INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE

INHESJ

TRAVAUX DES AUDITEURS

25e Session nationale « Sécurité et Justice » 2013-2014
Groupe de diagnostic stratégique (GDS) n°6

FICHIERS DE POLICE ET LIBERTÉS :
DES ENJEUX NATIONAUX, UNE NOUVELLE DONNE INTERNATIONALE

JANVIER 2015

Les Membres du Groupe de Diagnostic Stratégique ayant contribué à l'élaboration et à la validation du présent document sont :

Les **AUDITEURS** :

MINOT Corinne	Ministère de l'Intérieur
HAMON Bruno	MIRCA Sarl
PLOIX de ROTROU Virginie	BNP PARIBAS-CARDIF
BECUYWE Laurent	Ministère de la Justice
DECOUT-PAOLINI Rémi	Conseil d'État
GIAMARCHI Jean-Etienne	Avocat
JORAM Frédéric	Ministère de l'Intérieur
JOUSSEAUME Stéphane	Ministère de la Santé
LAURENT Frédéric	Ministère de la Défense
MARCELLIN Sabine	CREDIT AGRICOLE CIB
MAYET Nathalie	EPADESA
MINIOT Agnès	Ministère de l'Intérieur
NAZAT Dominique	Chirurgien-dentiste spécialiste en Orthopédie Dento-Faciale
PASCAL Benoît	Ministère de l'Économie et des Finances
ROUBA Abdelkader	Ministère de la Défense nationale – Algérie

Directeur de la publication M. Cyrille SCHOTT, directeur de l'INHESJ

AVANT-PROPOS

La question des fichiers de police et de leur acceptabilité par les opinions publiques qui a été proposée au GDS 6 s'est révélée éminemment intéressante, mais aussi complexe à traiter.

Parce qu'elle est étroitement liée à la problématique de la protection des données personnelles, elle touche, à des degrés divers, un large spectre de sujets spécifiques et souvent techniques. De manière non exhaustive, on peut citer évidemment celui de la sécurité et de la coopération policière nationale et internationale, mais aussi celui de l'informatique et du monde numérique en général, celui des nouvelles technologies, telles que la géo-localisation et la biométrie, le problème de l'utilisation des données personnelles dans le cadre des pratiques commerciales et de la banalisation des réseaux sociaux et, plus généralement, la question fondamentale du droit des individus, de l'exercice des libertés et du respect de la vie privée.

Pour la même raison, elle fait l'objet d'une attention permanente des médias, notamment depuis l'affaire PRISM et les révélations relatives à la captation massive de données par la NSA [1]. De ce fait, elle connaît un développement constant qui se concrétise par une activité journalistique et institutionnelle continue, tant au niveau national qu'international.

Ces spécificités ont généré un certain nombre de difficultés à surmonter et d'écueils à éviter.

En raison de la variété des questions à aborder, de leur cloisonnement relatif et des connaissances spécialisées (techniques et/ou juridiques) dont il faut disposer pour les étudier sérieusement, la présentation exhaustive de la problématique des fichiers de police constitue une gageure. De ce fait, le choix a été fait d'approfondir les points les plus importants, et d'évoquer les thèmes connexes de manière lapidaire, en s'appuyant sur un plan détaillé plus que sur un travail rédigé.

Le sujet est, par ailleurs, particulièrement sensible et il a été largement défriché en amont. Tout ou presque a été écrit sur la question, souvent par d'éminents contributeurs, de sorte que la marge d'innovation du GDS s'est révélée relativement restreinte. Le foisonnement des études, analyses et propositions de toutes natures, parfois non dénuées d'esprit polémique, a contraint le groupe à opérer un important travail de recherche et un tri drastique de la documentation disponible en privilégiant les contributions transverses et prospectives. En raison de son impact sur l'exercice des libertés publiques et privées et de l'attention que lui porte le corps social, la question des fichiers de police et, plus globalement, celle de la protection des

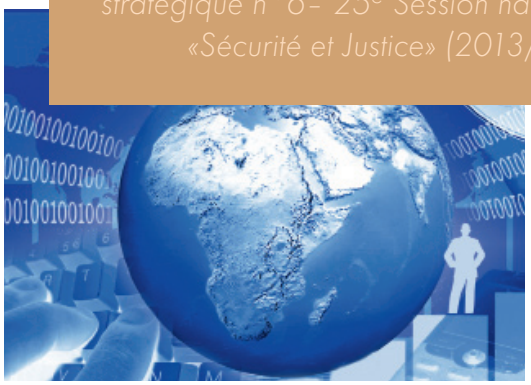
(1) NSA : *National Security Agency*.

données personnelles, ont acquis une dimension éminemment politique. Le choix de la documentation a donc été également sous-tendu par la nécessité de se garder de tout parti pris en s'attachant à rester neutre et objectif en toutes circonstances.

Au total, l'étude de ce sujet fut particulièrement enrichissante, en raison, notamment, de la diversité des pistes à explorer. Le GDS en a tiré la conviction que la perception sociétale d'un sujet aussi sensible reste directement liée au sentiment d'insécurité, lequel n'est pas obligatoirement réel. Dans ce contexte, c'est bien le droit, allié à des technologies parfois arides, qui peut rendre plus acceptables des solutions *a priori* trop audacieuses, en délimitant leur cadre juridique et en permettant de réunir les conditions techniques de leur contrôle.

FICHIERS DE POLICE ET LIBERTÉS : des enjeux nationaux, une nouvelle donne internationale

Rapport du Groupe de diagnostic stratégique n°6 - 25e Session nationale «Sécurité et Justice» (2013/2014)



Sommaire

INTRODUCTION

Au cours de la dernière décennie, la lutte contre le terrorisme et contre la criminalité est devenue plus âpre et s'est globalisée. Parallèlement, le développement sans précédent des nouvelles technologies de la communication a rendu possible l'interopérabilité de tous les vecteurs et la circulation instantanée des données, estompant non seulement les frontières entre les nations, mais aussi entre domaine public et domaine privé, entre stockage physique et stockage dématérialisé des informations.

Du même coup, les données personnelles sont devenues le « carburant du numérique »[2] et les marqueurs de l'individu, y compris dans sa vie sociale.

En France, la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (LIL) encadre, sous le contrôle vigilant de la CNIL[3], les traitements de données à caractère personnel qui concourent, notamment, à « l'offre de sécurité ».

Amendée en 1991 puis en 2004, complétée par le décret d'application n°2005-1309 du 20 octobre 2005, ses conditions de mise en œuvre dans le domaine des fichiers de police ont été examinées en 2006, puis en 2008 par le groupe de contrôle des fichiers de police et de gendarmerie, dit « groupe BAUER », mandaté par le ministre de l'intérieur, de l'outre-mer et des collectivités territoriales de l'époque, suite au scandale médiatique déclenché par le projet EDVIGE[4]. Son dernier rapport, remis le 11 décembre 2008[5] (cité ci-après sous le vocable « rapport BAUER ») continue de faire autorité en la matière.

Le 7 mai 2009, les députés Delphine BATHO et Jacques-Alain BENISTI, déjà auteurs d'un rapport d'information sur les fichiers de police[6] (ci-après nommé « RI 2009 »), ont déposé la proposition de loi n°1659[7], visant à modifier la loi « informatique et libertés ». Ce projet a été rejeté le 24 novembre 2009 par la majorité de l'Assemblée nationale.

Le 21 décembre 2011, les deux parlementaires déposent un nouveau rapport d'information sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police[8] (ci-après cité sous le terme « RI 2011 »). Si le constat est globalement plus optimiste qu'en 2009, les rédacteurs déplorent notamment le *statu quo* législatif en matière de fichiers et l'insuffisance des progrès en matière de protection des droits individuels. *A contrario*, ils saluent un certain nombre d'avancées portant sur les relations entre le ministère de l'intérieur et la CNIL, le développement d'une culture « informatique et libertés » dans l'utilisation des fichiers de police ainsi que la modernisation de la gouvernance et la rénovation réussie de fichiers majeurs.

Un tel état des lieux ne contribue évidemment pas à atténuer l'opposition culturelle qui existe, en France, entre fichiers de police et libertés publiques.

Alimentée par la médiatisation de la création de nouveaux traitements automatisés de données personnelles détenus par l'État et jugés potentiellement « liberticides », ainsi que par la révélation sporadique d'atteintes bien réelles à la vie privée résultant d'une utilisation frauduleuse des fichiers, elle se traduit par une perception péjorative

(2) Interview de Mme Isabelle FALQUE-PIERROTIN, présidente de la CNIL pour *Le Monde*, propos recueillis par Laure BELOT, le 21 mai 2012.

(3) CNIL : Commission nationale de l'informatique et des libertés.

(4) Exploitation documentaire et valorisation de l'information générale, créé par décret n°2008-632 du 27 juin 2008 abrogé le 20 novembre 2008.

(5) Rapport du groupe de travail sur les fichiers de police présidé par M. Alain BAUER (20 mars 2008). Un précédent état des lieux avait été réalisé sous la direction de M. Alain BAUER en décembre 2006 à la demande M. Nicolas SARKOZY, alors ministre de l'Intérieur et de l'aménagement du territoire.

(6) Rapport d'information sur les fichiers de police de Mme Delphine BATHO et M. Jacques Alain BENISTI (24 mars 2009).

(7) Proposition de loi sur les fichiers de police présentée par Mme Delphine BATHO et M. Jacques Alain BENISTI le 7 mai 2009.

(8) Rapport d'information sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police de Mme Delphine BATHO et M. Jacques Alain BENISTI (21 décembre 2011).

du fichage, souvent fantasmatique et parfois erronée qui nourrit à la fois des craintes d'atteintes aux libertés publiques et des attentes sécuritaires fortes, telles que l'interpellation immédiate des criminels dangereux ou la prévention infaillible des actes criminels majeurs. En fonction des événements, l'acceptabilité des fichiers par le corps social oscille au gré de l'une ou l'autre de ces tendances.

Cet état d'esprit détone par rapport à l'insouciance avec laquelle nos concitoyens confient des données personnelles sur Internet par le truchement de réseaux sociaux, de moteurs de recherche et de sites commerciaux contrôlés par des entreprises étrangères. C'est pourquoi les sociétés européennes n'ont pris que tardivement conscience que la captation et l'exploitation des données personnelles constituent désormais un enjeu commercial et sécuritaire majeur.

Dans un contexte international et globalisé de concurrence économique et de lutte contre le terrorisme et la criminalité organisée, la notion de données prévaut désormais sur la logique de fichier, et les mêmes flux intéressent non seulement les grandes entreprises d'Internet mais aussi les forces de sécurité et les services de renseignement des États les plus développés. Le concept même de « donnée sensible » devient évolutif au gré des profondes modifications de nos pratiques sociales et commerciales.

Les instances de l'UE[9] ont bien compris que la vision « continentale » européenne de la protection des données, partiellement inspirée du droit français, s'inscrivant dans le cadre de territoires et de champs de compétences bien identifiés, peut sembler inadaptée pour contrôler des flux transfrontaliers dans le contexte du monde numérique actuel[10] et constitue, de ce fait, un facteur de vulnérabilité face à d'autres États qui privilégient davantage la sécurité collective par rapport à la protection des libertés individuelles.

(9) UE : Union européenne.

(10) Alex TÜRK *in* « Fichage et listing, quelles garanties pour les individus ? » *Cultures & conflits* n°76, hiver 2009, page 115 et suivantes.

Les consultations et les négociations préalables à l'adoption d'un nouveau règlement devant concilier la simplification et l'harmonisation de la protection des données avec les valeurs humanistes européennes ont ainsi débuté laborieusement en 2010 pour déboucher sur une proposition concrète en janvier 2012.

L'affaire PRISM et les toutes récentes révélations d'espionnage électronique opéré par la NSA ont mis en lumière l'absence de l'Europe dans un monde numérique, désormais dominé par les États-Unis (pour le *software*) et la Chine (pour le *hardware*) et ont parallèlement stimulé l'émergence d'un consensus qui n'était pas acquis d'avance.

En dépit de cet essor prometteur, les négociations semblent actuellement marquer le pas, de sorte que l'adoption d'un nouveau règlement européen sur la protection des données personnelles n'est toujours pas envisageable dans un avenir proche.

La recherche du nouvel équilibre entre préservation des droits individuels et accroissement de la sécurité collective qui rendrait plus acceptables les fichiers de police dans notre société doit donc être intégrée dans une réflexion plus large portant sur les voies d'amélioration de notre dispositif, sur son adaptabilité aux technologies émergentes et à l'évolution de la menace et sur l'impact des besoins pressants de coopération policière internationale avec des États extra-européens.

Dans un tel contexte, la gestion de nos traitements automatisés de sécurité et les modalités régissant l'exercice des droits conférés par la loi « informatique et libertés » devront nécessairement faire l'objet d'adaptations car ils ne sauraient offrir un niveau de protection inférieur à celui qui sera fixé par les instances de l'UE lorsque les règles communes de protection des données personnelles auront été finalisées.

LES FICHIERS AU SERVICE DES POLITIQUES DE SÉCURITÉ

Des outils au service de l'État dans sa mission régalienne de protection de la société

Définition d'un fichier de police

L'expression « fichier de police » correspond aux traitements de données à caractère personnel [11] relevant de la définition de l'article 26 de la loi du 6 janvier 1978, c'est-à-dire mis en œuvre pour le compte de l'État et ayant pour finalité :

- la sûreté de l'État, la défense ou la sécurité publique ;
- ou la prévention, la recherche, la constatation ou la poursuite des infractions pénales.

Bien que la loi ne leur donne pas tout à fait le même sens, les termes « fichier » et « traitement de données » peuvent être utilisés indifféremment.

Les fichiers de police obéissent à un régime juridique particulier. Ils doivent être autorisés par un acte réglementaire pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés. Il faut observer que les traitements utilisés par les services de sécurité ne relèvent pas tous des fichiers dits de police.

Ainsi les services de police et de gendarmerie ont-ils fréquemment recours pour l'accomplissement de leurs missions à des fichiers administratifs recensant par exemple les permis de conduire ou les passeports, lesquels se distinguent des fichiers de police par leur finalité.

Par ailleurs, s'ils sont mis en œuvre pour le compte de l'État, les fichiers de police ne sont pas nécessairement gérés et utilisés par les services du ministère de l'intérieur. Des traitements répondant à la définition de l'article 26 de la loi du 6 janvier 1978 peuvent en effet être administrés par d'autres services de sécurité (ex : douane) ou d'autres ministères (ex : le FIJAIS [12] par le ministère de la Justice).

(11) Au sens de l'article 2 de la loi de 1978, qui définit un traitement de données à caractère personnel comme « toute opération ou tout ensemble d'opérations portant sur de telles données à caractère personnel, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».

(12) FIchier Judiciaire national automatisé des Auteurs d'Infractions Sexuelles.

Les catégories de fichiers

Le rapport BAUER distingue huit catégories de fichiers :

- Les applications bureautiques telles que la BB 2000 [13] de la Gendarmerie nationale, ou l'application internet de pré-plainte en ligne;
- Les fichiers administratifs tels AGRIPPA [14] ou le FNIS [15];
- Les fichiers de police judiciaire : par exemple FOVES [16], LAPI [17];
- Les fichiers de renseignement : par exemple la BDSP [18] de la Gendarmerie nationale, PASP [19] pour la Police nationale ;
- Les fichiers d'antécédents judiciaires tels que le STIC [20] et le JUDEX [21], désormais fusionnés au sein du TAJ [22];
- Les fichiers d'identification judiciaire : FIJAIS, FPR [23], etc...
- Les systèmes de traitement du renseignement judiciaire tels que SALVAC [24] et ANACRIM [25];
- Les fichiers d'identification administratives (ex : le FSDRF [26], FNPC [27]).

(13) Bureautique Brigade 2000, formule actualisée et centralisée sous le nouveau titre Pulsar.
(14) Application de Gestion du Répertoire Informatisé des Propriétaires et Possesseurs d'Armes.
(15) Fichier National des Interdits de Stade.
(16) Fichier des Objets et VEhicules Signalés.
(17) Lecture Automatisée des Plaques d'Immatriculation.
(18) Base de Données de Sécurité Publique (ex-Athén@) qui donne notamment accès au GIPASP (« Gestion de l'intervention et prévention des atteintes à la sécurité publique »).
(19) Prévention des Atteintes à la Sécurité Publique.
(20) Système de Traitement des Infractions Constatées.
(21) Système JUdiciaire de Documentation et d'EXploitation.
(22) Traitement d'Antécédents Judiciaires.
(23) Fichier des Personnes Recherchées.
(24) Système d'Analyse des Liens de la Violence Associée au Crime.
(25) ANAlyse CRIMinelle.
(26) Fichier de Suivi des titres de circulation Délivrés aux personnes sans Domicile ni Résidence Fixe.
(27) Fichier National des Permis de Conduire.
(28) La France est le troisième pays à se doter d'une telle loi après l'Allemagne en 1971 et la Suède en 1973.

Un dispositif étroitement contrôlé par une autorité indépendante

La France précurseur en la matière

L'adoption précoce, dès 1978, d'une loi encadrant la création et l'usage des fichiers (loi « informatique et libertés » du 6 janvier 1978) a permis à la France de se hisser parmi les États européens les plus vertueux dans la lutte contre les atteintes aux libertés individuelles pouvant résulter de l'utilisation de l'outil informatique. Par amendements successifs, la loi s'est adaptée à l'évolution du monde numérique, conférant à la France l'un des régimes juridiques les plus protecteurs dans le domaine.

Le rôle et les missions actuelles de la CNIL

Le législateur français a choisi en 1978 de confier à une autorité administrative indépendante la mission de contrôle des traitements de données à caractère personnel. Certains États européens ont opté pour un contrôle parlementaire. Le parlement français s'est prononcé à plusieurs reprises sur la création de catégories de bases de données. Les fichiers de police ont également fait l'objet de plusieurs rapports parlementaires [29].

(29) Rapports de Mme Delphine BATHO et M. Jacques Alain BENISTI.

Définies par la loi du 6 janvier 1978 relative à l'informatique et aux libertés, les missions de la CNIL sont multiples. S'agissant des fichiers de police, cette autorité administrative indépendante est chargée d'émettre un avis préalable à l'autorisation par un acte réglementaire. Cet avis est publié.

Elle exerce une mission de contrôle, qui peut donner lieu à des rapports rendus publics. Celle-ci est, depuis peu, complétée par l'action de l'autorité de contrôle des fichiers judiciaires prévue par le code pénal.

La CNIL exerce en outre le droit d'accès des particuliers aux données les concernant, dans le cadre de la procédure dite du droit d'accès indirect, couramment utilisée s'agissant des fichiers de police. Ainsi, en 2012, le nombre de droits d'accès indirects exercés s'est élevé à 3 682, soit 75 % de plus qu'en 2011.

La CNIL accompagne enfin les évolutions technologiques des traitements de données.

Le développement d'une culture informatique et libertés au sein des services de l'État [30]

(30) C'est la « démarche qualité » évoquée dans la recommandation n°4 du « rapport BAUER ».

Conscients des enjeux de protection des libertés individuelles et de pérennisation de leurs outils de travail et parfois soumis à la critique publique, les services de l'État utilisateurs de fichiers de police ont entrepris le développement d'une culture « informatique et libertés » en leur sein.

Cette politique se traduit par plusieurs démarches concrètes :

La création de nouvelles structures de gouvernance et la rénovation réussie de nombreux fichiers centraux [31]

(31) Voir RI 2011, quatrième partie, paragraphes A et B.

- La création du service des technologies et des systèmes d'information de la sécurité intérieure (ST(SI2)) ;
- Les fichiers TAJ, EASP [32], PASP et BDSP.

(32) Fichier des enquêtes administratives liées à la sécurité publique.

Le recensement et la régularisation des fichiers non déclarés

(33) RI 2011, 1ère partie, paragraphe C-1.

(34) Rapport BAUER, recommandation n°6 et RI 2011 première partie, paragraphe C-1.

(35) Recommandation n°3 du rapport BAUER, RI 2009 titre VI-B et RI 2011 1ère partie, paragraphe C-1.

(36) Fichier Alphabétique de Renseignement détenu par la Gendarmerie nationale.

- **La régularisation de nombreux fichiers centraux**, *a posteriori* et en amont [33] ;
- **La régularisation des fichiers locaux** par le biais de nombreux actes cadres [34] ;
- **La destruction des traitements inutiles**, non conformes ou obsolètes [35] : le cas du FAR [36].

Une amélioration de la fiabilité dans l'alimentation des fichiers :

- **La formation des utilisateurs** et des agents chargés de l'alimentation des fichiers[37], réseau des CIL[38] ou des RIL[39] (*voir la recommandation n°5 du rapport BAUER et l'exemple de la gendarmerie*), codes de déontologie spécifiques ;
- L'existence d'un **contrôle qualité** dans l'enregistrement des données ;
- Le respect de la proportionnalité des données recueillies : l'exemple du SILCF[40] utilisé par la douane française qui limite les données recueillies aux seuls renseignements douaniers.
- Une **mise à jour des données améliorée** : le fichier CASSIOPEE[41] du ministère de la Justice et son interconnexion au TAJ, la purge automatique du système d'information ROC de la direction des douanes.

(37) Recommandations n°15 et 16 du rapport BAUER et voir aussi 3e partie, paragraphes A et B du RI 2011.

(38) Correspondants Informatique et Libertés.

(39) Référents Informatique et Libertés.

(40) Système d'Information de Lutte contre la Fraude.

(41) Chaine Applicative Supportant le Système d'Information Oriente Procédure Pénale et Enfants, voir aussi 3e partie paragraphe B-2 du RI 2011.

Un meilleur contrôle des utilisateurs

- **L'avantage du contrôle pour les forces de sécurité** : légitimité de leur action et fiabilité des procédures ;
- L**es conditions d'habilitation** et la gestion des droits d'accès[42] (*voir le RDA[43] de la Gendarmerie nationale et celui de la douane pour la base de données ROC[44]*) ;
- **L'impératif de traçage et de contrôle des consultations**, la capacité à déceler les utilisations anormales[45] (*exemple : le module de contrôle interne de la Gendarmerie nationale*) ;
- Le rôle des organes d'inspection internes[46] (*exemple : le BCEF[47] au sein de la Gendarmerie nationale et de l'IGPN au sein de la Police nationale*).

(42) Recommandations n°9 et 10 du rapport BAUER.

(43) Référentiel des Droits d'Accès adossé au logiciel de gestion des ressources humaines AGORA.

(44) Recherches Orientées Contrôles.

(45) Recommandation n°8 du rapport BAUER et propositions n°45 et 46 du RI 2009.

(46) Recommandations n°11 et 12 du rapport BAUER et 3e partie paragraphe C du RI 2011.

(47) Bureau du Contrôle et de l'Évaluation des Fichiers de l'IGGN.

La création de nouveaux fichiers plus strictement encadrée

Le ministère de l'Intérieur a créé en 2006 puis pérennisé par arrêté du 20 octobre 2009 le groupe de travail sur l'amélioration du fonctionnement et du contrôle des fichiers de police.

Composé de représentants des différentes administrations concernées, de syndicats, d'avocats, de journalistes, d'associations et d'autorités de contrôle (CNIL, Défenseur des droits), le groupe est compétent pour l'examen des projets de création ou de modification des fichiers de la police et de la gendarmerie.

Les avis du groupe de travail ne sont pas juridiquement contraignants. Selon M. DEBOVE, qui en assure actuellement la présidence, il agit davantage en « éclaireur » et en « démineur » par le biais des échanges et discussions qui sont menés en son sein. Il s'érige donc véritablement en outil de vigilance, au service du ministère de l'Intérieur. C'est d'ailleurs ainsi que la CNIL envisage les travaux de ce groupe.

Cette politique des services de l'État a permis une amélioration sensible du dialogue avec la CNIL. Si celle-ci souligne les progrès importants restant encore à accomplir[48], elle reconnaît publiquement les progrès réalisés par la police et la gendarmerie au cours des dernières années. Surtout, la CNIL se montre favorable à des évolutions répondant au besoin des services de l'État, comme par exemple la création, selon des modalités à définir, d'un régime juridique dérogatoire permettant d'expérimenter de nouveaux traitements de données avant que ceux-ci aient pu être autorisés par un texte réglementaire.

(48) *Cf.* par exemple le rapport de contrôle de la CNIL sur les traitements d'antécédents judiciaires rendu public en juin 2013.

Un enjeu de sécurité s'inscrivant dans un cadre européen et international

État de la coopération européenne et internationale en matière d'échange d'informations de sécurité

Présentation des bases de données européennes en matière de sécurité

- SIS[49] et son évolution vers SIS II, le VIS[50], EURODAC[51]: cadre légal et réglementaire européen en vigueur, modalités du contrôle (*ACC, rôle des autorités de contrôle nationales*);
- La proposition de règlement du Parlement européen et du Conseil COM(2009)93 du 24 juin 2009 puis COM(2010)93[52] du 19 mars 2010 visant à confier la gestion opérationnelle de SIS II, VIS et EURODAC à une même agence.

(49) Système d'Information Schengen.

(50) Visa Information System: système d'échange de données sur les visas entre les États Schengen.

(51) EURODAC: base de données adossée à un système automatisé de reconnaissance d'empreintes digitales concernant les étrangers entrés illégalement dans l'un des États Schengen ou des États associés.

(52) Proposition de règlement portant création d'une agence pour la gestion opérationnelle des systèmes d'information à grande échelle dans le domaine de la liberté, de la sécurié et de la justice.

L'accès aux bases de données européennes par des pays tiers: les modalités de la participation d'États et organisations tiers aux fichiers SIS, VIS et EURODAC

EUROPOL

- **Une montée en puissance progressive contrebalancée par un contrôle plus étroit de l'agence**

La Convention EUROPOL de 1995 définit l'unité de coopération policière comme une structure duale comprenant d'une part, un service chargé d'analyser et de produire des bases de données (composé de personnes engagées directement par Europol, il traite une grande quantité d'informations sensibles concernant les individus) et, d'autre part, un service d'officiers de liaison qui facilite les coopérations bilatérales et/ou multilatérales entre les États membres.

Europol a connu de profonds changements du fait de l'adoption en 2000, 2002 et 2003 de protocoles successifs qui ont modifié la Convention de 1995 qui l'avait créé. Il a fallu en moyenne plus de cinq ans pour que ces protocoles soient ratifiés par l'ensemble des pays membres.

En janvier 2006, la présidence autrichienne a ouvert un débat sur l'avenir d'Europol. Ce débat s'est notamment orienté vers une optimisation de son fonctionnement, *via* la mise en place d'une *corporate governance* et le développement de ses capacités opérationnelles.

Aux termes de négociations diplomatiques intenses entre les États membres, il a également été décidé qu'Europol deviendrait une agence de l'Union européenne à partir du 1er janvier 2010. Cette montée en puissance de l'unité policière s'est accompagnée d'un certain nombre de critiques portant, notamment, sur l'importance donnée à l'analyse au détriment de la coopération pratique et sur la question de « l'interopérabilité » des bases de données telles que SIS II, les bases de données Europol et le VIS.

Dans ce contexte, le contrôle de ces supports techniques, ainsi que la conformité juridique et constitutionnelle des accords et cadres institutionnels qui les sous-tendent, notamment vis-à-vis du respect des libertés publiques, constituent l'enjeu principal du développement de l'unité policière.

Le 27 mars 2013, la commission européenne a élaboré une proposition de nouveau règlement relatif à Europol (COM 2013/173) visant, notamment, à accroître son efficacité dans ses activités de collecte et d'analyse d'informations et d'en faire véritablement le centre névralgique de l'échange et de l'analyse des informations sur la grande criminalité. Ce faisant, le règlement accroît et précise l'obligation imposée aux États membres de fournir des données à Europol (il est ainsi prévu d'établir un rapport annuel sur la quantité et la qualité des données fournies par les États membres).

En parallèle, la proposition accroît la responsabilité d'Europol à l'égard du Parlement européen et des parlements nationaux. Elle renforce la protection des données à caractère personnel et les droits des personnes concernées et confie le contrôle externe de la protection des données au CEPD[53].

(53) Contrôleur Européen de la Protection des Données.

Le Parlement européen, qui a déjà obtenu de nouveaux pouvoirs à l'égard de cette agence de l'UE, intervient directement dans la direction de ses activités. Quant aux parlements nationaux, ils ont jusqu'à présent exercé une surveillance essentiellement indirecte, par le biais des représentants des États membres au sein du conseil d'administration d'Europol.

Dans cette logique, la commission des libertés civiles propose de créer un groupe de contrôle parlementaire conjoint, composé de députés européens et nationaux, pour surveiller les activités d'Europol.

De hauts fonctionnaires de l'agence, des représentants de la Commission et le CEPD seraient tenus de se présenter devant le groupe à sa demande, afin de débattre des opérations d'Europol et du respect des droits fondamentaux, en particulier de la protection des données personnelles.

Les rapports d'activité annuels, les programmes de travail et les évaluations d'Europol devraient également être présentés aux députés européens et nationaux, qui doivent avoir accès à tous les documents pertinents, notamment les informations classées.

– **Rôle de l'Autorité de Contrôle Commune (ACC)** :

Composée de représentants des autorités de contrôle nationales (dont la Commission de la protection de la vie privée), l'ACC est chargée de surveiller l'activité d'Europol afin de s'assurer que le stockage, le traitement et l'utilisation des données dont disposent les services d'Europol ne portent pas atteinte aux droits des personnes.

Elle contrôle en outre la licéité de la transmission des données qui ont pour origine Europol, et s'acquitte de cette tâche en effectuant des inspections au sein de l'agence.

L'ACC détermine si Europol observe les principes de la protection des données dans un certain nombre de domaines spécifiques. Il s'agit essentiellement : de l'examen et du commentaire de l'ouverture de fichiers d'analyse spécifiques, du contrôle des autorisations de transmission de données provenant d'Europol, de l'examen des questions concernant la mise en œuvre et l'interprétation de la convention Europol, de l'analyse des règles régissant la transmission de données à caractère personnel par Europol à des organes tiers et des États non membres, et de l'élaboration de solutions communes aux problèmes existants.

L'ACC est également garante du droit d'information des individus et, notamment, de la gestion des recours contentieux exercés par les personnes qui ont sollicité l'accès à des informations les concernant mais qui ne sont pas satisfaites de la suite donnée par Europol.

– **La coopération d'Europol avec les États et organisations tiers**

Europol est autorisé à conclure des accords de coopération avec des pays tiers et des organisations internationales, y compris Interpol.

La décision 2009/935/JAI du 30 novembre 2009 du Conseil européen établit, dans son annexe 1, la liste des États et organisations tiers avec lesquels Europol est autorisé à conclure ces accords. C'est actuellement au Conseil qu'il revint d'établir la liste de ces États et organisations. L'article premier de la décision dispose que ces accords permettent l'échange de données personnelles, sauf si le conseil d'administration en décide autrement.

Sous le contrôle de l'ACC, l'agence est également chargée de vérifier le caractère proportionné et nécessaire des demandes américaines formulées dans le cadre du TFTP[54]. Europol peut ainsi approuver ou refuser le transfert de données SWIFT[55] vers les États-Unis. TFTP et SWIFT sont évoqués plus complètement au paragraphe 2.3.1 ci-dessous.

(54) Terrorist Finance Tracking Program.

(55) Society for Worldwide Interbank.

INTERPOL[56]

(56) International Police ou Organisation internationale de police criminelle (OIPC), créée le 7 septembre 1923.

L'échange et le traitement d'informations policières à caractère personnel, telles que les noms et les empreintes digitales ou les profils ADN (bientôt, les empreintes faciales), s'opèrent sur une base volontaire entre les 190 pays membres d'Interpol et constituent la pierre angulaire de l'activité de l'Organisation dans la lutte contre la criminalité internationale.

Il est donc essentiel de maintenir un climat de confiance entre les pays membres pour encourager une participation constante, effective et la plus large possible au développement de la coopération policière internationale qui constitue la mission principale d'Interpol.

Cet échange d'informations s'effectue dans le cadre des lois en vigueur dans les différents pays et dans l'esprit de la Déclaration universelle des Droits de l'Homme (*Article 2 du règlement d'Interpol sur le traitement des données et l'article 2 du Statut d'Interpol*).

- **Le règlement relatif au contrôle des informations et à l'accès aux fichiers d'Interpol**

Adopté par l'Assemblée générale de l'Organisation dans sa résolution AG-2011-RES-07, il est entré en vigueur le 1er juillet 2012.

Il organise le contrôle indépendant des fichiers détenus par Interpol, établit la commission du contrôle des fichiers et détermine également les conditions dans lesquelles une personne peut avoir accès aux fichiers de l'Organisation.

Il marque ainsi une étape importante, dans la mesure où le dispositif réglementaire se trouve renforcé et plus cohérent tout en permettant à Interpol de conserver une position dominante en matière de respect des normes relatives à la protection des données personnelles.

- **La Commission de contrôle des fichiers (CCF) d'Interpol**

La création de la CCF résulte initialement d'un problème de contrôle des fichiers qu'il importe de rappeler car il illustre parfaitement les enjeux de l'échange d'informations entre États ne partageant pas la même conception de la protection des données personnelles. Interpol s'opposait en effet à La France qui souhaitait que sa loi « informatique et libertés » s'applique aux données nominatives détenues par l'Organisation, ce qui lui conférait un droit d'accès à ces données exercé par le biais de la CNIL.

Interpol lui opposait que les informations dont elle est dépositaire ne sont pas sa propriété, mais celle des pays membres dont elles proviennent et que cette mesure pouvait porter atteinte à la coopération policière internationale en dissuadant certains États de communiquer des informations qui risquaient d'être divulguées à des organismes français.

La signature, le 3 novembre 1982, d'un nouvel Accord de siège entre la République française et Interpol, entré en vigueur le 14 février 1984, auquel est annexé un Échange de lettres, a permis de constituer la base de la mise en place du système de contrôle des fichiers d'Interpol en instaurant la CCF, organe collégial de contrôle indépendant (article 36 du Statut).

La CCF contrôle l'application des règles adoptées par Interpol en matière de protection des données à caractère personnel et s'assure que les opérations de traitement de ces données (notamment les projets de création de nouveaux fichiers ou de nouveaux modes de diffusion d'information à caractère personnel) ne portent pas atteinte aux droits fondamentaux des individus.

La Commission conseille l'Organisation pour toute question impliquant un traitement d'information à caractère personnel.

Elle est également compétente pour recevoir toute demande d'une personne désireuse d'exercer son droit d'accès aux informations la concernant détenues par Interpol et répond aux requérants. (*Article 6 de l'Échange de lettres entre la République française et l'Organisation*). Ce droit d'accès inclut un droit à la rectification et, le cas échéant, à l'effacement d'informations (*article 9 du RCI*).

– Le bureau de la Confidentialité

Actif depuis 2011, il gère la mise en œuvre du régime de confidentialité des documents d'Interpol. Cela se traduit par l'application de mesures de sécurité propres à chaque niveau de classification d'un document. Il veille au respect des procédures ainsi qu'à l'accès aux informations.

– Les difficultés rencontrées en matière de protection des données

La résolution des demandes d'arrestations ou d'extraditions s'inscrit dans un cadre juridique précis où la volonté de partage des informations doit nécessairement prendre en compte les conséquences de leur diffusion dans des États ne partageant pas nécessairement les normes européennes de protection des données personnelles et de la vie privée.

Un besoin de coopération renforcée nécessitant la création de nouvelles bases de données adaptées à l'évolution de la menace

Le Traité EUCARIS

Initié au début des années 1990 par les Pays-Bas, EUCARIS[57] a été officialisé par un Traité multilatéral signé le 29 juin 2000. Il permet de vérifier l'enregistrement de véhicules, et dans certains cas des permis de conduire. Il a pour but de faciliter les contrôles et d'empêcher les fraudes et vols transfrontaliers de voiture.

« L'initiative suédoise » et la décision-cadre 2006/960/JAI[58]

– Le principe de disponibilité des données : les conclusions du Conseil européen de Tampere d'octobre 1999 avaient confirmé la nécessité d'approfondir l'échange d'informations en matière répressive entre les pays de l'UE. Le programme de La Haye de novembre 2004 a renouvelé cette exigence et introduit le principe de « mise à disposition » des données[59] (ou principe de disponibilité).

– « L'initiative suédoise » (2005) avait pour objet la création d'un cadre juridique commun d'échange d'informations et de renseignement applicable à tous les services répressifs nationaux. Elle sera notamment déclinée dans la décision cadre du 18 décembre 2006 sur la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'UE.

(57) EUropean CAR and driving licence Information System.

(58) Décision-cadre 2006/960/JAI du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne.

(59) « *Les informations accessibles à certaines autorités dans un État membre doivent également être communiquées aux services équivalents des autres États membres. Ces informations doivent pouvoir être échangées aussi rapidement et aussi facilement que possible entre les services des États membres et de préférence dans le cadre d'un accès en ligne* » (avis du CEPD sur la proposition de décision-cadre COM(2005)490 final relative à l'échange d'information en vertu du principe de disponibilité).

Le Traité de Prüm[60]

Une étape essentielle de la coopération est franchie avec le traité de Prüm (Schengen III) du 27 mai 2005 qui améliore substantiellement la coopération entre les États signataires en renforçant les échanges d'informations entre les États membres.

- Le Traité prévoit de nouveaux échanges de données (ADN et données dactyloscopiques) en simplifiant le droit d'accès des États membres qui s'autorisent désormais un droit d'accès réciproque automatique aux données de certains fichiers spécifiques : ADN (FNAEG[61] pour la France), empreintes dactyloscopiques (FAED[62] pour la France) et registres d'immatriculation des véhicules. La consultation fonctionne selon un système de concordance/ non concordance : les États membres ont accès à une mise à jour anonymisée du fichier biométrique et n'obtiennent la totalité des données personnelles qu'en cas de concordance.
- Dans leur rapport de 2009, les députés Delphine BATHO et Jacques Alain BENISTI considèrent qu'il ne s'agit pas d'une interconnexion de fichiers mais que le Traité va plus loin que la future décision-cadre de 2008, puisque cette dernière n'autorise pas la mise à disposition automatisée des données figurant dans les fichiers administratifs et judiciaires nationaux.
- Les décisions 2008/615/JAI[63] du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière et 2008/616/JAI[64] du 23 juin 2008 qui en précise les conditions de mise en œuvre, intègrent les dispositions du Traité de Prüm dans le cadre de l'UE.

Le projet de « smart borders » (« frontières intelligentes ») européen

- La proposition COM(2013)95[65] de la Commission européenne portant création d'un système d'entrée-sortie (EES[66]) et d'un programme d'enregistrement des entrées et sorties (RTP[67]) de ressortissants des pays tiers franchissant les frontières Schengen utilisant des données biométriques.
- L'avis du CEPD sur EES et RTP : « une mesure coûteuse, insuffisamment justifiée et intrusive »[68].

(60) Traité de coopération signé le 27 mai 2005 en dehors du cadre institutionnel de l'UE, initialement entre la Belgique, l'Allemagne, l'Espagne, la France, le Luxembourg, les Pays-Bas et l'Autriche en vue de renforcer la coopération transfrontalière dans la lutte contre le terrorisme, la criminalité organisée et l'immigration illégale.

(61) Fichier National Automatisé des Empreintes Génétiques, créé par la loi n° 1998-468 du 17 juin 1998, dite « loi Guigou ».

(62) Fichier Automatisé des Empreintes Digitales.

(63) Décision 2008/615/JAI du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière.

(64) Décision 2008/616/JAI du 23 juin 2008 concernant la mise en œuvre de la décision 2008/615/JAI relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière.

(65) Proposition de règlement du Parlement européen et du Conseil portant création d'un système d'entrée/sortie pour l'enregistrement des entrées et sorties des ressortissants de pays tiers franchissant les frontières extérieures des États membres de l'Union européenne (28 février 2013).

(66) Entry/Exit System.

(67) Registered Traveller Program.

(68) Communiqué de presse EDPS/2013/08 du 19 juillet 2013.

LA RECHERCHE D'UN NOUVEL ÉQUILIBRE ENTRE SÉCURITÉ COLLECTIVE ET PROTECTION DES DROITS INDIVIDUELS DANS UN CONTEXTE TECHNOLOGIQUE ET SÉCURITAIRE FORTEMENT ÉVOLUTIF

Des progrès à réaliser[69] pour disposer d'outils plus fiables

(69) Voir par exemple les conclusions du contrôle de la CNIL sur les fichiers d'antécédents judiciaires du ministère de l'Intérieur (rapport du 13 juin 2013).

Clarifier le cadre légal régissant la création des fichiers

Dans leur rapport du 24 mars 2009, les députés BATHO et BENISTI dénoncent la coexistence de deux régimes juridiques présidant la création des fichiers et préconisent que « seule la loi puisse autoriser la création d'un fichier de police »[70] (notamment lorsqu'elle se traduit par la collecte de données sensibles), au prétexte qu'elle seule garantit le débat public devant nécessairement présider à cette création.

(70) RI 2009, proposition n°2.

En décembre 2011, ils constatent un *quasi statu quo* législatif et déplorent que le rôle du Parlement n'ait pas été renforcé[71].

(71) RI 2011, 1re partie, paragraphe A-3.

PROPOSITION DU GDS

Les principes instaurés par la loi « informatique et libertés » et ses modifications successives semblent adaptés et n'appellent pas d'évolution législative à court terme.

Pour préserver ce cadre juridique, il est recommandé d'inciter les autorités françaises à Bruxelles à promouvoir ce cadre dans la perspective de la révision en cours du règlement relatif à la protection des données personnelles et de la directive afférent aux données personnelles traitées à des fins de détection et de prévention des infractions pénales.

Poursuivre le recensement et la régularisation des traitements de données personnelles locaux

En dépit de l'important effort de régularisation entrepris par les forces de sécurité depuis plusieurs années, de nombreux fichiers doivent encore faire l'objet d'une autorisation par un acte réglementaire conformément à la loi « informatique et libertés ».

Améliorer la fiabilité technique des bases de données anciennes

Si le niveau de confiance du corps social et de la CNIL est aujourd'hui faible, c'est principalement en raison de la mauvaise qualité de certains traitements déjà anciens, et celle-ci est directement liée au coût et à des compétences insuffisantes.

La conception des nouveaux systèmes d'informations s'appuie désormais sur l'expertise reconnue du STSI(SI) (*voir page 11*) et remplit les règles posées par l'ANSSI[72], lorsqu'elle est consultée mais la mise à niveau des bases de données anciennes continue de se heurter à des problèmes budgétaires et au délai de développement classique, nécessairement long.

(72) Agence Nationale de la Sécurité des Systèmes d'Information créée le 7 juillet 2009 et rattaché au SGDSN.

Le directeur de l'ANSSI considère plus globalement que la centralisation donne la masse critique pour disposer des compétences techniques[73]. Cette concentration est un des principaux moyens de fiabiliser et de sécuriser les traitements de données opérés par les personnes publiques.

(73) Entretien du GDS avec M. Patrick PAILLOUX le 12 février 2014.

Les ministères doivent faire appel à leur DSI[74] pour l'expertise technique des moyens appropriés à retenir, s'appuyer sur les compétences de leur RSSI[75] pour réagir ou se prémunir des attaques de *hacking* et ne pas hésiter à se rapprocher des partenaires institutionnels tel que l'ANSSI, voire la CNIL, qui dispose elle aussi de collaborateurs qualifiés dont l'expertise technique en matière de sécurité des systèmes d'informations peut apporter des solutions aux correspondants CNIL de chaque entité administrative.

(74) Direction des Systèmes d'Information.

(75) Responsable de la Sécurité des Systèmes d'Information.

Le respect des finalités dans le cadre d'un accès élargi aux fichiers de police

Les données doivent être recueillies pour une finalité précise et explicite, même si le Conseil constitutionnel admet, par exemple, l'utilisation de fichiers judiciaires à des fins administratives[76]. Selon la CNIL, la « dilatation » des finalités est une évolution naturelle des fichiers qui doit être maîtrisée. La CNIL est très attachée au principe de sectorisation des fichiers, selon lequel chaque fichier de police doit avoir une finalité ou un ensemble cohérent de finalités.

(76) Voir notamment le titre V du RI 2009.

Le FNAEG constitue un exemple flagrant de dilatation des finalités: initialement créé pour recueillir les empreintes génétiques des personnes impliquées dans des infractions à caractère sexuel ; son utilisation a été ensuite étendue par le biais de lois successives à de nombreux autres crimes et délits. En janvier 2013, un député proposait de l'étendre aux délits routiers et à la délinquance financière.

La finalité et l'usage d'un fichier apparaissent désormais indissociables, particulièrement sous l'angle juridique. Cette approche impose un cloisonnement des traitements de données qui se traduit in fine par la multiplication des fichiers.

Parallèlement, l'élargissement de la consultation des bases de données à des utilisateurs nouveaux (par exemple, par les policiers municipaux[77] ou du fait du rapprochement entre sécurité publique et sécurité privée) et l'émergence de nouveaux besoins émanant de forces de sécurité différentes peuvent concourir au même résultat.

(77) Recommandation n°14 du rapport BAUER.

La convergence des besoins ne doit pas donner lieu à la création de bases de données parallèles répondant aux mêmes finalités. Ainsi, évoquant la demande récurrente d'accès aux fichiers régaliens des policiers municipaux[78], le ministre de l'intérieur qualifiait cette revendication de « dossier prioritaire ».

(78) Allocution de M. VALLS le 13 février 2014 devant la Commission consultative des polices municipales.

Écartant l'accès direct et généralisé, il préconisait un « accès sélectif, procédure par procédure et motivé par l'exercice concret des missions des policiers municipaux (fourrière, contraventions, accidents,...) et respectant le besoin d'en connaître, le principe de traçabilité des consultations et l'information de l'OPJ territorialement compétent.

PROPOSITION DU GDS

L'application trop stricte du principe de spécialité des fichiers peut conduire à une prolifération antinomique avec le contrôle des bases de données.

À ce titre, les services et administrations recherchant les mêmes finalités doivent pouvoir accéder aux systèmes d'informations déjà existants répondant à leur besoin, sous réserve que les accès des utilisateurs soient rigoureusement contrôlés et limités aux seules données dont ils ont à connaître.

Les besoins convergents non couverts par des bases de données existantes doivent également se traduire par la création de nouveaux systèmes d'informations accessibles aux entités partageant ces besoins.

La pluralité de finalités doit également être envisagée pour une même base de données techniquement fiable, si cette démarche permet d'éviter la création de nouveaux traitements automatisés ou si elle permet la suppression de bases de données techniquement obsolètes.

La pertinence et la fiabilité des données

La nature et la proportionnalité des données

- Création d'un référentiel commun[79] et encadrement de la notion de « signalement »[80].
- Collecte et conservation des données personnelles de personnes simplement suspectées ou mises hors de cause (voir condamnation de la France par la CEDH[81] en avril 2013[82] au fondement que la conservation dans le FAED des empreintes d'une personne ayant fait l'objet d'une enquête mais n'ayant jamais été condamnée constituait une atteinte disproportionnée au droit au respect de la vie privée garanti par l'article 8 de la Convention EDH).

(79) Rapport BAUER, recommandation n°7.

(80) Rapport BAUER, recommandation n°23, proposition n°72 du RI 2009 et 2e partie, paragraphe D-1 du RI 2011.

(81) Commission européenne des Droits de l'Homme.

(82) Décision 19522/09 M. K c/ France du 18 avril 2013.

L'exactitude des informations, leur conservation et leur mise à jour

Si le casier judiciaire et le fichier des personnes recherchées (au titre des décisions judiciaires) sont entièrement gérés par leurs gestionnaires, le TAJ (*article 230-9 CPP*), les logiciels de rapprochements judiciaires (*article 230-24 CPP*), le FIJAIS (*article 706-53-1 CPP*) et le FNAEG (*article 706-54 CPP*) sont tous placés sous le contrôle de magistrats.

La CNIL a signalé de manière récurrente le taux d'erreur important des données contenues dans le TAJ[83] (qui résulte de la fusion du STIC et de JUDEX) et les conséquences sur les droits de personnes voulant notamment exercer une profession réglementée (*voir liste des professions pour lesquelles la consultation des fichiers d'antécédents judiciaires est autorisée*[84]). Selon M. Alain BAUER, ce taux avoisinerait les 60% à l'heure actuelle. Le code de procédure pénale (*article 230-6 et suivants*) prévoit que toute personne sollicitant la mise à jour des données qui la concernent peut saisir le procureur de la République compétent ou le magistrat « référent » prévu à article 230-9 de la loi n°2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure.

Pour être fiable, une information doit être pertinente, lisible et non corrompue, c'est à dire complète et actualisée (rafraîchissement des données par mises à jour). Elle doit être correctement retranscrite pour une diminution significative des erreurs de saisies. La proportion de données erronées contenue dans certains fichiers pourrait être réduite de manière drastique en s'appuyant sur les outils et les méthodes de traçabilité de l'information et d'encadrement des utilisateurs, tout en dégageant les moyens humains et financiers pour permettre d'atteindre cet objectif.

Actuellement, la mise à jour par l'autorité judiciaire des informations figurant au TAJ est effectuée par les Parquets qui adressent les documents sous forme « papier » au gestionnaire du fichier. À terme, l'application Cassiopée du ministère de la Justice devrait automatiser cette mise à jour par des échanges inter-applicatifs. Contrairement à ce que pratiquent la police et la gendarmerie nationales pour les traitements dont elles sont responsables, le ministère de la justice n'a pour le moment pas créé de structure unique pour contrôler les utilisateurs de Cassiopée. Par ailleurs, il n'existe aucun moyen automatisé permettant de vérifier l'exactitude et de la mise à jour des données personnelles détenues par l'autorité judiciaire.

(83) Voir les conclusions du contrôle de la CNIL sur les fichiers d'antécédents judiciaires du ministère de l'Intérieur (*rapport du 13 juin 2013*) et RI 2009, titre III.

(84) Décret 2005-1124 du 06 septembre 2005.

PROPOSITION DU GDS

Le contrôle des informations nominatives confiées au ministère de la Justice n'est actuellement pas correctement réalisé ou confié à plusieurs magistrats. La création d'une structure unique dotée d'un droit d'accès et de rectification ainsi que d'un pouvoir de recommandation pourrait être envisagée.

L'application de l'article 230-8 du CPP

L'article 230-8 du code de procédure pénale précise que lorsqu'une décision judiciaire fait l'objet d'une mention (*dans les fichiers d'antécédents STIC-JUDEX/TAJ*), les données relatives à la personne concernée ne peuvent faire l'objet d'une consultation dans le cadre des enquêtes administratives notamment prévues à l'article L. 114-1 du code de la sécurité intérieure. Cette disposition avait été introduite par le biais d'un amendement au projet de LOPPSI 2 du 14 mars 2011, dans le but de renforcer la protection des données à caractère personnel dans le cadre d'une consultation administrative.

Cette disposition s'applique à toutes les enquêtes administratives, y compris celles applicables aux agents de sécurité privée, aux militaires de la Gendarmerie nationale et aux agents de la Police nationale et municipale.

Dans le cas de ces enquêtes administratives, et quelle que soit la cause d'un classement sans suite, c'est-à-dire même si le parquet avait considéré que des faits de nature pénale étaient parfaitement caractérisés, voire si l'auteur en avait reconnu la commission, les policiers ou gendarmes en charge de l'enquête de moralité (qui n'est pas judiciaire mais administrative) n'ont pas accès aux mentions concernées (consultation du fichier en mode enquête administrative), seuls apparaissant les faits ayant donné lieu à condamnation définitive par un tribunal. La prohibition de consultation des mentions STIC/JUDEX-TAJ dans le cadre des enquêtes administratives prévues pour l'accès aux activités de sécurité privée (et aux fonctions de policiers et gendarmes) constituerait un certain risque de recrutement de profils inappropriés dans ces secteurs.

Le président du CNAPS a soulevé la difficulté rencontrée dans le cadre de la réalisation des enquêtes administratives nécessaires à la délivrance des agréments, autorisations et cartes professionnelles du secteur de la sécurité privée, au vu des conditions fixées par l'article 230-8 du code de procédure pénale qui tendent selon lui à vider de sens ces procédures.

Les dispositions de l'article 230-8 du CPP devraient donc pouvoir être révisées. Un décret en Conseil d'État déterminerait les mentions qui peuvent faire l'objet d'une consultation dans le cadre des enquêtes relatives à l'accès à des emplois de professions réglementées liées à la sécurité.

Un décret en Conseil d'État détermine les mentions qui peuvent faire l'objet d'une consultation dans le cadre des enquêtes relatives à l'accès aux emplois visés aux articles L. 411-1 et L. 411-2, L. 421-1, L. 511-1, L. 611-1 et 621-1 du code de la sécurité intérieure. Lorsque l'administration envisage de prendre à l'issue d'une des enquêtes susmentionnées une décision défavorable fondée sur une mention contenue dans le traitement, l'intéressé est mis en mesure de présenter ses observations

D'une part, l'extension de la consultation aux mentions concernerait les seules enquêtes administratives menées sur les militaires de la Gendarmerie nationale, les agents de la Police nationale, les agents de la Police municipale, les agents de sécurité privée et de recherches privées régis par le livre VI du CSI.

D'autre part, le renvoi à un décret en Conseil d'État permettrait de :

- limiter l'accès à certaines mentions inscrites au cours des cinq dernières années par analogie avec les préconisations de la commission nationale de l'informatique et des libertés (CNIL) pour ce qui concerne les faits les moins graves ;
- fixer les modalités de la phase « pré-contradictoire » afin que l'intéressé puisse faire valoir ses observations sur les mentions, lorsque celles-ci sont susceptibles de fonder une décision qui lui serait défavorable.

PROPOSITION DU GDS

La responsabilisation des gestionnaires de fichiers passe, entre autre, par l'obligation de garantir l'exactitude et la validité des données qu'ils détiennent.
L'homogénéisation des règles de vérification, de conservation et de purge des données doit être recherchée aussi souvent que possible, en fonction des finalités propres à chaque fichier.

L'article 203-8 du CPP devrait faire l'objet d'une nouvelle rédaction. Il pourrait être assorti d'un décret en Conseil d'État élaboré par le ministère de l'Intérieur qui déterminerait les mentions qui peuvent faire l'objet d'une consultation dans le cadre des enquêtes relatives à l'accès à des emplois de professions réglementées liées à la sécurité.

Le contrôle des utilisateurs

Les modalités de gestion des accès aux bases de données et de contrôle des utilisateurs qui ont été développées par certaines institutions, telles que la gendarmerie et la police nationales ainsi que la douane, devraient être généralisées à l'ensemble des fichiers de police. Le développement d'outils de monitoring spécifiques permettant de gérer les remontées d'alertes signalant les consultations anormales du système d'information (en nombre et en répartition dans le temps) s'est révélé souvent utile et dissuasif, à condition qu'un organe de contrôle interne à l'institution utilisatrice soit en mesure d'exploiter ces alertes, de diligenter des enquêtes et de prononcer les sanctions éventuellement souhaitables.

Ces modalités de contrôle devraient pouvoir être appliquées à tous les utilisateurs des fichiers de police, y compris au stade de la saisie des informations si celle-ci résulte d'une démarche manuelle de l'opérateur. C'est par exemple le cas du ministère de la justice qui, faute de moyens, recourt à des vacataires peu au fait des pratiques judiciaires et devrait s'appuyer sur la réserve civile des personnels du ministère de la Justice.

Le cas particulier des fichiers de souveraineté détenus et exploités par des services spécialisés de la défense, du renseignement ou de la protection de la sûreté de l'État

Touchés dans leur champ d'activité par le phénomène montant de la « judiciarisation » de la société et au cœur d'un débat public légitime réclamant

un renforcement du contrôle démocratique sur les activités de renseignement[85], les services de renseignement se trouvent confrontés à des revendications fortes visant la confidentialité de leurs données.

(85) Rapport parlementaire de MM. URVOAS et VERCHERE du 14 mai 2013.

Un contrôle global revendiqué par la CNIL

L'article 44 de la loi du 6 janvier 1978 prévoit la possibilité de ne pas soumettre au contrôle de la CNIL les fichiers « intéressant la sûreté de l'État ».

Il existe actuellement une liste de 8 fichiers concernés, fixée par décret du 15 mai 2007. Ces fichiers sont détenus et exploités par des services de renseignement.

La CNIL n'exerce donc qu'un contrôle ponctuel sur ces fichiers, au travers de la mise en œuvre d'un droit d'accès indirect prévu par l'article 41 de la loi informatique et libertés.

La présidente de la CNIL a récemment formulé auprès du président de la République la proposition de renforcer son contrôle sur ces fichiers de renseignement.

Cette démarche aurait cependant un impact significatif sur le fonctionnement même des services concernés et la sécurité de leur action, livrant un accès à l'architecture de leurs outils techniques et mettant en question les principes de cloisonnement et du « besoin d'en connaître » qui garantissent la protection des secrets de la défense nationale.

Selon le coordonnateur du renseignement, un nécessaire équilibre est à trouver entre les exigences de la défense des intérêts fondamentaux de la nation et la protection des libertés, mais, pour autant, il estime qu'il est légitime d'assumer le secret.

Le cadre juridique du droit d'accès aux fichiers mis en question

Dans le cadre du droit d'accès indirect aux fichiers de souveraineté, l'article 41 de la loi informatique et libertés prévoit l'accord du responsable du fichier pour permettre à la CNIL de communiquer les données au demandeur.

De fait, une application accommodante de cette règle est généralement effectuée au profit du requérant, à l'exception des fichiers de renseignement.

La simple indication qu'une personne figure ou non dans un tel fichier est en effet considérée comme incompatible avec la finalité d'une base de données qui concourt à la sécurité nationale. La loi prévoit donc la possibilité que la CNIL réponde simplement qu'« il a été procédé aux vérifications ».

Cependant cette disposition législative est actuellement mise à mal par plusieurs décisions du tribunal administratif de Paris, fondées sur la jurisprudence Moon (Conseil d'État, 6 novembre 2002) qui considère que les données des fichiers de souveraineté sont « divisibles ».

Selon le juge administratif, la partie des données ne mettant pas en cause la finalité du traitement devrait être communiquée au requérant.

S'agissant des données dont le responsable du fichier, et même la CNIL, considèrent la communication comme portant atteinte à sa finalité, le juge réclame les pièces lui permettant d'apprécier la nature des données écartées et les raisons de leur exclusion.

Le fait que ces pièces doivent être versées au dossier contradictoire constitue de manière évidente une atteinte à la finalité du fichier et parait incompatible avec la protection de la défense des intérêts nationaux. On est bien ici au cœur de la problématique sécurité versus libertés individuelles.

Ces décisions confirmées en appel, sont à présent en instance devant le Conseil d'État et constituent un enjeu primordial pour les services de renseignement.

En cas de validation de cette jurisprudence par la haute juridiction, une modification de l'article 41 de la loi du 6 janvier 1978 pourrait être envisagée pour garantir une protection renforcée aux fichiers intéressant la sûreté de l'État.

PROPOSITION DU GDS

La question du contrôle des fichiers intéressant la sûreté de l'État dépasse le cadre strict des fichiers de police. Elle doit s'intégrer à la réflexion plus large sur le renforcement du contrôle démocratique des activités de renseignement.

Le respect de l'exercice des droits prévus par la loi « informatique et libertés »

Le rapport BATHO-BENISTI du 21 décembre 2011 déplorait l'insuffisance des progrès accomplis dans ce domaine.

Le rapport BAUER de décembre 2008 préconisait dans sa recommandation n°2 de « fournir à la population une information pédagogique sur les fichiers » afin d'en renforcer l'acceptabilité.

S'agissant de l'utilisation d'internet, la CNIL souhaiterait renforcer l'information des usagers à deux niveaux[86] par :

- une présentation des finalités de la collecte de données par chaque site ;
- une présentation plus détaillée de l'usage qui en est fait.

Cette démarche constitue une piste intéressante qui pourrait être explorée s'agissant des bases de données gérées par l'État.

(86) La formation des usagers constitue aussi l'un des défis futurs. La CNIL a ainsi promu un label formation qu'elle délivre aux organismes privés ou publics qui se lancent dans une telle démarche. La gendarmerie nationale a présenté le 12 décembre 2013 le programme national qu'elle a développé avec AXA Prévention pour sensibiliser les enfants du primaire et leurs parents à l'utilisation du web et, notamment des réseaux sociaux.

PROPOSITION DU GDS

Le défaut de communication entretient la défiance et peut rendre n'importe quelle base de données, même fiable, inacceptable à l'opinion publique.

Il importe donc, outre l'action de la CNIL, que les gestionnaires de fichiers renforcent l'information du public sur les droits que leur confère la loi « informatique et libertés » et sur le rôle de l'autorité de contrôle indépendante, mais aussi sur :

- **les finalités des principales bases de données administratives ou judiciaires ;**
- **les mesures prises par le gestionnaire pour garantir que ces données ne seront pas utilisées ou consultées à d'autres fins que celles qui ont été prévues par le législateur ;**
- **les raisons motivant l'inscription dans ledit traitement et de la durée de conservation des données qu'il contient ;**
- **les droits afférents à l'accès et à la rectification de ces données.**

Vers une évolution du rôle et des pouvoirs de l'autorité de contrôle indépendante ?

Si son activité et sa croissance sont en progression constante, la CNIL serait sous-dimensionnée par rapport à ses homologues allemand et britannique. Pour autant, son indépendance est reconnue et respectée, de même que sa compétence à contrôler les fichiers de police, laquelle ne constitue pas une règle au sein de l'UE. Elle estime cependant que son pouvoir de sanction mériterait d'être renforcé, notamment sur le plan financier (*voir la condamnation de Google le 09 janvier 2014*).

La possibilité de donner davantage de poids au groupe de travail sur l'amélioration du fonctionnement et du contrôle des fichiers de police, dit « groupe DEBOVE », doit être envisagée.

Plus globalement, et sans remettre en cause le rôle de la CNIL en qualité d'autorité indépendante, le cloisonnement des tâches entre organismes consultatifs, organe de contrôle et de sanction, organe d'audit et de conseil milite pour une plus grande centralisation des tâches dans un contexte de compétences élargies.

PROPOSITION DU GDS

Donner au groupe de travail sur l'amélioration du fonctionnement et du contrôle des fichiers de police une dimension interministérielle en le rattachant au Premier ministre. Sa compétence pourrait ainsi être étendue à l'ensemble des traitements de données à finalité de sécurité placés sous la responsabilité de l'État. Il pourrait être également autorisé à recueillir des avis d'experts en technologie informatique.

Adapter les traitements de données à l'évolution des nouvelles technologies et à l'évolution de la menace

Sous l'influence des technologies de pointe, des nouvelles pratiques sociales et économiques et de la dynamique de globalisation qui les accompagne, la logique de « fichier » a perdu beaucoup de sa portée au profit de la notion de donnée personnelle. Celle-ci s'est d'ailleurs elle-même transformée au point d'être supplantée par le concept de donnée « relationnelle », voire « transactionnelle »[87]. La différence entre données personnelles et données non personnelles s'est ainsi estompée et les mêmes flux intéressent désormais non seulement les grandes entreprises d'Internet mais aussi les forces de sécurité et les services de renseignement des États les plus développés.

Dans un tel contexte, la notion de « donnée sensible » a également évolué et sa définition est plus malaisée[88]. Traditionnellement considérées comme étant celles qui présentent un risque potentiel d'atteinte à la vie privée, à la liberté,

(87) Dominique BOULLIER, in « Vie privée à l'horizon 2020, paroles d'experts », Cahier de la CNIL Innovation et Prospective n°1, p. 32.

(88) « De nouvelles données sensibles ? » in « Vie privée à l'horizon 2020, paroles d'experts », Cahier de la CNIL Innovation et Prospective n°1, p. 34-35.

voire à l'identité humaine, elles bénéficient à juste titre d'un régime juridique très protecteur. Pour autant, certaines d'entre elles, notamment celles qui sont héritées de l'Histoire, sont en passe d'être supplantées par d'autres données devenues plus discriminantes pour les individus en raison de la révolution du monde numérique.

Ces changements ont une influence directe sur les fichiers de police, au sens où la recherche constante d'une plus grande efficacité dans la prévention et la lutte contre le terrorisme, la criminalité organisée et la délinquance en général incite naturellement à recourir à de nouvelles technologies, banalisées par ailleurs dans la sphère commerciale ou privée.

Parallèlement, l'évolution de la menace stimule de manière pressante le besoin de coopération interservices et interministériel et favorise l'élargissement de l'accès aux fichiers ainsi que la concentration des moyens.

L'utilisation des techniques innovantes par l'État, fut-ce pour protéger la sécurité collective, ne fait pas l'unanimité au sein des opinions publiques, relayées en cela par la CNIL et, dans une moindre mesure, par le groupe de travail sur l'amélioration du fonctionnement et du contrôle des fichiers de police et de gendarmerie qui considèrent qu'il faut se garder de recourir de manière excessive à des technologies nouvelles en matière de fichiers, notamment pour céder à la facilité.

Les objections qui sont traditionnellement avancées sont le risque de dilatation des finalités, la disproportion des données collectées par rapport au but recherché, l'atteinte potentielle à la vie privée et à la liberté qui rendrait l'individu « transparent aux yeux de l'État »[89].

(89) Pierre PIAZZA: « La biométrie, un nouveau sésame ? » in « Vie privée à l'horizon 2020, paroles d'experts », Cahier de la CNIL Innovation et Prospective n°1, p. 24.

Considérant que sa mission consiste aussi à accompagner les évolutions technologiques des traitements de données, la CNIL préconise ainsi de réévaluer les traitements automatisés à chaque fois que l'introduction d'une technologie nouvelle vient en dénaturer la version initiale.

Le sujet sensible des bases d'analyse sérielle et des logiciels de rapprochement judiciaire[90]

(90) Rapport BAUER, recommandation n°25.

Autorisés par le code de procédure pénale (*article 230-12*), les traitements d'analyse sérielle servent à établir des liens entre des individus, des événements ou des infractions, afin d'identifier les auteurs des crimes ou délits présentant un caractère sériel. Ces fichiers rassemblant un grand nombre de données sur des individus, la loi a limité les infractions à propos desquelles ils peuvent être utilisés[91].

(91) Le seuil de peine fixé par la loi est de cinq ans d'emprisonnement.

Ces traitements sont utilisés par un très petit nombre d'enquêteurs de services spécialisés de police judiciaire.

Procédant de la même volonté d'améliorer l'efficacité des services d'enquête par le rapprochement des informations, les logiciels de rapprochement judiciaire reposent sur une base juridique différente (*article 230-20 du code de procédure pénale*).

Ils permettent aux services de police judiciaire d'effectuer des rapprochements entre des infractions de même type, afin de déterminer si elles peuvent être le fait des mêmes auteurs. Le Conseil constitutionnel a soumis l'utilisation de ces logiciels à de strictes conditions (autorisation préalable de l'autorité judiciaire et utilisation dans le cadre d'une même enquête)[92].

(92) *Cf.* la décision n°2011-625 DC relative à la loi de programmation pour la performance de la sécurité intérieure.

Utilisés par les forces de police de nombreux pays, les logiciels d'analyse sérielle et de rapprochement judiciaire constituent des outils aujourd'hui indispensables à l'action des services d'enquête.

L'interconnexion des bases de données : quelles perspectives ?

L'interconnexion entre fichiers est un des sujets les plus complexes et sensibles actuellement dans le cadre du développement du numérique.

Elle est encadrée par la loi « informatique et libertés », afin de veiller strictement au respect du principe de spécialité des fichiers.

Elle répond pourtant à un besoin récurrent et croissant des forces de sécurité[93].

(93) RI 2011, 4e partie, paragraphe B-4 a.

La CNIL, comme le président du groupe de travail sur l'amélioration du fonctionnement et du contrôle des fichiers de police et de gendarmerie, opposent plusieurs objections au développement de l'interconnexion des fichiers, notamment le risque de dilatation des finalités et la disproportion des moyens employés qui rendrait une telle base de données inacceptable pour la population.

Pourtant, l'interconnexion est également souvent le moyen de mieux protéger les libertés individuelles. Elle permet en effet de fiabiliser les données contenues dans différents fichiers. C'est précisément l'objet de l'interconnexion entre CASSIOPEE, le traitement du ministère de la justice, et le traitement d'antécédents judiciaires du ministère de l'intérieur.

A contrario, l'ANSSI estime que la polémique sur l'interconnexion des fichiers est un débat dépassé et dénué de sens dans le contexte numérique actuel qui banalise cette pratique dans le domaine privé. Elle considère que cette évolution technique est inéluctable.

PROPOSITION DU GDS

Certains États de l'UE, tels que la Suède, autorisent ponctuellement l'interconnexion de traitements sous réserve de l'autorisation d'une entité compétente et clairement désignée. L'interconnexion des fichiers doit pouvoir être admise si elle concerne des bases de données fiables et qu'elle est accompagnée de mesures de contrôle adaptées.

Les enjeux de la biométrie

La biométrie se définit comme « l'analyse des caractéristiques physiques strictement propres à une personne (empreintes digitales, iris, éléments de visage et/ou du crâne, voix,...) ». À ce titre, l'assimilation de l'ADN à une donnée biométrique ne peut s'envisager que par extension, la nécessité de prélèvement d'un échantillon physique (tissu ou fluide corporel) étant préalable à tout traitement technique.

La biométrie bénéficie d'un essor certain dû à d'importantes potentialités. Au regard du droit et des libertés individuelles, elle constitue l'exemple type qui invite à la recherche d'un équilibre entre respect de la vie privée lié à la protection des données personnelles et intérêts sécuritaires collectifs. Selon la CNIL, elle représente l'un des défis majeurs de l'avenir en matière de police technique et scientifique.

En France, 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 informatique et libertés, contient une disposition qui soumet le traitement des données biométriques à un régime d'autorisation préalable, dotant ainsi la France de l'un des régimes juridiques les plus protecteurs en la matière. Le 29 avril 2014, le Sénat a examiné un projet de loi visant à limiter l'usage des techniques biométriques en encadrant le pouvoir d'autorisation de la CNIL. Le projet conditionne l'autorisation de la mise en œuvre d'un traitement de données biométriques à une « *stricte nécessité de sécurité* » en excluant de son champ d'application les traitements de données biométriques mis en œuvre pour le compte de l'État et ceux qui sont mis en place pour l'exercice d'activités strictement personnelles.

L'utilisation de la biométrie se doit de ne pas constituer une atteinte potentielle au principe de proportionnalité des données recueillies et exploitées.

Des fichiers biométriques contemporains, de qualité existent depuis plus de vingt-cinq ans : le FNAEG (*loi du 17/06/98*), le FAED (*décret du 08/04/87*). Les modalités d'accès en sont strictes mais le champ des sollicitations ne cesse de s'élargir, rendant leur contrôle plus délicat.

Comme tous les traitements automatisés, ils sont potentiellement menacés par le risque de dilatation.

La première version de la loi 2012-410 du 27 mars 2012, relative à la protection de l'identité, a été censurée par le Conseil constitutionnel[94] qui en a notamment abrogé les articles 3, 5, 7 et 10. Ceux-ci prévoyaient la création d'un fichier biométrique national d'identification des données provenant de toutes les cartes d'identité et des passeports ainsi que la possibilité pour ces cartes d'identité de servir à l'identification sur internet et de permettre la signature électronique.

(94) Décision 2012-652 DC du 22 mars 2012.

Les perspectives de développement sont liées à la finalité des données. Celle-ci doit être déterminée, explicite et légitime.

L'intégration sociétale de la démarche biométrique est soumise à quatre facteurs : le sentiment d'insécurité (perception de la vulnérabilité personnelle), la valeur accordée à la biométrie, le rapport à la technologie, la confiance ou la méfiance accordée à l'autorité légale utilisatrice.

En mars 2014, la disparition d'un Boeing *777* (*Malaysia Airlines*) a relancé les débats sur les contrôles biométriques, tant aux frontières que sur les sites d'embarquement.

Il est impératif de faire évoluer les potentialités internationales d'identification biométrique, ainsi que cela s'est toujours fait. L'histoire policière, de Bertillon aux premières notices d'Interpol (1946, « notices rouges ») est, à ce titre, particulièrement édifiante.

PROPOSITION DU GDS

Le recueil d'informations faciales, voire cranio-faciales, est un des enjeux majeurs de la biométrie en ce début de XXIe siècle.

La création d'un fichier biométrique à part entière dont l'une des entrées pourrait être la vidéo-protection / vidéosurveillance [95] devrait être étudié dans un cadre réglementaire adapté.

L'alimentation de cette base de données par les passeports biométriques et les futures cartes d'identité de même nature est à réévaluer.

Les *Notices d'Interpol* doivent maintenant progresser et intégrer un cinquième critère d'identification anthropométrique qui sera *cranio-facial et radiographique* [96].

Géo-localisation et interception

La géo-localisation des terminaux de communication téléphoniques ou informatiques comme moyen de recueil de renseignement ou d'enquête fait l'objet de nombreux débats depuis plusieurs mois. Les services de renseignement comme ceux de police judiciaire ont recours à la géo-localisation pour l'accomplissement de leurs missions administratives et judiciaires.

Ce moyen fait depuis peu l'objet d'une base juridique explicite en droit français, dans le cadre administratif du recueil de renseignement [97] comme dans celui des enquêtes judiciaires [98].

Au-delà des questions soulevées par ce moyen d'enquête, le traitement des données ainsi recueillies doit faire l'objet d'un encadrement juridique conforme aux lois précitées et à la loi « informatique et libertés ».

Ce dernier devra garantir que l'usage des informations sera strictement limité aux finalités de leur recueil.

– Le projet de PNIJ [99]

Le projet, en cours de finalisation, de plate forme nationale des interceptions judiciaires, consiste à centraliser les opérations d'interceptions de communications requises par l'autorité judiciaire, au sein d'une plate forme technique. Le groupe Thalès s'est vu confier sa mise en œuvre.

Selon le Directeur de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) [100], ce dispositif centralisé est garant de la sécurité de ces opérations d'interception. Il permettra un haut niveau de contrôle qui n'était pas réalisable avec des centres d'interception disséminés sur le territoire national et une diversité d'opérateurs.

(95) L'utilisation de la vidéo-surveillance est étroitement liée à la problématique de la biométrie au sens où toute photo peut désormais être considérée comme une donnée biométrique grâce à l'exploitation qui peut en être faite au moyen d'un logiciel de reconnaissance faciale. Plusieurs États étrangers, dont l'Allemagne, se sont dotés de tels outils utilisés à des fins d'identification d'individus suspects. En France, certains projets incomplets ou trop précoces ont été envisagés dans un passé récent, puis abandonnés (annonce du DGPN en août 2011 et projet abandonné par la RATP en mai 2013). En Europe, le projet INDECT (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment ou Système d'information intelligent soutenant l'observation, la recherche et la détection pour la sécurité des citoyens en milieu urbain) vise à installer des systèmes de surveillance intelligents en vue de détecter les menaces criminelles de manière automatisée grâce aux flux de données fournis par des caméras de vidéo-surveillance. Sa mise en place s'est heurtée à de vives controverses.

(96) NAZAT, D., Insertion of cranio-facial x-ray files in the Interpol Notices: from the present to the future; a new way of thinking, Journal of Forensic Odonto Stomatology, Vol. 31, Sup. n°1, P. 110, Oct. 2013.

(97) Article 20 de la loi n°2013-1168 du 18 décembre 2013 relative à la loi de programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.

(98) Loi n°2014-372 du 28 mars 2014 relative à la géolocalisation.

(99) Plate-forme nationale des interceptions judiciaires.

(100) M. Patrick PAILLOUX au moment du recueil de ces propos, le 12 février 2014.

L'élargissement de l'accès aux fichiers

La loi de programmation militaire 2014-2019 votée en décembre 2013 comporte plusieurs dispositions relatives à l'accès des services de renseignement aux fichiers :

- l'accès élargi des services de renseignement (défense,...) aux fichiers administratifs et aux fichiers judiciaires: la loi de programmation militaire élargit les possibilités d'accès des services de renseignement à plusieurs fichiers administratifs (ex : fichier des cartes nationales d'identité) pour l'accomplissement de leurs missions et la sécurité de leurs agents. Les modalités de ces nouveaux accès devront être définies par décret en Conseil d' État pris après avis de la CNIL.
- l'accès des services de renseignement aux fichiers PNR [101] et API [102], l'expérimentation jusqu'en 2017 d'un traitement de données PNR français conforme au projet de directive européenne [103].
- la possibilité pour les services de renseignement des ministères de la défense, de l'intérieur et de l'économie et du budget d'accéder aux données conservées par les opérateurs de communications électroniques, les fournisseurs d'accès à Internet et les hébergeurs dans le cadre de la recherche de renseignements intéressant la sécurité nationale, la sauvegarde des éléments essentiels au potentiel scientifique et économique de la France, la prévention du terrorisme, de la délinquance et de la criminalité organisée, de la reconstitution ou du maintien de groupements dissous existe depuis la loi du 10 juillet 1991 relative au secret des correspondances. La loi de programmation militaire (*art.*20) fusionne ce régime juridique avec celui de la loi anti-terroriste du 23 janvier 2006.

(101) Passenger Name Record.

(102) Advanced Passenger Information.

(103) Le PNR est présenté en détail page 35.

L'utilisation des nouvelles technologies pour sécuriser nos traitements de données et les adapter au monde numérique actuel

L'évolution rapide des technologies numériques

L'observation des technologies de l'information a fortement évolué depuis une dizaine d'années : développement de la puissance de calcul, des réseaux de télécommunications (internet, wifi, etc.), multiplication des terminaux portables (smartphones, tablettes, paiement sans contact,...) et interopérabilité des moyens de communication et d'information.

La combinaison de ces phénomènes bouleverse les modèles économiques dits classiques. Les mutations sont visibles : développement des réseaux sociaux, dématérialisation des activités, évolution du stockage de données, nouvelles formes de partages de fichier, etc. Le *Cloud Computing* se développe du fait du développement des volumes, de l'accessibilité des données et des facilités de stockage proposées par des prestataires ayant réalisé de lourds investissements pour construire des centres de données (*data center*).

Parallèlement, se sont développées de nouvelles techniques d'exploitation des données, telles que le *data mining* ou « exploration de données » qui permet d'exploiter un grand nombre de données dans le but d'en extraire un savoir ou une information.

Réalité et risques de la cyber-menace

Le développement des activités sur internet peut être porteur de libertés et de croissance. Cependant les échanges informationnels ou financiers qui y transitent attirent la convoitise des États, des « *hackers* » et des organisations criminelles. Le développement des menaces doit être appréhendé par tous les acteurs, et plus spécifiquement par les services publics qui gèrent des données sensibles. L'exemple de l'accès illicite à des données « Schengen » par un *hacker* suédois en décembre 2013 laisse perplexe.

Internet nous démontre l'hétérogénéité des réglementations nationales, notamment en matière de protection des personnes et des biens matériels ou immatériels. Dans le domaine de la surveillance, l'affaire PRISM [104] a révélé à l'opinion publique mondiale, les pratiques de cyber-surveillance des États-Unis, en application notamment de leur texte législatif, dit FISAA [105].

Le *Privacy Act* de 1974 ne protège que les citoyens américains, sans principe juridique de finalité, ni de durée de conservation des informations. Les implications en termes de souveraineté des données et de protection des droits individuels sont importantes mais, paradoxalement, la réaction des Européens a été peu vigoureuse. Faisant implicitement référence aux écoutes massives de la NSA, la Commission et le Conseil européens ont rappelé au Président des États-Unis en visite à Bruxelles en mars 2014, le nécessaire respect d'un cadre juridique ou « les limites légales et légitimes » d'une pratique jugée trop invasive, dans l'espoir d'obtenir une « meilleure compréhension » de leur interlocuteur [106].

Aujourd'hui, il est nécessaire de développer et de promouvoir la cybersécurité auprès de tous les acteurs et utilisateurs. Les moyens de riposte, sont à considérer mais dépassent le cadre de la présente étude.

En France, différents textes imposent la sécurisation des systèmes d'information publics comme privés :

- la loi « informatique et libertés » qui impose l'obligation de sécurité des données personnelles ;
- la loi de programmation militaire, adoptée le 13 décembre 2013, qui renforce les obligations en matière de sécurité de l'information des opérateurs d'importance vitale (OIV), notamment pour ce qui concerne l'obligation de notification des incidents. Elle étend également les pouvoirs de l'ANSSI en lui permettant de réaliser des contrôles et audit chez les OIV.

Au plan européen, la mise en place de structures telles que l'ENISA [107] et l'EC3 [108] démontre la volonté de coordonner les actions de cybersécurité. Différents projets de règlements et directives intègrent des dispositions en matière de sécurité des systèmes, et, notamment, le projet de Règlement sur l'identification électronique et les services de confiance (dit eIDAS [109]), dans sa version adoptée par le Parlement le 3 avril 2014.

(104) Programme américain de surveillance électronique par la collecte de renseignements sur internet et d'autres services électroniques. Piloté par la NSA conformément au FISAA de 2008, il a été révélé le 6 juin 2013. L'affaire se développe jusqu'en octobre 2013 où elle culmine par la révélation que 35 dirigeants pour la plupart Européens auraient été espionnés dans le cadre de ce programme.

(105) Foreign Intelligence Surveillance Amendment Act, amendement de la FISA de 1978 décrivant les procédures des surveillances physiques et électronique, ainsi que la collecte d'information sur des puissances étrangères soit directement, soit par l'échange d'informations avec d'autres puissances étrangères. L'amendement a été voté en 2008 et prorogé jusqu'en 2017 le 28 décembre 2012.

(106) « OBAMA à Bruxelles : tour d'horizon des sujets qui fâchent », Philippe RICARD et Jean-Pierre STOOBANTS, *Le Monde*, 26 mars 2014.

(107) Agence européenne créée en 2004 et chargée de la sécurité des réseaux et de l'information (European Network and Information Security Agency).

(108) Centre européen de lutte contre la cybercriminalité (European Cybercrime Center), créé en janvier 2013.

(109) electronic identification and trust services.

Quelles pistes pour l'avenir ?

Pour la CNIL, le progrès technique doit avant tout servir à élever le niveau de sécurité des traitements de données.

Le « *cloud computing* » ou « informatique en nuage » est une pratique qui se développe au sein des entreprises. Pour autant, il pose de réels problèmes de sécurité et il implique l'élaboration d'un cahier des charges imposant des règles de sécurité strictes. L'un des risques majeurs est la localisation des données dans des pays étrangers où la réglementation de la protection des données personnelles peut être méconnue, différente voire contradictoire avec celle qui est applicable en France ou au sein de l'UE.

PROPOSITION DU GDS

L'utilisation de technologies de pointe pour sécuriser les traitements de données et en améliorer le contrôle contribue indéniablement à rendre plus acceptables les fichiers de police vis-à-vis de l'opinion publique. *A contrario*, le recours au *cloud computing* comme alternative au stockage des données sensibles gérées par les services de l'État n'est pas envisageable dans le contexte actuel.

Qu'est ce qu'une base de données « acceptable » ?

Les conditions d'acceptabilité

Le développement de tout nouveau moyen nécessite d'être entouré des garanties qui le rendront acceptable pour les citoyens.

Selon la CNIL, c'est le principe d'acceptation de la collecte des données qui est au cœur du problème.

Celle-ci repose sur la proportionnalité des données collectées par rapport aux finalités et à la cohérence de ces finalités dans le cadre d'un État de droit moderne. L'acceptabilité n'est pas mesurable et varie sensiblement en fonction des circonstances. Par ailleurs, il convient de se garder des réactions trop immédiates dictées par la pression médiatique.

Dans un contexte mondialisé, l'évolution technique et sociologique modifie la perception de la notion d'atteinte aux libertés publiques et selon les approches, le consensus sur le point d'équilibre à trouver entre préservation des libertés individuelles et sécurité collective émerge difficilement.

Pour l'ANSSI, c'est la sécurité du système d'information qui est garante de son acceptabilité par la population. Celle-ci repose sur plusieurs conditions : la fiabilité technique du traitement qui dépend du respect de règles validées par une autorité de sécurité indépendante et mises en œuvre par des experts, la pertinence et la qualité du contrôle des utilisateurs, la transparence du dispositif s'appuyant sur une bonne communication vis-à-vis de la population.

Une base de données de nouvelle génération, le PNR

Une directive européenne de 2004[110] oblige les transporteurs à communiquer les données relatives aux voyageurs. Elle inscrit l'échange des données PNR dans la lutte contre le terrorisme, le crime organisé, l'immigration illégale et la fraude fiscale.

(110) Directive 2004/82/CE du Conseil du 29 avril 2004.

Dans l'Union européenne, seul le Royaume-Uni dispose d'un tel système de surveillance. En France, une mission interministérielle regroupant des représentants des quatre ministères compétents (Intérieur, Défense, Transports et Budget) a été créée en juillet 2011. Son objectif était de mettre en place, la plate-forme d'exploitation des données PNR, et solliciter des fonds ISEC (programme européen de lutte contre la criminalité) alloués par la Commission pour la mise en œuvre du projet de directive. La Commission européenne a rendu un avis d'attribution de 17,8 millions d'euros, pour le projet PNR France.

Les données des dossiers passagers (ou PNR) sont des données personnelles concernant tous les détails d'un voyage pour les passagers aériens. L'accord du 17 mai 2004 entre l'Union européenne et les États-Unis fixe la liste des données pouvant être communiquées aux services américains des douanes et de sécurité par les agences de voyages et les compagnies aériennes européennes lors de la réservation d'un vol à destination ou *via* les États-Unis.

L'exploitation de ces données est entourée de garanties. Ainsi, elles ne peuvent être utilisées que dans le cadre strictement défini par la directive. Elles sont effacées après un délai maximal de trois ans et six mois, sauf pour les données consultées dans le cadre d'investigations spécifiques ou bien manuellement. Un accord semblable a été conclu entre l'Union européenne et le Canada.

La plateforme (PIU [111]) de traitement des données API-PNR a été confiée à la douane. Elle sera localisée sur le site aéroportuaire de Roissy-CDG. Elle seule sera habilitée à consulter la totalité des données, servant ainsi d'interface aux autres utilisateurs.

(111) Unité Informations Passengers.

Le dispositif mis en œuvre repose sur un processus de recherche perfectionné associant le criblage (interconnexion avec le FPR) et le ciblage permettant une consultation limitée aux agents habilités. Les autorités compétentes (police, douane, gendarmerie...) n'auront que des données filtrées (requêtes automatisées du système ou demandes précises à la PIU)

La montée en charge du système doit être rapide et il doit être suffisamment dimensionné pour traiter le volume de données recueillies. En 2018, l'ensemble des vols extracommunautaires à destination ou au départ de la France drainera un volume estimé à 164 millions de voyageurs. À terme, le système devrait également intégrer les passagers des vols intracommunautaires, soit 100 millions de passagers, en plus, par an.

Le système API-PNR va permettre à la douane d'affiner sa connaissance des flux voyageurs sur le vecteur aérien. Le ciblage anticipé existe déjà sur le fret avec le système ICS-ECS [112]. Il sera désormais aussi possible pour les voyageurs.

(112) Import Control System et Export Control System.

Le système API-PNR sera alimenté en deux temps par les compagnies aériennes : une première saisie s'effectuera 48 heures au plus tard avant le départ du vol, une seconde saisie suivra immédiatement la clôture de celui-ci.

Si le projet PNR ne concerne actuellement que les passagers des compagnies aériennes, il est envisagé de l'étendre aux vecteurs maritimes et terrestres, selon la montée en charge et le succès du PNR aérien.

Comment rendre fiable un système d'information ?

PROPOSITION DU GDS

Les caractéristiques techniques de tout nouveau système d'information fiable et acceptable pourraient être les suivantes :

- **Un système conçu par des experts sur la base de règles techniques élaborées par une autorité de sécurité indépendante, type ANSSI, compatible avec les normes de l'UE en matière de protection des données individuelles (responsabilisation du détenteur des données).**
- **S'appuyant sur un cadre juridique solide et conçu dans la transparence, sur la base d'une large concertation assortie d'une vaste campagne de communication.**
- **Une base de données non répliquée privilégiant un système informatique centralisé et sécurisé intégrant une sauvegarde en temps réel.**
- **Doté d'outils d'aide à la saisie liés au processus d'exploitation, permettant le recueil des données non dupliquées et sauvegardées automatiquement.**
- **Une normalisation par formats d'échanges de données (basée sur celle des archives nationales) permettant leur pérennisation et leur accès à long terme associés à des progiciels communs ou totalement compatibles (bureautique et bases de données).**
- **Doté d'outils d'intégration automatique autorisant une fusion des systèmes d'information (ex : STIC et JUDEX fusionnés dans le TAJ), avec purge sécurisée des données erronées ou redondantes utilisant des programmes informatiques dédiés.**
- **Un système d'exploitation éventuellement couplé à une base d'indicateurs de performance anonymisés permettant de le rentabiliser par l'élaboration de statistiques d'activités.**
- **Une sécurisation reposant à la fois sur des référentiels de droits d'accès définissant des profils d'utilisateurs et d'administrateurs valables pour une durée limitée et renouvelables en tant que de besoin.**
- **Une procédure d'accès reposant sur un système d'authentification forte (biométrie –iris, empreintes digitales- matériels de type carte à puce, clé USB, certificats chiffrés permettant d'accéder à des réseaux sécurisés dont l'efficacité peut être renforcée par des systèmes de chiffrement associés à des algorithmes complexes) dépendant du niveau de sécurité requis par les outils matériels (sédentaires ou portables) mis en œuvre et intégrant une étape obligatoire de justification des motifs de consultation.**
- **Un système fiable de traçage des connexions couplé à un dispositif d'alerte permettant de déceler les utilisations anormales ;**
- **Un organisme interne au service utilisateur, seul habilité à exploiter les outils de contrôle et doté d'un pouvoir de sanction.**
- **Une mise à jour en temps réel des outils informatiques pour adapter le système aux nouvelles législations et aux éventuelles réformes.**
- **Un volet informatif public permettant aux usagers d'accéder aux informations détaillées page 25.**

S'adapter au besoin de coopération avec des États ne partageant pas la conception française et européenne de protection des données personnelles

La difficile coopération avec les États-Unis

Il n'y a pas de réglementation fédérale globale sur la protection des données aux États-Unis : seules quelques réglementations sectorielles existent et chaque État est libre d'adopter ses propres lois en la matière. La notion de « données sensibles » y est aussi très différente de celle qui prévaut au sein de l'UE

Un exemple de difficile équilibre entre protection des données et lutte contre le terrorisme : l'affaire SWIFT et le TFTP[113]

Suite à l'affaire SWIFT et TFTP[114], l'UE a envisagé de créer le SSFT[115], censé être l'alternative européenne au problème de l'extraction des données. Les objectifs du SSFT étaient les suivants: contribuer à limiter le volume de données à caractère personnel transférées aux États-Unis, contribuer à couper l'accès des terroristes aux sources de financement et aux substances NRBC[116], suivre leurs transactions[117].

Estimant que l'intérêt de créer un système de type SSFT n'était pas clairement démontré en raison du coût de création et d'entretien pour sécuriser la base de données contenant toutes les informations relatives aux transferts financiers des citoyens de l'UE, la Commission européenne a émis un avis défavorable à la création du SSFT[118].

L'accord PNR entre UE et États-Unis (avril 2012)

Des tensions justifiées par un niveau de protection des données personnelles inférieur aux États-Unis : champ d'application trop large, absence de proportionnalité dans la collecte des données, durée de conservation trop longue et droit de consultation discrétionnaire des données par les Américains,...

(113) Terrorist Finance Tracking Program.

(114) La SWIFT (*Society for Worldwide Interbank*), société de droit belge traitant de flux financiers autorisait depuis le 11 septembre 2001, l'accès à ses données aux autorités américaines dans le cadre du programme de lutte contre le terrorisme TFTP. Révélé en 2006, cet échange a été vivement dénoncé par le Parlement européen. SWIFT ayant décidé de rapatrier ses activités en Europe, un accord entre l'UE et les Etats-Unis devenait dès lors nécessaire pour pérenniser le transfert d'informations. Commence alors un long processus de négociation qui aboutit cependant à la signature d'un accord SWIFT II le 1er août 2010. Cet accord prévoit la création d'un TFTP interne à l'UE qui lui permettrait de mener ses propres requêtes et de n'envoyer aux États-Unis que les données relatives à une piste terroriste précise. EUROPOL est chargé d'étudier les requêtes américaines transmises à l'UE pour vérifier qu'elles répondent aux critères de finalité et de nécessité de protection des données personnelles. Enfin, il est prévu que la loi américaine traite les recours à égalité de traitement, quelle que soit la nationalité de requérant.

(115) Système européen de surveillance du financement du terrorisme.

(116) Nucléaire, radiologique, biologique et chimique.

(117) Communiqué européen IP/11/877 du 13 juillet 2011.

(118) Déclaration IP/13/1160 du 27 novembre 2013.

Au sein même de l'UE, la conception de la protection des données personnelles se heurte à des divergences de fond, souvent culturelles, qui nécessitent qu'elle soit uniformisée

Conception anglo-saxonne de « common law » versus conception « continentale » de protection des données personnelles :

- Le système anglo-saxon privilégie l'enjeu économique au détriment de la protection du consommateur (*privacy*) tandis que le monde européen accorde davantage d'importance à la protection des individus et de la vie privée.
- L'opposition sur la notion de propriété des données personnelles entre la vision de « *common law* » (le prestataire est propriétaire des données qu'il héberge) et la vision « continentale », notamment française (les données confiées à un tiers restent propriété du client).
- Une différence de conception de la responsabilité : en droit européen, le prestataire reste responsable de la confidentialité et de la sécurité des données.

La « fragmentation de la mise en œuvre de la protection des données personnelles au sein de l'UE » [119]

Le « consensus minimaliste »[120] des directives européennes a laissé une marge de manœuvre importante aux États membres qui s'est traduit par des retards de transposition importants et de grandes disparités dans les législations nationales : la directive 95/46[121] qui est le texte européen de référence en matière de protection des données personnelles, n'a été transposée qu'en 2004 dans la loi « informatique et libertés ». La directive-cadre 2008/977/JAI relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale devait, quant à elle, être transposée avant le 27 novembre 2010 par les États membres. En novembre 2011, seuls 14 États membres sur 26 l'avaient effectivement mise en œuvre dans leur législation. Neuf États membres (dont la France) ne l'avaient mise en œuvre que partiellement[122].

(119) Article 7 de la COM(2012)011 final du 25 janvier 2012.

(120) Voir RI 2009 titre V, paragraphe D.

(121) Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

(122) Rapport de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions fondé sur l'article 29, paragraphe 2, de la décision-cadre du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (COM/2012/012 final).

La nécessaire harmonisation des règles de protection des données personnelles au niveau européen

L'état des négociations au sein de l'UE

Initiées dès novembre 2010, les négociations pour la révision de la directive 95/46 CE ont abouti à une proposition, présentée le 25 janvier 2012[123]. Elle vise à élaborer un corpus unique de règles de protection des données personnelles valable pour l'ensemble de l'UE et fondée sur une approche plus souple et plus protectrice des individus, privilégiant la responsabilisation des acteurs et la notion de risque effectif. Le hasard du calendrier fait qu'elle correspond parfaitement au besoin de reprendre le contrôle des données personnelles dans le contexte de l'après-PRISM et du cyber-espionnage de la NSA.

(123) Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), COM(2012)11 final du 25 janvier 2012.

Comme le précise la Communication de la Commission au Parlement européen [124], le projet de règlement remplaçant la directive 95/46 CE est accompagné d'un projet de directive destiné à remplacer la directive 2008/977/JAI énonçant des règles relatives à la protection des données à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ainsi que d'activités judiciaires connexes [125]. Elle repose sur les mêmes fondements que ceux de 2008 mais tend à démontrer la volonté d'intégrer plus complètement dans la législation des États membres la conception européenne de la protection des données en matière pénale. Elle prévoit de nouvelles clauses qui tendent à rééquilibrer la relation entre sécurité et protection des données et introduit notamment les traitements nationaux dans le champ du texte (*article 2 de la proposition COM(2012)10*) bien que celui-ci comporte encore un certain nombre de dérogations en dépit des amendements qui relèvent considérablement le niveau de protection fixé initialement [126].

Les deux projets ont été adoptés par la commission LIBE [127] du Parlement européen le 21 octobre 2013 sous une forme plus protectrice que la version initiale, vote salué par le CEPD comme « *une étape importante vers une protection plus forte et plus efficace des données en Europe* ». Pour autant, les négociations sont au point mort depuis cette date, alors que d'aucuns envisageaient une présentation du projet aux États membres dès le premier semestre 2014.

Il importe de souligner que la CNIL s'est résolument mobilisée sur ce projet et que ses propositions ont souvent été entendues, notamment en ce qui concerne le contrôle des autorités de protection sur les demandes d'autorités administratives et judiciaires de pays tiers d'accéder aux données relatives à des citoyens européens.

Des objectifs ambitieux garantissant un haut niveau de protection de l'individu

Les principales propositions concourant à élever le niveau de protection des données personnelles sont les suivantes :

- Le renforcement des droits des personnes concernées (notion de consentement explicite, accès simplifié et « droit à l'oubli numérique »).
- La mise en avant du principe d'*accountability* [128] imposant de nouvelles obligations pour les responsables de traitements automatisés qui se trouvent de fait directement responsabilisés (analyse d'impact et de profilage, obligation de notification de violation des données, obligation de conclure des contrats de sous-traitance en cas d'externalisation du traitement des données). Cette mesure introduit un véritable changement de paradigme, puisque le détenteur de données ne doit désormais plus se contenter d'être en conformité avec la loi de 1978, mais s'assurer qu'il garantit en toute circonstance la sécurité des données qui lui sont confiées.
- Le renforcement des autorités nationales indépendantes de protection des données (pouvoir de sanction, contrôle des transferts de données hors UE).

(124) Rapport de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions : protection de la vie privée dans un monde en réseau. Un cadre européen relatif à la protection des données, adapté aux défis du XXIe siècle, COM(2012)9 final du 25 janvier 2012.

(125) Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, COM (2012)10 final du 25 janvier 2012.

(126) Projet de rapport sur la proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, COM(2012)0010 du 20 décembre 2012.

(127) Commission des libertés civiles, de la justice et des affaires intérieures.

(128) « Processus permanent et dynamique de mise en conformité d'une entreprise aux principes informatique et libertés grâce à un ensemble de règles contraignantes et de bonnes pratiques correspondantes menées en collaboration avec l'autorité de régulation » Mme FALQUE-PIERROTIN in Question d'Europe du 3 septembre 2012 (Fondation Robert Schuman).

– La mise en cohérence des règles au sein de l'UE permettant aux entreprises de ne plus être confrontées à des règles et à des autorités législatives nationales divergentes (notion d'établissement principal).

Le concept français « d'habeas corpus numérique »

Imaginé dès 2011 par l'ambassadeur François ZIMERAY qui le définit comme « *l'ensemble des règles et principes applicables au domaine des technologies de l'information et du stockage de données numériques, visant à rendre compatible le développement de la société de l'information avec le respect des droits individuels et des libertés fondamentales* », il fait référence au texte voté en 1679 par le Parlement britannique pour protéger l'individu de l'arbitraire de la fonction publique et de l'État.

Le concept, repris en octobre 2012 par la ministre déléguée à l'économie numérique dans la continuité des engagements électoraux du Président François HOLLANDE, devait se traduire par un projet de loi censé être présenté à l'Assemblée nationale au premier semestre 2013.

Le projet comporte un volet économique porté par la ministre déléguée à l'économie numérique et un volet traitant de la protection des données personnelles et de la vie privée des internautes porté par la ministre de la justice.

Ces mesures de protection destinées à restaurer la confiance des internautes ont d'ores et déjà été anticipées par la CNIL qui a instauré le label « audits de traitement ». Celui-ci permet aux entreprises de se distinguer par la qualité de leur service et constitue pour les utilisateurs un indicateur de confiance.

Le concept « d'*habeas corpus* numérique » pourrait avoir un écho au sein de l'UE au moment où les négociations sur l'harmonisation des règles de protection des données personnelles entre États membres semblent être au point mort.

Le député britannique travailliste Claude MORAES s'y est ainsi expressément référé dans son rapport[129] sur le programme de surveillance de la NSA (janvier 2014) adopté par la Commission LIBE en février dernier. Il évoque ainsi un « *habeas corpus* européen » décliné en plusieurs actions détaillées aux points 113 et 114 dudit rapport et va jusqu'à proposer de conditionner l'approbation de la prochaine Commission européenne à un engagement ferme des futurs commissaires sur ce sujet.

(129) Projet de rapport sur le programme de surveillance de la NSA, les organismes de surveillance dans divers Etats membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures (2013/2188(INI)).

Quelles conséquences pour les bases de données régaliennes et la protection des flux transfrontaliers de données personnelles sensibles ?

Le débat relatif à la protection des données s'est renforcé avec l'impact de PRISM dans l'opinion publique internationale et les relations avec les États-Unis se sont ponctuellement tendues. La suspension temporaire des négociations du partenariat transatlantique avec les États-Unis (TTIP[130]) en est le parfait exemple. La coopération internationale en matière de police et justice s'est considérablement structurée ces dernières années (INTERPOL, EUROPOL, EUROJUST, etc.). Cependant l'acceptabilité sociale des transferts de données sensibles nécessite l'existence de règles communes et d'autorités de contrôle

(130) Partenariat transatlantique de commerce et d'investissement : traité de libre-échange UE-USA.

dotées d'un réel pouvoir. Le dispositif de règles générales et spécifiques de protection des données personnelles actuellement en cours d'élaboration au sein de l'UE, s'appliquera probablement aux données personnelles traitées et échangées à des fins de détection et de prévention des infractions pénales. Ces négociations sont cependant actuellement au point mort en dépit de l'essor qu'elles avaient pris au lendemain de l'affaire PRISM.

De nombreux États avec lesquels l'UE ou ses États membres entretiennent une coopération policière et judiciaire ont une conception et une approche juridique différentes de la protection des données personnelles.

Dans un tel contexte, on peut légitimement se demander si la solution ultime ne résiderait pas dans une législation universelle de la protection des données personnelles dont le respect serait placé sous le contrôle d'autorités indépendantes dotées d'importants pouvoirs de sanction et pouvant coordonner leur action au niveau international. Elle mettrait fin à la fragmentation juridique de la protection des données qui rend les droits illisibles et complique l'exercice des droits des personnes. À ce jour, le concept semble utopique. Cependant, les bouleversements en cours du secret bancaire et de la transparence fiscale démontrent que des changements profonds de la réglementation et des pratiques de transfert de données sensibles sont à l'œuvre. Les données personnelles traitées et échangées à des fins de détection et de prévention des infractions pénales pourraient difficilement rester en marge de cette évolution.

* * *

BIBLIOGRAPHIE

BATHO, D et BENISTI, J-J : Rapport d'information sur les fichiers de police (24 mars 2009).

BATHO, D et BENISTI, J-J : Proposition de loi relative aux fichiers de police présentée le 7 mai 2009.

BATHO, D et BENISTI, J-J : Rapport d'information sur la mise en œuvre des conclusions de la mission d'information sur les fichiers de police (21 décembre 2011).

BAUER, A., et C. SOULLEZ, Les fichiers de police et de gendarmerie, Paris, Presses Universitaires de France, coll. « Que sais-je ? », 2009.

BAUER, A., et F. FREYNET, Vidéosurveillance et vidéoprotection, 2nd éd., Paris, Presses Universitaires de France, coll. « Que sais-je ? », 2012.

BAUER, A., et C. SOULLEZ, Une histoire criminelle de la France, Paris, Odile Jacob, 2012.

CNIL : Conclusions du contrôle des fichiers d'antécédents judiciaires du ministère de l'intérieur, rapport adopté en séance plénière le 13 juin 2013.

CNIL: Vie privée à l'horizon 2020 – paroles d'experts, in Cahier Innovation et Prospective n°1.

COMMISSION EUROPEENNE: Proposition de règlement du Parlement européen et du Conseil portant création d'une agence pour la gestion opérationnelle des systèmes d'information à grande échelle dans le domaine de la liberté, de la sécurité et de la justice, COM (2010)93 final du 19 mars 2010.

COMMISSION EUROPEENNE : Rapport de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions fondé sur l'article 29, paragraphe 2, de la décision-cadre du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (COM/2012/012 final).

COMMISSION EUROPEENNE : Rapport de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions : protection de la vie privée dans un monde en réseau. Un cadre européen relatif à la protection des données, adapté aux défis du XXIe siècle, COM(2012)9 final du 25 janvier 2012.

COMMISSION EUROPEENNE: Proposition de règlement du Parlement européen et du Conseil portant création d'un système d'entrée/sortie pour l'enregistrement des entrées et sorties des ressortissants de pays tiers franchissant les frontières extérieures des États membres de l'Union européenne, COM (2013)95 final du 28 février 2013.

CONSEIL CONSTITUTIONNEL : Décision n°2012-652 DC du 22 mars 2012 sur la loi relative à la protection de l'identité du 7 mars 2012.

CONSEIL DE L'UE : Décision-cadre 2008/977/JAI du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

CONSEIL DE L'UE : Décision-cadre 2006/960/JAI du 18 décembre 2006 relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne.

CONSEIL DE L'UE : Décision 2008/615/JAI du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière.

CONSEIL DE L'UE : Décision 2008/616/JAI du 23 juin 2008 concernant la mise en œuvre de la décision 2008/615/JAI relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière.

CONSEIL DE L'UE : Directive 2004/82/CE du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers.

CUSSON, M., B. DUPONT et F. LEMIEU, Traité de sécurité intérieure, Montréal, Hurtubise HMH, 2007, et Lausanne, Presses polytechniques et universitaires romandes, 2008.

CONTRÔLEUR EUROPEEN DE LA PROTECTION DES DONNEES : Communiqué de presse EDPS/2013/08 du 19 juillet 2013.

CUSSON, M., L'art de la sécurité. Ce que l'histoire de la criminologie nous enseigne, Lausanne, Presses polytechniques et universitaires romandes, 2011.

DELBECQUE, E., L'Insécurité, un scandale français, Paris, L'œuvre ed., 2012.

FALQUE-PIERROTIN, I : Quelle protection européenne pour les données personnelles ? in Question d'Europe n°250 du 3 septembre 2012.

EUROPOL: Proposal for a regulation of the european parliament and of the council on the European Union Agency for Law Enforcement Cooperation and Training (Europol), COM (2013) 173 final du 27 mars 2013.

GAUDIN, M., et BAUER, A., Livre blanc sur la sécurité publique, Paris, La documentation Française, 2011.

GAUDIN, M., G. GLIN, et C. SOULLEZ, Peur sur la ville ? Contributions pour un grand Paris de la sécurité, Les Cahiers de la FNAIM Paris Ile de France, n°1, FNAIM ed., 2012.

GROUPE DE TRAVAIL SUR LES FICHIERS DE POLICE ET DE GENDARMERIE (présidé par A.BAUER) : Rapport remis le 20 mars 2008 au ministre de l'Intérieur, de l'outre-mer et des collectivités territoriales.

H.C.F.D.C., Ouvrage collectif, Rapport Défense Civile 2008 : Constats et propositions pour une vision globale de la sécurité, Paris, HCFDC ed., 2009.

INTERPOL, Proceedings of the 16th International Forensic Science Symposium, Interpol General Secretariat, Lyon, 2010.

INTERPOL, Rapport annuel 2012, Secrétariat général d'Interpol, Lyon, 2013.

INTERPOL, Proceedings of the 17th International Forensic Science Managers Symposium, Interpol General Secretariat, Lyon, 2013.

INTERPOL : Règlement d'Interpol sur les traitements de données, résolution AG-2011-RES-07.

INTERPOL : Statut de l'OIPC-Interpol (I/CONS/GA/1956(2008).

LAMAN-LANGLOIS, S., et J.-P. BRODEUR, Les technologies de l'identification. Une note de recherche, Revue internationale de criminologie et de police technique et scientifique, n° 1, 2005, pp. 69-82.

LOWE, D., Distinctive image features from scale-invariant key points, InternatioInal journal of computer vision, 60(2), pp. 91-110, 2004.

MINISTERE DE L'INTERIEUR, DE L'OUTRE-MER ET DES COLLECTIVITES TERRITORIALES: Arrêté du 20 octobre 2009 portant création d'un groupe de travail sur l'amélioration du contrôle et de l'organisation des bases de données de police (JORF n°0244 **du 21 octobre 2009, page 17483, texte n°26).**

NAZAT, D., Insertion of cranio-facial x-ray files in the Interpol Notices: from the present to the future; a new way of thinking, Journal of Forensic Odonto Stomatology, Vol. 31, Sup. n°1, P. 110, Oct. 2013.

PARLEMENT ET CONSEIL EUROPEENS : Directive 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

PARLEMENT ET CONSEIL EUROPEENS : Proposition de règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), COM(2012)11 final du 25 janvier 2012.

PARLEMENT ET CONSEIL EUROPEENS : Proposition de directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, COM (2012)10 final du 25 janvier 2012.

PARLEMENT EUROPEEN-Commission des Libertés civiles, de la justice et des affaires intérieures : Projet de rapport sur la proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, COM(2012)0010 du 20 décembre 2012.

PARLEMENT EUROPEEN-Commission des Libertés civiles, de la justice et des affaires intérieures : Projet de rapport sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures (2013/2188(INI)).

RICARD, P et STROOBANTS, J-P : « OBAMA à Bruxelles, tour d'horizon des sujets qui fâchent » in Le Monde du 26 mars 2014.

SANCHEZ, J., PERRONNIN, F., MENSIK, T., and VERBEEK, J., Image classification with the Fischer vector: theory and practice, International journal of computer vision, 105(3), pp. 222-245, 2013.

SHARMA, G., UL HUSSAIN, S., and JURIE, F., Local higher-order statistics for texture categorization and facial analysis, Proceedings of the european conference on computer vision, Florence, 2012.

SIMONYAN, K., PARKHI, O., VEDALDI, A., and ZISSERMAN, A., Fisher vector faces in the wild, Proceedings of the british machine vision conference, Bristol, 2013.

TÜRK, A : La difficile quête d'un équilibre entre impératifs de sécurité publique et protection de la vie privée propos recueillis par Pierre PIAZZA in Cultures & conflits n°76, hiver 2009, page 115 et suivantes.

URVOAS, J-J et VERCHERE, P : Rapport d'information en conclusion d'une mission d'information sur l'évolution du cadre juridique applicable aux services de renseignement déposé à l'Assemblée nationale (14 mai 2013).

Annexe

LISTE DES PERSONNES RENCONTRÉES PAR LE GDS

MINISTÈRE DE L'INTÉRIEUR / POLICE NATIONALE / DIRECTION CENTRALE DE LA POLICE JUDICIAIRE

M. Georges BONNEFONT, commissaire divisionnaire, adjoint au chef de la division des relations internationales.

M. Fabrice CORSAUT, commissaire de police, chef de la Section Centrale de Coopération Opérationnelle de Police (SCCOPOL).

M. Bertrand MICHEL, lieutenant-colonel de gendarmerie, adjoint au chef de la SCCOPOL

Ministère de l'intérieur / gendarmerie nationale / Inspection générale de la Gendarmerie nationale.

Colonel Alexis JARAUD, chef de bureau du contrôle et de l'évaluation des fichiers.

SYNDICAT DE LA MAGISTRATURE

M. Eric BOCCIARELLI, magistrat, secrétaire général du syndicat.

M. Xavier GADRAT, magistrat, secrétaire national du syndicat.

COUR D'APPEL DE GRENOBLE

M. Paul MICHEL, procureur général, magistrat chargé de suivre la mise en œuvre et la mise à jour du TAJ.

MINISTÈRE DU BUDGET / DIRECTION GÉNÉRALE DES DOUANES ET DROITS INDIRECTS

M. Julien COUDRAY, Inspecteur principal des douanes, adjoint au chef du bureau de la lutte contre la fraude.

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE / ANSSI

M. Patrick PAILLOUX, Directeur général (au 12 février 2014).

COMMISSION NATIONALE « INFORMATIQUE ET LIBERTÉS »

M. Edouard GEFFRAY, Secrétaire général.

Professeur Alain BAUER, Professeur de criminologie et consultant en sécurité.

M. Frédéric DEBOVE, maître de conférences des universités, directeur de l'institut de droit et d'économie de l'Université Panthéon-Assas Paris II, président du groupe de travail sur l'amélioration du contrôle et de l'organisation des bases de données de police.

REPRÉSENTATION PERMANENTE DE LA FRANCE AUPRÈS DE L'UNION EUROPÉENNE

Olivier MORTET, conseiller pour la coopération policière auprès de la RP.

INTERPOL

Mme Mireille BALLESTRAZZI, inspectrice générale de la Police nationale, présidente du Comité exécutif d'INTERPOL.

M. Serge ANTONY, commissaire divisionnaire.

Mme Anna SVEDBERG, commissaire de police (Suède), auditrice de la 25e SNE de l'INHESJ.

ÉCOLE MILITAIRE
1 place Joffre
Case 39
75700 PARIS 07 SP
Tél.: 33 (0)1 76 64 89 00 – Télécopie : 33 (0)1 76 64 89 27
www.inhesj.fr