Centre Français de Recherche sur le Renseignement

TRIBUNE LIBRE N°11

LA SURVEILLANCE PREVENTIVE EN SUISSE EN 2010

Sylvain Métille

Sylvain Métille est avocat suisse et docteur en droit. Il est l'auteur de l'ouvrage Mesures techniques de surveillance et respect des droits fondamentaux, en particulier dans le cadre de l'instruction pénale et du renseignement *(2010), ainsi que de nombreuses contributions dans des revues juridiques. Il alimente également régulièrement un blog (ntdroit.wordpress.com) consacré à l'actualité juridique et plus particulièrement aux technologies de l'information et à la protection de la sphère privée. Il est actuellement Visiting Scholar à l'Université de Californie à Berkeley (Berkeley Center for Law and Technology).*

La surveillance préventive est l'une des activités essentielles des services de renseignement. Elle a pour principale caractéristique qu'elle ne s'applique pas à la poursuite d'infractions pénales qui auraient été commises, mais qu'elle vise à la détection d'un danger ou d'une menace pour la sécurité du pays. Elle inclut également la recherche d'informations politiques, économiques et militaires. La personne qui est visée par ces mesures techniques de surveillance n'est donc pas l'objet d'une procédure judiciaire et elle ne jouit pas des droits réservés à un prévenu au sens de la procédure pénale. Elle n'est la plupart du temps même pas soupçonnée d'avoir commis ou de vouloir commettre une infraction au sens du droit pénal, mais sa personne ou ses activités pourraient représenter un risque pour la sécurité intérieure.

En Suisse, la surveillance préventive civile repose essentiellement sur la Loi fédérale instituant des mesures visant au maintien de la sûreté intérieure (LMSI[1]) et consiste en la recherche d'informations. La LMSI prévoit également d'autres mesures particulières comme le contrôle de sécurité pour les personnes travaillant pour le compte de l'Etat et ayant accès à des informations sensibles, la protection des bâtiments de la Confédération et des parlementaires, magistrats et agents de la Confédération particulièrement exposés, ainsi que les mesures contre la violence lors de manifestations sportives.

La recherche d'informations se compose essentiellement de l'exploitation de sources accessibles au public, des informations transmises par d'autres autorités et la

[1] http://www.admin.ch/ch/f/rs/c120.html

surveillance de lieux publics et librement accessibles. Le Service de renseignement de la Confédération (SRC[1], et jusqu'à fin 2009 le Service d'analyse et de prévention de la Confédération) reste très discret sur ses activités. La LMSI mentionne différents types de surveillance comme les opérations préventives, les programmes de recherche préventifs, les programmes d'examen et la liste d'observation. Pour simplifier, on peut dire qu'il s'agit de cas différents lors desquels la surveillance est opérée et les principes-cadres concernant la manière dont elle doit être conduite.

LES MOYENS TECHNIQUES

Les moyens techniques actuellement autorisés

La loi suisse ne permet actuellement pas de procéder à une surveillance aussi intrusive à titre préventif que dans le cadre d'une enquête pénale par exemple. La surveillance de la correspondance par poste et télécommunication, la surveillance des relations bancaires, ou la surveillance de lieux qui ne sont pas librement accessibles au moyen d'appareils techniques ne sont ainsi pas permises par la LMSI, de même que la perquisition d'un système informatique. Si les mesures portant le plus atteinte à la sphère privée ne sont pas autorisées, c'est surtout parce qu'à ce stade, aucune infraction ou acte préparatoire à la commission d'une infraction au sens pénal n'a été commis. Une atteinte à la sphère privée, comme cela est toléré dans d'autres pays, n'est pas admissible en Suisse. En revanche, si une infraction pénale a été commise ou est en cours de commission (comme la participation à une organisation criminelle ou la commission d'actes préparatoires délictueux), la situation est différente. On se retrouve alors dans le cadre d'une enquête pénale classique confiée à la police judiciaire et dans laquelle les mesures de surveillance précitées peuvent être autorisées par un magistrat.

Si l'Etat ne bénéficie a priori pas du droit de procéder à une surveillance préventive de manière beaucoup plus étendue qu'une personne privée, il bénéficie en revanche de compétences nettement plus larges en matière de traitement des informations dont il dispose. Les services de renseignement suisses peuvent établir et traiter des profils de personnalité des individus soupçonnés d'avoir un comportement représentant une menace pour la sûreté du pays. Ils peuvent également traiter d'autres données sensibles s'il ressort d'informations existantes que ces données ont un lien avec la préparation ou l'exécution d'activités terroristes, d'espionnage ou d'extrémisme violent, ou ont un lien avec le crime organisé.

Pas d'autres moyens à court terme

Un projet de révision de la LMSI (appelé LMSI-II) a débuté en 2006, par la publication d'un avant-projet de loi par un office de l'administration fédérale, ce qui est plutôt inhabituel. Cette révision prévoyait pour les autorités et les transporteurs commerciaux un devoir de transmission de certaines informations, la possibilité pour les services de renseignement de surveiller la correspondance par poste et télécommunication, ainsi que la possibilité d'utiliser des systèmes de surveillance techniques dans des lieux non accessibles au public.

[1] http://www.vbs.admin.ch/internet/vbs/fr/home/departement/organisation/ndb.html

Les deux chambres du parlement fédéral (Conseil national et Conseil des Etats) ont choisi de renvoyer le projet au Conseil fédéral le 28 avril 2009. Le 27 octobre 2010, le Conseil fédéral a adopté une nouvelle mouture du projet LMSI-II. Cette seconde variante remaniée renonce à l'utilisation de moyens spéciaux d'acquisition d'informations tels que la surveillance de la correspondance ou l'observation de lieux non librement accessibles, y compris à l'aide d'appareils techniques de surveillance. Le Conseil fédéral suisse a déjà annoncé qu'il n'abandonnait pas complètement cette idée et que la nécessité d'avoir recours à de telles mesures serait réévaluée dans le cadre de la future loi unifiée sur les services de renseignement ,dont le projet est annoncé pour 2012.

LE CONTROLE DES ACTIVITES DE SURVEILLANCE

Les organes de contrôle

On trouve principalement trois organes différents qui interviennent dans le contrôle de l'activité de surveillance effectuée par les services de renseignement civils en Suisse : la Surveillance SR, le Préposé fédéral à la protection des données et à la transparence (PFPDT) et la Délégation des Commissions de gestion des Chambres fédérales (DélCdG).

La surveillance administrative appartient au Conseil fédéral et est actuellement exercée par le Département fédéral de la Défense, de la Protection de la population et des Sports (DDPS), plus précisément par la Surveillance SR, un organe composé de trois personnes et rattaché à l'état-major du chef du Département. S'agissant d'un organe de contrôle interne, les rapports de la Surveillance SR ne sont pas publics.

Le Préposé fédéral à la protection des données et à la transparence (PFPDT[1]) est un organe indépendant (mais rattaché administrativement à la Chancellerie fédérale) chargé de surveiller de manière générale le respect par les organes fédéraux suisse des normes relatives à la protection des données. Il a encore d'autres compétences en matière de protection des données traitées par des privés ou au sujet de l'application par l'administration suisse du principe de transparence. En matière de renseignement, il intervient surtout dans le cadre du droit d'accès indirect, lorsqu'un individu lui demande de vérifier que des données éventuellement traitées à son sujet, dans le système d'information du Service de renseignement de la Confédération SRC (en abrégé ISIS, soit la principale base de données des services de renseignement), le sont conformément au droit en vigueur. Dans ce cas, le Préposé a accès à l'ensemble des informations liées à chaque inscription concernant la personne en question. Cette personne n'aura toutefois pas accès aux données, mais le Préposé lui transmettra une réponse standard confirmant qu'aucune donnée la concernant n'a été traitée illégalement ou que, dans le cas d'une éventuelle erreur dans le traitement des données, il a adressé la recommandation d'y remédier au Service de renseignement de la Confédération.

La Délégation des Commissions de gestion des Chambres fédérales (DélCdG) exerce la haute surveillance parlementaire. Elle est composée de membres du Conseil national et du Conseil des Etats et a pour mandat de contrôler en détail les activités dans les domaines de la sécurité de l'Etat et des services de renseignement.

Elle dispose des mêmes droits d'investigation qu'une commission d'enquête parlementaire (CEP) et peut notamment accéder à de nombreux documents couverts

[1] http://www.edoeb.admin.ch/index.html?lang=fr

par le secret de fonction ou le secret militaire, ainsi que procéder à des auditions.

Les Commissions de gestion et la Délégation des Commissions de gestion des Chambres fédérales publient chaque année un rapport dont une partie concerne l'activité des services de renseignement. Lorsqu'elle est confrontée à des problèmes ou des questions de portée générale, la Délégation procède à une enquête formelle et consigne ses conclusions dans un rapport public, comme elle l'a fait s'agissant du traitement des données dans le système d'informations relatif à la protection de l'Etat (ISIS[1]).

Le rapport de la délégation relatif à ISIS

De graves lacunes avaient été relevées à la fin des années 1990 par la Commission d'enquête parlementaire alors constituée pour investiguer au sujet des événements survenus au Département fédéral de Justice et Police (DFJP), communément appelée en Suisse « affaire des fiches ». On pouvait s'attendre à ce que la collecte d'informations erronées ou inutiles ne soit plus pratiquée aujourd'hui, mais le dernier rapport de la Délégation des commissions de gestion des Chambres fédérales (DélCdG) montre malheureusement que ce n'est pas encore le cas.

Il ressort de ce rapport que la Délégation a découvert lors de ses contrôles que les enregistrements dans ISIS (la principale base de données des services suisses de renseignement civil) ne correspondaient pas suffisamment aux exigences légales. Ainsi, des personnes présentées comme inoffensives ou plus du tout actives étaient enregistrées, alors que d'autres l'étaient uniquement parce qu'elles avaient fait l'objet d'un contrôle de photos d'identité à la frontière, ou en raison d'une demande d'informations émanant de l'étranger. Des informations liées à l'engagement politique ou à l'exercice des droits découlant de la liberté d'opinion, d'association et de réunion étaient également enregistrées alors qu'elles n'auraient pas dû l'être. Le service de renseignement suisse, le Service d'analyse et de prévention (SAP, auquel a succédé depuis le 1er janvier 2010 le Service de renseignement de la Confédération SRC), considérait pour sa part qu'il pouvait enregistrer des informations à décharge des personnes concernées, ce qui ne correspond pourtant pas à un danger pour l'Etat comme le confirme le rapport de la Délégation.

En plus d'enregistrer des données que la loi ne permettait pas, le SAP ne procédait pas aux contrôles périodiques requis, ceux-ci ayant précisément pour but de s'assurer que les données conserver sont encore justes et pertinentes. Le contrôle initial consécutif à la saisie des données n'avait lieu que par sondage et les contrôles périodiques qui devaient avoir lieu après cinq ans, puis trois ans, et lors de nouvelles inscriptions, n'ont pas été réalisés. Il est difficile de savoir si ces manquements sont dus à un manque de personnel ou un choix du service de préférer la quantité d'informations à la qualité, comme cela s'est produit dans de nombreux autres pays. Plus grave encore, de fausses dates de contrôle ont été indiquées. Quelques 16 000 contrôles initiaux et 40 000 contrôles périodiques n'ont pas été effectués ces cinq dernières années, en violation des prescriptions légales. L'effacement de données obsolètes qui aurait dû avoir lieu lors des contrôles périodiques, n'a pas pu avoir lieu et des enregistrements ont été conservés bien au-delà de la durée maximale de conservation prévue par le droit suisse.

Globalement, la Délégation a constaté que les services de renseignement reçoivent un grand nombre de données qu'ils ne maîtrisent pas. Au lieu de vérifier

[1] http://www.parlament.ch/f/organe-mitglieder/delegationen/geschaeftspruefungsdelegation/isis-inspektion/Pages/default.aspx

l'authenticité des données et de n'enregistrer que les données pertinentes, les services de renseignement ont préféré enregistrer toutes les données et renoncer aux contrôles prévus. Ils disposent ainsi d'un grand nombre d'informations peu utiles. D'autre part, on constate à la lecture du rapport de la Délégation que les agents ne sont visiblement pas assez sensibles à la question de la protection des données et des droits des citoyens qui en découlent. Cela est d'autant plus inquiétant que ces droits ne sont pas là uniquement pour restreindre l'activité des services de renseignement, mais parce qu'ils ont une légitimité propre que l'Etat doit également respecter.

LES AMELIORATIONS

L'avis du Conseil fédéral

Comme la loi le prévoit, le Conseil fédéral suisse a pris position, le 20 octobre 2010, sur le rapport de la Délégation des commissions de gestion des Chambres fédérales concernant le traitement des données dans le système d'information relatif à la protection de l'Etat ISIS.

Le Gouvernement suisse reconnaît globalement la nécessité d'agir en matière de gestion des données et d'assurances qualité, et cela de manière urgente. Il insiste sur le fait que la qualité doit être privilégiée à la quantité. Des mesures ont déjà été prises, parmi lesquelles l'organisation d'une formation juridique de base destinée aux collaborateurs ; l'analyse des prescriptions juridiques et la présentation de leur application dans les processus de déroulement des travaux ; la révision des règles de saisie des données ; la garantie d'une gestion systématique et contrôlée des informations pendant toute la période de traitement des données ; ainsi que la nouvelle diffusion de règlements et de directives ayant trait au traitement des données. A lire ces premières mesures, on est partagé entre se réjouir de cette nouvelle sensibilité au respect de la loi et s'inquiéter si ce n'était pas encore le cas auparavant.

Le Conseil fédéral n'en défend pas moins l'administration dont il est le supérieur et on ne saurait le lui reprocher. Il justifie également l'activité des services de renseignement, bien que cette activité ne soit pas remise en cause, et regrette que la difficulté de trouver un équilibre entre la protection de l'Etat et la protection de la personnalité des citoyens n'ait pas été mieux prise en compte par la Délégation.

Le Conseil fédéral émet un avis plus nuancé sur différents problèmes soulevés par la Délégation. Alors que la Délégation reprochait aux services de renseignement de ne pas avoir procédé aux contrôles périodiques exigés par la loi, et d'avoir introduit des dates de contrôle erronés, le Conseil fédéral estime que des contrôles de qualité initiaux ont été effectués, même si les contrôles périodiques n'ont pas eu lieu comme ils auraient dû. Il précise encore qu'il faut distinguer les dossiers en suspens de ceux qui n'ont pas été contrôlés. Finalement, le Conseil fédéral précise encore que le fait d'avoir procédé à une nouvelle programmation, avec une date au 31 décembre 2004, a permis de rétablir les délais de calcul.

Ce point de vue ne peut pas être complètement suivi. Si l'introduction de cette nouvelle date a permis de réparer certaines erreurs dans le calcul des délais, elle a aussi fait croire que des contrôles périodiques avaient eu lieu et empêché la suppression de données obsolètes. S'agissant des dossiers en suspens, si on peut admettre à la décharge du Service d'analyse et de prévention qu'il n'avait peut être pas renoncé à procéder aux contrôles imposés par la loi, l'analyse de la Délégation doit être retenue : la loi prévoit un contrôle périodique qui n'a pas eu lieu (ou pas eu

lieu à temps) et les exigences légales n'ont donc pas été respectées pour ces dossiers.

La Délégation reprochait ensuite l'enregistrement de données qui n'auraient pas dû l'être, comme des données à décharge, par exemple des informations indiquant que la personne n'est pas dangereuse pour l'Etat. En se basant sur un avis de l'Office fédéral de la Justice, le Conseil fédéral suisse retient que des personnes qui ne font pas elles-mêmes l'objet de soupçon (mais qui sont contactées par des personnes soupçonnées) peuvent être enregistrées. En résumé, les personnes pour lesquelles ils n'existent qu'une « esquisse de soupçon » peuvent être enregistrées, mais les données doivent être effacées dès que la levée du soupçon intervient. Ainsi, une personne ne devrait pas être fichée à décharge ou, du moins, pas durablement.

Les améliorations prévues

Une lecture plus attentive de l'avis du Conseil fédéral du 20 octobre 2010 permet cependant de constater que si les recommandations formulées par la Délégation sont en principe admises au premier abord, les solutions de détail envisagées par le Conseil fédéral ne les suivent pas complètement.

La Délégation demandait de verrouiller provisoirement l'accès à toutes les données saisies depuis cinq ans ou plus et qui n'ont pas fait l'objet d'une appréciation générale depuis (recommandation 1). Le Conseil fédéral admet un verrouillage provisoire de l'accès à ces données jusqu'à ce que leur pertinence et leur véracité soient vérifiées. L'accord d'un organisme indépendant serait nécessaire pour accéder aux données qui n'auraient pas encore été contrôlées.

La deuxième recommandation concernait l'enregistrement systématique des photos d'identité prises lors des contrôles de frontières pour les ressortissants de certains pays. Ce programme de contrôle sera abandonné, mais un nouveau projet le remplacera. L'accès aux données recueillies dans ce nouveau programme serait toutefois limité à certaines personnes seulement au sein des services de renseignement. Les données actuellement stockées, et qui ne sont pas effectivement utilisées à des fins de protection de l'Etat, seront effacées.

Le fait d'enregistrer les informations de citoyens étrangers en raison de leur seule nationalité ou pays de provenance paraît choquant, car elle peut laisser penser que leur nationalité ou provenance constitue un risque pour la sécurité du pays. Nombreux sont pourtant les pays à procéder à des tels contrôles à l'entrée sur leur territoire (voire de manière anticipée). Certains pays vont d'ailleurs jusqu'à procéder systématiquement à l'enregistrement de données biométriques.

Le Conseil fédéral suisse accepte ensuite les recommandations liées à la saisie des données et à l'assurance qualité. Un organe externe apportera le soutien nécessaire et un rapport sera adressé à la Délégation.

En se basant sur l'avis de l'Office fédéral de la Justice, le Conseil fédéral s'écarte des recommandations 6 et 9, même s'il donne l'impression de les suivre. Pourront donc continuer à être enregistrées des personnes en soi irréprochables et qui n'ont malheureusement pas conscience des contacts problématiques qu'elles entretiennent. Les informations à décharge d'une personne ou d'une organisation seront aussi enregistrées dans le système. Le Conseil fédéral tente toutefois de rassurer en précisant que lorsque le soupçon est définitivement levé, les données doivent être effacées rapidement. Il n'empêche que durant une certaine période des personnes qui ne devraient pas l'être sont enregistrées, avec les conséquences que cela peut avoir. Cela n'est pas satisfaisant et s'il n'est vraiment pas possible de procéder autrement, ces données ne devraient être accessibles qu'à un nombre très limité de personnes et porter une mention particulière. Devraient en particulier être

évités la transmission à des services étrangers ou le traitement automatique de ces données de la même manière que les autres enregistrements.

Finalement, le Conseil fédéral utilisera l'élaboration de la future loi unifiée sur les services de renseignement pour examiner s'il faut prévoir d'augmenter les moyens techniques à disposition des services de renseignement (écoutes téléphoniques, caméras, micros, etc.) et si le droit d'accès de l'individu aux données le concernant ne devrait pas être réglé par les dispositions habituelles de la loi sur la protection des données.

Sylvain Métille
Janvier 2011