ASSEMBLÉE NATIONALE

13ème législature

fichiers informatisés

Question écrite n° 20299

Texte de la question

Mme Chantal Robin-Rodrigo attire l'attention de Mme la ministre de l'intérieur, de l'outre-mer et des collectivités territoriales sur l'utilisation des fichiers confidentiels de la Police Nationale. Dernièrement un commissaire de police, chef de la brigade des fraudes aux moyens de paiement, soupçonné de corruption, a fait l'objet d'une enquête de l'IGS pour violation du secret professionnel et corruption active et passive d'une personne dépositaire de l'autorité. Il aurait monnayé a des tiers des informations recueillies dans le fichier STIC (Système de Traitement des Infractions Constatées). Ce fichier comme tous les fichiers relatifs aux personnes sont sous le contrôle de la Commission Informatique et Liberté. Or de l'aveu même de son Président « de nombreux fonctionnaires ont la possibilité de consulter le STIC ; la vérification de leurs motivations, obligatoires, est aléatoire. Les risques de dérapage pourraient être considérablement réduits si une vérification systématique avait lieu, cela dissuaderait. » De plus, ce fichier contiendrait des informations concernant des personnes relaxées. L'enquête menée par la CNIL en 2004 avait révélé un taux d'erreur de 25 %. Elle lui demande donc quelles mesures urgentes elle compte prendre afin que de tels abus ne se reproduisent pas.

Texte de la réponse

Le système de traitement des infractions constatées (STIC) mis en oeuvre par les services de police a pour finalité de permettre aux services enquêteurs d'exploiter les informations contenues dans les procédures judiciaires déjà réalisées. Le fonctionnement de ce fichier s'accompagne des garanties nécessaires à la protection des libertés individuelles, fixées par le décret du 5 juillet 2001 en portant création. Le traitement des données à caractère personnel est opéré sous le contrôle du procureur de la République et d'autres garanties proviennent, par exemple, des dispositions relatives à l'alimentation du fichier et à l'effacement, l'ajout ou la rectification des données à caractère personnel, effectués à la demande notamment du procureur de la République ou du mis en cause. S'agissant de l'exactitude des informations contenues dans ce fichier, l'article 6 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés impose au gestionnaire du traitement d'enregistrer des données exactes, complètes et mises à jour. Cette obligation repose sur les services de police, cependant largement tributaires des informations transmises par les parquets et relatives aux suites réservées à la procédure. Le procureur de la République doit en effet transmettre aux services de police les décisions judiciaires favorables aux mis en cause (décisions de non-lieu, de relaxe, d'acquittement et de classement sans suite) pour leur permettre une mise à jour du STIC. À cet égard, 19 397 suites judiciaires ont été prises en compte en 2007, aboutissant à 8 456 effacements et 10 941 ajouts de mentions. Par ailleurs, le ministère de la justice renouvellera prochainement son système d'informations, grâce à l'application informatique CASSIOPEE. Une passerelle informatique devrait ainsi être mise en oeuvre en 2008 pour favoriser les échanges entre services d'enquête et tribunaux et faciliter les opérations de mise à jour. Les informations enregistrées dans le STIC sont donc vérifiées et une attention particulière portée à leur mise à jour. Ainsi, en 2007, 7 743 fiches ont-elles été effacées ou corrigées suite à la demande d'un magistrat ou aux observations formulées après exercice du droit d'accès indirect. Ces modifications et suppressions s'ajoutent à l'apurement automatique des mentions atteintes par la prescription (1,3 million lors de l'installation de la chaîne d'apurement

automatique, 167 222 en 2007 en régime normal). Au total, les dysfonctionnements demeurent limités au regard du nombre de procédures enregistrées dans la base nationale du STIC (34 134 536 en 2007). Les particuliers peuvent en outre exercer leur droit d'accès indirect auprès de la commission nationale de l'informatique et des libertés (CNIL) en application de l'article 41 de la loi du 6 janvier 1978 précitée. S'agissant du « taux d'erreurs de 25 % » évalué par la CNIL en 2004, il convient d'observer que le STIC a depuis évolué et dispose désormais d'un module d'apurement automatique des données permettant une mise à jour plus efficace du fichier. Par ailleurs, les grilles d'analyse auxquelles recourt la CNIL pour ses statistiques ne correspondent pas exactement à celles utilisées par le ministère de l'intérieur. À cet égard, conformément à l'une des recommandations formulées par le groupe de travail sur les fichiers de police et de gendarmerie (dit groupe Bauer) en novembre 2006, le ministère de l'intérieur et la CNIL ont mis en place un groupe de travail destiné à harmoniser leurs méthodes statistiques. Concernant l'accès au STIC, il est soumis à de strictes conditions et contrôlé. L'article 5 du décret du 5 juillet 2001 énumère limitativement les catégories de personnels pouvant le consulter (notamment policiers et gendarmes individuellement désignés et spécialement habilités, magistrats pour les recherches relatives aux infractions dont ils sont saisis). La consultation est autorisée pour les seules finalités fixées à ce fichier par le décret du 5 juillet 2001 (constater les infractions pénales, en rassembler les preuves et en rechercher les auteurs, exploitations statistiques) pour les besoins des enquêtes judiciaires. Les personnels investis de missions de police administrative ont un accès restreint et strictement encadré pour les seules enquêtes listées par un décret en Conseil d'Etat. En 2007, 97 597 personnes étaient habilitées à accéder au STIC dans le cadre d'une mission de police judiciaire, de police administrative ou de fonctions de gestion du fichier. Les contrôles d'accès au STIC résultent aussi des modalités concrètes de sa consultation. L'accès à ce fichier, comme à la plupart des applications de police, s'effectue en effet par le portail CHEOPS (circulation hiérarchisée des enregistrements opérationnels de la police sécurisés), dont les règles de fonctionnement permettent de limiter les accès, de maîtriser et de connaître précisément les personnes autorisées à consulter le fichier. Le passage obligatoire par ce portail d'accès constitue une importante garantie. La traçabilité des interrogations est assurée et les traces de toute intervention effectuée conservées cinq ans. Le système CHEOPS permet en effet de déterminer les connexions des utilisateurs au moyen de plusieurs paramètres, dont le matricule du fonctionnaire concerné, le nom « IP » de la machine sur laquelle s'est faite la connexion, sa date et son heure. Ce suivi des traces de connexion permet en particulier de répondre aux demandes de l'autorité judiciaire ou administrative lorsque des soupçons de consultation abusive existent. Par ailleurs, des contrôles sont effectués périodiquement par la direction de l'administration de la police nationale, gestionnaire de CHEOPS, ainsi qu'un suivi statistique du volume de connexions mensuelles, permettant de mener des vérifications a priori sur l'usage des fichiers. Le gestionnaire de CHEOPS procède en outre à des audits ponctuels et aléatoires sur les connexions aux applications effectuées par les services. En application de la loi du 6 janvier 1978 précitée, la CNIL peut en outre effectuer des contrôles sur place et sur pièce. Lorsque des fonctionnaires utilisent des informations de ce fichier à des fins personnelles et non prévues par les textes, les services d'inspection (IGPN) et le cas échéant l'autorité judiciaire sanctionnent ces dérives. Le nombre d'infractions liées à l'utilisation abusive de fichiers à des fins personnelles demeure toutefois limité. À titre d'exemple, l'IGPN n'a ainsi été saisie depuis 2000 que de 39 enquêtes (dont 22 relatives au STIC), soit une moyenne de 5 par an. Lorsque les faits sont avérés, ils entraînent de manière générale, sans préjudice des sanctions judiciaires, un blâme ou une exclusion temporaire des fonctions et conduisent, dans les cas les plus graves, à des révocations, des déplacements d'office ou des mises en fin de contrat s'agissant des adjoints de sécurité. Le ministère de l'intérieur attache la plus grande importance au strict respect des règles de consultation des fichiers. Un rappel écrit a ainsi été adressé à l'ensemble des services de police en mai 2006, pour souligner la nécessité d'un respect rigoureux et permanent des règles de sécurité (installations et contrôles d'accès, formation et contrôle du personnel à l'application des mesures de sécurité, protection des documents et des supports, etc.).

Données clés

Auteur : Mme Chantal Robin-Rodrigo
Circonscription : Hautes-Pyrénées (2e circonscription) - Socialiste, radical, citoyen et divers gauche
Type de question : Question écrite
Numéro de la question : 20299

Version web : https://www.assemblee-nationale.fr/dyn/13/questions/QANR5L13QE20299

Rubrique : Droits de l'homme et libertés publiques
Ministère interrogé : Intérieur, outre-mer et collectivités territoriales
Ministère attributaire : Intérieur, outre-mer et collectivités territoriales

Date(s) clée(s)

Question publiée le : 8 avril 2008, page 2969
Réponse publiée le : 17 juin 2008, page 5206