Projet de loi sur le renseignement : les 5 sujets qui fâchent

Levée de boucliers de la part des associations et des syndicats représentant les industries du numérique, menace des hébergeurs de quitter le territoire, avis réservé de la CNIL : en quelques semaines, et malgré le contexte post-attentats en France, le projet de loi sur le renseignement s'est attiré de nombreuses critiques. Alors que **les opposants manifestaient aujourd'hui à Paris** pour protester contre ce texte, revue des détails des 3 principaux points qui fâchent. Le projet de loi, défendu par Manuel Valls, Bernard Cazeneuve (Intérieur, en photo), Jean-Yves Le Drian (Défense) et Christiane Taubira (Justice), est actuellement examiné devant le Parlement, selon la **procédure accélérée** (un seul passage à l'Assemblée et au Sénat).

1) L'extension du champ des écoutes

Quelques semaines après les attentats contre Charlie Hebdo, la loi semble pensée pour la prévention des actes de terrorisme. Sauf qu'elle déborde très largement de ce champ. Les pratiques et techniques décrites par le texte s'étendent à la Défense Nationale, aux intérêts de politiques étrangères, à **l'exécution des engagements européens et internationaux de la France**, aux intérêts économiques et scientifiques majeurs, à la prévention de la criminalité et de la délinquance organisés, ou encore **aux violences collectives pouvant porter gravement atteinte à la sécurité nationale**. Bref, ce texte, qui légalise la surveillance d'individus avec des techniques très intrusives (balises GPS, keyloggers enregistrant toutes les frappes des claviers, micros, introduction sur des systèmes tiers, utilisation de fausses bornes mobiles appelées IMSI Catcher), s'applique à… à peu près tout. Y compris à l'espionnage économique et à la surveillance de mouvements sociaux. D'ailleurs, un amendement déposé par quelques députés PS critiques vis-à-vis du gouvernement (ceux qu'on appelle communément les 'frondeurs'), dont les ex-ministres Aurélie Filippetti et Benoît Hamon, propose de restreindre le texte à la prévention du terrorisme et à la protection des intérêts fondamentaux de la nation. « *Les sept finalités de la politique de renseignement identifiées dans l'article L. 811□3 ouvrent la voie à une surveillance massive de la population française* », écrivent les frondeurs.

A ce champ très large, **échappant à tout contrôle judiciaire**, s'ajoute l'extension des mesures de surveillance à « *l'entourage de la personne visée par l'autorisation* » de mise en place des écoutes. L'article 852-1 prévoit que ces relations de la personne suspectée pourront être visées par les mesures d'écoute si elles sont « *susceptibles de jouer un rôle d'intermédiaire, volontaire ou non, pour le compte de celle-ci ou de fournir des informations au titre de la finalité faisant l'objet de l'autorisation* ». Là encore une définition trop large pour mettre en place des garde-fous clairs.

2) Très opaques boîtes noires

« *Nous avons annoncé un plan d'investissement de 400 millions d'euros sur trois ans. Nous devons décider d'ici à septembre comment répartir cette somme et où investir. Si la loi est votée, nous irons mettre nos*

serveurs ailleurs ». Dans *Les Echos*, **Octave Klaba**, le fondateur d'OVH, la principale réussite française en matière d'hébergement Web, n'y va pas par quatre chemins pour dire au gouvernement quelles seront les conséquences pratiques des boîtes noires, ces équipements de surveillance opérés par les services de renseignement directement sur les réseaux des opérateurs, FAI et hébergeurs. A elle seule, cette mesure est parvenue à fédérer cette dernière profession, jusqu'alors peu organisée : vendredi, plusieurs hébergeurs, dont les poids lourds OVH et Online, ont publié une lettre ouverte au gouvernement menaçant de s'exiler si le Parlement votait l'installation de boîtes noires sur leur réseau. Principal problème, selon eux : cette mesure de « *surveillance de masse* » va **saper la confiance de leurs clients**. De facto, même dans le contexte intra-européen, le dispositif risque de faire tiquer. Notamment les entreprises ayant des activités en Allemagne, le pays du continent le plus exigeant à l'heure actuelle en matière de protection des données personnelles.

L'efficacité de ces boîtiers, censés repérer des signaux faibles indiquant des activités potentielles de préparation d'actes terroristes, est elle aussi sujette à caution. « *Les moyens techniques et financiers des services français ne sont pas proportionnés pour traiter la masse totale des données* », résument les hébergeurs dans leur lettre ouverte. A moins d'aller vers des algorithmes de Machine Learning, censés repérer seuls, par itération, les comportements suspects. Un mécanisme qui rappellerait alors furieusement les 'précogs' de Minority Report, imaginés par l'écrivain Philip K. Dick en 1956.

A ces questions éthiques, s'ajoutent des aspects pratiques, relatifs à l'installation d'équipements**, dotés d'algorithmes classés secret défense**, opérés par des services de l'Etat sur des réseaux d'opérateurs ayant, eux, des engagements contractuels vis-à-vis de leurs clients. Un mécanisme qui soulève bien des questions en matière de responsabilité, de maintenance et de création de risques nouveaux (en matière de sécurité et de qualité de service), comme nous l'expliquions récemment. Interrogé par la commission des Affaires culturelles, Stéphane Richard, le patron d'Orange, s'est d'ailleurs dit « *assez réticent à l'idée de voir s'installer dans nos réseaux, des équipements étrangers à l'entreprise.* »

Officiellement, les données interceptées par les boîtes noires seront anonymisées. Un emballage juridique qui masque une réalité technique plus crue. « *Les boîtiers intercepteront bien des données personnelles, qui seront stockées. Ce n'est qu'ensuite que des moyens techniques seront mis en œuvre pour garantir leur protection* », remarquait récemment Maxime Kurkdjian, le directeur associé d'Oxalide, qui héberge bon nombre de sites de presse en France. Comment seront tracés et contrôlés les accès à cette base de données personnelles ? Où sera-t-elle stockée ? De quel niveau de sécurité bénéficiera-t-elle ? Autant de questions sans réponse à ce jour.

3) Les Imsi Catchers en liberté peu surveillée

La technique n'est certes pas nouvelle. Mais elle deviendrait légale sans l'aval d'un juge. Un Imsi Catcher est en réalité une fausse borne GSM qui s'insère dans la communication entre un réseau d'opérateur et un téléphone mobile. Récupérant au passage les metadonnées des terminaux qui s'y connectent et le contenu des communications. Avec ce genre d'appareils, on est loin de la pêche au harpon tant vantée par le rapporteur du texte, Jean-Jacques Urvoas, qui file volontiers les métaphores halieutiques. Ces dispositifs récupèrent en effet **toutes les communications et échanges Internet des téléphones situés dans leur rayon d'action** (de 500 m à 1 km). Y compris ceux de quidams passant par là. Et, selon Le Canard Enchaîné, les données recueillies sur ces

engins peuvent être effacées sans laisser de traces, rendant tout contrôle réel de leur utilisation illusoire. Le projet de loi prévoit que ces filets pélagiques puissent être installés pour une durée maximale… de 6 mois.

Dans Le Point, Céline Berthon, secrétaire générale adjointe du principal syndicat des commissaires de police (SNCP), défend le dispositif : « *Il y a un mythe derrière tout ça, comme si les services de renseignement avaient le temps de s'intéresser à toutes les autres conversations privées captées autres que celles intéressant l'enquête.* » Comme avec les boîtes noires, les craintes des opposants au texte ne prendraient pas en compte la réalité des moyens des services. On peut toutefois se demander, dès lors, pourquoi le projet de loi ne s'aligne pas sur ladite réalité…

4) Des garanties en carton-pâte

Les promoteurs du texte se retranchent généralement derrière les garanties et moyens de contrôle qu'offrirait le texte. A commencer par la création d'une nouvelle commission, la CNCTR (Commission nationale de contrôle des techniques de renseignement), en lieu et place de la CNCIS (Commission nationale de contrôle des interceptions de sécurité). L'actuel président de cette dernière ne s'est pas privé de dézinguer publiquement le projet de loi, estimant, chez nos confrères de La Tribune, que *« la CNCTR ne sera pas en état de contrôler les dispositifs techniques employés par les services* ». Notamment parce les données brutes des interceptions ne se trouveront dans les locaux de future commission, contrairement à la situation actuelle. Pour Jean-Marie Delarue, la CNCTR sera « *un colosse aux pieds d'argile* ».

De son côté, le syndicat de la Magistrature relève surtout que cette commission n'exercerait aucun contrôle a priori : « *elle donne un simple avis et qu'il soit favorable ou pas, la décision revient au Premier ministre. En réalité, on refuse un vrai regard indépendant de l'exécutif sur des mesures extrêmement intrusives* », commente **Laurence Blisson**, la secrétaire nationale du syndicat.

De même, on peine à croire que la CNCTR, dotée de 9 membres, sera à même de surveiller efficacement les multiples pratiques d'interception des divers services. D'ailleurs, le président de l'actuelle CNCIS ne dit pas autre chose. Ce dernier explique ainsi : *« L'un des services de ce pays (il parle ici de la DGSE, NDLR) dispose de moyens informatiques extrêmement puissants. J'en suis ravi. Mais lorsque nous allons voir ses instruments, notre intervention relève plus de la contemplation que de l'investigation. Si je dis à ce service que j'ai besoin d'aller voir ce qu'il fait, il va me bâtir un logiciel pour répondre à ma demande. Comment vérifier que ce logiciel répond effectivement à ma demande ? »* La présence d'un 'technicien' au sein de la future CNCTR, un membre désigné par l'Arcep (l'autorité de régulation des télécoms), ne risque guère de changer les choses…

Signalons que le projet de loi introduit une voie de recours, devant le Conseil d'Etat, pour les citoyens s'estimant injustement traqués. « *Mais un citoyen n'aura pas moyen de se défendre dans le cadre d'un recours de ce type devant le Conseil d'Etat. Il ne saura même pas si les techniques de surveillance qu'il soupçonne ont bien été mises en œuvre ou pas* », dénonce Laurence Blisson, du Syndicat de la Magistrature.

5) Communications avec l'étranger : la voie de la NSA

Une ficelle made in NSA ? En tout cas cela y ressemble fort. L'**interception des communications émises ou reçues à l'étranger** fait en effet l'objet d'un article à part (854-1). « *Le projet de loi légalise l'interception des communications émises ou reçues depuis l'étranger. Autrement dit une bonne partie du trafic Internet*, explique la Quadrature du Net. *Cet article du projet de loi permet de mettre en place des mouchards sur les cœurs de réseau comme le fait la NSA dans le cadre de son programme Upstream*. » Pour l'association, le projet de loi présente donc des **similitudes avec la Section 702 du Foreign Intelligence Surveillance Act** (FISA), derrière laquelle s'est abritée la NSA pour espionner largement la population américaine tout en faisant mine de ne cibler que des personnes étrangères.

Les conditions de mise en œuvre de cette surveillance (stockage, destruction des données, contrôles techniques exercés) seront précisées par un décret du Conseil d'Etat… non publié. Ajoutons à cela que le délai de conservation des communications ainsi interceptées « *court à compter de la date de leur première exploitation* » (12 mois pour les contenus des communications, cinq ans pour les métadonnées). De facto, le gouvernement Valls met donc bien à disposition de ses services de renseignement les outils pour organiser une collecte massive de données pouvant être stockées sur de longues périodes, et permettant d'organiser des analyses à posteriori sur des individus ou groupes d'individus. Exactement la méthode privilégiée de l'agence de Fort Meade et abondamment décrite par les révélations d'Edward Snowden.

A lire aussi :

Loi sur le renseignement : pour les opposants, un parfum de NSA
Projet de loi sur le renseignement : « dangereux », « liberticide », « stupide »