

## 仏政府、ネット監視強化を計画：業界は反発

シャルリー・エブド襲撃事件を受けて、仏政府はインターネット監視強化策を準備している。インターネット業界はこれに反発している。

事件前から、政府の依頼を受けて通信監視関連法案の準備を進めていたユルボア下院議員（社会党）は1月14日、スカイプやWhatsApp、フェイスブック・メッセンジャーなどのインスタント・メッセンジャーを直接に盗聴する可能性が法案には盛り込まれると言明。これと平行して、カズヌーブ内相は、バルス首相からの指示を受けて、ネット監視強化を目的とする追加措置の準備を開始した。この追加措置について、ルメール・デジタル経済閣外相は14日、国会での答弁で、特別法によらず、既存の法令の枠内で可能な措置を導入すると説明、過度な規制強化に対する懸念の打ち消しに努めた。

しかし、これにインターネット業界は反発を強めている。仏ソフト・情報処理業界団体サンテック・アンフォルマティックは、テロ対策という大義に理解を示しつつも、令状なしで捜査当局・諜報部門がインターネットを盗聴することには反対の姿勢を見せている。同団体は、2014年12月に成立した国防計画法により、捜査当局・諜報部門は、令状なしでインターネット・ユーザーの接続記録にアクセスする権限を既に得ているとも指摘している。

インターネット権利擁護 NGO のカドラチュール・デュ・ネットも、新法案は世界的なスキャンダルとなった米 NSA（国家安全保障局）の通信監視と同じ論理に基づいていると主張、政府はテロを機会に、準備していた監視強化を一気に推進しようとしていると批判した。また、NSA のスキャンダル以来、テロリストはロシアや旧ソ連諸国などのツールを利用して監視の目を逃れようとしており、スカイプなどの米インターネット大手のツールの監視を強化しても効果はないとの見方もある。

Les Echos 2015-01-16

### 【原文】

La grogne monte face aux ambitions de la cyberpolice  
SANDRINE CASSINI

Le gouvernement multiplie les annonces contre le cyberterrorisme. Les professionnels d'Internet dénoncent un « opportunisme politique ».

Depuis les attentats contre « Charlie Hebdo », les annonces de mesures visant à renforcer les dispositifs de surveillance de la Toile ont le vent en poupe. Mercredi,

Le député Jean-Jacques Urvoas a levé le voile sur le projet de loi dit « renseignement », laissant supposer une possibilité de mise sur écoute en direct du Web. Seraient par exemple visés Skype, WhatsApp, Facebook Messenger ou toute autre messagerie privée. En parallèle, le ministre de l'Intérieur, Bernard Cazeneuve, a été chargé par Manuel Valls d'imaginer des dispositifs supplémentaires. Pour calmer le jeu, la secrétaire d'Etat au Numérique, Axelle Lemaire, a assuré à l'Assemblée nationale mercredi que seraient prises des mesures « à droit constant, sans droit d'exception ».

L'activisme gouvernemental a été fraîchement accueilli par le monde du numérique. « C'est légitime que l'on se pose des questions. Je ne suis pas un libertaire bisounours. Mais aller écouter Internet sans l'intervention d'un juge, non », s'insurge Guy Mamou-Mani. Le président du Syntec numérique, qui représente les éditeurs de logiciels et les SSII, rappelle que la loi de programmation militaire votée en décembre dernier élargit déjà les pouvoirs de la police et des services de renseignement en leur permettant d'accéder aux données de connexion des internautes sans décision judiciaire.

« Avec la loi renseignement, on est dans la logique de la NSA, dont la dérive est la surveillance de masse. Depuis "Charlie-Hebdo", on voit sortir à toute vitesse des choses qui étaient dans les cartons depuis longtemps. On assiste à un opportunisme politique débridé », se désole Adrienne Charmet, coordinatrice de campagne à La Quadrature du Net. De fait, les décrets d'application permettant l'application de la loi terrorisme du 13 novembre dernier et prévoyant le blocage des sites terroristes ont été notifiés à Bruxelles, au lendemain des attentats, par un gouvernement s'estimant insuffisamment armé face à la menace terroriste qui se fond dans un Internet difficile à surveiller. « Depuis 1986, il y a eu une quinzaine de lois ou morceaux de lois renforçant l'anti-terrorisme. Voyons déjà ce qui est efficace », préconise un grand acteur du Net. L'Asic, qui représente les grandes plates-formes Internet (Facebook, Google, Twitter...) assure que tous collaborent déjà « activement avec tous les services d'enquête afin de les aider à identifier les divers auteurs de crimes ». Certains vont plus loin, contestant même la réelle utilité d'une mise sous surveillance du cyberspace. « Depuis Snowden, les terroristes ont compris qu'il ne fallait pas aller sur les plates-formes américaines de communication sur le Web », explique un proche des services de renseignement. Les djihadistes utilisent plutôt des outils dans des pays peu regardants, comme la Russie ou certaines républiques de l'ex-URSS.

En quête de compétences

Reste à savoir comment réagiront les géants américains si la loi française leur impose

d'ouvrir leurs plates-formes aux autorités. Pendant longtemps, les services de renseignement ont visiblement « écouté » les outils permettant de communiquer sur le Web. « Le chiffrement des plates-formes a été renforcé à cause de Snowden. Il faut que les Etats imposent leur décryptage », recommande cette même source, qui considère que « c'est politiquement le moment de faire passer des lois ». En attendant, les services de renseignement, qui investissent depuis six ou sept ans, disposent de puissants outils d'interception. Mais ils manquent des compétences nécessaires pour interpréter ces masses de données. Le gouvernement a promis le recrutement, pour la Direction générale du renseignement intérieur (DGSI), de 430 analystes, interprètes ou chercheurs.