

Google, Amazon : le pognon avant la liberté d'expression

Accusées par les médias, haïes par nos gouvernements, outils populaires de contournement des censures dans les États durs et répressifs, les messageries chiffrées Telegram et Signal sont aujourd'hui chassées des serveurs Google et Amazon sous l'exigence de la Russie et de l'Iran.



Phase 1 : normaliser, réguler, intimider

Depuis presque un an se joue un conflit entre le gouvernement russe, à travers le FSB (l'agence qui a pris la suite du KGB) et la messagerie Telegram. Comme l'ensemble des gouvernements au niveau mondial, c'est à la suite d'un attentat, celui du 3 avril 2017 dans un métro de Saint-Pétersbourg, que Vladimir Poutine a fait adopter de nouvelles lois sécuritaires visant à accroître le contrôle policier sur sa population. Cela est passé en juin dernier par la création d'un registre national qui, par le suivi d'un certain nombre de règles, permet aux entreprises et à leurs services de messagerie de demeurer « légales » aux yeux de l'État. Une procédure qu'avait entamée le fondateur de la messagerie Telegram... sans la mener jusqu'au bout aux yeux des autorités. Elles exigent la livraison des clés de déchiffrement de la célèbre messagerie, conspuée sous nos latitudes par les gouvernements comme une technologie à l'usage des terroristes et pourtant largement utilisée en Russie (10 millions d'utilisatrices et utilisateurs) et en Iran (40 millions!) où les libertés démocratiques et droits d'expression sont très restreints.

À défaut de subir les foudres du pouvoir politique et législatif, ce qui est appelé par les médias « messagerie(s) cryptée(s) » (pour la version impropre) ou « messagerie(s) chiffrée(s) » (pour la version correcte) passe régulièrement sous le feu des critiques des ministres et autres députés ou sénateurs, en France, au Royaume-Uni, en Allemagne... qui appellent dans le pire des cas à l'interdiction de ces messageries ou, par des propos moins émotifs, à l'intégration de portes dérobées systématiques sur tout appareil, à l'affaiblissement du chiffrement des applications ou encore à la centralisation des clés de déchiffrement par l'État. Pas besoin d'avoir d'être encarté à l'extrême droite : ces types de propos sont tenus sous nos latitudes par des « démocrates » et des « républicains » qui trouvent toujours des reproches anti-démocratiques à formuler à la Russie de Poutine, mais qui semblent parfois y trouver une source d'inspiration pour leurs méthodes gouvernementales.

Ces messageries ont en commun d'utiliser le chiffrement de bout en bout, une technique cryptographique asymétrique assurant la capacité au seul destinataire du message de pouvoir le lire. Les messages sont en effet chiffrés avec une « clé » et déchiffrés avec une autre. L'application de mathématiques d'un niveau très évolué autorise la construction d'algorithmes de chiffrement qui ne permettent pas de déduire la formule de déchiffrement. On peut alors distinguer une « clé publique » (que tout le monde peut utiliser) pour envoyer un message à une personne particulière qui déchiffre grâce à sa « clé privée » qui, comme son nom l'indique, reste à l'usage de la personne concernée seule. La particularité des messageries populaires chiffrées (WhatsApp, Signal, Telegram) c'est qu'elles laissent seule l'utilisateur ou l'utilisatrice détenteur ou détentrice de sa clé privée. Ces systèmes ne procèdent à aucune récupération, et ce dans le but parfois explicitement avoué de ne pas pouvoir et devoir collaborer avec l'autorité policière d'un État pour des motifs (politiques) qui ne la regardent pas. Ce faisant, elles évitent aussi de posséder un « point unique de défaillance » : le stockage de l'ensemble de ces clés privées sur une infrastructure compromise par une attaque pirate rendrait l'usage de ce service de messagerie peu sûr pour l'ensemble des utilisatrices et utilisateurs. Alors que dans l'autre cas, cette compromission ne peut être qu'à l'échelle individuelle.

Phase 2 : durcir, avilir, anéantir

Le 13 avril, l'autorité russe de surveillance des télécoms, Roskomnadzor, prononce l'interdiction ; elle demande aux fournisseurs d'accès internet (FAI) russes de bloquer les adresses IP identifiées comme des serveurs Telegram. Préparés à cette éventualité, les services fermés se sont vus relayés par d'autres à des adresses IP différentes. C'est une multiplication de censures d'IP qui ont été alors opérées de façon massive, dépassant les 15 millions.

L'impact d'un tel jeu du chat et de la souris a été gigantesque et a bousculé bon nombre d'organisations et d'entreprises qui ont parfois elles-mêmes été mises hors-ligne, parfois juste certains de leur service. Parmi ces millions d'adresses IP, la plus grande part relevait des services Google et Amazon, via leurs services clouds, utilisées par des entreprises, des associations, ou des individus : des hébergements de serveur Telegram peuvent y être installés, sans compter l'usage des VPN et autre proxys qui servent aussi à contourner la censure locale.

Au bout de deux jours, Roskomnadzor annonçait fièrement avoir diminué les capacités de Telegram de 30%. De son côté, Telegram indiquait que la majorité des Russes n'ont rien senti dans leur usage de la messagerie chiffrée.

Les Russes ont réagi à cette interdiction. D'abord le lundi 16 avril, premier jour d'application de l'interdiction technique, en manifestant devant le siège du FSB, et jetant des avions en papier (référence au logo de l'application Telegram) multicolores. Le 30 avril, une manifestation organisée autour de la liberté sur Internet était

organisée, en réaction plus spécifiquement à cette interdiction : 8000 personnes comptabilisées à Moscou.

Ce même 30 avril, c'est le pouvoir Iranien qui interdit l'application Telegram sur son territoire. L'application avait déjà été suspendue fin décembre/début janvier suite aux insurrections populaires. Son rétablissement momentané obéissait davantage à une nécessité économique qu'au rétablissement d'une certaine liberté d'expression : l'application est en effet tellement populaire et utilisée par les IranienEs (une personne sur deux l'utilise !) qu'elle fait partie intégrante des relations économiques et sociales. L'économiste Imam Behboudi estime ainsi que l'usage de Telegram permet à 1 millions d'IranienEs de travailler et de rapporter 9 millions d'euros par mois.¹ La justification de la nouvelle interdiction s'est faite sous le paravent de l'ouverture d'un procès de 26 personnes accusées d'une possible implication de deux attentats survenus à Téhéran le 7 juin 2017 et assimilées à Daesh. Et pour permettre la continuité économique tout en attaquant la confidentialité des échanges, le gouvernement promeut de nouvelles solutions de messagerie « maison ».

Dans cette tourmente, les deux entreprises US en pointes sur le cloud, Amazon et Google, ont pris des mesures préventives contre une autre messagerie chiffrée de bout en bout : Signal. Cette dernière utilise une technique dite de « domain-fronting » permettant de faire passer son service de messagerie pour un autre service et donc de demeurer invisible. Le plus pratique étant de se cacher derrière des services Google et Amazon. Mais l'un et l'autre des géants du Web ont annoncé l'impossibilité technique de recourir dorénavant au domain-fronting sur leur propre infrastructure. La première le 18 avril, la seconde le 27 du même mois. Pour justifier cette interdiction, on ne parle pas de ces militantEs et autres citoyenEs opprimés dans des États autoritaires, mais on évoque les « méchants » qui souhaitent déstabiliser les démocraties occidentales, comme le groupe de hacker russe APT29 qui a piraté le Parti démocrate au cours des dernières élections aux États-Unis et qui a utilisé cette technique pour masquer son méfait.

Phase 3 : entreprendre, extraire, soumettre

S'accordant des valeurs humanistes, universelles, s'opposant à la politique de Trump, jouant du modernisme technologique et du bien-être contre le nationalisme réactionnaire vieillot, obtus et haineux, les masques tombent rapidement chez les entreprises HighTech américaine lorsque les sources de profits menacent de leur être retiré. Plutôt sacrifier l'engagement (si ce n'est la vie) de courageux militantEs pour les libertés, l'égalité sociale, la démocratie, que le chiffre d'affaires. Un « appel de conscience » d'ailleurs exprimé le 19 avril par Alexandre Janov, dirigeant de Roskomnadzor, explicitement adressé à Amazon et Google afin qu'ils fassent primer « le business et non la politique. » Un homme qui pense d'ailleurs maintenant au cas Facebook : sous couvert de lutter contre l'exploitation et la marchandisation des données des citoyenEs russes, le gouvernement russe cherchera avant tout à pouvoir

accéder à ces données pour contrôler davantage sa population. Une logique qui a déjà fonctionné par le passé en Chine où Facebook a dû obéir aux injonctions du gouvernement chinois pour demeurer sur son marché ; ainsi que Microsoft qui a développé une édition spéciale - sous couvert d'une amélioration de la sécurité (mais pour qui ?).

La maxime de Janov est représentative de la façon de penser des dirigeantEs, en France, en Europe, dans le monde : séparer le champ d'une économie régie mathématiquement et froidement et celui de la politique, la cohésion de la population faisant place, dans la décrépitude du capitalisme en crise, à un contrôle accru sur la population. Le combat pour une autre société passe, à l'inverse, par la réappropriation économique sous la politique des travailleurEs, des classes exploitées et opprimées. La solidarité avec les combats démocratiques et sociaux en Russie, en Iran, ou dans n'importe quel autre État, passe par le maintien des services de communication contournant le contrôle de ces États. Mais cette solidarité nécessite de revendiquer l'expropriation des capitalistes dirigeant ce type d'entreprise, et le contrôle de ces dernières par les salariéEs, seulEs à même de construire cette solidarité avec les exploitéEs du monde entier. C'est par cette voie, que l'on pourra élargir et développer les droits démocratiques et sociaux.

¹GOLSHIRI Ghazal, *Le Monde*, "En Iran, le blocage de Telegram touche l'économie du pays", https://www.lemonde.fr/proche-orient/article/2018/01/12/en-iran-le-blocage-de-telegram-touche-l-economie-du-pays_5241115_3218.html, consulté le 04/05/2018

Frédéric Lorie, le 23 mai 2018