Les moyens offerts au service des activités de renseignement, et de police judiciaire

publié le **22/08/2015**, vu **3736 fois**, Auteur : Vincent Julien

Le projet de loi sur le Renseignement ouvre de nouvelles perspectives aux services spécialisés dans ces activités ; ils complètent les moyens déjà offerts aux services de police...

I/ Police

Si la police disposait déjà de moyens d'investigation spéciaux, mais finalement classiques, de nouveaux moyens prometteurs, mais surtout intrusifs sont développés : ils visent logiquement à renforcer l'exercice d'une sécurité policière générale dans nos sociétés.

§.1/ Les moyens d'investigation spéciaux, mais classiques

Les techniques spéciales d'enquête, réservées classiquement aux cas de criminalité organisée, ont été étendues aux nouvelles technologies du numérique : elles permettent dorénavant d'intercepter les conversations téléphoniques et électroniques, ou de capter les données informatiques.

Concernant les interceptions de correspondance, celles-ci étaient possibles dans le seul cadre d'une instruction et ne concernaient que les infractions dont la peine encourue était égale ou supérieure à deux ans emprisonnement : ordonnées par un juge d'instruction pour une durée maximale de quatre mois, renouvelable dans les mêmes conditions de forme et de durée, elles étaient effectuées sous son autorité et son contrôle. Depuis 2004 cependant, ces interceptions peuvent intervenir au cours de l'enquête : elles sont dorénavant menées par le procureur de la République, et placées sous le contrôle du juge des libertés et de la détention. Elles sont prévues pour une durée initiale d'un mois, renouvelable encore une fois dans les mêmes conditions de forme et de durée.

Or, si la notion de correspondance visait principalement les lettres postales, l'émergence des nouvelles technologies de l'information et du numérique a non permis non seulement d'étendre le champ d'application de la notion aux correspondances téléphoniques, mais encore à l'ensemble des correspondances émises par la voie de communication électroniques, incluant de fait les SMS ou messageries instantanées comme les courriers électroniques.

Plus encore, la généralisation des réseaux sociaux de type « Facebook » a posé de nouvelles questions concernant le principe de vie privée, au regard notamment du fil de discussion encore appelé « Mur » : les paramétrages du compte d'utilisateur du réseau social détermineront ici s'il est question d'une correspondance privée, protégée par le secret, ou d'une communication au public en ligne qui lorsqu'elle héberge des allégations susceptibles de constituer des faits d'apologie du terrorisme, peut donner lieu au jeu des circonstances aggravantes.

Parallèlement, la loi LOPPSI II a progressivement permis aux autorités judiciaires d'accéder aux

données stockées au sein d'un système informatique dans le cadre des prérogatives d'enquêtes permettant de recourir aux perquisitions classiques :

Intervenant dans le seul cadre d'une information portant sur un crime ou un délit relevant du champ d'application de l'article 706-73 du code de procédure pénale, le recours au procédé était subordonné aux seules nécessités de l'information judiciaire et devait faire l'objet d'une ordonnance motivée du juge d'instruction précisant l'infraction concernée, la localisation ou la description du système informatique concerné ainsi que la durée de l'opération. Lorsque tous ces critères étaient réunis, le dispositif permettait dorénavant aux enquêteurs judiciaires d'accéder, en tous lieux, à des données informatiques, de les enregistrer, les conserver et les transmettre telles qu'elles s'affichent sur un écran pour l'utilisateur d'un STAD ou telle qu'il les y introduit par saisie de caractères, sans que le consentement des intéressés ne soit logiquement requis, ce qui suggère par ailleurs l'introduction dans le lieu d'habitation de l'intéressé devant respecter les heures légales entre 21heures du soir et 6heures du matin.

§.2/ Les moyens d'investigation prometteurs, mais intrusifs

Le procédé de géolocalisation en temps réel, si elle apparaît comme un prolongement classique des techniques de surveillance et de filatures traditionnellement mises en œuvre par la police, suscite de nouvelles questions plus problématiques pour les libertés individuelles :

Il s'agit notamment de la géolocalisation par balise GSM ou téléphone portable qui, si elle se généralise avec nouvelles technologies de l'information et du numérique, permet dorénavant aux enquêteurs de suivre non seulement le parcours de l'individu suspect en temps réel, mais plus encore de retracer l'ensemble de ses déplacements. Menace d'autant plus accentuée pour les droits et libertés fondamentaux, que ce procédé ne faisait l'objet d'aucun régime juridique précis jusqu'en 2014 :

La géolocalisation permettait de localiser un objet numérique posé sur un véhicule ou un ordinateur portable afin de suivre les mouvements d'un ou plusieurs suspects afin de reconstituer la carte complète des déplacements de ces derniers : tandis que la technique de localisation par satellite fût considérablement développée pour les utilisateurs de les téléphones « intelligents », ces outils pouvaient dorénavant être géolocalisés par trois satellites distincts avec une marge d'erreur de seulement dix mètres. Les données de localisation, une fois transmises par le satellite au téléphone, étaient de nouveau transmises du téléphone à l'antenne-relais, laquelle transmettait ces mêmes données aux opérateurs de télécommunication. Par la suite, une simple réquisition de l'officier de police judiciaire amenait ces opérateurs à transférer ces données sur le serveur de la police. Il s'agissait donc non seulement d'un dispositif particulièrement intrusif dans les droits et libertés de ces utilisateurs de téléphones, mais aussi d'un procédé relativement simple à mettre en œuvre pour les autorités judiciaires. Surtout jusqu'à l'année dernière, le seul texte encadrant le recours au procédé de géolocalisation résidait « [dans la possibilité] pour le juge d'instruction [de] procéder, conformément à la loi, à tous les actes d'information qu'il juge utiles à la manifestation de la vérité ».

L’inexistence de tout texte de loi préalable à la prise de décision du juge d’instruction, laissait à ce dernier toute la discrétion imaginable pour décider de la mise en place de ce dispositif sans qu’aucune condition légale de fond ou de forme ne soit à respecter : c’est dire que la géolocalisation pouvait concerner l’enquête de flagrance ou l’information judiciaire, viser un délit puni de six mois d’emprisonnement ou un crime puni de quinze ans de réclusion. Surtout, elle pouvait s’exercer pour toute la durée jugée nécessaire par le juge d’instruction. Le flou juridique entourant ce procédé particulièrement intrusif fût notamment sanctionné par les juges de la Cour de cassation dans deux arrêts rendus en 2014, nécessitant ainsi le développement de la sécurité juridique des particuliers face aux nouveaux dispositifs policiers sur le terrain numérique.

II / Renseignement :

Le projet de loi relatif au renseignement a été adopté à l’Assemblée Nationale le 5 mai 2015, Il sera définitivement voté lors d’un vote solennel le 9 juin 2015 : si ce texte officialise certaines pratiques anciennes, il consacre aussi nouveaux outils controversés à disposition des services de renseignement, et consacre le privilège d’une sécurité politique dans nos sociétés.

§.1/ L’encadrement d’anciens outils généraux nécessaires à la prévention des menaces globales :

L'article L.811-3 du projet de loi prévoit que les services spécialisés de renseignement peuvent, dans l'exercice de leurs missions, recourir à certaines techniques couvertes par le secret. Les motifs justifiant la mise en œuvre de ces techniques sont cependant publiés, ils sont au nombre de sept :

Quand l'un de ces objectifs est poursuivi, l’article L.851-6 du projet de loi prévoit l’utilisation de dispositifs permettant de localiser en temps réel un véhicule ou un objet : l'utilisation de la technique de géolocalisation devra être autorisée par décision "(…)écrite et motivée du Premier ministre ou d'une des personnes des assemblées parlementaires(…)", ou par "(…)décret du Conseil d'Etat, pris après avis de la CNCTS ou des services spécialisés de renseignement relevant de ministres de la Défense et de l'Intérieur, de l'économie, du budget ou des douanes". Cependant, "(…) en cas d'urgence liée à une menace imminente ou à un risque très élevé de ne pouvoir effectuer l'opération [de prévention des atteinte aux intérêts publics...], le dispositif mentionné [de géolocalisation] peut être installé et exploité sans autorisation préalable [mais sera susceptible de faire] l'objet d'une autorisation dans les 48heures après avis de la CNCTS.". L'impératif de préservation des intérêts publics, ou plus globalement de la souveraineté de l'Etat sur son territoire au niveau national, permet donc de prendre des mesures de police exorbitantes à l'encontre des droits des citoyens : il conduit alors à contrôler l'exercice des libertés personnelles, afin de protéger la sécurité de l'Etat.

Parallèlement, l’article L.852-1 du second chapitre prévoit que les interceptions de sécurité, qui ne concernaient que les communications téléphoniques, est étendue aux communications électroniques : si ces mesures devront classiquement intervenir pour la sauvegarde des intérêts publics de l'Etat, elles suscitent néanmoins des problématiques quant à la préservation des libertés citoyennes.

C'est que l'article dispose que "lorsqu'une ou plusieurs personnes appartenant à l'entourage de la personne visée par l'autorisation sont susceptibles de jouer un rôle d'intermédiaire, volontaire ou pour le compte de celle-ci, ou de fournir des informations au titre de la finalité faisant l'objet de l'autorisation, celle-ci peut être accordée également pour ces personnes" : or, une telle mesure est susceptible de porter des atteintes disproportionnées aux personnes de l'entourage du suspect, tandis que la notion d'intermédiaire reste relativement floue. Par ailleurs, si les services de

renseignement jugent nécessaire de mettre sous surveillance la personne appartenant à l'entourage du suspect initial, sur la base des seuls agissements "volontaires ou pour le compte (…)" ainsi que la [fourniture] "d'informations", elle laisse en suspens la question de son utilité, sinon de sa conformité avec certains faits justificatifs exonératoires de responsabilité pénale.

C'est que l'agissement de la personne de l'entourage "pour le compte" du suspect principal pourrait très bien être un acte commis sous la contrainte, en principe exonératoire de responsabilité pénale, tandis que la fourniture d'"informations" pourrait se heurter au principe contenu à l'article 434-1 du code pénal selon lequel "sont exceptés [de l'obligation de prévenir les autorités judiciaires ou administratives de la survenance d'un crime dont il est encore possible de prévenir ou d limiter les effets] les parents en ligne directe et leurs conjoints, ainsi que les frères et sœurs et leurs conjoints, de l'auteur ou complice du crime (…)". En définitive, ces nouveaux moyens offerts aux services de renseignement privilégient nettement le principe de sécurité policière politique et militaire, sur le traditionnel principe de sécurité juridique : tandis que les intérêts publics se confondent avec les "intérêts d'Etat", il s'agira notamment de "préserver l'ordre public" à l'intérieur des frontières, quand la "loyauté" est érigée en première vertu du citoyen, que la "raison d'Etat" justifie les immixtions dans les sphères privées.

§.2/ La consécration de nouveaux outils spécifiques justifiés par la prévention des menaces « cyber-terroristes » :

L’article 2 du projet de loi définit les techniques spéciales de recueil du renseignement et consacre, dans un premier chapitre, l’accès administratif aux données de connexions :

Les données de connexion peuvent être recueillies immédiatement pour les « (…) seuls besoins de la prévention du terrorisme », pour autant qu’elles concernent des « (…) personnes préalablement identifiées comme présentant une menace terroriste. »: L’article 2 du projet de loi prévoit donc l’installation sur les réseaux des opérateurs de téléphonie et des fournisseurs d’accès à Internet de dispositifs permettant de recueillir, en temps réel, les données de connexion ou « métadonnées ». On appelle ce dispositif la « boîte noire » :

Les données susceptibles d’être récoltées sont diverses : il s’agit des « informations ou documents traités ou conservés par [les] réseaux ou services de communications électroniques, y compris les données techniques relatives à l’identification des numéros d’abonnement ou de connexion des services de communications électroniques [ainsi] que la liste des numéros appelés et appelants, la durée et la date des communications. ». Par la suite, sur la base de ces informations, mais « pour les seuls besoins de la prévention du terrorisme […] le Premier ministre, ou l’un des personnes déléguée par lui peut, après avis de la Commission nationale de contrôle des techniques de renseignement […] mettre en place un dispositif destiné à révéler, sur la seule base de traitements automatisés d’éléments anonymes, une menace terroriste. ». Désormais, la menace terroriste sera susceptible d’être appréhendée par le biais de l’outil numérique, sur la base des données de connexion recueillies et analysées grâce à un dispositif unique : l’ « algorithme ».

Parallèlement, l’article L.851-7 permet dorénavant, « lors d’opérations, l’utilisation de dispositifs mobiles de proximité permettant de capter directement les données de connexion strictement nécessaires à l’identification d’un équipement terminal ou du numéro d’abonnement de son utilisateur [ou encore] les données relatives à la localisation des équipements terminaux utilisés» : là encore, seule la menace de survenance d’actes terroristes justifie que ces dispositifs soient utilisés pour la captation des correspondances numériques. Cependant, si la menace terroriste est avérée, l’utilisation du dispositif pourra être autorisé dans pour une durée maximale de 144heures : il permettra ainsi aux services de renseignement « (…) d’intercepter directement les correspondances émises ou reçues [entre utilisateurs suspectés de vouloir commettre des actes

de terrorisme] par l’équipement terminal. »