Un décret autorise les captations de données et de conversations Skype en temps réel

	Un décret autorise les captations de données et de conversations Skype en temps réel

Dans le calme d'un dimanche précédent le début des vacances de Noël, le gouvernement a publié au Journal officiel un décret autorisant les forces de l'ordre à surveiller toutes les informations apparaissant sur l'ordinateur d'un suspect (de ses conversations Skype à ses sites consultés), dans le cadre de procédures judiciaires.

Permettre à des enquêteurs de capter en temps réel (et à distance) les données informatiques de suspects, c'est possible. Depuis le vote de la LOPPSI de 2011, l'article 706-102-1 du Code de procédure pénale autorise en effet les officiers et agents de police judiciaire à accéder et enregistrer des données « telles qu'elles s'affichent sur un écran » ou telles que l'utilisateur d'un ordinateur « les y introduit par saisie de caractères » – et ce à partir du moment où un juge d'instruction a émis une ordonnance motivée en ce sens, prise après avis du Procureur de la République.

Cette procédure, activable uniquement pour des crimes et délits relativement graves (terrorisme, association de malfaiteurs, meurtre, crime de fausse monnaie, escroquerie ou prêt illicite de main d'œuvre en bande organisée, etc.), a même été élargie suite à l'adoption de la loi anti-terroriste de novembre 2014 aux données « reçues et émises par des périphériques audiovisuels ». L'objectif ? Pouvoir capter aussi les sons, comme ceux d'une conversation Skype par exemple.

Captation de tout ce qui apparaît à l'écran, les conversations Skype, etc.

Avec ce décret entré en vigueur ce lundi 21 décembre 2015, le gouvernement vient de permettre l'application de ces dispositions en autorisant la création de traitements de données à caractère personnel, destinés à recevoir les fameuses informations extirpées par les forces de l'ordre dans ce type de procédures. « Les traitements autorisés par le présent décret permettent de collecter, enregistrer et conserver les données informatiques ainsi captées et de les mettre à la disposition des enquêteurs de la police et de la gendarmerie nationales comme de la douane judiciaire », précise le texte.

Les opérations, bien que placées sous le contrôle du juge, permettront aux services de se pencher sur « l'ensemble des données captées », y compris s'il s'agit de données personnelles sensibles. Toutes les informations enregistrées devront être « conservées dans le traitement jusqu'à la date de clôture des investigations ». À ce moment, poursuit le décret, elles seront « placées sous scellés fermés et effacées ». Une transcription des enregistrements effectuée par les forces de l'ordre devra néanmoins être transmise à l'autorité judiciaire, pour être versée au dossier de la procédure – en vue d'un éventuel procès.

En donnant son avis sur ce qui n'était alors qu'un projet de décret, la Commission nationale de l'informatique et des libertés (CNIL) prévenait l'exécutif que l'utilisation de tels dispositifs de surveillance risquait de conduire à la collecte de « données relatives à d'autres personnes que l'utilisateur [suspecté], telles que, par exemple, l'identité des personnes en relation avec l'utilisateur du système d'information surveillé ».

La gardienne des données personnelles affirmait par ailleurs que le gouvernement ne faisait pas explicitement référence à la mise en œuvre de dispositifs de reconnaissance vocale ni d'analyse comportementale des dynamiques de frappe au clavier (keylogging). « Si de tels mécanismes devaient à l'avenir être mis en œuvre, la commission devra être saisie pour avis sur un projet de décret modificatif prévoyant expressément le recours à de tels dispositifs » mettait-elle en garde.

Un dispositif qui n'était pas encore totalement opérationnel en avril dernier

Tout en regrettant « de ne pas avoir été destinataire de l'ensemble du dossier technique (…), certains éléments n'ayant été communiqués qu'à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) », la CNIL soutenait qu'au moment de rédiger son avis, le dispositif prévu par le ministère de l'Intérieur « ne permet[tait] pas encore la captation de données émises ou reçues par des périphériques audiovisuels ». La délibération de l'autorité administrative indépendante date toutefois du 2 avril 2015, ce qui signifie que les choses ont pu grandement évoluer depuis…

La CNIL ajoutait néanmoins qu'elle prenait acte « que lorsqu'un nouveau dispositif aura été développé dans cette perspective, des informations complémentaires ser[aient] portées à sa connaissance ». Nous n'avons cependant pas réussi à joindre l'institution afin de savoir si elle avait depuis obtenu de nouveaux éléments.

Sur un plan technique, la CNIL expliquait qu'au regard des éléments à sa disposition, « la solution retenue pourra s'adapter à l'environnement applicatif des utilisateurs visés par une enquête (système d'exploitation, applications tierces, etc.). Des tests de fonctionnement seront exécutés afin de s'assurer de la correcte adaptation de l'outil à l'environnement de chaque utilisateur. Une procédure de suppression automatique de l'outil sur les terminaux informatiques visés est prévue. L'architecture de collecte sera en outre pourvue de mesures visant à assurer la sécurité et le cloisonnement des données collectées. »

Rappelons enfin que la récente loi sur le renseignement permet à de nombreux services d'utiliser des dispositifs intrusifs à l'insu des personnes surveillées (à l'image des ISMI catcher), sans toutefois qu'un juge soit cette fois mis dans la boucle…

Réagissez à cet article

Source : *Un décret autorise les captations de données et de conversations Skype en temps réel*