Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

LE PRESIDENT DU CONSEIL NATIONAL DU NUMERIQUE

Paris, le 29 avril 2015

Monsieur le Président,

Le Conseil national du numérique a été auditionné par votre commission le 28 avril 2015 au sujet du projet de loi relatif au renseignement. Comme convenu lors de cet entretien, vous trouverez ci-après une synthèse des éléments exposés durant cette audition.

Je vous prie d'agréer, Monsieur le Président, l'expression de ma considération la plus distinguée.

Benoît Thieulin

Monsieur Philippe Bas
Président de la Commission des lois
Sénat
Palais du Luxembourg
15, rue de Vaugirard
75291 Paris Cedex 06

CNNum
Conseil National du Numérique

BATIMENT ATRIUM – 5 PLACE DES VINS DE FRANCE 75572 PARIS CEDEX 12
TÉL. 01 53 44 21 27 - MÉL. INFO@CNNUMERIQUE.FR

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

LE PRESIDENT DU CONSEIL NATIONAL DU NUMERIQUE

Note à l'attention de Monsieur le Sénateur Philippe Bas,
Président de la commission des lois du Sénat

Synthèses des éléments exposés par le Conseil national du numérique à l'occasion de son audition du 28 avril 2015

La menace terroriste est protéiforme et sans précédent. Il n'est donc pas anormal que les services de renseignement cherchent à adapter leurs outils et le cadre juridique. Une loi apparaît donc nécessaire pour « *toiletter* » le texte de 1991, intervenu à une époque où Internet n'avait rien à voir avec le réseau d'aujourd'hui.

Sommes toutes, le texte présente des certaines avancées. Le dispositif général permettra notamment de réduire les « *zones grises* » : les services ne pourront (théoriquement) plus plaider l'absence d'interdiction pour utiliser certaines pratiques *sous le manteau*. Ce texte est également l'occasion d'instaurer un contrôle accru – par la création d'une structure renforcée – ainsi qu'un droit de recours - devant une juridiction nouvelle à laquelle on ne pourra opposer le secret défense. Enfin, le renseignement fait depuis quelques semaines l'objet d'un véritable débat contradictoire, dans le Parlement et en dehors.

A l'instar de nombreux acteurs du numérique, le Conseil exprime toutefois de sérieuses inquiétudes à l'endroit de certaines dispositions du projet de loi relatif au renseignement.

****

1. Une extension problématique du périmètre du renseignement

Il est regrettable que le débat tende à se concentrer autour de la menace terroriste, alors même qu'il ne s'agit que d'une seule des sept finalités du renseignement élargies par le projet de loi. Le texte permet ainsi de généraliser les méthodes extrêmement intrusives de la lutte contre le terrorisme à des domaines beaucoup plus vastes.

Il est notamment question de « *la prévention de la délinquance et de la criminalité organisée* », dont le régime est tentaculaire puisqu'il regroupe un nombre impressionnant d'infractions, sitôt qu'elles sont commises en « *bande organisée* » - une notion floue en droit pénal. Le projet de loi autorise par ailleurs les services à recourir aux techniques de surveillance pour deux nouveaux motifs aux contours extrêmement flous, à savoir « *la prévention des violences collectives de nature à porter gravement atteinte à la paix*

CNNum
Conseil National du Numérique
BATIMENT ATRIUM – 5 PLACE DES VINS DE FRANCE 75572 PARIS CEDEX 12
TÉL. 01 53 44 21 27 - MÉL. INFO@CNNUMERIQUE.FR

publique », qui soulève des inquiétudes du fait de ses nombreuses interprétations, ainsi que « *les intérêts majeurs de la politique étrangère* », difficile à cerner tant la diplomatie française est complexe. Pour tous ces motifs, le projet de loi s'en tient à ces finalités générales et ne définit pas en profondeur les missions de chacun des services de renseignements, reléguées aux décrets. Enfin, le Conseil regrette l'abandon du caractère exceptionnel des écoutes.

2. L'introduction de nouvelles techniques de renseignement, dont la plus problématique : la « *boîte noire* » installée chez les opérateurs et hébergeurs

Tout d'abord, la formulation du dispositif est inquiétante car extrêmement large. Le dispositif ne se définit que par sa finalité (la lutte contre le terrorisme) sans prévoir les moyens de sa mise en œuvre, qui restent l'apanage de l'exécutif. Or ceux-ci peuvent être extrêmement divers et inégalement attentatoires aux libertés individuelles. Le Conseil est conscient du défi légistique qui s'est posé aux rédacteurs du texte (une formulation trop précise risquerait de révéler les techniques spéciales utilisées). Il devrait toutefois être possible de trouver un juste milieu. Par ailleurs, ce dispositif vise indistinctivement tous les acteurs de l'Internet : opérateurs télécoms, prestataires techniques, jusqu'aux hébergeurs et fournisseurs de services.

Cette technique suppose une surveillance indiscriminée du trafic par un algorithme, confinant ainsi à de la surveillance de masse[1]. Ce dispositif revient dès lors à placer l'algorithme au cœur de notre mode de gouvernance. Il semble par là aller à rebours de la lettre et l'esprit de l'article 10 de la loi Informatique et Libertés, modifié par la loi du 6 août 2004, qui dispose qu' « *aucune décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité* ». Cette disposition montre que le législateur avait déjà bien conscience des dangers de ce type de dispositifs.

Par ailleurs, son efficacité apparaît relative. Le parallèle avec la surveillance pratiquée par les géants du net n'apparaît pas pertinente car les activités « *terroristes* » ne présentent pas une fréquence suffisante pour permettre de nourrir une méthode automatisée. Ces algorithmes devront donc procéder par induction, alors même que ces méthodes ont démontré leur inefficacité outre-Atlantique.

Enfin, comme le remarque la CNIL – les données collectées par l'algorithme ne sauraient constituer des éléments anonymes dans la mesure où les métadonnées sont indirectement ou directement identifiantes. Il est en effet très facile d'assurer l'identification d'un individu en combinant un petit nombre de traitements de données. De nombreuses études[2], ainsi que la Cour de justice de l'Union européenne l'ont expliqué très clairement : « *ces données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises*

[1] En effet pour de simples raisons de ressources humaines, une surveillance de masse ne peut être
[2] Par exemple : http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/

BATIMENT ATRIUM – 5 PLACE DES VINS DE FRANCE 75572 PARIS CEDEX 12
TÉL. 01 53 44 21 27 - MÉL. INFO@CNNUMERIQUE.FR

concernant la personne dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci »[3].

Pour toutes ces raisons, le Conseil national du numérique recommande à votre Commission l'abandon pur et simple de ce dispositif de détection automatique des comportements « *suspects* ».

3. Ce projet fait peser un risque économique majeur aux intérêts économiques de la France en favorisant la fuite de l'offre et de la demande

Ce projet de loi s'inscrit à rebours de l'ambition affichée par ce gouvernement de construire une véritable stratégie numérique, de concurrencer les géants américains de l'Internet et de relancer la croissance française. Dans un contexte post-Snowden où la protection des données personnelles tend en effet à devenir de plus en plus déterminante pour les consommateurs, ces dispositions menacent la confiance des utilisateurs, condition *sine qua none* du développement de l'économie numérique.

Par ailleurs, certaines dispositions du projet de loi pourraient asphyxier l'activité de certaines entreprises numériques. L'offre de biens et de produits numériques étant le corollaire de sa demande, dès lors, la fuite de cette dernière entraînant irrémédiablement celle du premier. Le risque étant une décrédibilisation de ces entreprises vis-à-vis de leurs clients, obligeant celles-ci à délocaliser progressivement leurs serveurs pour être à même de rivaliser avec des concurrents internationaux qui ne sont pas sous le spectre d'une surveillance généralisée. Il existe dès lors un risque de voir s'egratiner le potentiel de croissance de notre économie numérique, ce qui ne manquera pas de pérenniser la position déjà dominante des acteurs américains sur le marché.

4. Renforcer les garanties de contrôle et la voie de retour démocratique

Il est regrettable que ce projet de loi ne soit pas l'occasion de créer durablement une voie de retour démocratique entre les services secrets et la société. II est impossible de faire abstraction des révélations d'Edward Snowden car elles posent la question de la confiance. Le manque de pont entre la Nation et ses services de renseignement amène à un climat de défiance ainsi qu'à des réactions épidermiques et suspicieuses. L'ouverture du chantier législatif devrait dès lors consister à développer la redevabilité (*accountability*) de la communauté du renseignement, qui doit communiquer et rendre des comptes au public sur son action. Dans cette relation, le contrôleur doit jouer un rôle de tiers de confiance et pour ce

[3] CJUE, arrêt du 8 avril 2014 (C-293/12 et C-594/12).

BATIMENT ATRIUM – 5 PLACE DES VINS DE FRANCE 75572 PARIS CEDEX 12
TÉL. 01 53 44 21 27 - MÉL. INFO@CNNUMERIQUE.FR

faire, il doit disposer de moyens à la mesure des pouvoirs des services. A ce titre, la mise à niveau n'apparaît pas suffisante, la nouvelle Commission de contrôle des techniques de renseignement (CNCTR) ne disposant que d'un pouvoir de contrôle et d'enquête limités.

Pour ce qui concerne le contrôle *a priori*, l'extension du périmètre du renseignement devrait se traduire par une procédure d'avis conforme, d'application obligatoire pour l'exécutif. Concernant le contrôle *a posteriori*, la CNCTR devrait disposer d'un accès permanent aux données brutes collectées par les services de renseignement. Elle devrait en outre disposer d'un pouvoir d'audition, d'accès aux locaux et aux documents pertinents illimités. Il conviendrait à ce titre de s'inspirer du contrôleur britannique (*Intelligence Service Commissionner & Interception of Communication Commissionner*), qui dispose de véritable pouvoirs d'enquêtes : visites à discrétion dans les services, possibilité d'entendre tous les agents de son choix, droit d'accès aux documents sans entrave.

Enfin, l'expérience américaine ainsi que les révélations d'Edward Snowden devraient nous conduire à renforcer les moyens humains et **techniques** de la CNCTR.

Benoît Thieulin
Président du Conseil national du numérique

CNNum
Conseil National du Numérique

BATIMENT ATRIUM – 5 PLACE DES VINS DE FRANCE 75572 PARIS CEDEX 12
TÉL. 01 53 44 21 27 - MÈL. INFO@CNNUMERIQUE.FR