'ils pourraient être utilisés sans respect du principe de proportionnalité.

---

[28] Batho D. et Bénisti J.-A., Rapport parlementaire 2011 : « L'évolution constatée dans le précédent rapport de la mission, qui avait trait à la croissance continue du nombre de personnes inscrites dans des fichiers de police, persiste aujourd'hui. Le fichier des antécédents judiciaires de la police nationale, le STIC, a poursuivi sa croissance de façon régulière. Alors qu'il comportait, en 2009, 3,96 millions de fiches de personnes mises en cause et 28 millions de fiches relatives à des victimes d'infraction, il recensait, au 1er novembre 2011, 6,5 millions de mis en cause et 38 millions de victimes. L'accroissement très important du fichier des empreintes génétiques (FNAEG), qui est passé de 806 356 profils génétiques en 2008 à 1,79 million en novembre 2011, est particulièrement révélateur de cette tendance de fond. Le fichier des empreintes digitales (FAED), qui comportait moins de trois millions d'empreintes fin 2008, en comptait 4,06 millions au 1er novembre 2011.

[29] Décret n° 2009-1249 du 16 octobre 2009 portant création d'un traitement de données à caractère personnel relatif à la prévention des atteintes à la sécurité publique et décret n° 2011-340 du 29 mars 2011 portant création d'un traitement de données à caractère personnel relatif à la gestion de l'information et à la prévention des atteintes à la sécurité publique.

[30] Les données personnelles qui sont recueillies inclues notamment l'origine géographique, élément ayant fait l'objet de précision par le décret n° 2013-390 du 7 mai 2013 modifiant le décret n° 2009-1249 du 16 octobre 2009 portant création d'un traitement de données à caractère personnel relatif à la prévention des atteintes à la sécurité publique et le décret n° 2011-340 du 29 mars 2011 portant création d'un traitement de données à caractère personnel relatif à la gestion de l'information et à la prévention des atteintes à la sécurité publique. Cet élément est circonscrit à trois données : lieu de naissance, lieux de résidence et zones d'activité. Ce relatif encadrement fait suite aux précisions données par la décision du Conseil d'État, 11 mars 2013, Association SOS Racisme – Touche pas à mon pote, req. n° 348613 relatif à la contestation du décret n° 2011-340 du 29 mars 2011 (GIPASP).

2. Les scandales de la société de surveillance

L'actualité a été riche sur les agissements des États. C'est le cas des fadettes dans l'affaire Bettencourt avec l'ex-patron du renseignement intérieur, Bernard Squarcini, poursuivi pour délit de « collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite », tout comme antérieurement le juge Courroye. La violation du secret des sources n'est pas spécialement glorieux dans une société qui doit composer avec le quatrième pouvoir. Plus sulfureuses sont les investigations réalisées par l'Agence nationale de sécurité américaine (NSA) aux États-Unis dévoilées par Edward Snowden, informaticien américain, ancien employé de l'Intelligence service (CIA) et de la NSA, qui a révélé les détails de plusieurs programmes de surveillance. S'agit-il de l'expression du devoir de désobéissance à l'ordre manifestement illégal ou de la folie d'un traître inculpé pour espionnage. La question jette le trouble et fait resurgir le mythe ou la réalité de *big brother*.

La politique de l'hyper surveillance affaiblit le service public de la surveillance, réduit sa légitimité et au final dessert les particuliers en raison des atteintes à leur vie privée au-delà de l'espionnage des États ou groupe d'États. Dans cette perspective, la logique veut que les particuliers chercheront de plus en plus à brouiller l'accès à leurs données personnelles[31]. De plus, a contrario, dans une forme de réciprocité, la société civile et les médias traquent les forces de l'ordre astreintes à une certaine transparence dans la collecte des données personnelles et dénoncent toutes offenses et régime dérogatoire[32].

Pourtant les députés Batho et Bénisti ont bien compris le problème : la police et la gendarmerie ne peuvent se priver des fichiers au cœur de leur métier et pour cela il faut que le service public de la surveillance acquière pleinement sa maturité en intégrant complètement et non pas partiellement tous les enseignements offerts par les divers rapports et avis sur la question.

À défaut, nous sommes face au service de l'hyper surveillance au détriment de tous et donc de la société démocratique.

II. Le service de l'hyper surveillance au détriment de tous

L'évolution des technologies et des mœurs de la société informatique a favorisé la mise en place d'une société d'extrême surveillance, subie mais aussi créée par les individus. En effet, les particuliers sont trop souvent en même temps complices et victimes de l'exploitation des données personnelles qu'ils exposent sur des sites.

Le service de la surveillance peut ainsi exploiter sinon l'exhibition une certaine transparence qui est une mine d'informations pour le renseignement dans

[31] Ainsi certains auteurs considèrent-ils non sans raison que les fichiers de police sont davantage au service de la sécurité intérieure qu'au service des citoyens et reprochent un état de suspicion, *in* Koubi G., *op. cit.*, *Sécurité intérieure, les nouveaux défis*, juin 2013, p. 244.

[32] En ce sens, l'analyse de Alain Bauer et Christophe Soullez, *op. cit.*, « ...les fichiers, qui ont souvent été cachés par les services de l'État au cours des siècles, font aujourd'hui l'objet d'une visibilité accrue du fait tant de la législation en vigueur obligeant à leur déclaration, que de la veille médiatique et associative ».

une optique défense et sûreté de l'État et ce d'autant plus utilement que les groupes criminels ou terroristes sont utilisateurs des nouvelles technologies.

A. La surveillance exploite la transparence

La nouvelle société du web permet facilement d'empiéter sur la vie privée des individus, de faire de nombreux recoupements sur le profil des personnes. Notamment sur un plan commercial, les données sont exploitées afin de connaître les goûts et centres d'intérêt du consommateur pour procéder à de la publicité finement ciblée. Les incursions sont « banales » et constatées régulièrement par tout utilisateur du web. Parfois les immixtions dans la vie privée dépassent l'admissible et des sanctions tombent. La CNIL a ainsi infligé une amende à Google en mars 2011 de 100 000 euros. Google avec la googlecar pour répertorier sur googlemap les points d'accès Wi-Fi disponibles, a pu ainsi collecter des données personnelles de particuliers. La CNIL considère que Google a bien procédé à de la « captation de données dite de contenu » à l'insu de personnes concernées (collecte sans aucune autorisations des identifiants, mots de passe, données de connexion, échanges de courriels...)[33]. Soit ! Mais ce genre de sanction est-elle dissuasive et donc protectrice ?

En dehors de la prospection marchande, les biens liés aux nouvelles technologies sont extrêmement intéressants pour les besoins des forces de sécurité. Certains éléments techniques peuvent être exploités sous réserve d'autorisation par les services de police et de gendarmerie : la géolocalisation par les téléphones portables ou par les cartes bancaires par exemple.

Les moyens de traque semblent décuplés avec ces nouvelles technologies qui offrent une certaine traçabilité.

Ainsi, au delà des capacités d'investigation (énormes) des pouvoirs publics sur les données via les fichiers de police et de gendarmerie, notamment les fichiers de renseignement, celles-ci sont renforcées (démultipliées) grâce à la possibilité d'exploiter les données mises volontairement par les particuliers sur les réseaux sociaux, soit grâce à la connivence des sociétés elles-mêmes telles que Facebook, Google, Microsoft, Apple, Skype (en ce sens le partenariat avec des organismes tels que NSA, FBI) soit par exploitation directe (possibilité de craquer l'accès aux données, surveillance des transactions financières par la NSA dénoncée par la presse Allemande, Der Spiegel).

A contrario, les services de police et de gendarmerie sont eux-mêmes tenus à une certaine transparence puisque les contre pouvoirs publics via des rapports traquent eux aussi les failles des services, énumèrent les différents fichiers et mettent à jour les dysfonctionnements existants et ce, sans complaisance. Notamment il y a une traçabilité des consultations de fichiers (au moins quantitative par service).

[33] La CNIL précise la liste des informations recueillies par les Google Cars : « de nombreuses données concernant des particuliers, identifiés ou identifiables, données de connexion à des sites web, mots de passe de messagerie, adresses de courrier électronique, échanges de courriels révélant notamment des informations sensibles sur l'orientation sexuelle ou la santé des personnes ». http://www.clubic.com/internet/univers-google/google-maps/actualite-405654-cnil-prononce-amende-100-000-google.html

La transparence exigée des services ne les conduit-elle pas à préférer mettre en œuvre les dispositions de la loi de 78 qui leur permet un régime dérogatoire plus opaque pour certains fichiers de police?

En effet, comme le rapellent D. Batho et J.A. Bénisti en 2009, « la loi du 6 janvier 1978 a prévu deux dispositions spécifiques pour les fichiers de police. En premier lieu, les demandes d'avis auprès de la CNIL pour la création de ces fichiers peuvent, dans certains cas, ne pas comporter certaines des mentions obligatoires pour les autres traitements de données. En second lieu, de manière exceptionnelle, certains actes réglementaires portant création de fichiers de police peuvent ne pas être publiés ».

L'article 29 de la loi prévoit que les demandes d'avis de création adressées à la CNIL concernant les fichiers de police doivent préciser l'identité et l'adresse du responsable du traitement, les caractéristiques, la finalité et la dénomination du traitement ainsi que la description générale de ses fonctions, le service chargé de sa mise en œuvre, le service auprès duquel s'exerce le droit d'accès, les catégories de personnes qui peuvent avoir accès aux informations enregistrées, les informations nominatives traitées, leur origine et leur durée de conservation ainsi que leur destinataire, les rapprochements et interconnexions, les dispositions de sécurité prises, et si le traitement est destiné à l'expédition d'informations nominatives à l'étranger.

Or l'article 30 dispose que « les demandes d'avis portant sur les traitements intéressant la sûrcté de l'État, la défense ou la sécurité publique peuvent ne pas comporter tous les éléments d'information énumérés ci-dessus », notamment les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ainsi que la durée de conservation des informations[34].

De même, le paragraphe III de l'article 26 de la loi informatique et libertés prévoit que : « Certains traitements mentionnés au I et au II peuvent être dispensés, par décret en Conseil d'État, de la publication de l'acte réglementaire qui les autorise ; pour ces traitements, est publié, en même temps que le décret autorisant la dispense de publication de l'acte, le sens de l'avis émis par la commission ».

[34] Le décret en Conseil d'État du 15 mai 2007, pris après avis de la CNIL, fixe la liste de ces traitements, qui peuvent ne pas comporter tous les éléments d'information généralement requis. Relèvent ainsi de la dérogation prévue à l'article 30 de la loi du 6 janvier 1978 :

- le décret portant création au profit de la direction centrale du renseignement intérieur d'un traitement automatisé de données à caractère personnel dénommé CRISTINA ;
- le décret portant application des dispositions de l'article 31 de la loi n° 78-17 du 6 janvier 1978 aux fichiers d'informations nominatives mis en œuvre par la direction générale de la sécurité extérieure ;
- le décret portant application des dispositions de l'article 31 de la loi n° 78-17 du 6 janvier 1978 aux fichiers de la direction de la protection et de la sécurité de la défense ;
- le décret portant application des dispositions de l'article 31 de la loi n° 78-17 du 6 janvier 1978 au fichier d'informations nominatives mis en œuvre par la direction du renseignement militaire ;
- l'arrêté relatif au traitement automatisé d'informations nominatives mis en œuvre par la direction de la protection et de la sécurité de la défense ;
- l'arrêté relatif au traitement automatisé d'informations nominatives « fichier de la DGSE » mis en œuvre par la direction générale de la sécurité extérieure ;
- l'arrêté relatif au traitement automatisé d'informations nominatives « fichier du personnel de la DGSE » mis en œuvre par la direction générale de la sécurité extérieure ;
- l'arrêté relatif au traitement automatisé d'informations nominatives de personnes étrangères mis en œuvre par la direction du renseignement militaire.

Du coté des particuliers, face à la traque possible de leurs données personnelles, une réflexion et une réaction s'organisent pour brouiller leur propre visibilité : les avatars et les fausses informations semblent des pistes sérieusement envisagées (« Faut-il instituer un droit au mensonge, à la désinformation, à la transparence réciproque, à la construction d'avatars disposant de tous les attributs d'une personne ? Faut-il considérer les données à caractère personnel comme un actif, un patrimoine négociable ? »)[35].

Delphine Batho et J. A. Bénisti en 2009 mentionnant le système anglais particulièrement poussé indiquaient : « un récent rapport de la Chambre des Lords, intitulé Surveillance : les citoyens et l'État, a estimé que l'accroissement des pratiques de surveillance, tant publiques que privées, représente l'un des changements les plus significatifs dans la vie de la nation depuis la fin de Deuxième Guerre mondiale ». Il y est ainsi relevé que « la généralisation de la surveillance, devenue massive et routinière, exerce une influence puissante sur la nature des relations entre l'État et les citoyens ».

Si la relation modifiée pousse à une attitude de défiance, la question qui se pose est celle-ci : n'y a-t-il pas un risque d'un trouble au deux sens du terme (perturbation et opacité) organisé en riposte ?

Cependant l'exploitation des données personnelles affichées par les individus volontairement n'est qu'une couche d'informations supplémentaire pour les fichiers du renseignement (qui sont eux-mêmes nimbés dans un certain flou dans l'optique de la sûreté/défense) face à la large base constituée par les fichiers judiciaires (comme le traitement des antécédents judiciaires, TAJ) ou plus purement administratifs (comme le fichier des passeports), lesquels doivent pouvoir être utilement exploitables, fiables et exemplaires dans un souci de légitimité et de confiance envers les particuliers. Ainsi la difficulté de ces fichiers de police tient en la différence de contenu de ceux-ci et le terme de fichier de police recouvre des démarches qui devraient être dissociées. La confusion des genres tient en ce que les forces de police et de gendarmerie établissent des fichiers dans une perspective de prévention, tant dans l'optique de la sûreté de l'État que dans la volonté de réduire la délinquance au sens large du terme au regard des multiples infractions énumérés par l'article 706-55 du code de procédure pénale.

Certes, il est impensable « que les forces de sécurité soient privées des nouvelles potentialités offertes par l'informatique », mais indispensable, « que des principes extrêmement clairs les encadrent et qu'un contrôle démocratique constant puisse s'exercer »... et « interdire aux services de police de vivre avec leur temps et d'utiliser les outils d'aujourd'hui pour traquer délinquants et criminels reviendrait à se tirer une balle dans le pied, alors qu'il appartient à l'État d'assurer la protection des personnes et des biens »[36]. Cette idée avait été également exprimée par Alain Bauer et Christophe Soullez : « Pourtant, pour protéger la population, et donc garantir les droits des individus à vivre en sécurité en retrouvant des criminels, il est

[35] Groupe de travail « informatique et libertés 2.0 », 26 mai 2008 http://archives.fing.org/identitesactives.net/index.html%3Fq=groupe-de-travail-informatique-et-libertes-20.html

[36] Batho D. et Bénisti J.-A., Rapport d'information déposé en application de l'article 145 du Règlement par la commission des lois constitutionnelles, de la législation et de l'administration générale de la République *sur les fichiers de police*, 24 mars 2009.

essentiel de conserver, retraiter et rapprocher des informations. La mobilité des personnes et des flux et l'exigence de la preuve qui fonde l'État de droit rendent nécessaire le recours à des informations nominatives. Les systèmes informatiques des services de sécurité doivent également s'adapter aux structures sociales, aux mutations technologiques mais également aux évolutions des groupes criminels ou terroristes qui sont aussi les premiers utilisateurs des nouvelles technologies »[37].

Incontournables, les fichiers informatiques de collecte, traitement et stockage de données font parties des métiers de police et de gendarmerie. Ils sont indiscutablement un élément fort du service public de la sécurité/ surveillance mais selon un régime qui se doit d'être suffisamment mature et abouti et qui devrait passer par une meilleure acception de la notion de fichier de police[38].

En l'occurrence, existent les indices d'un service public de la surveillance en voie de maturité, même si ce ne sont que les prémices.

B. Les indices d'un service public de la surveillance en voie de maturité

Les signes d'une amélioration dans le sens de la conciliation entre ordre et libertés sont perceptibles à la capacité de critique. En effet, les rapports parlementaires comme ceux de la CNIL témoignent d'une certaine bonne santé de la démocratie au moins dans son affichage. Reste qu'un affichage qui peine à être formalisé juridiquement rend de moins en moins crédible la portée de tels rapports. Une société qui n'a pas que l'apparence de la démocratie offre nécessairement le flanc à la critique.

1. Une mise en exergue sans concession des difficultés liées aux fichiers de police

Les rapports Batho et Bénisti comme ceux de la CNIL sont particulièrement riches d'enseignements et exposent en conscience la multiplicité des problèmes concrets posés par les fichiers de police. De même, Nicolas Sarkozy[39] dans sa lettre de mission à Alain Bauer décidait dès 2006 de l'objectif de créer un groupe de travail visant l'amélioration du contrôle et de l'organisation des fichiers de police et de gendarmerie afin d'éviter le maintien d'informations erronées ou dépassées, et de vouloir recenser les outils existants. Par ailleurs, les informations postées sur le web sont parfois édifiantes, même s'il faut être prudent sur leur contenu. Ainsi à propos du FNAEG, une proposition de transaction aurait été faite par les pouvoirs publics français pour inciter un faucheur d'OGM qui a refusé le prélèvement de ses empreintes génétiques, à renoncer au recours intenté devant la CEDH[40].

Sans chercher davantage la controverse, les rapports officiels sont déjà suffisamment sévères pour alimenter le progrès. Sont particulièrement dénoncés les points majeurs suivants et sur lesquels certaines avancées ont été réalisées.

---

[37] Bauer A. et Soullez C., *op. cit.*, Introduction, 2e éd., QSJ, PUF, 2011.

[38] Koubi G., *op.cit.*, Sécurité intérieure, les nouveaux défis, p. 243 : « aucune définition attestée ne peut être donnée du fichier de police ».

[39] Rapport missionné par Nicolas Sarkozy, ministre de l'Intérieur, *Les fichiers de police et de gendarmerie, comment améliorer leur contrôle et leur gestion ?* 2006, http://www.ladocumentation francaise.fr/var/storage/rapports-publics/064000885/0000.pdf

[40] Pour information et sous toute réserve : http://www.slate.fr/story/47639/adn-fichiers

1. Le Fichage est perfectible. En effet, les dysfonctionnements et les inexactitudes dans la gestion des fichiers portent préjudice aux citoyens comme aux utilisateurs.

Il est ainsi dénoncé comme :

- excessif (une peccadille devient un cas pendable, les mineurs insuffisamment protégés malgré des progrès encore insuffisants pour les deux parlementaires),
- erroné et ce durablement (problème du transfert des erreurs lors de la fusion des fichiers STIC et JUDEX en TAJ indiqué par la CNIL dans son rapport de juin 2013 qui exhorte à « anticiper les dysfonctionnements qui menacent d'ores et déjà le bon fonctionnement du projet d'un «nouveau système d'information lié à l'investigation» (NS2i) notamment caractérisé par l'interconnexion du nouveau fichier d'antécédents du ministère de l'intérieur (TAJ) avec celui du bureau d'ordre national du ministère de la Justice (CASSIOPEE) »).
- insuffisamment mis à jour (les procureurs lourdement vilipendés par la CNIL, bien que la LOPPSI de 2011 a étendu l'obligation de mise à jour des fichiers d'antécédents).
- touchant des données sensibles : la question de l'origine géographique dénoncée et partiellement traitée par le décret du 7 mai 2013 modifiant le décret du 16 octobre 2009 portant création d'un traitement de données à caractère personnel relatif à la prévention des atteintes à la sécurité publique et le décret du 29 mars 2011 portant création d'un traitement de données à caractère personnel relatif à la gestion de l'information et à la prévention des atteintes à la sécurité publique.

2. Le déficit démocratique concerne parfois le parlement. En 2009, les rapporteurs Batho et Bénisti sont consternés par le fait qu'avant cette date bien tardive au regard de l'ancienneté de la pratique, « jamais le Parlement jusqu'ici n'avait étudié l'ensemble de cette problématique complexe, afin de disposer d'une vision d'ensemble sur la nature et l'évolution des fichiers de police ». Un rôle insuffisant du parlement en ce qui concerne la création des fichiers est notamment dénoncé.

3. La consultation des fichiers : particulièrement nombreuses, élargies par circulaires malgré la mise à l'écart des polices municipales à leur grand regret.

4. Droit d'accès :

- La pugnacité nécessaire pour demander, parfois même à juste titre en raison d'une décision de justice ordonnant celui-ci, l'effacement des données personnelles montre le très fort déséquilibre des rapports entre les pouvoirs publics et les particuliers. L'acharnement des derniers à faire valoir leur droit contraste avec l'inertie des premiers. Les délais de procédure sont très brefs et fortement encadrés pour les personnes privées

et certaines améliorations restent encore énigmatiques telles que le « magistrat référent » des fichiers de police judiciaire[41].

Par ailleurs pour faire vérifier cet effacement, la démarche est loin d'être aisée.

5. Un grand nombre de fichiers : faut-il un répertoire de fichier ? Cependant l'analyse n'est pas forcément négative et les députés D. Batho et J.-A. Bénisti en 2009, estimaient que le nombre était paradoxalement un gage au profit des libertés : « Les fichiers de police peuvent d'une certaine manière être d'autant plus nombreux qu'ils répondent à des besoins précis et ciblés et que leurs finalités distinctes sont très encadrées. De fait, leur multitude et leur segmentation mêmes témoignent de l'inexistence d'une forme de « méta fichier » tentaculaire. Le refus d'un fichage de police massif et généralisé ou d'une interconnexion des fichiers suppose nécessairement l'existence d'un certain nombre de fichiers aux finalités spécifiquement définies ».

2. L'obligation du politique : un aboutissement normatif d'envergure

Il est temps d'avoir une réelle doctrine, une stratégie des fichiers compatible avec les droits fondamentaux de manière à « accroître la sécurité tout en renforçant la protection de la vie privée et des données à caractère personnel » comme le soulignait déjà Franco Frattini[42]. L'idée d'une évolution convergente des intérêts s'impose et se trouve communément admise. Mais de l'idée d'une norme à la norme elle-même, le chemin est long.

Fin 2011, il était alarmant de lire sous la plume des députés que la révolution n'a pas eu lieu quant au cadre juridique des fichiers. En 2013, les progrès sont maigres malgré des décrets qui s'inspirent partiellement des enseignements de la CNIL ou des rapporteurs parlementaires. De citer alors, non sans une once de pessimisme, Edgar Faure et cette fois, intégralement : « L'immobilisme est en marche et rien ne peut l'arrêter ».

[41] Pour notre part, ce n'est qu'à la lecture du rapport de la CNIL en date de juin 2013 que nous avons pu apprendre et uniquement en note de bas de page (page 5, note 3) , qui est ce magistrat référent : ce magistrat, actuellement M. Paul Michel, procureur général près la Cour d'appel de Grenoble, est chargé de suivre la mise en œuvre et la mise à jour des fichiers d'antécédents (art. 230-9 CPP).

[42] Frattini F., *op. cit.*, 20 novembre 2007, http://europa.eu/rapid/press-release_IP-07-1726_fr.htm?locale=FR