NOUVEL HAY MAGAZINE
SANS FRONTIÈRES

Telegram de Russie

Pavel Valerievitch Dourov, né soviétique à Leningrad en 1984, passe son enfance en Italie, où son père enseigne, avant de retourner dans sa ville natale, redevenue Saint-Pétersbourg.

Après avoir vécu en Europe de l'Ouest, le Russe a du mal avec la politique du président Poutine. Et veut devenir le Mark Zuckerberg des jeunes Slaves.

Il lance à 22 ans, VKontakte ou vk.com, un réseau social qui ressemble à Facebook. En 2018, le site a 300 millions d'abonnés dans le monde et devient le second site le plus visité de Russie (14e au monde) .

Dourov revend les 13% du capital qu'il détenait pour 300 millions de dollars. A la suite d'une «mauvaise blague» dans laquelle il annonçait sa démission de la présidence de son groupe, en 2014, cet opposant assumé à Vladimir Poutine est débarqué pour de vrai (et par la justice) de son entreprise.

Le Kremlin reprend VKontakte en main. Craignant pour sa «santé», Dourov part s'installer à Saint-Christophe-et-Niévès, l'archipel découvert par Christophe Colomb en 1493.

Aux Antilles, le riche Russe apprécie le climat et le fisc du pays : il en devient citoyen. Cet exil s'explique aussi par le bijou informatique de Dourov, que le Kremlin n'a pas pu lui prendre : Telegram.
Cette application est réputée inviolable. C'est avec son frère mathématicien, Nikolaï, que Pavel Dourov a imaginé cet outil au codage informatique si compliqué que les «grandes oreilles» du Kremlin ne pourraient pas l'intercepter.
Et ils n'y sont pas parvenus donc ont censuré Telegram. La Chine pareil. Mais dans le reste du monde, l'appli est utilisée chaque jour par plusieurs centaines de millions de

personnes, dont des politiques, businessmen et quelques dizaines de milliers de djihadistes, terroristes qui préfèrent rester discrets sur leurs activités.

Depuis, Pavel Dourov est devenu un itinérant multipliant les voyages pour mieux fuir les éventuels problèmes. A la tête d'une fortune estimée à 1,7 milliard de dollars, il vivrait entre Londres, Helsinki, Bali, Dubaï… Mais ni en Russie ni en Iran, où Telegram est accusé de favoriser l'insurrection. A la suite des attentats de 2015, la France et l'Allemagne ont demandé à l'Union européenne de légiférer sur ces messageries cryptées.

En vain. Il s'agissait de contraindre les frères Dourov à dévoiler les clés de cryptage.

Mais pour les frères Dourov , la liberté (d'échanger en secret) est supérieure à toute raison d'Etat.

———

Selon l'hebdomadaire *L'Express*, de nombreux dirigeants politiques français et leurs équipes utilisent cette application à droite comme à gauche[21,22]. Sont notamment citées les équipes de François Fillon et Nicolas Sarkozy ainsi que Jean-Luc Mélenchon, Emmanuel Macron et Arnaud Montebourg, ce dernier expliquant qu'il « faut se méfier du pouvoir en place… et de ses suivants ». Pourtant, divers spécialistes critiquent la sécurité de cette application, lui préférant d'autres, notamment fondées sur un format ouvert (cf. *infra*, section « Sécurité »).

Censure en Russie

Le 13 avril 2018, un tribunal de Moscou ordonne le blocage de Telegram en Russie, au motif qu'elle a refusé de fournir au FSB les clés permettant de lire les messages des utilisateurs[23].

Selon la position des tribunaux russes sur la base de la « loi de Yarovaya », Telegram est tenu de stocker les clés de chiffrement de toute la correspondance de l'utilisateur et de les fournir à la demande du FSB [24,25]. La gestion des « télégrammes » insiste sur le fait que cette exigence est techniquement impraticable (les clés sont stockées sur les appareils des utilisateurs et n'atteignent pas les serveurs du messager), et contredit également la constitution russe.

Une semaine après l'arrêt, Roskomnadzor (le Service fédéral de supervision des communications) a bloqué 19 millions d'adresses IP, dont beaucoup appartenant à Amazon Web Services ou Google Cloud, afin de bloquer Telegram, qui « jongle » avec ces adresses pour permettre les communications [26]. Utilisée avec succès, un an auparavant, contre Zello (en), la manœuvre a évidemment eu des effets collatéraux importants, entre autres sur le réseau Mastercard ou l'appli TamTam de Mail.Ru. Roskomnadzor a depuis réduit la voilure de l'opération, tandis que le gouvernement maintenait la pression sur Apple afin qu'ils cessent de proposer l'appli sur leur AppStore [26].

Bien qu'Apple ait refusé de céder sur ce point (alors qu'il l'a fait en Chine), il a accepté, en revanche, avec Google, de bloquer (en avril 2018) la technique du « *domain fronting* », sous pression de Moscou [27,28]. Cette technique est aussi utilisée par le réseau Tor ou l'application Signal [26].

ICO et projet TON

En janvier 2018 Telegram révèle son intention de procéder à une ICO pour lever près d'un milliard de dollars et développer une plateforme de services décentralisés, basée sur sa propre blockchain[29].

Caractéristiques

Compte[modifier | modifier le code]

La création d'un compte se fait de façon similaire à LINE[30], WhatsApp ou WeChat[31] avec une vérification par SMS ou appel téléphonique[32]. Il est possible d'accéder à son compte et de recevoir ses messages à la fois sur mobile et ordinateur. Il est possible de créer un pseudonyme afin d'envoyer et recevoir des messages sans divulguer son numéro de téléphone. Les comptes peuvent être supprimés à tout moment et le sont automatiquement après une durée d'inactivité paramétrable (6 mois, par défaut).

Messages

Les messages réguliers sont chiffrés via un procédé de chiffrement maison nommé *MTProto* (cryptographie symétrique) et transitent via les serveurs de Telegram[33]. Les messages sont déchiffrables pour Telegram LLC et stockés durablement sur leurs serveurs. Les utilisateurs peuvent envoyer des messages, photos, GIFs animés (transformés au format MPEG-4), vidéos, sons et URL, ainsi que des documents sans limite de taille[6]. Il est possible d'envoyer des messages groupés ainsi que de créer des canaux publics. Les messages peuvent contenir des hashtags, permettant de les retrouver ensuite via la partie recherche. L'avertissement à un utilisateur se fait via le symbole arobase (@). Les URL envoyées sont décodées et permettent d'afficher directement l'image s'il s'agit d'une image, ou un entête et une image, s'il s'agit d'une page web.

Les chats secrets

Une option de Telegram permet d'envoyer des messages chiffrés de bout en bout qui ne sont accessibles que sur l'appareil ayant initié ou accepté le chat[34]. L'invitation et l'acceptation du chat secret scellent l'envoi automatique des clés de chiffrement. Il est possible de fixer une autodestruction des messages dans le chat secret.

D'après Telegram, le *chat* secret atteindrait le niveau de confidentialité persistante[35,36].

Robots

Depuis juin 2015, la plateforme Telegram est accessible aux développeurs externes afin de créer des robots[37]. Ces derniers sont des comptes Telegram opérés par des programmes informatiques. Ils peuvent lire et répondre à des messages ou être ajoutés à des groupes. Selon le fondateur de Telegram, l'une des sociétés créant ces robots aurait eu une proposition de rachat se chiffrant en dizaines de millions, symbole selon lui de la valeur de Telegram[16].

source : wikipedia