Accès administratifs aux données de connexion : pareil qu'aujourd'hui… mais en pire

Il aura fallu attendre le 26 décembre pour que le gouvernement publie le **décret d'application de la loi de programmation militaire (LPM)**. Ce texte, relatif à l'accès administratif aux données de connexion, organise la collecte de données par les autorités sur les réseaux des hébergeurs, opérateurs télécoms et FAI, en l'**absence de toute réquisition judiciaire**. Il fixe les modalités d'application de l'article 20 de la loi (au départ connu comme l'article 13), très décrié lors du vote de ce texte… en décembre 2013. Article liberticide pour les uns, qui dénoncent une dérive à l'américaine. Simple prolongation d'un arsenal existant pour les promoteurs de la LPM.

Le décret d'applications permet de mieux cerner la portée de ce fameux article 20. D'abord en donnant **la liste – très large – des services pouvant avoir recours à cette procédure** de réquisitions de données au ministère de l'Intérieur (DGSI, police nationale, police aux frontières, gendarmerie et préfecture de police), au ministère de la Défense (DGSE, renseignement militaire…), ainsi qu'à Bercy (Tracfin, douanes). Ensuite, il faut noter que ce régime d'interceptions **reprend les principes des écoutes téléphoniques**, avec un organisme centralisant les requêtes, le groupement interministériel de contrôle (GIC), placé sous l'autorité du Premier ministre (échappant ainsi à l'Intérieur), requêtes qui sont ensuite mises en œuvre par les opérateurs, FAI et hébergeurs. Il n'est donc pas question, dans ce décret, d'installer des mouchards exploités directement par les services de renseignement. Les opérateurs, FAI et hébergeurs « *transmettent sans délai les informations ou les documents demandés au groupement interministériel de contrôle, qui les met à disposition de l'auteur de la demande pour exploitation* », précise le décret publié le lendemain de Noël. Comme dans le cas des écoutes téléphoniques, le dispositif est placé sous la supervision de la Commission nationale de contrôle des interceptions de sécurité (CNCIS), organisme composé de trois membres, dont deux parlementaires, et réputé plutôt docile vis-à-vis des services d'enquête.

Bien plus que le seul terrorisme

Surtout, le décret précise les données auxquelles s'applique le texte. **Seules les métadonnées** (identités de l'utilisateur et, le cas échéant, du destinataire, dates et heures des communications…) sont concernées. Un champ plutôt étroit surtout si on le compare à la formulation très floue (« des informations et documents ») employée dans le texte de loi de la LPM. Ce glissement sémantique résulte des **pressions exercées par la CNIL** sur le gouvernement, la Commission craignant que la LPM n'entraîne « *un élargissement des données pouvant être requises par rapport à celles pouvant actuellement être demandées aux opérateurs, qui sont limitées à des 'données d'identification'* ». Concrètement, la CNIL redoutait une extension aux interceptions de contenus ou aux perquisitions en ligne. Un risque que ses pressions sur le gouvernement ont fini par écarter, Les Echos signalant que, dans les projets de décret provisoires, l'exécutif a longtemps tenté d'entretenir le flou sur ce point, en maintenant sa formulation de départ, avant de finalement céder.

Au final, dans sa délibération, la CNIL replace cet article 20 à son juste niveau : une prolongation de ce qui existe déjà. En effet, la LPM se traduit concrètement par **une extension des services pouvant demander un accès aux données** (avec quelques bizarreries, comme le service chargé des événements à la préfecture de police de Paris !) ainsi qu'**une extension des finalités** pour lesquelles peuvent être requises lesdites données. Sur ce point, la liste est si large qu'on voit mal quel cas précis pourrait échapper aux motifs précisés dans le décret : « *recherche des renseignements intéressant la sécurité nationale* », « *sauvegarde des éléments essentiels du potentiel scientifique et économique de la France* », et « *prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous* » (sic).

« *La commission relève que les données détenues par les opérateurs qui peuvent être demandées sont de plus en plus nombreuses, sont accessibles à un nombre de plus en plus important d'organismes, sur réquisitions judiciaires ou administratives ou en exécution d'un droit de communication, et ce pour des finalités très différentes* », résume la CNIL dans sa délibération.

Inconventionnalité ?

Rappelons que, jusqu'à ce décret entrant en vigueur au 1er janvier, le cadre juridique actuel, datant de 2006, prévoit déjà un accès d'agents spécialement habilités aux données de connexion conservées par les opérateurs, FAI ou hébergeurs. Mais ces réquisitions administratives (**déjà au nombre de 30 000 par an**) sont limitées à la prévention des actes de terrorisme. Avec le nouveau texte, ces demandes d'accès devraient se multiplier pour devenir une arme couramment utilisée par les services d'enquête dans le cadre d'affaires criminelles, financières ou relevant de l'espionnage économique.

Au passage, la CNIL adresse un coup de griffe au gouvernement, lui rappelant que la **Cour de justice de l'Union** européenne (CJUE) a **invalidé la directive européenne sur la rétention de données**, par un arrêt datant d'avril dernier. « *Cet arrêt conduit à s'interroger sur le risque d'inconventionnalité des dispositions de la Loi de programmation militaire* », glisse la Commission. Un terme qui permet à l'autorité administrative d'éviter l'emploi d'inconstitutionnalité : rappelons que, suite à un imbroglio au Parlement, la LPM n'a pour l'instant pas été soumise à l'examen du Conseil Constitutionnel. Toute saisine des Sages de la rue Montpensier doit désormais attendre la promulgation de la loi, au 1er janvier.

A lire aussi :

Loi de programmation militaire : l'article 13, juste la partie émergée de l'iceberg ?
Programmation militaire : le Parlement adopte l'extension de la surveillance électronique

Crédit photo : spiber.de / Shutterstock