La loi sur le Renseignement et ses impacts SEO

Par Alexandre Diehl

Domaine :	**Recherche**	**Référencement**
Niveau :	**Pour tous**	Avancé

En termes de déréférencement de site web pour de nombreux motifs (le principal étan tbien sûr le côté illicite des contenus proposés), l'arsenal judiciaire était déjà assez conséquent en France. La récente Loi sur le Renseignement amène une couche supplémentaire de possibilités et pourrait ajouter plusieurs contraintes, de limitations et de charges aux moteurs de recherche. Décryptage.

La loi n°2015-912 du 24 juillet 2015 relative au renseignement est venue compléter le dispositif existant sur les possibilités laissées aux gouvernants de limiter l'accès à certains sites ou de déréférencer certains contenus. Si le droit positif français connaissait déjà ces pratiques, la nouvelle loi a créé des modalités complémentaires extraordinaires et très discutables. Au-delà de l'aspect polémiste, les mécanismes créés doivent être connus, car ils auront à s'appliquer très rapidement et potentiellement de manière spectaculaire.

Rappels de principes généraux

Pour que les principes nouveaux soient appréhendables par tous, certaines bases doivent être rappelées :

• Traditionnellement, dans les démocraties, les trois pouvoirs sont séparés. Ainsi, le législateur définit et vote la loi, l'exécutif la fait respecter et détermine ses modalités et la justice applique et sanctionne. Le rôle du juge, dans les démocraties, repose sur une totale impartialité théorique. Ainsi, le juge ne définit pas si une action était bien ou pas, mais si elle était conforme à la loi ou pas. Il faut bien comprendre que ce qu'on appelle le « pouvoir administratif » ou « exécutif » est souvent décrit comme le pouvoir politique, en d'autres termes, des administrations qui ne répondent qu'aux demandes des politiques au pouvoir et non aux textes qui les encadrent.

• De surcroît, toutes les démocraties (voire même quasiment tous les pays modernes) appliquent le principe de la théorie des normes ou encore la hiérarchie des normes où chaque principe / thème est rangé à un étage de la hiérarchie, avec compétence spéciale à une entité pour un rang (en d'autres termes, des droits spécifiques associés à un profil). Les principes les plus importants sont du domaine du peuple alors que les détails sans importance relèvent de fonctionnaires inconnus du public.

Le droit français repose donc sur une hiérarchie des normes contrôlée par les juges. Ce principe s'applique à tous les domaines et notamment à ce qui touche Internet de près ou non.

Le champ d'application de la loi Renseignement

La loi Renseignement a été votée officiellement en réaction aux attentats de janvier 2015 en France (même si la loi était très largement dessinée avant ces évènements). Elle a pour finalité de permettre de lutter plus efficacement contre le terrorisme et son financement, mais également pour légaliser des pratiques habituelles des services et de la police non couvertes par la loi.

Contrairement à ce que certains pourraient croire, les services de l'Etat n'ont jamais pratiqué l'interception à grande échelle de mails, le blocage de site ou le déréférencement de contenus en violation de la loi. Cette nouvelle loi est donc l'arrivée d'une ère nouvelle en matière d'intervention de l'Etat sur les blocages de sites et déréférencement.

Le nouvel article 801 du Code de la Sécurité Intérieure dispose que les techniques prévues par la loi *« ne peuvent être décidées que si :*
(…)
4° Elles sont justifiées par les menaces, les risques et les enjeux liés aux intérêts fondamentaux de la Nation ;
5° Les atteintes qu'elles portent au respect de la vie privée sont proportionnées aux motifs invoqués. »

Or, les intérêts fondamentaux de la Nation comprennent :
« 1. L''indépendance nationale, l'intégrité du territoire et la défense nationale ;
2° Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ;
3° Les intérêts économiques, industriels et scientifiques majeurs de la France ;
4° La prévention du terrorisme ;
6° La prévention de la criminalité et de la délinquance organisées ;
7° La prévention de la prolifération des armes de destruction massive. »

Pour que soient bien compris les enjeux du champ d'application de la loi (et donc d'appréhender dans quels cas le régime ci-après décrit peut être appliqué à chacun d'entre nous), il faut bien préciser que la notion de « criminalité et de la délinquance organisées » ne vise pas simplement les mafias, mais également tout type de délit ou crime qui a été organisé, préparé et prémédité par au moins deux personnes qui se concertent et se répartissent des rôles pour pouvoir tirer, chacune, un profit d'un crime à venir. Par exemple, une fraude fiscale organisée entre dans le champ de la loi Renseignement. Ou encore une faillite organisée par des amis peut également entrer dans le champ de la loi…

En d'autres termes, cette loi ne vise pas uniquement à lutter contre le terrorisme et les mafias, mais contre toute sorte de crime et délit « organisé ». Le champ est donc

beaucoup plus large que l'on pourrait penser et, donc, peut s'appliquer beaucoup plus souvent qu'on ne le pense.

Le régime du blocage et déréférencement avant la loi Renseignement

Dans le cadre de plusieurs Lettres R&R par le passé, nous avons eu l'occasion de préciser les atteintes à la liberté d'expression qui se formalisent notamment par les possibilités, pour les pouvoirs (judiciaires et politiques), de bloquer des contenus, les déréférencer et/ou d'en demander un contrôle *a priori*.

Par exemple, l'article 6 rappelle que les FAI, les hébergeurs, mais également les moteurs de recherche et autres intermédiaires doivent lutter activement contre les sites racistes, antisémites, pédopornographiques, etc. en mettant *« en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance »* de tels contenus.

De plus, plusieurs dispositifs permettent désormais à l'autorité judiciaire de demander la suspension de l'accès à certains sites web. Cette pratique est apparue surtout dans des affaires propres à des sites illégaux de paris en ligne où l'ARJEL avait demandé au Tribunal de Grande Instance de Paris de bloquer certains sites. Autre exemple, le 4 décembre 2014, le Tribunal de Grande Instance de Paris a ordonné à Bouygues, Free, Orange et SFR, d'empêcher l'accès de leurs abonnés, depuis le territoire français, au site thepiratebay.se et aux sites de redirection, sites miroirs et proxies associés.

Autre exemple, depuis la loi de programmation militaire du 18 décembre 2013, les services de police, les services secrets et les services de Bercy (y compris l'administration fiscale…) peuvent solliciter de la part des personnes désignées à l'alinéa I.2 de l'article 6 de la LEN (et donc des moteurs de recherche) :

- *« des informations ou documents traités ou conservés par leurs services »,*
- *« les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications ».*

Pis, ces documents et informations *« peuvent être recueillis sur sollicitation du réseau et transmis en temps réel par les opérateurs aux agents »*. Ces demandes ne sont pas contrôlées par un juge, mais par une *« personnalité qualifiée placée auprès du Premier ministre ».*

D'un point de vue judiciaire (en passant par un juge qui va trancher), le champ d'application est encore plus large concernant les moteurs de recherche. En vertu de plusieurs dispositions, les moteurs doivent lutter de manière positive (c'est-à-dire en

mettant en œuvre des mesures spécifiques, en mobilisant des équipes, en touchant s'il le faut aux résultats naturels fournis) contre notamment :

- Le terrorisme et son financement,
- La contrefaçon,
- Les contenus propres à l'apologie des crimes contre l'humanité, à la provocation à la commission d'actes de terrorisme et de leur apologie, à l'incitation à la violence, à l'incitation à la haine raciale, à la haine à l'égard de personnes à raison de leur sexe, de leur orientation ou identité sexuelle ou de leur handicap,
- La pornographie enfantine,
- Les activités illégales de jeux d'argent.

En conséquence, dès qu'un contenu illicite est repéré, il est possible de demander à un juge d'obtenir son blocage. Dans ce cas précis, le moteur de recherche est assigné et peut donc présenter des arguments, quitte à ce qu'ils soient favorables au blocage du site. En toutes hypothèses, cette procédure démocratique permet un dialogue entre les parties prenantes au dossier et non une décision unilatérale du pouvoir en place s'imposant aux moteurs.

Les ajouts de la loi Renseignement

Il est important de comprendre que la loi Renseignement n'a retiré aucune possibilité aux autorités de contrôler, bloquer et/ou déréférencer des contenus sur Internet, mais a ajouté une couche supplémentaire de moyens juridiques.

D'une part, les éventuels prestataires de cryptologie (chiffrement et cryptographie, dont les certificats SSL) doivent remettre les clés de déchiffrement aux services quand ils le demandent. La plupart des prestataires étant basés à l'étranger, il sera intéressant de voir comment cette disposition s'appliquera dans le temps.

D'autre part, dans le prolongement de la loi de programmation militaire, les services de police, les services secrets et les services de Bercy peuvent toujours solliciter de la part des intermédiaires les mêmes informations et documents (données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques). En revanche, la nouveauté par rapport à la loi de programmation militaire est que ces documents et informations « peuvent être recueillis en temps réel par les opérateurs aux agents », sans demande spécifique (donc les services se « servent » directement sur les serveurs des opérateurs et intermédiaires), s'il s'agit d'une personne préalablement identifiée comme présentant une menace terroriste.

De plus, l'autorisation d'interception délivrée peut imposer aux intermédiaires, pour les seuls besoins de la prévention du terrorisme, la mise en œuvre sur leurs réseaux de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste. En d'autres termes, une nouvelle charge potentielle pour les opérateurs et moteurs.

Les membres de la commission de contrôle des techniques de renseignement (créée pour l'occasion et composée de députés, sénateurs, conseillers d'Etat et magistrats uniquement) peuvent « entrer » à tout moment dans les locaux des opérateurs et intermédiaires pour contrôler la mise en œuvre effective des mesures demandées. Idem, la plupart des prestataires étant basés à l'étranger, il sera curieux de connaitre comment cette disposition s'appliquera dans le temps.

La loi a eu la décence de préciser que « *les surcoûts identifiables et spécifiques éventuellement exposés par les opérateurs (…) font l'objet d'une compensation financière de la part de l'Etat* ». Evidemment, il n'est pas précisé combien…

Année après année, le pouvoir en place ajoute des couches juridiques de plus en plus administratives (donc contrôlées par les politiques) et de moins en moins judiciaires (pouvoir indépendant du politique) permettant le contrôle du contenu sur Internet et le blocage de sites. Si les raisons sont toujours louables, les faits sont que les intermédiaires (moteurs, hébergeurs, etc…) connaissent de plus en plus de contraintes, de limitations et de charges.

Alexandre Diehl, *Avocat à la Cour, cabinet Lawint (http://www.lawint.com/)*