L'accès aux grandes bases de données policières et judiciaires

Fichage, bases de données, fichiers de données voici des termes qui évoquent souvent pour certains l'image bien connue de « *Big Brother* » et la crainte qui s'accompagne d'être répertorié ou surveillé dans ses moindres faits et gestes. Mais avant de paniquer, il semble opportun de se pencher sur ce que veulent vraiment dire ces termes.

Ils recouvrent plus ou moins la même réalité. Si l'on souhaite faire une distinction, nous pourrions avancer que le fichage est l'action de recueillir et conserver des renseignements concernant des personnes. Ces données étant conservées dans des bases ou fichiers de données.

L'article 2 c) de la Directive 95/46/CE du 24 octobre 1995 définit les fichiers de données comme « *tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique* ».

Cette définition pouvant recouvrir un grand nombre de domaines, nous nous intéresserons dans ce développement à la question des bases de données policières et judiciaires qui se réfèrent donc à des missions régaliennes.

Ainsi, dans le cadre de ces missions étatiques, certaines données peuvent être enregistrées et constituent dès lors un « traitement de données à caractère personnel » tel que définit à l'article 2 b) de la Directive 95/46/CE du 24 octobre 1995 c'est-à-dire « *toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que 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* ».

Ajoutons que, à partir du moment où il y a traitement de données personnelles dans le cadre des missions judiciaires et policières des agents de l'Etat, il y aura nécessairement soumission aux obligations posées par la loi informatique et libertés du 6 janvier 1978. L'article 39 4° de cette loi dispose que « *toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir, la communication sous une forme accessible des données à caractère personnel qui la concerne ainsi que de toute information disponible quant à l'origine de celle ci* ». Les personnes physiques disposent donc d'un droit d'accès direct à leurs données personnelles.

Néanmoins, les données policières et judiciaires sont des données sensibles, c'est pourquoi la loi informatique et libertés de 1978 les soumet à un régime juridique dérogatoire, atténuant le principe du droit d'accès direct aux données.

Notons, que la notion de donnée sensible est visée à l'article 8 de la directive 95/46/CE relatif aux « *traitements portant sur des catégories particulières de données* ». Cet article pose une interdiction de principe pour certains traitements concernant les données sensibles, puis il prévoit des exceptions, notamment en son 5° qui permet le traitement de données issues des missions de la police et de la justice.

1. La question de la déclaration de ces bases de données et de leur accès

Déclaration

Un bref rappel sur la CNIL : c'est la Commission nationale de l'informatique et des libertés qui est une autorité administrative indépendante française (AAI). Elle a pour mission de veiller à ce que l'informatique soit au service du citoyen et ne porte atteinte ni à l'identité humaine, ni aux Droits de l'Homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Cette autorité administrative indépendante a été créée par la loi n°78-17 du 6 janvier 1978.

Outre la création de la CNIL, cette loi, en son chapitre IV pose les formalités préalables à la mise en œuvre des traitements.

Le principe, posé à l'article 22, est celui d'une « simple » déclaration auprès de la CNIL, mais comme tout principe, celui-ci comporte une exception s'agissant des données policières et judiciaires qui, du fait de leur caractère sensible nécessitent un encadrement plus spécifique.

Les articles 25 à 27 de la loi de 1978 établissent le régime juridique préalable à la mise en œuvre des traitements de ces données.

L'article 25 8° pose un régime d'autorisation à la CNIL concernant « *les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes* ».

L'article 26 dispose que sont soumis à un régime d'autorisation par arrêté ministériel après avis motivé et publié de la CNIL : « *les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat et qui intéressent la sûreté de l'État, la défense ou la sécurité publique ou qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté* »

Enfin, l'article 27 établit un régime d'autorisation par décret en Conseil d'État pris après avis motivé et publié de la CNIL pour : « *1° Les traitements de données à caractère personnel mis en œuvre pour le compte de l'État, d'une personne morale de droit public ou d'une personne morale de droit privé gérant un service public, qui portent sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques ; 2° Les traitements de données à caractère personnel mis en œuvre pour le compte de l'État qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes* ».

Accès

Après avoir évoqué la mise en place de telles bases de données policières et judiciaires, il convient de se poser la question de l'accès à ces dernières. Comme nous l'avons vu précédemment, le principe est celui de l'accès direct, mais il s'atténue lorsque ces données sont collectées pour des fichiers policiers ou judiciaires.

En effet, dans ces circonstances, l'accès se fera de manière indirecte selon le régime prévu aux articles 41 et 42 de la loi informatique et liberté de 1978.

D'après ce régime, le droit d'accès indirect est strictement personnel et concerne, les fichiers intéressant la sûreté de l'État, la défense et la sécurité publique ainsi que certains fichiers du ministère de la Justice.

Dans ces hypothèses, il reviendra à la CNIL et non pas au responsable de traitement de gérer les demandes de droit d'accès indirect. Néanmoins, cette autorité ne gérant pas ces fichiers, elle ne peut avoir connaissance des personnes répertoriées.

Le droit d'accès ainsi que de rectification sera exercé par un magistrat de la Commission pour le compte de la personne qui en fait la demande. A cette occasion, le magistrat pourra demander, en cas d'informations incomplètes, obsolètes ou non conforme aux textes régissant le fonctionnement des fichiers, que celles-ci soient complétées, mises à jour ou encore supprimée.

2. Quelques exemples de bases de données policières et judiciaires en France

Aux anciennes bases sous format papier se sont substituées celles au format numérique. Le contenu a également changé, les données ne sont plus uniquement administratives mais peuvent aussi être désormais biologiques.

Les évolutions technologiques ne sont pas sans lien avec l'augmentation du nombre de fichiers policiers et judiciaires, mais s'ajoute également à cela une volonté accrue de surveillance et le changement de la fonction pénale se centrant toujours davantage sur la question de la dangerosité des délinquants.

Quelques chiffres :
•361 fichiers (Rapport Bauer de 2007)
•450 fichiers (Rapport Bauer de 2008)
•584 fichiers (Rapport Batho & Bénesti de 2009)

Face à ce grand nombre de fichiers, nous ne sélectionnerons, afin de conserver l'attention de nos lecteurs, qu'une infime partie d'entre eux, à savoir le **STIC** et le **FNAEG**.

STIC : Système de traitement des infractions constatées

Issu du plan Joxe de 1985, le STIC a été définitivement mis en place en 1998, puis officialisé en 2001.

Ce fichier répertorie des informations provenant des comptes rendus d'enquêtes effectuées après l'ouverture d'une procédure pénale. Il recense à la fois les personnes mises en cause dans ces procédures et les victimes des infractions concernées. Il vise à faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs. Il permet également d'élaborer des statistiques.

Ce fichier contient diverses informations concernant les personnes mises en cause, les victimes et les faits objets de l'enquête.

La durée de conservation des données varie en fonction de la qualité de la personne inscrite. Par principe, les informations concernant le mis en cause majeur sont conservées vingt ans, pour ce qui est d'un mineur, la conservation est de cinq ans et enfin, les informations des personnes victimes sont conservées pour un maximum de quinze ans.

Pour ce qui est de la communication ou de la rectification des données, toute personne identifiée dans le STIC en qualité de victime peut s'opposer à la conservation, dans ce fichier, d'informations nominatives la concernant dès lors que l'auteur des faits concernés a été condamné de façon définitive. Pour obtenir la suppression de la fiche correspondante, il faut adresser une demande, accompagnée d'une attestation du tribunal ayant condamné l'auteur des faits, à la Direction générale de la police nationale au Ministère de l'Intérieur.

Une personne identifiée en qualité de personne mise en cause peut demander la rectification ou la suppression de la fiche la concernant en s'adressant au procureur de la République territorialement compétent ou au procureur général près la cour d'appel en cas de décision prononcée par cette juridiction, dans des cas restrictivement prévus.

Quelques chiffres :
En décembre 2008, le STIC recensait :
- 36 500 000 de procédures
- 37 911 000 infractions
- 5 552 313 individus mis en cause
- 28 329 276 victimes
- 10 millions d'objets

D'après le bilan 2009 des vérifications du STIC par la CNIL, sur les 1 385 vérifications effectuées par la CNIL dans le STIC dans le cadre du droit d'accès indirect, 683 personnes étaient fichées dans le STIC en tant que mises en cause.

17 % des fiches des personnes mises en cause ont été supprimées du fichier ;
20 % des fiches étaient rigoureusement exactes ;
63 % des fiches ont été modifiées.
Le taux d'erreurs est de 25%.

FNAEG : Fichier national des empreintes génétiques

Le FNAEG a été créé en juin 1998, par la loi Guigou qui fait suite à l'arrestation en mars 1998 de Guy Georges, identifié « grâce à son ADN ».

Ce fichier à pour objectif de faciliter l'identification et la recherche des auteurs d'infractions à l'aide de leur profil génétique ainsi que de personnes disparues à l'aide du profil génétique de leurs descendants ou de leurs ascendants.

Le FNAEG centralise les empreintes génétiques de personnes non identifiées par les prélèvements effectués sur les lieux d'une infraction et celles de personnes identifiées condamnées ou mises en cause. Ces empreintes sont complétées par d'autres informations telles que l'identité de la personne, le service ayant procédé à la signalisation, la date et le lieu d'établissement de la fiche ainsi que la nature de l'affaire et la référence de la procédure.

L'enregistrement de ces empreintes ou traces est réalisé dans le cadre d'une enquête pour crime ou délit, d'une enquête préliminaire, d'une commission rogatoire ou de l'exécution d'un ordre de recherche délivré par une autorité judiciaire.

Ces données sont conservées 40 ans pour les personnes définitivement condamnées, les personnes décédées, les personnes disparues et les traces ou 25 ans pour les personnes mises en cause, sauf irresponsabilité pénale.

Au 30 janvier 2010, le FNAEG contenait les profils génétiques de 1 257 182 individus dont :
- 972 042 personnes mises en causes
- 285 140 personnes condamnées
- 64 774 traces non identifiées

En 2010, Le rapport de l'activité des services et de gendarmerie effectué par le Ministère de l'Intérieure considère que, près de 2,65% de la population française.

Pour ce qui est des données contenues dans ces deux fichiers, il est possible d'en demander la communication ou la rectification en s'adressant au directeur central de la police judiciaire au ministère de l'intérieur.

En cas de refus d'effacement, il est possible de former un recours devant le juge des libertés et de la détention, puis devant le Président de la chambre de l'instruction en cas de nouveau refus.

Anouk Arzur

Jeanne Bonacina Lhommet

SOURCES

- http://www.inhesj.fr/fichiers/ondrp/Bulletinannuel/dgpn.pdf
- http://www.senat.fr/rap/a09-106-11/a09-106-114.html
- http://fr.wikipedia.org/wiki/Fichage_en_France
- http://questions.assemblee-nationale.fr/q13/13-68468QE.htm
- http://www.cnil.fr/

- 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.

- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée le 6 août 2004.

- Article 41 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée le 6 août 2004 :

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

- Article 42 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée le 6 août 2004 :

« *Les dispositions de l'article 41 sont applicables aux traitements mis en œuvre par les administrations publiques et les personnes privées chargées d'une mission de service public qui ont pour mission de prévenir, rechercher ou constater des infractions, ou de contrôler ou recouvrer des impositions, si un tel droit a été prévu par l'autorisation mentionnée aux articles 25, 26 ou 27* ».