Paris le 29 mai 2024

Proposition de loi "ingérences étrangères", une nouvelle étape dans l'escalade sécuritaire

L'Observatoire des Libertés et du Numérique* demande aux parlementaires de s'opposer à l'extension des finalités des boîtes noires de renseignement inscrite dans la proposition de loi "ingérences étrangères".

"L'ingérence étrangère", un énième prétexte à l'extension de la surveillance de masse

La proposition loi "Prévenir les ingérences étrangères en France", présentée par le député Sacha Houlié avec le soutien du camp présidentiel, a été adoptée par l'Assemblée Nationale (27 mars) et le Sénat (22 mai) avec le soutien des partis Les Républicains et Rassemblement national - alliés naturels du gouvernement pour les lois sécuritaires, mais ici, avec également le soutien du PS et d'EELV.

L'objectif affiché de cette loi est de limiter les intrusions d'autres Etats via l'espionnage et les manipulations pour contraindre les intérêts géopolitiques de la France. Mais, alors que le gouvernement dispose déjà de nombreux outils pour éviter ces intrusions, ce texte fraîchement adopté ne peut qu'inquiéter.

En effet, ces dispositions pourraient avoir pour conséquence de soumettre des associations d'intérêt public œuvrant pour l'intérêt collectif à des obligations de déclaration des subventions de fondations étrangères, renforçant ainsi les possibilités de contrôle gouvernemental.

Par ailleurs, dans une logique constante de solutionnisme technologique, le texte promeut l'extension d'une technique de renseignement dite de l'algorithme de détection ou "boîte noire de renseignement".

Des gardes fous toujours remis en cause

Cette technique a été instaurée par la loi renseignement de 2015 nos organisations s'y étaient alors fermement opposées. Elle implique, en effet, la nécessaire surveillance de l'intégralité des éléments techniques de toutes les communications de la population (qui contacte qui ? quand ? comment ? voire pourquoi ?), qu'elles soient téléphoniques ou sur internet, tout cela pour poursuivre l'objectif de détecter automatiquement des profils effectuant un certain nombre d'actions déterminées comme étant "suspectes". Ces profils seront ensuite ciblés et plus spécifiquement suivis par des agents du renseignement. Cette technique agit donc à la manière d'un énorme "filet de pêche", jeté sur l'ensemble des personnes résidant en France, la largeur de maille étant déterminée par le gouvernement.

En raison de son caractère hautement liberticide, cette mesure avait été limitée à la stricte lutte contre le risque terroriste et instaurée de façon expérimentale pour quelques années avec des obligations d'évaluation. Malgré des résultats qui semblent peu convaincants et des rapports d'évaluation manquants, cette technique a, depuis, été pérennisée et explicitement élargie à l'analyse des adresses web des sites Internet.

Un dévoiement des finalités

L'OLN dénonçait déjà les risques induits par l'utilisation de ce dispositif avec la finalité de "lutte contre le terrorisme", notamment en raison de l'amplitude de ce que peut recouvrir la qualification de terrorisme, notion du reste non définie dans le texte.

L'actualité vient confirmer nos craintes et l'on ne compte plus les usages particulièrement préoccupants de cette notion : désignation " d'écoterroristes " pour des actions sans atteinte aux personnes, multiples poursuites pour "apologie du terrorisme", pour des demandes de cessez-le-feu et des propos liés à l'autodétermination du peuple palestinien, condamnations pour une préparation de projet terroriste sans qu'un projet n'ait pu être établi par l'accusation.

Cette proposition de loi élargira cette technique de l'algorithme à deux nouvelles finalités de renseignement :

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 ;

Là encore, la définition des finalités est bien trop vague, sujette à de très larges interprétations, pouvant inclure les actions suivantes : militer contre des accords de libre-échange, lutter contre des projets pétroliers, soutien aux migrants, remettre en cause les ventes d'armement ou les interventions militaires de la France...

Un encadrement bien limité

Si un contrôle théorique de ses finalités doit être opéré par la Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR), ses avis peuvent ne pas être suivis.

De même, si la proposition de loi est, là encore, prévue pour une phase "expérimentale" pendant 4 ans et avec des obligations de documentation, peu de doutes sont permis sur ce qu'il adviendra, au vu des précédents sur le sujet.

Un élargissement des "techniques spéciales d'enquête"

Dans le cadre de ce nouveau texte sécuritaire, le Sénat en a aussi profité pour aggraver le barème des peines et créer une nouvelle circonstance aggravante dite "générale" applicable à l'ensemble des infractions [au même titre que l'usage de la cryptologie...] permettant de monter d'un palier la peine de prison encourue (3 à 6, 5 à 7, 7 à 10...) dès que l'infraction est commise "*dans le but de servir les intérêts d'une puissance étrangère, d'une entreprise ou d'une organisation étrangère, ou sous contrôle étranger* ». Cette aggravation de peine permettra l'utilisation des techniques spéciales d'enquête, soit les intrusions les plus graves dans la vie privée (écoutes téléphoniques, balises GPS, la prise de contrôle d'appareil, hacking informatique...). Là où ces techniques étaient censées n'être utilisées que pour les

crimes les plus graves, elles sont, texte après texte, étendues à un nombre toujours plus important d'infractions.

Quelle lutte contre quelles ingérences ?

Le Gouvernement ne ferait-il pas mieux de s'inquiéter de certaines ingérences étrangères bien réelles, telles que la captation des données de santé des Français exploitées par les autorités étasuniennes dans le cadre du Health Data Hub, d'autres captations frauduleuses par les entreprises du numérique américaines ou encore la vente de technologies de pointe par des société étrangères, notamment israéliennes, comme PEGASUS, permettant de surveiller des personnalités politiques françaises au plus haut niveau ? https://www.amnesty.org/fr/latest/news/2021/07/the-pegasus-project/

Des outils terrifiants au service d'un pouvoir qui continue sa fuite en avant autoritaire

Les boîtes noires comme les autres techniques d'intrusion du renseignement offrent des possibilités terrifiantes, qu'elles soient prévues par la loi ou utilisées abusivement. Cette démultiplication des capacités de surveillance participe à l'actuelle dérive autoritaire d'un pouvoir qui se crispe face aux contestations pourtant légitimes de sa politique antisociale et climaticide et devrait toutes et tous nous inquiéter alors que les idées les plus réactionnaires et de contrôle des populations s'intensifient chaque jour un peu plus.

Espérer un retour à la raison

Espérant un retour à la raison et à la primauté des libertés publiques, passant par la fin de la dérive sécuritaire et de son terrible "effet cliquet" nous appelons la Commission mixte paritaire qui aura à se prononcer sur ce texte puis les parlementaires à rejeter l'article 4 (élargissement du barème de peine et techniques spéciales d'enquête) et l'article 3 (élargissement des finalités des boites noires) de cette proposition de loi, et, *a minima,* à s'en tenir à une restriction d'utilisation de cette technique à des cas beaucoup plus précis et définis (par exemple au risque d'attentat causant des atteintes à la vie et les ingérences étrangères graves telles qu'envisagées aux articles 411-1 à -8 du Code pénal).

Signataires :

Le Syndicat de la magistrature

La Quadrature du Net

Le Syndicat des Avocats de France

Le CECIL

CREIS-TERMINAL

GLOBENET