Loi de programmation militaire : l'article 13, juste la partie émergée de l'iceberg ?

Adopté définitivement mardi 10 décembre, le projet de loi de programmation militaire (LPM) 2014-2019, dont **l'article 13** qui étend l'accès administratif aux données de connexion et de géolocalisation, sans contrôle judiciaire, ouvrirait la porte à la surveillance généralisée d'après ses nombreux détracteurs, acteurs du numérique et organisations citoyennes. Quel est vraiment l'impact de l'article 13 sur le cadre juridique applicable aux services de renseignement ?

Un « Patriot Act » à la française

Dans un avis du 6 décembre, le **Conseil national du numérique** a jugé inopportune la *« modification du dispositif créé par **la loi de 2006 relative à la lutte contre le terrorisme** »*. Pour **Pascal Cohet**, auteur d'un document de l'Ifrei (Institut de formation et recherche sur l'environnement informationnel) relatif aux *« éléments d'évaluation du risque législatif lié à l'article 13 »*, cette évolution législative n'a pas pour origine la loi du 23 janvier 2006, mais serait inspirée du **Patriot Act** américain.

Cette loi antiterroriste a été signée par le prédécesseur de **Barack Obama** à la présidence des États-Unis, **George W. Bush**, en octobre 2001 dans l'ombre des attentats du 11 septembre. Le Patriot Act permet aux agences du renseignement américain, dont la **NSA** vilipendée pour son programme de surveillance **Prism** révélé par **Edward Snowden**, d'obtenir auprès d'une société de droit américain des informations, y compris sur les métadonnées et données hébergées par ses filiales à l'étranger.

À la suite du Patriot Act, la loi du 15 novembre 2001 relative à la sécurité quotidienne (LSQ) a vu le jour en France. Le texte, qui visait à renforcer la lutte contre le terrorisme, comporte des mesures spécifiques concernant Internet, la conservation et le chiffrement de données, adoptées à l'origine pour une durée *« allant jusqu'au 31 décembre 2003 »*. Or, observe le journaliste Jean-Marc Manach, la mesure fut prolongée jusqu'au 31 décembre 2005. Entre-temps, la loi pour la confiance dans l'économie numérique (LCEN) a été promulguée le 21 juin 2004.

Très décriée, la LCEN a renforcé la responsabilité des hébergeurs et fournisseurs d'accès Internet en leur imposant de stocker identifiants, mots de passe et historique, une mesure confirmée par la loi du 23 janvier 2006 relative à la lutte contre le terrorisme. Mais les prestataires techniques n'ont pas été soumis *« à une obligation générale de surveiller les informations qu'(ils) transmettent ou stockent, ni (…) de rechercher des faits ou des circonstances révélant des activités illicites »*.

Cette même année 2006, **la conservation des données de connexion a été prolongée jusqu'au 31 décembre 2008, avant de l'être à nouveau jusqu'au 31 décembre 2012, puis au 31 décembre 2015**… L'article 13 de la LPM ne serait donc que la partie émergée de l'iceberg. D'après Pascal Cohet, une quinzaine d'articles répartis sur une dizaine de lois en France intéressent la conservation des données de connexion au titre de la lutte contre le terrorisme et le crime organisé.

À quoi sert l'article 13 ?

Pour les promoteurs de la LPM, dont **Jean-Louis Carrère**, président de la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat et rapporteur du texte, *« ce nouveau dispositif ne modifie aucunement ni la nature des données concernées, ni la procédure permettant aux services de renseignement d'avoir accès à ces données ».* Quant à **l'article 13**, il vise à ***« clarifier le régime juridique de la géolocalisation en temps réel »*** et à ***« refondre le régime juridique de l'accès aux données de connexion »***.

Il ajoute que *« les demandes, motivées, d'accès aux données de connexion seront soumises à la décision d'une personne qualifiée auprès du Premier ministre et non auprès du ministre de l'Intérieur comme aujourd'hui ; et que chaque demande fera l'objet d'un contrôle effectué par la Commission nationale de contrôle des interceptions de sécurité (CNCIS) »*.

Enfin, insiste Jean-Louis Carrère, *« **aucune extension du champ des données accessibles par rapport au droit existant n'est prévue**. L'accès aux contenus des communications reste du ressort exclusif du régime des interceptions de sécurité, qui demeure totalement inchangé »*. D'après le rapporteur du texte, *« le nouveau dispositif constitue par conséquent un progrès indiscutable du point de vue des libertés publiques ».*

La filière numérique et les organisations de défense des libertés ne partagent pas ce point de vue, bien au contraire. Pour elles, comme pour **Benoît Thieulin**, président du Conseil national du numérique, instance consultative auprès des pouvoirs publics, **le risque de basculer vers *« une société de surveillance totale »* est bien réel**. Jeudi 12 décembre, à la suite de l'Association des services Internet communautaires (Asic), plusieurs organisations, dont la FIDH, la LDH, Renaissance numérique et le Syndicat de la magistrature, ont demandé aux parlementaires de saisir le Conseil constitutionnel, afin que celui-ci examine la conformité de ce texte avec la loi fondamentale.

crédit photo © Vladislav Kochelaevs Fotolia.com

Voir aussi

Rétrospective : la saga PRISM