



Commission

RÉVOLUTION NUMÉRIQUE

Affaiblir la sécurité des communications pour combattre le narcotrafic et le terrorisme ?

Mars 2025

Il y a de ces sujets qui reviennent dans le débat public régulièrement. Le chiffrement des communications est de ces sujets. Depuis le début du développement d'Internet, le contrôle de ce cyberspace sans frontières et numérique a été un sujet politique pour les États. Aux États-Unis, les attentats de 2001 ont mené à la mise en place d'un système de surveillance généralisée des communications révélé par Snowden en 2013. La réaction a été notamment l'adoption par les usagers d'outils de communication plus sécurisés. Pas que nous poursuivions des activités illicites, mais bien parce qu'en régime démocratique promouvant les libertés individuelles et collectives, il est sain de pouvoir communiquer avec qui on veut sans avoir le doute d'être écouté par qui que ce soit. C'est le principe du secret des correspondances postales, téléphoniques ou numériques tel que défini par la loi.

La situation a changé en France en 2015 après la série d'attentats terroristes qu'a connus le pays. **Le régime d'État d'urgence a permis à l'État de mettre sur écoute le réseau**, peut-être pour de bonnes raisons, mais sans contrôle et avec des violations des droits, comme de nombreux juristes et journalistes l'ont montré par la suite. L'essor des moyens de chiffrement robustes et des smartphones changent la donne. Comme le reconnaît la directrice de la DGSi dans le Journal du Dimanche du 15 mars: « Le constat que nous faisons [...] c'est que les objectifs sur lesquels nous travaillons pour prévenir le terrorisme utilisent de plus en plus des applications de

messaging chiffrées. Alors que nous utilisons jusqu'à aujourd'hui des outils d'interception téléphonique, inscrits dans la loi depuis 1991, en coopérant avec les opérateurs traditionnels de téléphonie, les messaging chiffrées rendent ces méthodes obsolètes. Très concrètement, nous sommes aveugles sur le contenu des conversations de nos cibles ». Tout est clair, les messaging chiffrées, Telegram, Signal, WhatsApp, pour ne citer qu'elles rendraient inopérants les services de renseignement pour lutter contre les menaces de notre société : terrorisme, narcotrafiquants, extrémistes de tout genre. C'est à cela que le ministre Retailleau, et d'autres avant lui, cherche à s'attaquer. Rendre ses yeux aux renseignements. Pour cela, une loi « narcotrafic » et un article, le 8ter. Cet article doit obliger les applications à mettre en place des portes dérobées (ou backdoor) « sécurisées » pour permettre, sur demande des autorités judiciaires, de déchiffrer des communications. Étrange proposition qu'une vulnérabilité volontaire est une bonne chose pour la sécurité de tous. C'est en réalité un risque immense. Cette même faille, même si elle était implémentable techniquement, pourrait être utilisée par les services de renseignement d'autres États ou même par des attaquants peu scrupuleux. **Dans ce domaine ou d'autres, affaiblir les droits de tous pour un semblant de sécurité n'est ni une bonne chose pour les droits, ni pour la sécurité.**

Flavien Ronteix,
commission Révolution Numérique.