Les révélations d’Edward Snowden, à l’été 2013, sur les programmes de cyberespionnage de la National Security Agency (NSA), ont suscité de vives réactions de la part de certains Etats ou organisations internationales qui en étaient la cible (voir *REM*, n°28, p.66). Le président de la République François Hollande avait demandé l’arrêt de ces procédés auprès de son plus proche allié, tandis que diverses associations, en Europe comme aux Etats-Unis, défendaient les libertés publiques. L’opinion publique internationale découvrait alors l’étendue de la surveillance numérique opérée par les Etats-Unis dans le monde entier à partir de divers programmes de la NSA. Quelques mois plus tard, la France prend de nouvelles dispositions qui harmonisent les usages de la surveillance numérique sur de nouvelles bases juridiques. La loi de programmation militaire (LPM) 2014-2019 et le projet de loi discuté au Sénat et à l’Assemblée nationale début 2014 doivent permettre aux services de renseignement et de police d’accéder aux données techniques de connexion, en temps réel, de personnes susceptibles de porter atteinte à la défense et à la sécurité nationale (terrorisme, espionnage, criminalité organisée, déstabilisation des institutions républicaines), non sans provoquer certaines réactions des défenseurs des libertés.

La loi de programmation militaire 2014-2015, examinée au Sénat en octobre dans une quasi-indifférence, et adoptée à l’Assemblée le 18 décembre 2013, reconnaît, dans l’article 20, de nouvelles dispositions liées à la collecte des données de connexion (historique des utilisateurs, métadonnées des communications, géolocalisation) et au contenu des correspondances. Cet article, examiné à l’Assemblée nationale le 26 novembre, d’abord sous le nom d’article 13, permet de clarifier des pratiques déjà existantes en un seul régime juridique, jusqu’alors reposant sur deux dispositifs législatifs : la loi de 1991 relative aux interceptions de sécurité, la loi relative à la lutte antiterroriste de 2006 dont est issu l’article 34-1-1 du code des postes et des communications électroniques. Ce nouveau régime s’inscrit dans la continuité de l’application du code de la sécurité intérieure pour le contenu des communications.

L’article L. 241-2 autorisait déjà l’accès au contenu des correspondances pour une durée de 4 mois, réduite à 30 jours renouvelables dans l’article 20 (L 246-3), tout en garantissant leur secret. L’article 20 de la LPM harmonise ces dispositions en permettant, sur décision du Premier ministre (et non plus du ministre de l’intérieur), l’accès aux données liées à l’historique de connexion des utilisateurs de l’internet et la consultation des contenus des messages. Il étend également le nombre des ministères pouvant demander l’interception administrative des communications, concernant jusqu’alors ceux de la défense, de l’intérieur et des douanes, et désormais élargi à ceux de l’économie et du budget. Enfin, il donne la possibilité de réclamer des données, en temps réel, à un plus grand nombre d’entités comme les fournisseurs d’accès à l’internet, les opérateurs de téléphonie mobile et les hébergeurs de contenus.

Le 24 décembre dernier, un nouveau projet de loi a été adopté par le Conseil des ministres au nom de la protection des citoyens français pour permettre la géolocalisation dans un cadre légal par les services de renseignement et de police. Jusqu’à présent, ces investigations suivaient des « *dispositions très générales du code de procédure pénale* ». La géolocalisation, c’est-à-dire la capacité de localiser précisément un

individu grâce à son téléphone ou un objet sur lequel serait fixée une balise, serait autorisée par le procureur, puis éventuellement prolongée après quinze jours par la décision d'un juge des libertés ou d'un juge d'instruction. Elle ne serait mise en application que si elle « s'*avère nécessaire à la conduite d'investigations concernant un crime ou un délit puni d'au moins trois ans d'emprisonnement* ».

Ce projet de loi proposé par la garde des Sceaux doit être examiné par le Sénat le 20 janvier et par l'Assemblée le 6 février, dans un contexte peu favorable. Une décision de la Cour européenne des droits de l'homme, puis un arrêt de la Cour de cassation du 22 octobre dernier en France, considère que la géolocalisation est « *une ingérence dans la vie privée dont la gravité nécessite qu'elle soit exécutée sous le contrôle d'un juge* ». La Commission nationale informatique et libertés (CNIL) ne semble pas avoir été consultée pour l'élaboration du texte. En outre, l'adoption de l'article 20 de la LPM continue de susciter diverses réactions des défenseurs des libertés qui y voient une surveillance généralisée des citoyens et une version à la française du *Patriot Act*.

Il y a tout lieu de penser que ces défenseurs se manifesteront de nouveau comme l'Association des sites internet communautaires, créée en 2007 pour promouvoir le « nouvel internet » des réseaux sociaux et réunissant les principaux opérateurs du Net et de la téléphonie (Facebook, Dailymotion, Google, Microsoft entre autres). Ceux-ci se sont opposés aux dispositions qui favorisent la surveillance de leurs clients. Lors des discussions parlementaires, les promoteurs de la LPM avaient alors assuré que des garanties seraient accordées au citoyen, comme le respect de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales signée par la France, comme la nomination d'une « personnalité qualifiée » auprès du Premier ministre pour contrôler les demandes des services des ministères et l'indépendance de la « commission nationale de contrôle des interceptions de sécurité » pour encadrer le recueil de données de connexion et de géolocalisation. De toute évidence, la LPM et le projet de loi discuté début 2014 apparaissent comme des effets indirects de l'affaire Snowden. L'Etat français avait alors vivement critiqué les procédés de la NSA au début de l'été 2013, mais avait été aussi accusé, par certains Etats et les principaux opérateurs, de suivre des pratiques que le législateur français tente désormais d'harmoniser dans un cadre légal.

Sources :

- « Téléphone, Internet : l'Etat pourra bientôt tout espionner », Jean-Marc Leclerc, *Le Monde*, 25 novembre 2013.
- « Surveillance d'Internet : inquiétudes autour de la la loi de programmation militaire », Martin Untersinger, *Le Monde*, 26 novembre 2013.
- « Cybersurveillance : Who Watches The Watchers ? », Jean-Dominique Merchet, *L'Opinion*, 26 décembre 2013.