JURIDIQUE

Projet de Loi relatif au Renseignement : la sécurité au détriment des libertés ?

Sans mauvais jeu de mot, nécessité fait loi. L'importance du débat autour du projet de loi sur le Renseignement, le tollé que ce projet a provoqué, notamment autour des fameuses « boîtes noires » des fournisseurs d'accès à Internet (FAI) motivent un retour éclairé sur ce projet de la part de l'un de nos chroniqueurs avisés, Maître Eric Caprioli, du cabinet d'avocats Caprioli & Associés.

L'auteur

Eric A. CAPRIOLI,

Avocat à la Cour, Docteur en droit, Vice-Président du CESIN.

Suite aux attaques perpétrées contre « Charlie Hebdo » et le supermarché « Hyper- Cacher » les 7, 8 et 9 janvier dernier, le gouvernement a pris une série de mesures retranscrites dans le projet de loi relatif au renseignement et destinées à contrer la menace terroriste qui pèse sur le France. Le projet de loi a été largement approuvé le 5 mai dernier devant l'Assemblée nationale, en première lecture, et il vient d'être examiné par les sénateurs pour aller devant la commission mixte paritaire avant son adoption définitive. La difficulté de trouver un équilibre entre la nécessité d'assurer la sécurité des Français et celle de préserver les libertés publiques est accentuée dans le cadre de ce projet de loi[1]. Pour beaucoup en effet, cette loi signe la fin de la protection de la vie privée en ce qu'elle aboutirait à une « surveillance de masse » des individus. De surcroît, certains concepts restent encore flous et les mécanismes technico-juridiques mis en place présentent quelques complexités dont certaines seront développées dans le présent article. Le projet est dénoncé avec force comme mettant en place une surveillance de masse, à la suite de pétitions en ligne et de la montée au créneau de plusieurs organisations (Ligue des droits de l'homme, Association des Fournisseurs d'Accès, Quadrature du Net, Syndicat de la Magistrature,...). Le juste équilibre entre sécurité et libertés reste toujours délicat à trouver selon le plateau de la balance sur lequel on met l'accent. Pour les tenants du respect des libertés et de la vie privée, le projet est liberticide, alors que pour les pouvoirs publics, l'impératif de sécurité nationale passe par le renforcement des mesures de contrôle et de surveillance.

Les mesures de sécurité existantes

Au préalable, il convient de rappeler brièvement que certaines mesures existent déjà en matière de renseignement.

- **La loi n°91-646 du 10 juillet 1991** relative au secret des correspondances instaure un régime général permettant d'autoriser les interceptions de sécurité en dehors de toute intervention du juge judiciaire et sous le contrôle de la Commission nationale de contrôle des interceptions de sécurité (CNCIS).
- **Après la première loi de 2001 (loi sur la sécurité quotidienne), la loi « anti-terroriste » du 23 janvier 2006** quant à elle étend les modalités d'accès aux données de connexion par les services de renseignement sous le contrôle d'une personnalité qualifiée.
- Ensuite, **la LOPSSI est intervenue en 2011.**
- Enfin, en décembre 2013, l**a loi de programmation militaire** du 18 décembre a complété partiellement certaines des dispositions de la loi du 10 juillet 1991. Elle unifie les régimes d'accès administratifs aux données techniques de connexion et introduit un régime spécifique à la géolocalisation grâce aux informations fournies par les réseaux ou services de communication électroniques[2]. L'article 20 de ladite loi prévoit en partie la possibilité pour les pouvoirs publics, dans le cadre de leur recherche de

[1] Marine Babonneau, Le projet de loi sur le renseignement est publié, Dalloz actualité du 20 mars 2015.

[2] Legifrance, Projet de loi relatif au renseignement ; Etude d'impact ; NOR: PRMX1504410L / Bleue-1, 18 mars 2015.

renseignements intéressant notamment la sécurité nationale ou la prévention du terrorisme, d'accéder via les opérateurs et hébergeurs, à tous les « documents » et aux « informations » stockés chez les hébergeurs ou transmis au travers des Fournisseurs d'accès à Internet (FAI). Cet article a fait l'objet d'un décret d'application en date du 24 décembre 2014. Il précise notamment les types de documents et informations pouvant être transmis. Il s'agit en réalité de ceux mentionnés aux articles R.10-13 et R.10-14 du Code des postes et des communications électroniques (par exemple sont visées les informations fournies lors de la création d'un compte auprès d'un hébergeur : identifiant de la connexion, noms et prénoms, adresse postale, email, numéros de téléphone ...).

• On rappellera également que **la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme** a, outre les disposition d'interdiction de sortie du territoire, d'interdiction administrative du territoire, d'assignation à résidence, de répression des actes de terrorisme et d'apologie du terrorisme sur l'internet, notamment modifié l'article 323-3 du code pénal afin de mieux protéger les organisations contre les fuites d'information en ajoutant les termes *« extraire, détenir, reproduire et transmettre »* les données contenues dans le système d'information[3]. La sanction est plus forte que celle réprimant le vol de données (reconnu récemment dans l'affaire BlueTouff par la chambre criminelle de la Cour de cassation le 20 mai 2015) : 5 ans d'emprisonnement (contre 3 ans pour le vol) et 75.000 euros d'amende.

Face à la menace terroriste, de nouvelles mesures exceptionnelles

Le projet de loi relatif au Renseignement devrait donner un cadre légal à certaines pratiques de surveillance des services de renseignement (ce qui n'était pas le cas jusqu'à présent) afin de les autoriser à recourir à des moyens techniques d'accès à l'information tout en garantissant le respect des libertés publiques et de la vie privée.

En ce sens, et dans le cadre de la lutte contre la diffusion de la propagande terroriste sur Internet la loi prévoit la possibilité pour l'autorité administrative de demander aux FAI de bloquer l'accès aux sites faisant l'apologie du terrorisme ou qui le provoquent. Par ailleurs, elle permet, lors d'opérations la mise en place de dispositifs mobiles de proximité *« permettant de capter directement des données de connexion strictement nécessaires à l'identification d'un équipement terminal ou de numéro de son utilisateur »* (article L. 851-7 du Code de la Sécurité Intérieure) ; ou encore l'utilisation de dispositifs permettant de localiser en temps réel un véhicule ou un objet (article L 851-6 du Code de la Sécurité Intérieure).

Mais elle prévoit surtout, pour les seuls besoins de la prévention du terrorisme, l'installation chez les FAI et certains grands sites internet (y compris les réseaux sociaux) d'un dispositif d'analyse automatique de données créé par les services de renseignements eux même. Ce dispositif est censé *« révéler une menace terroriste »* permettant ainsi l'accès administratif aux données de connexion des FAI. Ainsi, le Premier ministre, pourra ordonner aux opérateurs et aux FAI *« de détecter, par un traitement automatique, une succession suspecte de données de connexion »* (article L 832-3 du Code de la Sécurité Intérieure). Il s'agit en réalité d'installer des outils d'analyse automatique, les fameuses *« boites noires, dites algorithmiques »*, chez les réseaux des opérateurs afin de repérer automatiquement les comportements qui présentent des menaces pour la sécurité et ce, même si une personne n'est pas spécifiquement désignée. C'est au sein de ces « boîtes noires » que l'on trouve les algorithmes qui sont censés filtrer les « comportements suspects » figurant dans la masse de données recueillies. Et c'est précisément sur ce dernier point que doit se focaliser notre attention.

Au niveau du contrôle, la loi créée la Commission nationale de contrôle des techniques de renseignements (CNCTR) remplaçant l'actuelle CNCIS. Le projet de loi lui consacre un rôle majeur. En effet, bien que la mise en œuvre sur le territoire national des techniques de recueil du renseignement est soumise à autorisation préalable du Premier ministre, les autorisations sont délivrées, après avis de ladite Commission (article L 821-1 du Code de la Sécurité Intérieure)[4].

De surcroît, au-delà des autorisations données sous forme d'avis, le gouvernement a annoncé à plusieurs reprises que cette Commission sera chargée d'inspecter le code source du programme mit en place par l'algorithme afin de s'assurer des finalités de fonctionnement. Ceci implique nécessairement qu'elle soit dotée des compétences techniques spécifiques pour analyser l'algorithme et surtout son paramétrage. Le ministre de l'intérieur a précisé que dans les cas où l'algorithme détectera un comportement suspect, la surveillance supplémentaire qui en découlera passerait à nouveau par la CNCTR.

L'algorithme au cœur du contrôle

Ce sont les détails et le périmètre de la détection automatique qui suscitent l'inquiétude aussi bien de la part des individus que des entreprises. En effet, comment s'assurer concrètement que l'algorithme en question recueillera uniquement les informations pertinentes au regard d'une réelle menace terroriste ? Chaque connexion ou recherche effectuée par les internautes, y compris celles effectuées dans un but strictement professionnel serait ainsi soumise à surveillance ? Que deviendront les secrets d'entreprise ou le secret professionnel des avocats ? Nombreuses sont les interrogations de ce type.

Alors que le décret relatif à l'application de l'article 20 de la loi de programmation militaire de 2013 prévoyait que les « informations » et « documents » concernés seraient recueillis par les hébergeurs et opérateurs eux-mêmes, la loi sur le Renseignement prévoit, elle, un accès direct à ces informations par les services de l'Etat compétents.

Toujours en ce sens, la CNCTR, sur qui pèse l'entier poids du contrôle de l'algorithme et des mécanismes mis en place par le projet de loi, sera composée de 9 membres, en principe (sous réserve du texte final) deux députés, deux sénateurs, deux membres du Conseil d'Etat, deux magistrats et *« une*

[3] Eric A. Caprioli, La lutte contre la cybercriminalité, La semaine Juridique, éd. G, n°15-13 avril 2015 p.754.

[4] www.assemblee-nationale.fr n°2669 Projet de loi relatif au renseignement. (http://www.assemblee-nationale.fr/14/projets/pl2669.asp)

personnalité qualifiée pour ses connaissances en matière de communications électroniques». Deux remarques méritent ici d'être soulevées.

D'une part, on constatera que une présence de l'autorité judiciaire très minime, ce que de nombreux avocats déplorent. N'oublions pas que le juge est le gardien des libertés ! Les avocats revendiquent, notamment, que la CNCTR n'ait qu'un simple rôle consultatif étant donné que c'est la liberté des individus qui est en jeu. D'où la nécessité de l'intervention du juge judiciaire qui devrait disposer d'un rôle majeur dans ces dispositifs de contrôle afin de légitimer cette «entrave» aux libertés. Or, force est de constater que dans l'actuel dispositif son intervention est plus que limitée, et dans tous les cas a posteriori.

D'autre part, le fait qu'il ne soit prévu l'intervention que d'un seul expert chargé d'expertiser l'algorithme nous semble largement insuffisant notamment eu égard à la complexité et à la technicité du mécanisme envisagé par le projet de loi. De plus, le contrôle du paramétrage de la boîte noire sera délicat étant donné qu'il peut être modifié rapidement, alors que l'analyse technique risque de prendre du temps. D'ailleurs, pour certains spécialistes, même les algorithmes les plus performants présenteraient des failles. Le risque ici serait de soupçonner des personnes innocentes, tout en sachant que les mesures de surveillance seront utilisées à la fois pour les suspects, mais aussi pour les «*personnes appartenant à son entourage*» dans les cas où «*il existe des raisons sérieuses de croire qu'elles ont joué un rôle d'intermédiaire volontaire ou non*». Enfin, au-delà du monopole de contrôle donné à l'autorité administrative, bien que la loi prévoit l'anonymisation des données retranscrites par l'algorithme, tout est fait pour retrouver l'identité de la personne qui est «suspecte». Ainsi, en théorie, l'algorithme ne doit s'intéresser qu'aux seules données de connexion (les métadonnées) et non pas au contenu des communications. Cependant, en pratique, il paraît évident, ou à tout le moins possible, que l'on puisse clairement identifier les individus à partir des données collectées !

Finalement, force est de constater que le projet de texte opère un glissement significatif vers des procédures administratives au détriment du judiciaire. Ceci aurait pour conséquence de rompre l'équilibre dans la balance entre la sécurité et la liberté ; or, si la balance symbolise la justice, avec ce nouveau texte, il ne resterait que le glaive symbolisant la force du pouvoir de sanctionner s'appuyant non plus sur le juge, mais sur l'arbitraire des autorités administratives.

Ne dit-on pas que la nécessité fait loi ? Cette approche «administrative» qui tend à se généraliser, s'inscrit dans un mouvement européen plus large, voire mondial de lutte contre le terrorisme. Cela s'explique aussi sans doute par la lenteur des procès pénaux, versus la rapidité et l'efficacité des procédés envisagés. Les pouvoirs exceptionnels conférés au pouvoir administratif supposent des contre-pouvoirs et ne faut-il pas réfléchir dès à présent à l'édification d'un Ordre public numérique, protecteur des libertés numériques ? ■