Loi sur le renseignement : le casse-tête des boîtes noires pour l'Internet français

Des boîtes noires sur le réseau des FAI et, demain, sur celui de tous les acteurs de l'Internet pour repérer les comportements des terroristes ou apprentis terroristes. C'est l'une des mesures phare du projet de loi sur le renseignement, présenté en conseil des ministres la semaine dernière et qui sera examiné en séance publique à l'Assemblée à partir du 13 avril. Une des mesures les plus contestées aussi, comme le montraient les premières réactions au texte en fin de semaine dernière. Sur le fond pour **l'atteinte aux libertés individuelles**, mais aussi **sur l'aspect pratique**. En effet, même si le texte de loi ne détaille pas la mise en œuvre opérationnelle desdits boîtiers, il soulève un certain nombre d'interrogations. Visant à « *détecter, par un traitement automatique, une succession suspecte de données de connexion* », ces équipements doivent être installés sur le réseau des FAI dans un premier temps. Opérateurs, hébergeurs et plates-formes (comme Google, Facebook, etc. dont le trafic est chiffré) sont censés suivre.

Un mécanisme qui soulève un certain nombre de questions d'abord en termes de coûts. « *Cette mesure est techniquement envisageable, mais à un coût relativement important* », confirme **Maxime Kurkdjian**, le directeur associé d'Oxalide, qui héberge bon nombre de sites de presse en France. « *Rien que chez nous, cela représente 4 à 5 Gbit/s de trafic* ». Pour **Jérémy D'Hoinne**, directeur de recherche chez Gartner, en charge des sujets relatifs à la sécurité et ancien directeur de produits de NetAsq, « *une approche intelligente de cette problématique passerait par l'utilisation de l'infrastructure du FAI sur des règles de sélection de trafic très simples pouvant éventuellement déclencher des analyses plus poussées dans un équipement propriétaire* » , note-t-il. Or, ce n'est pas le schéma vers lequel semble s'orienter le gouvernement, qui présente ses équipements d'interception comme des **boîtes noires, dotés d'algorithmes classés secret défense**, auxquelles les équipes techniques des FAI ou opérateurs n'auraient pas accès. Bref, les règles de filtrage resteraient confinées au sein des équipements des services de renseignement. « *Quand ils vont rentrer dans le concret de l'opération, ils vont chercher à optimiser les coûts et les performances de ce système* », pronostique Jérémy D'Hoinne. Remarque qui vaut d'ailleurs tant pour les FAI, qui chercheront à minimiser l'impact de ces équipements sur les performances (le débit, la latence, l'impact sur les autres équipements) de leur infrastructure, que pour les personnes en charge des boîtes noires, qui vont devoir régulièrement optimiser les algorithmes, voire adapter le filtrage à la demande.

Légaliser ce qui existe déjà pour partie ?

Jérémy D'Hoinne note tout de même qu'on ne parle peut-être pas ici d'analyse ou de blocage en temps réel mais plutôt d'analyse en temps différé, moins complexe à mettre en œuvre. « *Il n'en reste pas moins qu'on est ici sur des échelles forcément coûteuses* », dit le directeur de recherche de Gartner. Même si, comme l'explique Tristan Nitot, invité par le gouvernement à une explication de texte en fin de semaine dernière en tant que membre du Conseil National du Numérique, le système imaginé par les services de renseignement ne vise à « *surveiller qu'un échantillon de l'Internet français* », et non son intégralité. Sur un système aussi distribué que l'Internet hexagonal, une surveillance globale impliquerait en effet des déploiements massifs. « *C'est au final plus simple d'espionner le trafic*

international qui passe par quelques backbones », glisse un observateur… qui ajoute que c'est d'ailleurs ce qui se fait déjà. Façon de dire que le mécanisme prévu par le projet de loi existe déjà pour partie sur le terrain. Et qu'il s'agit en réalité de le légaliser et de l'étendre.

Les décrets d'application de la future loi devront aborder la question du remboursement des coûts opérationnels que ces mesures supposent aux prestataires. Dans son avis sur le projet de loi, **l'Arcep** (le régulateur des télécoms) souligne que « *si les textes prévoient que les opérateurs doivent être indemnisés des surcoûts spécifiques exposés pour répondre à ces différentes demandes, les opérateurs rencontrent parfois avec certaines autorités administratives des difficultés dans le paiement des sommes correspondantes. A cet égard, l'Arcep invite le gouvernement à veiller à l'indemnisation rapide et homogène des surcoûts exposés par les opérateurs.* » Qu'en termes polis ces choses-là sont dites…

Une cible pour les hackers ?

Mais, en dehors de ces aspects financiers, l'installation d'un boîtier sur le réseau des acteurs techniques de l'Internet pose, en termes opérationnels, quelques autres questions pratiques. Selon Maxime Kurkdjian (Oxalide), pour être efficaces, ces boîtiers pourraient être **positionnés sur les liens d'interconnexion et sur les cœurs de réseau**. Et toucher l'ensemble de la chaîne allant du consommateur aux producteurs, c'est-à-dire les FAI, les opérateurs télécoms et les hébergeurs (ou fournisseurs de service comme Google, Twitter ou Facebook). « *Ces équipements seraient donc positionnés sur des segments de réseau sensibles. Cela soulève au moins deux problématiques. La première a trait à la* ***sécurité****. Car cette arme (les boîtiers d'analyse de trafic, NDLR) pourrait très bien se retourner contre l'Internet français : un hacker qui parviendrait à prendre le contrôle d'un de ces systèmes – qui devront par nature rester accessibles de l'extérieur – aurait accès à des capacités immenses. La seconde problématique touche à notre* ***responsabilité de prestataire technique****. Nous avons conçu un design de réseau qui prend en compte nos contraintes de disponibilité. Mais est-ce que ce type de boîtier n'est pas susceptible de mettre à mal ce design ?* » Ces interrogations légitimes devront être tranchées par les décrets d'application dont la rédaction s'annonce… sportive. « *Le gouvernement devra nous consulter pour ces aspects opérationnels* », veut croire Maxime Kurkdjian, qui regrette, comme d'autres, qu'aucune consultation n'ait eu lieu avant la présentation du projet de loi en conseil des ministres, Axelle Lemaire, la secrétaire d'Etat au Numérique, ayant été désignée en fin de semaine dernière seulement pour tenter de déminer un dossier qui suscitait déjà des remous dans l'industrie.

Les craintes des prestataires sont aussi renforcées par la nature même de l'algorithme qu'embarqueront les équipements. Car, pour le gouvernement, « *les procédures de communications [des terroristes] sont inventées mois par mois, mais ces comportements sont extraordinairement signants.* » Conséquence logique : le logiciel embarqué sera fréquemment mis à jour, à distance et sans intervention des administrateurs des prestataires. Là encore, un facteur qui inquiète ces derniers, qui craignent que ces **mises à jour** puissent être **source d'instabilité technique**.

Données anonymisées… oui mais quand ?

Enfin, soulignons la faiblesse des garde-fous imaginés par le gouvernement. Le contrôle du dispositif sera assuré par la Commission nationale de contrôle des techniques de renseignement (CNCTR), que crée le texte de loi en lieu et place de la CNCIS (Commission nationale de contrôle des

interceptions de sécurité) actuelle. La CNCTR pourrait vérifier la validité et la pertinence des algorithmes proposés par les services de renseignement. Selon Tristan Nitot, qui relate dans son billet de blog les explications de Matignon, si trop de suspects sont isolés par les algorithmes, alors la Commission de contrôle sera fondée à rejeter ces interceptions. Des garanties qui manquent de précision. Par ailleurs, les membres de cette CNCTR examineront des données anonymisées des suspects isolés par les algorithmes. La levée de l'anonymat sera décidée au cas par cas, et uniquement pour les activités liées au terrorisme. Mais cet emballage juridique 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* », remarque Maxime Kurkdjian. Comment seront tracés et contrôlés les accès à cette base de données ? Où sera-t-elle stockée ? De quel niveau de sécurité bénéficiera-t-elle ? Autant de questions sans réponse à ce jour.

Par ailleurs, le gouvernement précise que son système de boîtes noires se contentera d'**analyser des métadonnées**, afin d'isoler des pratiques de connexion suspecte. Une garantie bien faible tant ces éléments peuvent être parlants. « *Les entêtes des e-mails chiffrés, des URL de recherche Internet ou autres renferment des informations très significatives* », remarque Jérémy D'Hoinne (Gartner).

A lire aussi :

La France bricole un Patriot Act du pauvre

Après les attentats : l'Intérieur bricole un plan d'action, pas un Patriot Act

Loi anti-terroriste : un arsenal tout juste renforcé et bientôt chamboulé ?

Accès administratifs aux données de connexion : pareil qu'aujourd'hui… mais en pire

Crédit Photo : Scyther5-Shutterstock