Note relative au Projet de Loi de programmation militaire 2014 - 2019
- 3 décembre 2013 -

Depuis de nombreuses années, parlementaires et Gouvernements ont étendu les pouvoirs des services spécialisés en matière d'accès aux données.

Même si ce souhait est voulu dans un but de permettre une lutte efficace contre toutes les formes de criminalités, l'ASIC (Association des Services Internet Communautaires) s'alarme de ces propositions qui, si elles sont adoptées, pourraient mettre en péril l'écosystème innovant mais fragile de l'économie numérique en France. En adoptant de telles mesures, **la France provoquerait un déficit de confiance vis à vis des solutions nationales d'hébergement et pourraient handicaper le développement d'un secteur porteur de croissance.**

Créée en décembre 2007, l'ASIC (www.lasic.fr) est la première organisation française qui regroupe des intermédiaires du web 2.0 – moteurs de recherche, plateformes de transactions, sites de partage de contenus, réseaux sociaux, etc.

Cette note est destinée à revenir sur les changements opérés par l'article 13 de la Loi de programmation militaire en termes d'accès aux données et documents détenues par les intermédiaires de l'internet et, plus spécifiquement, les hébergeurs tels que définis à l'article 6.I.2 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique.

La note n'aborde pas la question des modifications instaurées par le Projet de Loi de programmation militaire sur les opérateurs de télécommunication et les fournisseurs d'accès à l'internet.

Elle souhaite se focaliser sur l'impact de ces mesures sur les seuls hébergeurs, tels que définis par la loi pour la confiance dans l'économie numérique, incluant les diverses plateformes de blog, de petites annonces, de vidéo, etc.

En droit français, trois régimes coexistent afin de permettre aux autorités de répondre aux enjeux de lutte contre la criminalité :

- l'accès aux données d'identification détenues par les intermédiaires de l'internet, permettant par exemple d'identifier qui est l'auteur de tel ou tel contenu (blog, commentaire, vidéo, petite annonce, etc.) ;

- l'interception des communications électroniques (téléphone, SMS, emails) échangées entre deux individus. Il s'agit d'une interception de ces communications pour le futur et une durée déterminée ;

- la perquisition des documents possédés par une personne soit sur un disque dur interne (ordinateur, etc.) soit dans le cloud (hébergement à distance).

Nous le verrons, le régime tel que proposé dans le Projet de Loi de programmation militaire tend à créer une confusion entre le premier et dernier de ces régimes et à offrir aux autorités, pour certaines finalités déterminées, un pouvoir de "perquisition" auprès d'hébergeurs sans qu'aucune des garanties prévues en la matière ne soient respectées.

*

* *

I. - Synthèse relative au régime d'accès aux données techniques avant et après le Projet de Loi de programmation militaire

1. - Cadre actuel de l'accès aux données techniques

Type de régime	Qui peut avoir accès aux données ?	Quel fondement ?	Pour quelles finalités	Quel type de contrôle ?	Quelles données sont visées ?
Régime de droit commun	Police, Gendarmerie, Services spécialisés (article 6.II. de la LCEN)	Réquisition judiciaire	Toute infraction	Réquisition pris dans le cadre d'une enquête ouverte sous le contrôle d'un magistrat	Les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires.
	DGFIP (L96G, L83 du livre des procédures fiscales)	Droit de communication	Contrôle de l'impôt	n/a	idem
	DNEF (L96G, L83 du livre des procédures fiscales)	Droit de communication	Contrôle de l'impôt	n/a	idem
	DGDDI (article 65 du Code des douanes)	Droit de communication / Réquisition judiciaire	Pouvoir général de droit de communication	Possible contrôle d'un magistrat	idem
	DGCCRF ou DDCSPP (L. 450-1 du Code de commerce)	Demande / Réquisition	Enquêtes et contrôles	Possible contrôle d'un magistrat	idem
	Autorité de la concurrence (L. 450-1 du Code de commerce)	Demande	Enquêtes et contrôles de l'AMF	n/a	idem

	Autorité des marchés financiers (L. 621-10 du Code monétaire et financier)	Droit de communication	Enquête et contrôles de l'AMF	n/a	idem
	URSSAF (L. 114-19 et L.114-20 du Code de la sécurité sociale)	Droit de communication	Contrôle et lutte contre la fraude	n/a	idem
Régime d'exception (en vigueur jusqu'au 31 décembre 2015)	Les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales spécialement chargés de ces missions (UCLAT)	Demandes administratives	Prévenir les actes de terrorisme.	Contrôle a posteriori de la CNCIS	idem

(*) ce tableau n'inclut pas le pouvoir détenu par certaines administrations d'accéder également à des documents en particulier à des pièces comptables (tel est le cas de la DGFIP et de la DNEF en application de l'article L96G ou de l'article 102B du livre des procédures fiscales) ou par l'intermédiaire de saisies.

2. - L'impact de la loi de programmation militaire sur le régime d'exception existant

Si le Projet de Loi de programmation militaire ne modifie pas le régime de droit commun, il procède à de nombreux ajustements prévus en matière de terrorisme. Ces modifications, détaillées ci-après, recouvrent notamment les données qui pourront être obtenues auprès des hébergeurs, la méthode de collecte et les personnes qui pourront y avoir accès.

Type de régime	**Qui peut avoir accès aux données ?**	**Quel fondement ?**	**Pour quelles finalités**	**Quel type de contrôle ?**	**Quelles données sont visées ?**
Régime d'exception (sans limitation de durée)	Les agents désignés et dûment habilités des services relevant des ministres chargés - de la sécurité intérieure - de la défense, - de l'économie - et du budget	Demandes administratives par "sollicitation du réseau" et en "temps réel".	Rechercher de renseignements intéressant - la sécurité nationale, - la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France, - la prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous	Contrôle a posteriori de la CNCIS	Informations ou documents traités ou conservés par leurs réseaux ou services (...), y compris les données techniques.

3. - Les principales modifications opérées par le Projet de Loi de programmation militaire

A l'issue de la discussion à l'Assemblée nationale, les principales modifications opérées par le Projet de Loi de programmation militaire concernent :

- la liste des personnes pouvant obtenir l'accès aux données sur la base du régime dit d'exception ;
- les finalités de l'accès à ces informations qui s'étendent au delà du périmètre des seuls cas de terrorisme ;
- les modalités d'accès à ces données (par sollicitation du réseau) alors qu'auparavant les intermédiaires étaient en mesure de réaliser un contrôle de chaque demande adressée par un examen de la réquisition et/ou du droit de communication reçu ;
- la nature des données accessibles : contrairement au régime actuel, le texte étend très largement les modalités d'accès puisque cet accès concerne non seulement les données techniques (auparavant seules accessibles sur ce régime de l'accès) à toute "information ou document" conservés par les hébergeurs ;
- la généralisation d'un régime d'exception qui était, à l'origine, destiné à ne pas se poursuivre au delà du 1er janvier 2008.

L'ensemble de ces mesures appelle de la part de l'ASIC plusieurs commentaires.

II. - Les questions soulevées par le Projet de Loi de programmation militaire

Le Projet de loi de programmation militaire soulève de nombreuses questions. Outre la généralisation d'un régime d'exception d'une première durée de moins de 2 ans, le texte vient faire tomber les protections existantes en matière de perquisition de données informatiques et de créer un régime - pourtant calqué sur celui des interceptions - qui ne reprend pas les garanties adoptées pourtant par le Parlement.

1. - La généralisation d'un régime d'exception

En application de l'article 32 de la loi du 23 janvier 2006, le régime d'exception existant en matière de prévention de terrorisme avait été initialement instauré jusqu'au 31 décembre 2007.

La loi du 1er décembre 2008 visant à prolonger l'application des articles 3,6 et 9 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers a prorogé une première fois ce régime jusqu'au 31 décembre 2012. La loi du 21 décembre 2012 relative à la sécurité et à la lutte contre le terrorisme a, de nouveau, prolongé ce régime d'exception jusqu'au 31 décembre 2015.

Par le Projet de Loi de programmation militaire, ce régime d'exception est dorénavant inscrit durablement dans le temps. Aucune mesure d'impact ou clause de rendez-vous n'ont été prévues.

Lors de chaque examen successif, les parlementaires avaient pourtant estimé que la mesure devait faire l'objet d'un examen et d'une évaluation avant d'être pérennisée. Il apparaît qu'à ce jour, cela n'a pas été le cas. Pourtant, la mesure est, elle, pérennisée.

Avant toute pérennisation, il est donc urgent qu'une évaluation soit menée de la mesure et des raisons justifiant son extension.

2. - Une confusion de deux régimes permettant un contournement des règles fondamentales protectrices en matière de perquisition

Initialement, la loi relative à la confiance dans l'économie numérique - et sa modification instaurée par la loi anti-terrorisme de 2006 - encadrait strictement le cadre des données qui pouvaient être obtenues par les autorités auprès des hébergeurs. Cela ne recouvrent que les données "*de nature à permettre l'identification quiconque a contribué à la création du contenu ou*

de l'un des contenus des services dont elles sont prestataires".

La liste de ces données a été précisée par un décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.

Comme le précise ce texte réglementaire, il s'agit de données purement techniques qui ne portent en aucun cas sur le contenu stocké par l'hébergeur.

En matière de contenu stocké par l'hébergeur, le décret limite l'accès aux seules données relatives aux opérations portant sur un contenu, c'est à dire par exemple, l'adresse IP de connexion, le nom d'utilisateur, la date et heure de l'opération sur le contenu.

La nouvelle formulation retenue par le Projet de Loi de programmation militaire étend très largement le cadre actuel puisqu'elle vise non seulement les données techniques ("y compris les données techniques") mais aussi plus largement toute "information ou document" stockés par l'hébergeur.

Ce mécanisme revient à offrir aux autorités, sans aucun contrôle préalable, un accès à tout document et/ou contenu stocké par un hébergeur sur ces serveurs. En outre, cet accès est prévu en "temps réel", par "sollicitation du réseau", ce qui revient à avoir un accès direct et permanent aux serveurs de l'hébergeur.

Cet accès à des données stockées sur des serveurs constitue en fait un autre régime juridique : la perquisition qui fait l'objet d'un encadrement supplémentaire.

Ainsi, et sans les garanties offertes par le régime juridique des perquisitions, il sera dorénavant possible à ces autorités et pour les finalités visées, d'avoir accès - par exemple - à tous les documents stockés dans un service de "cloud" souscrit par un internaute déterminé.

Il nous semble inquiétant que l'on fasse abstraction du régime juridique de la perquisition, que l'on confonde ce régime - qui fait l'objet d'un plus grand nombre de garantie - avec celui de l'accès aux données.

Cette fusion des deux régimes soulèvent de graves questions en termes de protection des droits et des libertés.

Enfin, le dispositif oublie que le statut de l'hébergeur peut recouvrir certains acteurs qui bénéficient d'un régime plus protecteur, comme par exemple, les sites de presse (voir, à ce sujet, tous les espaces contributifs des sites de presse en ligne ou les plateformes de blog du Monde ou de Mediapart qui seront donc soumis à ces nouvelles obligations d'interconnexion).

3. - Une transposition d'un régime en oubliant de transposer l'ensemble des garanties offertes

Le Projet de Loi de programmation militaire propose d'aligner le régime d'exception d'accès aux données sur celui des interceptions de communications électroniques. Or, les garanties offertes ne sont que partiellement transposées voire inopérantes dans certains cas.

Comparatif des garanties offertes entre le régime des interceptions et le régime de l'accès aux informations tel que prévu par le Projet de Loi de programmation militaire (en rouge les points saillants).

Régime des interceptions	**Régime de l'accès aux informations**	**Commentaires**
Limitation du nombre d'interceptions pouvant être réalisées simultanément (L.242-2 du CSI)	n/a	Cette mesure destinée à se prémunir de toute surveillance généralisée n'est pas ici reproduite
Limitation dans le temps de l'interception à 4 mois non renouvelable (L. 242-3 du CSI)	Limitation dans le temps de l'accès aux données à 30 jours renouvelable.	Si le délai initial demeure plus court, aucune limitation n'existe en terme de renouvellement
Seules les communications en lien avec la finalité (terrorisme, criminalité organisée) sont retranscrites. Les autres ne sont pas conservées. (L.242-5 du CSI)	n/a	La garantie d'une mesure proportionnée n'est pas ici reprise. Les autorités pourront obtenir l'ensemble des informations en lien ou non avec la finalité recherchée.
Les informations recueillies ne peuvent servir à d'autres fins que celles prévues par les finalités initiales (L. 242-5 du CSI)	n/a	Afin d'éviter l'usage d'un régime d'exception pour toute infraction, un garde-fou avait été prévu. Il n'a pas été repris. Les autorités pourront utiliser les données pour toute enquête, y compris pour des finalités ne relevant pas du régime d'exception.

Les enregistrement sous détruits sous 10 jours. Leurs transcriptions sont détruites dès que leur conservation n'est plus indispensable (L. 242-6 et 242-7 du CSI)	Renvoi à un décret le soin de fixer la modalité de conservation des données transmises	Alors que la loi avait prévu ce cadre pour le régime des interceptions, ici cet élément est renvoyé à un texte règlementaire. Le Parlement se voit dessaisi de son pouvoir d'élaborer une durée de conservation.
La décision est transmise dans les 48h à la CNCIS qui se réunit dans les 7 jours (L. 243-8 du CSI)	La décision est transmise dans les 48h à la CNCIS qui se réunit dans les 7 jours	Même contrôle a postériori de la CNCIS
La CNCIS peut s'auto-saisir ou être saisie par toute personne pour contrôler une interception (L.243-9 du CSI)	n/a	Le pouvoir d'auto-saisine ou de saisine par un tiers (par exemple, un hébergeur) n'a pas été repris.
La CNCIS dispose d'un pouvoir de recommandation de faire cesser une interception (L. 243-8 du CSI)	La CNCIS peut adresser des recommandations. Le Premier Ministre doit alors apporter ses observations dans les 15 jours	La mesure semble moins protectrice. Alors qu'en termes d'interceptions, le point intéressant pour les autorités est le "flux" (ie les nouvelles communications), ici, il s'agit d'accéder aux données stockées à un instant T par les hébergeurs. En conséquence, avoir une recommandation négative postérieurement à la captation des données est totalement inopérante au regard de l'objet même de la mesure. Les données auront déjà été collectées par les autorités (par exemple, récupération de toutes les données stockées dans le cloud).

Conclusion

L'ASIC considère que :

- il revient au Parlement et/ou au Gouvernement de réaliser une évaluation du régime d'exception existant permettant ainsi de justifier son extension et pérennisation ;
- le texte crée une confusion entre les régimes d'accès aux données et le régime des perquisitions sans offrir les garanties suffisantes ;
- le texte semble oublier un grand nombre de garanties essentielles pourtant d'ores et déjà prévues pour le régime des interceptions.

Dans ces conditions, **l'ASIC s'alarme de ce texte et demande que le Sénat réécrive profondément la mesure** en :

- **la limitant aux seuls cas de terrorisme ;**
- **la limitant, en ce qui concerne les hébergeurs, au seul accès aux données techniques conservées par eux et non à toute information et document ;**
- **supprimant, en ce qui concerne les hébergeurs, l'accès en "temps réels" et sur "sollicitation du réseau" ;**
- **réinstaurant, pour l'accès aux données techniques, l'ensemble des protections prévues et les pouvoirs offerts à la CNCIS, existants en matière d'interceptions**

Au delà, il convient également de rappeler qu'à plusieurs reprises, tant le Président de la République que le Premier Ministre ont pris des engagements forts sur la question de la surveillance des données internet.

Le 23 octobre dernier, le Premier Ministre, M. Jean-Marc Ayrault, avait déclaré devant l'Assemblée nationale à propos de la question de la surveillance des données Internet : "*La sécurité est une exigence, mais elle ne doit pas être garantie à n'importe quel prix ; elle ne doit porter atteinte ni aux libertés ni à la vie privée. Telle est la position de la France !*"

De même, le Président de la République, M. François Hollande avait indiqué, à l'issue du Conseil européen dédié au numérique le 25 octobre dernier, à propos de cette question de la surveillance de l'Internet : "***Je suis également convaincu avec les Européens de la nécessité de protéger les libertés individuelles et les droits fondamentaux. (…) Nous devons nous-mêmes être au clair et ne pas pratiquer ce que nous reprochons à d'autres***". Il ajoutait à propos des révélations sur un système de surveillance mis en oeuvre en France : "*Je ne voudrais pas qu'on laisse penser que, finalement, cette pratique de (surveillance) serait générale. Donc, il y a un cadre légal, il doit être respecté. Avec la CNIL, nous veillerons à utiliser toutes les informations dans le respect de la loi.*"

Dans ces conditions, **l'ASIC demande un moratoire et une évaluation complète des dispositifs de surveillance mis en oeuvre par l'Etat.**