Les fichiers « POLICE »
Audition du SICP par la mission d'information de la commission des lois de l'Assemblée Nationale le 5 septembre 2018

ASSEMBLÉE NATIONALE

Commission des Lois constitutionnelles, de la législation et de l'administration générale de la République

Mission d'information relative aux fichiers mis à la disposition des forces de sécurité

Le SICP a été entendu par la Commission des lois de l'Assemblée Nationale, à la suite de l'audition de représentants des barreaux sur ce sujet des fichiers mis à disposition des forces de sécurité… Il allait donc de soi que notre intervention se focaliserait, d'une part, sur nos attentes, bien différentes de celles des avocats craignant les *abus de policiers oeuvrant sans grand contrôle*, notamment sur les besoins d'extension d'accès aux fichiers et de davantage d'interconnexions pour leurs interrogations **et d'autre part, sur des précisions quant à la gestion des habilitations et aux modes de contrôle d'accès et de consultations en vigueur au sein de l'institution.**

Nous vous livrons la production écrite qui a servi de support à nos échanges.

Les fichiers mis à disposition de la Police sont multiples et relèvent pour la plupart du Ministère de l'Intérieur, qu'ils soient alimentés par les forces de sécurité intérieure (TAJ, FOVeS, FSPRT, FIJAIT, API-PNR, FIJAI, FBS etc) ou par d'autres structures du ministère (préfectures - SIV, agences nationales ANTAI-ADOC , ANTS etc)

Notre attente principale ne concerne pas la possibilité de création de nouveaux fichiers mais plutôt celle d'une **extension de l'accès des policiers à d'autres fichiers** dépendant d'autres organismes publics dans la mesure où ces accès seraient de nature à faciliter leur action.

Il s'agirait notamment des fichiers de la sécurité sociale, des services fiscaux mais aussi des fichiers CAF dont les données sont à la fois denses (relatives aux profession & revenus, composition familiale, domiciliation, numéros de téléphone etc) et d'un niveau de fiabilité avéré (on peut avoir intérêt à fournir à dessein une adresse erronée sur un certificat d'immatriculation de véhicule mais nettement moins pour recevoir les diverses prestations).

Ce besoin d'extension d'accès est particulièrement notable dans le domaine de la police judiciaire

Une telle extension serait parfaitement concevable dès lors qu'elle interviendrait pour des besoins d'enquête réalisées sous la responsabilité de magistrats (instructeurs ou du Parquet), selon des habilitations strictes et contrôlées, avec la traçabilité complète des consultations effectuées.

Actuellement, les enquêteurs ont un accès très large mais indirect aux données de l'ensemble des fichiers existants, par le biais de réquisitions judiciaires. Ces modalités d'accès peuvent générer de longs délais de réponse du fait d'un traitement majoritaire des réquisitions sous forme d'échange-papier.

Non seulement ces délais de réponse aux réquisitions ralentissent le déroulement des enquêtes mais ils imposent encore de mobiliser du personnel, parfois à plein temps, pour exploiter les données reçues.

Même si la P.N.I.J (Plateforme Nationale des Interceptions Judiciaires) n'est pas une réussite opérationnelle aujourd'hui selon les enquêteurs qui la subissent, cette plateforme a au moins le mérite de moderniser l'accès aux données détenues par les opérateurs de téléphonie (réquisitions dématérialisées des enquêteurs et réponse quasi immédiate).

Dans le même ordre d'idée, le fichier A.D.O.C. (Accès aux Dossiers des Contraventions) centralisant les données du CNT de Rennes de l'agence nationale du traitement automatisé des infractions (ANTAI) permet depuis 2014 aux OPJ d'obtenir en temps réel les données issues des contraventions dites radar (vitesse/feu rouge/passage à niveau), incluant les clichés, comme celles issues de toutes les contraventions relevées par PVe.

Dans le domaine du renseignement, le développement d'accès des agents habilités aux fichiers d'autres administrations que le ministère de l'intérieur est également nécessaire.

Cela impliquerait de revoir l'encadrement réglementaire actuel des consultations de fichiers, notamment les finalités pour lesquelles une autorisation serait possible ainsi que la détermination limitative des agents habilités aux consultations. La lutte contre le terrorisme semble aujourd'hui pouvoir constituer une finalité commune ou plus largement la défense des institutions républicaines ou la garantie des intérêts fondamentaux de la Nation.

Dans le domaine des enquêtes administratives, le développement de la consultation des données des fichiers de sécurité intérieure est encore primordial.

De telles enquêtes conduisent principalement soit à la délivrance des agréments nécessaires à l'exercice de professions privées particulièrement sensibles dans le domaine de la sécurité (métiers de la sécurité privée avec le CNAPS, agrément aéroportuaire etc…) soit à l'entrée dans des fonctions publiques dans le cadre de concours, notamment pour les policiers et gendarmes, magistrats, douaniers, personnels pénitentiaires etc.

Les antécédents des personnes intervenant pour prendre en charge la sécurité de nos concitoyens doivent être connus et aujourd'hui, seuls le TAJ et, depuis 2005, le FPR. sont prioritairement consultés.[1]

Une avancée récente notable doit être soulignée : la création du fichier A.C.C.R.e.D. (Automatisation de la Consultation Centralisée de Renseignements et de Données), « *ayant pour finalité de faciliter la réalisation d'enquêtes administratives* », qui permet depuis un an[2] une automatisation de la consultation des fichiers accessibles et, le cas échéant, une « *consultation automatique simultanée* » de 7 systèmes de « traitement de données à caractère personnel *aux seules fins de vérifier si l'identité de la personne concernée y est enregistrée* » (dont TAJ, FPR, FSPRT et FOVeS).

Ce fichier pour les enquêtes administratives s'inscrit dans la droite ligne de ce que les policiers de tous grades attendent de manière globale : **une centralisation des données, une homogénéisation des fichiers, une automatisation des recherches et consultations, avec des réponses produites à l'instar de celles qui résultent de l'utilisation d'un moteur de recherches sur internet**.

Aujourd'hui chaque administration produit son propre système informatique et son modèle de fichier, alors qu'une ergonomie globale aurait due être imposée, ne serait-ce que pour éviter que les effectifs soient contraints de se former à l'utilisation de chaque fichier, quitte à rapidement oublier la formation relative aux fichiers qui ne sont utilisés que de manière épisodique… sachant que de nombreux fichiers restent aujourd'hui peu consultés par méconnaissance voire par oubli.

Aux esprits chagrins qui verraient dans cette demande de moteur de recherches une 1ère étape préalable à une interconnexion généralisée, nous répondrons que les modalités que nous préconisons ne seraient qu'une centralisation des éléments de renseignements que chaque agent est aujourd'hui habilité à recueillir, sans aucun croisement ni enrichissement de données en permettant simplement des interrogations multiples de fichiers distincts déjà accessibles.

L'automatisation des consultations simultanées serait une exploitation optimale des ressources déjà accessibles qui aurait en outre le mérite d'alléger la charge des effectifs concernés.

1-décret N°2005-1124 du 6 septembre 2005
2-Décret N°2017-1224 du 3 août 2017

Le besoin de davantage d'interconnexions

La simple évocation d'interconnexion des fichiers que souhaitent consulter les forces de sécurité provoque la peur irrationnelle de déviances, d'intrusion inacceptable, comme si notre Etat par ce biais allait devenir le big brother d'Orwell.

La crainte du contrôle de la CNIL , qui veille à protéger les données à caractère personnel et doit autoriser la création et les accès aux bases de données, a rendu tabou le sujet des interconnexions dans la conception des systèmes de traitement automatisé.

Pour autant, les avancées technologiques permettent d'envisager aujourd'hui l'interconnexion comme une amélioration de la sécurisation du traitement des données au lieu de la considérer comme un facteur de risque. Désormais, de nombreux fichiers comme applications utilisent des données issues de connexion avec d'autres fichiers et constituent indubitablement à la fois un progrès et une garantie de fiabilité.

A titre d'exemples, nous pouvons citer :

-Le système de traitement automatisé des infractions actuellement en vigueur pour les contraventions dématérialisées, principalement en matière de code de la route, permet que toute infraction relevée par le contrôle automatisé comme par PVe fasse l'objet d'un croisement avec les données d'autres fichier (FOVES, SIV) afin de vérifier qu'il s'agit du bon véhicule et qu'il n'a pas été signalé comme volé avant tout envoi d'avis de contravention à l'adresse du titulaire de la carte grise;

-Les effets bénéfiques de l'interconnexion du système C.A.S.S.I.O.P.E. et du T.A.J. sont reconnus (notamment le fait d'éviter des saisies multiples par le rédacteur de procédure, puis par un secrétariat judiciaire, puis par le service de documentation de la DCPJ et enfin par l'institution judiciaire) et servent de fondement au chantier actuellement en cours de la procédure pénale dématérialisée;

-L'interconnexion des fichiers F.I.JA.I.T.[1] et A.P.I. P.N.R. avec le F.P.R : ces interconnexions permettent dans le 1er cas de constater lors d'un contrôle policier qu'une personne ne respecte pas ses obligations (ex. d'une personne sous IQTF qui veut embarquer pour l'étranger) et dans le second cas, qu'un individu ayant pris un vol à destination de la France est recherché sur notre territoire.

Pour davantage d'interconnexions, des besoins existent et qui ne concernent pas seulement les policiers :

-**Plus d'interconnexion avec le FPR**, notamment pour la délivrance des CNI ou passeports afin que les personnels en charge de la délivrance de ces titres soient avisés par une alerte sur leur écran que le demandeur de papiers qu'ils ont dans leur bureau est recherché par les services de Police;

-**Interconnexion des FNAEG /FNAED** pour aboutir à une base unique des personnes signalisées (comme cela est proposé par la cour des comptes) afin de lutter contre le phénomène d'utilisations répétées d'alias par certains malfaiteurs auxquels les forces de sécurité intérieure sont désormais régulièrement confrontées;

-**Interconnexion avec certains fichiers spécifiques** : les spécialistes de la lutte anti terroriste souhaiteraient par exemple une connexion entre le FPSRT et HOSPY pour connaître les antécédents psychiatriques des individus à surveiller. En effet, afin de permettre une orientation du travail des services de renseignement, objet même du FSPRT, la connaissance des antécédents psychiatriques des personnes qui y sont inscrites est un élément d'appréciation de leur dangerosité qui mérite d'être pris en compte (au même titre que la connaissance des antécédents psychiatriques est acceptée pour toutes les demandes liées aux autorisations de détention et acquisition d'armes à feu).

L'interconnexion des fichiers peut être effectuée sans obligatoirement aboutir à la visibilité des données d'un fichier dans un autre et sans aucun enrichissement par croisement des bases de données. La simple notification de l'existence de données dans telle ou telle application peut être le biais minimaliste retenu, sans rien changer aux niveaux d'habilitation nécessaires pour se connecter aux différents fichiers concernés.

1-FIchier Judiciaire national automatisé des Auteurs d'Infractions Terroristes
2-Advanced Passenger Information – Passenger Name Record

La commission souhaitait connaître tant notre avis sur le bilan de la mise en œuvre du FSPRT que notre jugement de l'utilité et des limites des fiches S

Concernant le FSPRT, notre organisation n'a pas eu connaissance d'un bilan de ce fichier créé depuis 3 ans[1] ; cela ne signifie pas qu'il n'en existe pas au niveau des services utilisateurs mais plutôt qu'ils n'ont pas été communiqués à la parité syndicale s'ils ont été effectués.

Une doctrine d'emploi de ce fichier doit bientôt être produite (mais encore en cours d'élaboration avant l'été…).

Le rôle exclusif du FSPRT est de permettre l'orientation et la priorisation du travail des services de renseignement au regard de l'alimentation par les données de l'U.C.L.A.T. (Unité de Coordination de la Lutte Anti Terroriste), du C.N.A.P.R. (Centre National d' Assistance et de Prévention de la Radicalisation) ou encore des états- major de sécurité des préfectures.

L'ensemble de ces données constituent de simples éléments à valeur de renseignement quant au risque que peut présenter la personne concernée par les informations recueillies.

Ces éléments ne suffisent pas à indiquer ni même à préjuger d'une dangerosité effective d'une personne mais permettent seulement d'établir le risque qu'elle représente. C'est seulement en conséquence d'un risque estimé important que l'individu concerné fera l'objet d'une attention particulière des services de renseignement, donc d'une surveillance par nature discrète .

Concernant les fiches S (surveillance)

Ce dispositif déjà ancien n'a jamais eu d'autre but que de permettre aux services de sécurité intérieure ayant ciblé un individu comme objectif de **demander** à tout policier ou gendarme qui le contrôlerait de relever discrètement les renseignements circonstanciés le concernant (lieux de sa présence, véhicule dans lequel il se trouvait, personnes en sa compagnie etc).

Désormais, du fait d'une médiatisation à outrance de la fiche S, tout individu que l'on sait a posteriori qualifié de fiché S devient dans l'esprit du public une personne signalée que les services spécialisés auraient dû suivre dans ses mouvements quotidiens…

Médiatiquement, la signification de sa lettre S a été transformée, de « surveillance » discrète à «signalement» pour un suivi alors même que des milliers de personnes font aujourd'hui l'objet de fiches S dont elles sont censées ignorer l'existence.

L' inscription d'un individu au FPR. dans le cadre d'une fiche S relève de la seule appréciation des services de police et de renseignement et, de ce seul fait, il paraît difficilement concevable qu'elle ait d'autres effets que ceux qu'elle produit actuellement.

A nouveau, l'interconnexion du FPR pourrait être envisagée ici en ce qu'elle améliorerait potentiellement le recueil d'informations, notamment par le biais des personnels des préfectures qui seraient en contact avec l'individu lors de ses démarches administratives.

Selon le président de la commission, le sujet des incompréhensions des agents quant à ce qu'ils doivent faire face à un individu fiché qu'ils contrôlent a été préalablement évoqué par une organisation du CEA. Des efforts de qualification de conduite à tenir seraient peut être à envisager lors de l'alimentation de ces fiches.

1-Décret du 5 mars 2015 portant création d'un traitement automatisé de données à caractère personnel dénommé « Fichier de traitement des signalements pour la prévention de la radicalisation à caractère terroriste » (FSPRT) modifié par le décret du 2 août 2017

Le contrôle de l'usage des fichiers : la gestion des habilitations et la traçabilité des consultations

En raison de la **préoccupation constante de notre institution** de ne pas être suspectée de carence de surveillance dans l'exploitation des données de fichiers de sécurité intérieure ou de dévoiement des données accessibles, l'accent est mis fortement sur les conditions d'accès qui garantissent le respect tant de la protection des libertés individuelles que de la sécurité les données concernées comme des finalités réglementaires auxquelles lesdits fichiers sont consacrés.

La sécurisation recherchée résulte tout particulièrement des modes de gestion des habilitations (contrôle *a priori*) et des dispositifs de traçabilité des consultations effectuées (contrôle *a posteriori*).

En effet, **seuls les agents spécialement et nominativement habilités peuvent avoir accès aux fichiers**. Chaque agent prend connaissance à l'occasion de son habilitation de la sensibilité des informations auxquelles il aura accès, des finalités pour lesquelles il pourra le faire et des risques d'engagement de sa responsabilité personnelle, disciplinaire ou pénale en cas de manquement.

Cet engagement à respecter le caractère sensible et confidentiel des données et à respecter les préconisations de sécurité (codes d'accès /mots de passe /cartes agents : strictement personnels) est concrétisé par la signature d'une charte de sécurité des systèmes informatiques.

Il est à noter que, depuis le 1er janvier 2014, figure dans le code de déontologie l'article R 434-21 qui précise que :

« *… le policier ou le gendarme respecte et préserve la vie privée des personnes, notamment lors des enquêtes à caractère personnel. Il alimente et consulte les fichiers auxquels il a accès dans le strict respect des finalités et des règles propres à chacun d'entre eux, telles qu'elles sont définies par les textes les régissant, et qu'il est tenu de connaître.* »

L'habilitation est une condition nécessaire mais pas suffisante : pour chaque agent, l'accès ou non aux différents fichiers est conditionné par le **profil d'utilisateur** qui lui est associé selon différents critères cumulatifs qui déterminent l'étendue des droits d'accès :

- qualification judiciaire (qualité OPJ/APJ)
- direction d'emploi
- service d'affectation
- grade et rang (chef de service, chef d'unité, chef de groupe etc)
- missions affectées

La détermination de ces profils est propre à chaque direction d'emploi, bien souvent avec une classification au niveau national, ce qui empêche de contourner le périmètre des droits d'accès : application d'un code de profil Cheops national par les RSSI (Responsables de la Sécurité des Systèmes d'Information) selon les qualités et affectations précises.

Les droits d'accès des agents habilités peuvent même varier selon le cadre juridique dans lequel ils s'inscrivent lors de la consultation. Tel est le cas pour le TAJ.

Les accès sont notamment distincts selon qu'un même agent exerce soit dans le cadre d'une enquête judiciaire soit dans celui d'une enquête administrative, les données accessibles étant moins nombreuses dans cette dernière hypothèse.

L'utilisation bientôt généralisée de dispositifs d'identification forte de connexion (avec l'association carte agent / mot de passe) accroît encore les garanties entourant le respect du principe d'individualisation des habilitations d'accès.

Les agents habilités sont soumis à de multiples contrôles et toutes leurs consultations sont aujourd'hui traçables selon plusieurs modalités :

-**Contrôle par la hiérarchie**

Les chefs de service ont la possibilité d'examiner la nature et la fréquence des consultations opérées par leurs effectifs sans pour autant avoir accès aux données qui ont été à visualiser. Cela permet de contrôler l'adéquation des accès avec les missions qu'ils leur ont confiées et le respect du caractère personnel de l'habilitation (par exemple en s'assurant qu'aucun accès n'est réalisé avec les identifiants d'un agent en dehors de ses heures de service).

-**Contrôle par les responsables de la sécurité des réseaux informatiques du Ministère**

Les R.S.S.I., qui œuvrent de manière autonome à renforcer la vigilance et à diffuser les bonnes pratiques, ont la traçabilité des consultations de leur périmètre d'activité.

-**Contrôle par les services d'inspection**

Ces 3 services des directions générales (I.G.P.N. , I.G.G.N., D.G.S.I.) disposent d'accès distants pour contrôler le bon usage des fichiers.

Des audits sont régulièrement et aléatoirement réalisés dans les services qui peuvent procéder aux poursuites disciplinaires et judiciaires en cas de constatations de manquements imputables à certains effectifs voire impacter significativement l'appréciation de leurs responsables hiérarchiques.

-**Contrôle par une autorité indépendante**

La C.N.I.L. (Commission Nationale Informatique et Liberté) peut conduire des missions de contrôle auprès des responsables des traitements sur place, sur pièce ou en ligne qui, si les dysfonctionnements avérés sont graves peuvent aboutir à des sanctions pécuniaires allant jusqu'à 300.000 € ou à une dénonciation à l'autorité judiciaire dans le cadre d'un article 40 du code de procédure pénale.

Les sanctions

Les manquements constatés engagent non seulement la responsabilité disciplinaire des agents (vis-à-vis de leurs obligations déontologiques) mais également pénale.

Le détournement de données à caractère personnel de leur finalité est en effet puni par l'article L 226-1 du code pénal de :
5 ans d'emprisonnement et de 15.000 euros d'amende.

Les fichiers de sécurité intérieure font donc l'objet d'un contrôle strict dont l'efficacité n'est pas contestée par les autorités indépendantes telle que la CNIL.

Lorsque des effectifs de Police ne respectent pas les règles de consultations des fichiers auxquels ils ont accès, les sanctions infligées sont sévères et conduisent parfois administrativement à leur révocation et pénalement à leur incarcération, notamment en cas de communication de données à des tiers qui n'avaient pas à en connaître.