Les techniques d'enquête des services de renseignement : de l’accès aux données de connexion aux dispositifs de géolocalisation

Pour cerner une réalité obscure, mal connue et mal comprise, cet ouvrage conçu par un spécialiste présente l'histoire, les méthodes et les acteurs du renseignement, en France, des origines à nos jours. Extrait du livre "Le renseignement: Histoire, méthodes et organisation des services secrets" de Christophe Soullez, aux éditions Eyrolles. 2/2

Avec Christophe Soullez

L’accès aux données de connexion Le recueil des données techniques de connexion, ouvert à l’ensemble des services de renseignement depuis le 1er janvier 2015 (suite au vote de la loi de programmation militaire de 2013), est repris en supprimant la procédure d’autorisation via une personnalité qualifiée. L’accès aux données de connexion, y compris en temps réel et « sur sollicitation du réseau » des opérateurs de communication électronique, est ainsi soumis au régime géné- ral d’autorisation. Les services peuvent donc recueillir auprès des opérateurs de communication électronique les données de techniques de connexion relatives à des individus ciblés. Il peut s’agir de l’identification des numéros d’abonnement ou de connexion, du relevé de l’ensemble des numéros d’abonnement ou de connexion d’une personne, de la localisation des équipements terminaux utilisés, ou encore de la durée et de la date des communications.

Il existe des dérogations par lesquelles les agents peuvent directement demander la mise en œuvre de cette mesure. Les données sont alors recueillies par un service du Premier ministre (le groupement interministériel de contrôle) et la Commission nationale de contrôle des techniques de renseignement peut y avoir un accès « permanent complet et immédiat ».

Pour les personnes soupçonnées d’être « les plus impliquées » dans des activités à caractère terroriste, la loi prévoit « un recueil des données techniques de connexion en temps réel et en permanence ». Contrairement à l’enregistrement des échanges via un logiciel espion placé sur un ordinateur, cette disposition vise à recueillir les données de connexion des comptes et services Internet utilisés par un individu, quel que soit le poste utilisé, afin de suivre ses déplacements et ses relations. Cet accès concerne des « personnes préalablement identifiées comme présentant une menace ». L’autorisation n’est délivrée que pour deux mois et la procédure d’urgence ne peut être mise en œuvre.

Les dispositifs de géolocalisation Les services de renseignement peuvent géolocaliser une cible selon deux méthodes :

• le recueil des données techniques d’un terminal,

• la pose d’une balise sur un objet ou un véhicule.

Dans ce dernier cas, cette opération peut même être réalisée sans autorisation préalable, en vertu de la procédure d’urgence. Les services sont également autorisés à utiliser des « dispositifs techniques de proximité » dits « IMSI-catchers », mais seulement pour

identifier un téléphone ou un numéro d'abonnement ou pour collecter « les données relatives à la localisation » des terminaux situés à proximité. L'autorisation est valable deux mois et renouvelable dans les mêmes conditions de durée. Dans des cas limités à la prévention du terrorisme, ce dispositif peut être utilisé afin « d'intercepter directement des correspondances émises ou reçues ». L'autorisation n'est alors délivrée que pour 48 heures renouvelables.

Les IMSI-catchers

Ce sont de fausses antennes relais qui permettent d'intercepter les conversations téléphoniques (l'IMSI est un numéro identifiant unique contenu dans la carte SIM). Les IMSI-catchers imitent le fonctionnement d'une antenne relais de téléphonie mobile, de manière à ce que les appareils situés à proximité s'y connectent. Cet équipement reçoit ensuite les communications de ces téléphones et peut, dans certains cas, accéder à leur contenu. Il transmet ensuite à son tour les communications à l'opérateur et l'appel a lieu normalement. Certains de ces outils disposent de fonctionnalités complémentaires, comme la lecture (ou l'envoi) de SMS, l'interception du trafic Internet mobile ou la capacité de bloquer tout appel tentant de parvenir à un téléphone donné. Tous les téléphones qui se trouvent à proximité sont trompés par cette « fausse antenne ».

Extrait du livre "Le renseignement: Histoire, méthodes et organisation des services secrets" de Christophe Soullez, aux éditions Eyrolles