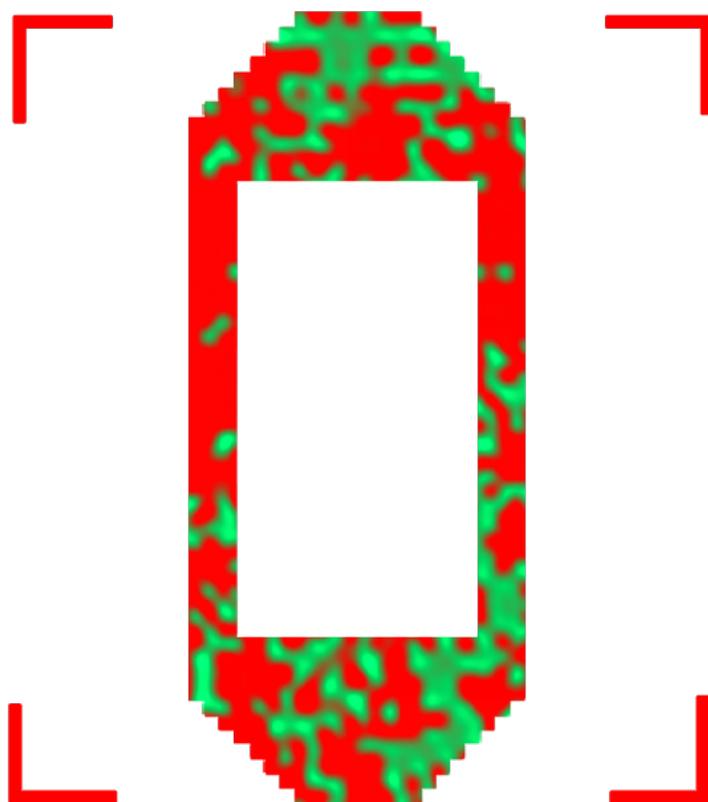


Le Kremlin est entré dans le chat

Les militants anti-guerre russes ont fait confiance à Telegram, une application de messagerie prétendument sécurisée. Comment le régime de Poutine semble-t-il connaître chacun de leurs mouvements ?



SUR LE FROID,Après-midi clair du 24 février 2022 - le jour où les forces de Vladimir Poutine ont lancé leur invasion à grande échelle de l'Ukraine - une poignée de politiciens de l'opposition russe se sont rassemblés devant le palais de la loi, de l'ordre et de la sécurité de Saint-Pétersbourg. Ils étaient venus demander officiellement l'autorisation d'organiser un rassemblement contre la guerre, ce qu'ils savaient serait refusé. Parmi le groupe se trouvait Marina Matsapulina, la vice-présidente du Parti libertaire de Russie, âgée de 30 ans. Matsapulina a compris que le rassemblement était un geste

symbolique et qu'il comportait de sérieux risques.

Neuf jours plus tard, Matsapulina a été réveillée vers 7 heures du matin par quelqu'un frappant à la porte de son appartement. Elle s'est glissée jusqu'à l'entrée mais était trop effrayée pour regarder par le judas, et elle s'est retirée dans sa chambre. Le martèlement a continué pendant deux heures, alors que Matsapulina a tenu sept amis de son parti informés lors d'une discussion de groupe privée sur Telegram. "Il est peu probable qu'ils le détruisent", a-t-elle écrit avec un vœu pieux.

Mais à 9h22, elle a entendu un bruit beaucoup plus fort. Elle eut juste le temps de verrouiller son téléphone avant que la porte ne s'effondre. Huit personnes entouraient le lit de Matsapulina. Ils comprenaient, se souvient-elle, deux policiers de la ville, une équipe SWAT de deux personnes brandissant des fusils et des lampes de poche lui braquant le visage, et deux agents du Centre de lutte contre l'extrémisme, du Service fédéral de sécurité ou du FSB, le successeur du KGB. Les policiers lui ont dit de s'allonger sur le sol face contre terre.

Ils ont dit à Matsapulina qu'elle était soupçonnée d'avoir envoyé un e-mail à un poste de police avec une fausse alerte à la bombe. Mais lorsqu'elle a été emmenée au service d'enquête du ministère de l'Intérieur, dit-elle, un policier lui a demandé si elle connaissait la véritable raison de son arrestation. Elle a deviné que c'était pour ses « activités politiques ». Il a hoché la tête et a demandé: "Savez-vous comment nous avons su que vous étiez à la maison?"

"Comment?"

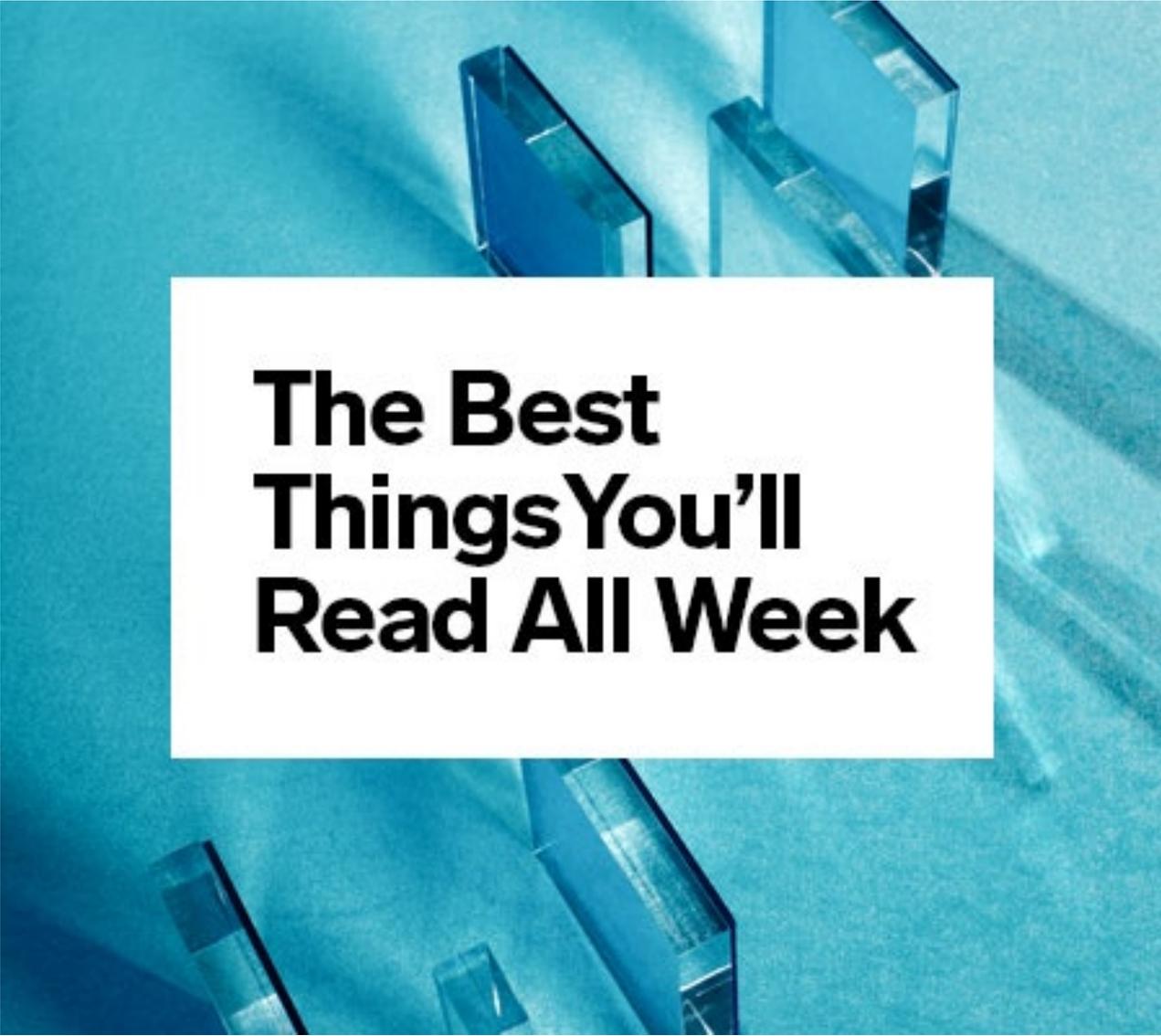
Elle dit que l'officier lui a dit que les enquêteurs avaient suivi ses conversations privées sur Telegram au fur et à mesure qu'elle les écrivait. "Tu étais là, assis là, écrivant à tes amis dans la salle de chat", se souvient-elle en disant. Il a ensuite cité sans passion mot pour mot plusieurs messages Telegram qu'elle avait écrits depuis son lit. "Il est peu probable qu'ils le démontent", a-t-il récité.

"Et alors," dit-il, "nous savions que vous étiez là."

Matsapulina était sans voix. Elle essaya de cacher son choc, espérant en savoir plus sur la façon dont ils avaient accédé à ses messages. Mais l'officier n'a pas précisé.

Lorsqu'elle a été libérée deux jours plus tard, Matsapulina a appris de son avocat que le matin de son arrestation, la police avait perquisitionné les maisons de quelque 80 autres personnes liées à l'opposition et en avait arrêté 20, les accusant chacune de terrorisme lié à l'alerte à la bombe présumée. Quelques jours plus tard, Matsapulina a rassemblé ses affaires et a pris un vol pour Istanbul.

Inscrivez-vous aujourd'hui



The Best Things You'll Read All Week

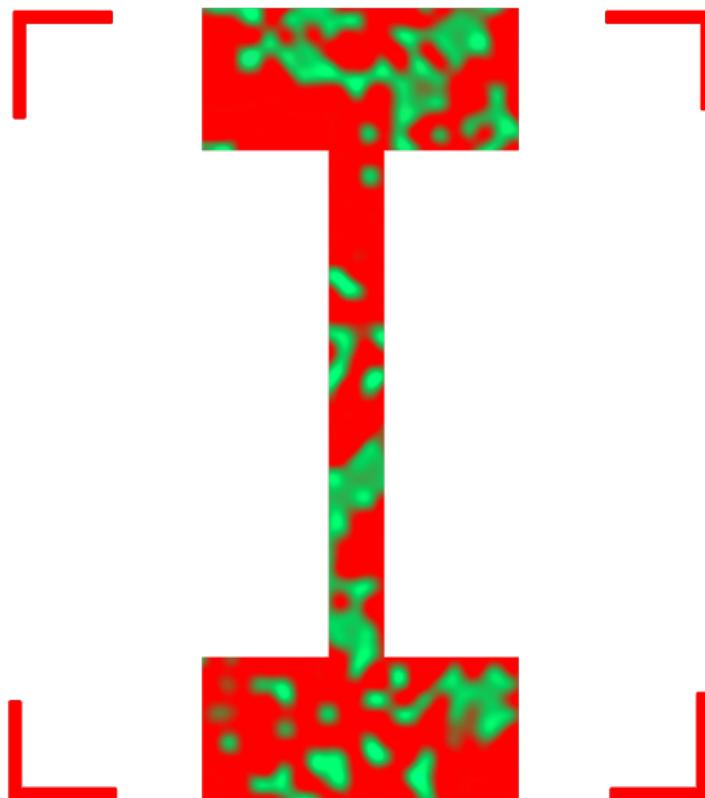
Inscrivez-vous à notre [newsletter Longreads](#) pour les meilleures fonctionnalités, idées et enquêtes de WIRED.

En avril, après être arrivée en toute sécurité en Arménie, Matsapulina a raconté l'épisode dans un fil Twitter. Elle a exclu la possibilité que quiconque dans son groupe très uni ait coopéré avec les forces de sécurité (ils avaient tous également quitté la Russie à ce moment-là), ce qui a laissé deux explications concevables sur la façon dont les officiers avaient lu ses messages privés Telegram. L'une était qu'ils avaient installé une sorte de logiciel malveillant, comme le tristement célèbre outil Pegasus du groupe NSO, sur son téléphone. D'après ce qu'elle avait recueilli, le logiciel coûteux était réservé à des cibles de haut niveau et n'aurait probablement pas été tourné vers un personnage de niveau intermédiaire dans un parti non

enregistré comptant environ 1 000 membres dans tout le pays.

L'autre explication "désagréable", écrit-elle, "est, je pense, évidente pour tout le monde". Les Russes devaient envisager la possibilité que Telegram, l'application prétendument antiautoritaire cofondée par le mercuriel natif de Saint-Pétersbourg Pavel Durov, se conforme désormais aux demandes légales du Kremlin.

Le cas de Matsapulina n'est pas un cas isolé, bien qu'il soit particulièrement troublant. Au cours de l'année écoulée, de nombreux dissidents à travers la Russie ont trouvé leurs comptes Telegram apparemment surveillés ou compromis. Des centaines d'entre eux ont vu leur activité Telegram exercée contre eux dans des affaires pénales. Ce qui est peut-être le plus troublant, c'est que certains militants ont découvert que leurs « discussions secrètes » - la fonction cryptée de bout en bout prétendument blindée de Telegram - se comportaient étrangement, d'une manière qui suggère qu'un tiers indésirable pourrait être en train d'écouter. Ces affaires ont déclenché un tourbillon de théories du complot, de paranoïa et de spéculations parmi les dissidents, dont la confiance dans Telegram s'est effondrée. Dans de nombreux cas, il est impossible de dire ce qui se passe réellement dans les comptes des gens - si des logiciels espions ou des informateurs du Kremlin ont été utilisés pour entrer par effraction, sans faute particulière de l'entreprise ; si Telegram coopère vraiment avec Moscou ; ou s'il s'agit d'une plate-forme si intrinsèquement dangereuse que cette dernière est simplement ce qui semble se passer.



DANS LA DÉCENNIE Depuis sa création en Russie, Telegram est devenu l'un des plus grands réseaux sociaux au monde, avec 700 millions d'utilisateurs, mais seulement une soixantaine d'employés. "Pour nous, Telegram est une idée", a déclaré Durov. "C'est l'idée que tout le monde sur cette planète a le droit d'être libre."

La plate-forme, désormais basée à Dubaï, a une modération de contenu minimale en dehors d'un engagement déclaré à éliminer la pornographie illégale, les violations des droits de propriété intellectuelle, les escroqueries et les appels à la violence. Souvent décrit dans la presse comme une application de messagerie "cryptée" ou "sécurisée", Telegram s'est façonné comme un refuge pour une communication sûre et anonyme, mais en fait, il oblige les utilisateurs à faire tout leur possible pour définir un chat comme "secret". ; contrairement à [WhatsApp](#) ou [Signal](#), le chiffrement de bout en bout n'est pas la valeur par défaut. Pourtant, Durov a réussi à plusieurs reprises à bénéficier des trébuchements d'autres géants de la technologie, en particulier lorsque la confidentialité des utilisateurs est en jeu. En janvier 2021, une crise de relations publiques entourant le partage de données de WhatsApp avec Facebook a contribué à pousser des millions de personnes vers Telegram, un exode que Durov a qualifié de « plus grande migration numérique de l'histoire de l'humanité ».

Telegram a la capacité de partager presque toutes les informations confidentielles demandées par un gouvernement. Les utilisateurs doivent simplement croire que ce ne sera pas le cas.

Aux États-Unis, Telegram a été relativement lent à s'imposer, bien qu'à la suite de l'interdiction de Facebook et Twitter par Donald Trump en janvier 2021, il soit de plus en plus devenu un foyer pour des groupes d'extrême droite comme les Proud Boys et les adeptes de QAnon. Mais dans de nombreuses régions du monde, Telegram est courant. Au Brésil, où l'application a été téléchargée sur plus de la moitié des smartphones du pays, une grande partie de l'insurrection de janvier 2023 était prévue sur la plateforme. Le télégramme a également été crucial pour les militants pro-démocratie à Hong Kong et dans les pays sous la coupe de la Russie, comme la Biélorussie et [l'Ukraine](#) . Dans ce dernier, il est devenu l'application préférée pour diffuser

les conseils du gouvernement pour éviter les frappes aériennes, ainsi que pour la désinformation russe.

Mais c'est en Russie même que Telegram est devenu presque indispensable au cours de l'année écoulée, grâce à la répression en temps de guerre du régime de Poutine contre la technologie occidentale. Depuis le début du conflit, les autorités russes ont qualifié le principal rival de Telegram, Meta, d'organisation « extrémiste », en partie pour avoir permis à certains utilisateurs en Ukraine de publier des appels à la violence contre l'armée russe. La Russie a ensuite bloqué le Facebook de Meta(qui comptait quelque 70 millions d'utilisateurs dans le pays) et Instagram (80 millions). La base d'utilisateurs russes de Telegram est passée de 30 millions en 2020 à près de 50 millions aujourd'hui, dépassant WhatsApp en tant que plate-forme de messagerie la plus utilisée en Russie. (Le Kremlin contrôle toutes les sociétés Internet les plus populaires basées en Russie, y compris VKontakte, un réseau social de type Facebook cofondé par Durov en 2006 qui compte près de 70 millions d'utilisateurs.)

Dès le début de la guerre, les experts en cybersécurité ont fait part de leurs inquiétudes quant à l'exposition des utilisateurs de Telegram aux autorités russes, même les utilisateurs qui se trouvent en dehors de la Russie. Le 24 février, Moxie Marlinspike, le cofondateur de Signal, le rival américain de Telegram, a posté sur Twitter : « Telegram est le messenger le plus populaire en Ukraine urbaine. Après une décennie de marketing et de presse trompeurs, la plupart des gens pensent qu'il s'agit d'une "application cryptée". La réalité est tout le contraire. » Outre les "discussions secrètes", les messages de Telegram sont accessibles aux personnes à l'intérieur de l'entreprise. « Chaque message, photo, vidéo, document envoyé/reçu au cours des 10 dernières années ; tous les contacts, les adhésions à des groupes, etc. sont tous accessibles à toute personne ayant accès à cette base de données », a tweeté Marlinspike. Elies Campo, qui dit avoir dirigé la croissance, les affaires et les partenariats de Telegram pendant plusieurs années, a confirmé cette caractérisation générale à WIRED, tout comme un ancien développeur de Telegram. En d'autres

termes, Telegram a la capacité de partager presque toutes les informations confidentielles demandées par un gouvernement.

Mais à bien des égards, les autorités russes n'ont peut-être même pas besoin de la coopération de Telegram pour surveiller les utilisateurs à grande échelle. C'est parce que Telegram a effectivement intégré cette capacité dans sa généreuse interface de programmation d'applications. Une API est un portail logiciel via lequel les développeurs d'applications et les chercheurs peuvent essentiellement se connecter à une plate-forme et en extraire des données pour leurs propres projets. Dans le cas de Telegram, ces données incluent le contenu textuel et les métadonnées de tout chat ou canal de groupe public, et même un enregistrement de la dernière fois que les utilisateurs étaient en ligne.

Comme la plupart des API, Telegram nécessite une clé d'accès ; mais ceux-ci sont disponibles pour tout utilisateur qui en fait la demande. Pendant des années, Durov a présenté l'API ouverte de la plate-forme comme un emblème de l'engagement de Telegram en matière de transparence, permettant à quiconque d'inspecter le code source de Telegram ou de créer des robots automatisés qui peuvent, entre autres fonctions, diffuser des brèves d'actualité, traiter des paiements ou transmettre des commandes à n'importe quel Internet. appareil connecté. Mais cela fait également de Telegram un outil potentiellement puissant pour la surveillance de masse.

Campo, qui est maintenant membre du Citizen Lab, un centre de recherche spécialisé dans les logiciels espions, affirme que l'API de l'application permet à tout utilisateur de sauvegarder et de cataloguer automatiquement un grand nombre de canaux publics et de discussions de groupe, une fonction qui n'est pas possible sur des plateformes comme WhatsApp et Instagram. Cela expliquerait, dit-il, comment les autorités auraient pu gratter même les petits canaux en indexant à grande échelle. "Telegram pourrait créer des mesures de sécurité pour rendre cela plus difficile, surtout s'il soupçonne que le Kremlin fait cela et veut le contrer, par exemple, plus de barrières contre les bots ; barrières qui identifient si les utilisateurs rejoignant des groupes ou des canaux sont humains ou non.

(Campo a été abondamment cité dans une histoire WIRED de 2022 sur [l'essor mondial de Telegram](#) . La société a affirmé, après la publication de cette histoire, que Campo n'avait jamais été employé par Telegram et n'était que brièvement bénévole. Campo a fourni à WIRED une documentation de 2016 à 2021 qui comprenait des copies de la correspondance par e-mail qu'il a entretenue, en utilisant une adresse Telegram, avec des dirigeants d'Apple, Spotify et Stripe au nom de Telegram, et des copies de contrats entre Telegram et d'autres sociétés avec la signature de Campo. Durov a également été inclus dans la correspondance.)

Quant à l'accès que son API offre aux chaînes publiques, "Telegram vous donne à peu près n'importe quoi", explique Jordan Wildon, enquêteur à l'Institute for Strategic Dialogue, un groupe de réflexion qui traque la désinformation et l'extrémisme. L'API a été inestimable pour la recherche de Wildon, dit-il, mais « il y a des risques évidents avec cela. Il peut être abusé. Au début de la guerre, par exemple, lui et un autre chercheur ont découvert qu'il était possible d'usurper l'API de localisation de Telegram pour identifier tout utilisateur dans un rayon de 2 miles s'il avait récemment activé sa localisation. D'innombrables utilisateurs se sont « accidentellement configurés [eux-mêmes] comme balise de guidage », explique Wildon. Il a pu localiser quatre personnes près de Tchernobyl avec une précision de 1 mètre juste au moment où les forces russes tentaient de s'emparer de la zone. Telegram conteste ce niveau de précision, mais peu de temps après que le partenaire de recherche de Wildon a rendu public ses méthodes, Telegram a discrètement modifié son code. Mais Wildon a découvert qu'il était toujours possible de localiser d'autres utilisateurs avec une précision d'environ 600 mètres. Bien que cela rende ses recherches plus difficiles, Wildon pense que l'accès aux données sur les utilisateurs de Telegram devrait être aussi "difficile que possible". Actuellement, dit-il, "avec suffisamment de volonté, des serveurs décents et suffisamment de clés API, vous pouvez archiver presque le lot de Telegram" - chacun des centaines de milliards de textes, fichiers audio et images partagés publiquement sur la plate-forme. Wildon pense que

l'accès aux données sur les utilisateurs de Telegram devrait être aussi "difficile que possible". Actuellement, dit-il, "avec suffisamment de volonté, des serveurs décents et suffisamment de clés API, vous pouvez archiver presque le lot de Telegram" – chacun des centaines de milliards de textes, fichiers audio et images partagés publiquement sur la plate-forme. Wildon pense que l'accès aux données sur les utilisateurs de Telegram devrait être aussi "difficile que possible". Actuellement, dit-il, "avec suffisamment de volonté, des serveurs décents et suffisamment de clés API, vous pouvez archiver presque le lot de Telegram" – chacun des centaines de milliards de textes, fichiers audio et images partagés publiquement sur la plate-forme.

En effet, certaines entreprises privées ont archivé des pans entiers de Telegram. TGStat, par exemple, est une entreprise russe qui fournit des mesures sur le canal Telegram et la croissance des utilisateurs dans différents pays. Dans sa politique de confidentialité, TGStat indique clairement qu'il est tenu par la loi de transmettre les données aux « autorités de l'État de la Fédération de Russie ». Parce que la société archive des données accessibles au public depuis des années, dit Wildon, les forces de sécurité pourraient hypothétiquement aller directement à TGStat pour obtenir une quantité impressionnante d'informations sur un utilisateur sans aucune aide directe de Telegram. Des données telles que le numéro de téléphone d'un utilisateur et les groupes dont il est membre pourraient faire l'objet d'une ingénierie inverse en agrégeant les listes de membres de nombreux groupes ou historiques de discussion. "Si vous pouvez identifier un seul utilisateur et avoir suffisamment de discussions enregistrées", déclare Wildon,

Dans un e-mail à WIRED, le fondateur de TGStat, Yury Kizhikin, a écrit : « La situation en Russie et dans le monde n'a aucune influence sur les activités de TGStat ». Il a confirmé que les données peuvent être transférées aux autorités russes mais a déclaré que "toutes les entreprises opérant en Russie ont une clause similaire dans leurs politiques" et que TGStat n'avait reçu aucune demande des autorités ou des forces de l'ordre.

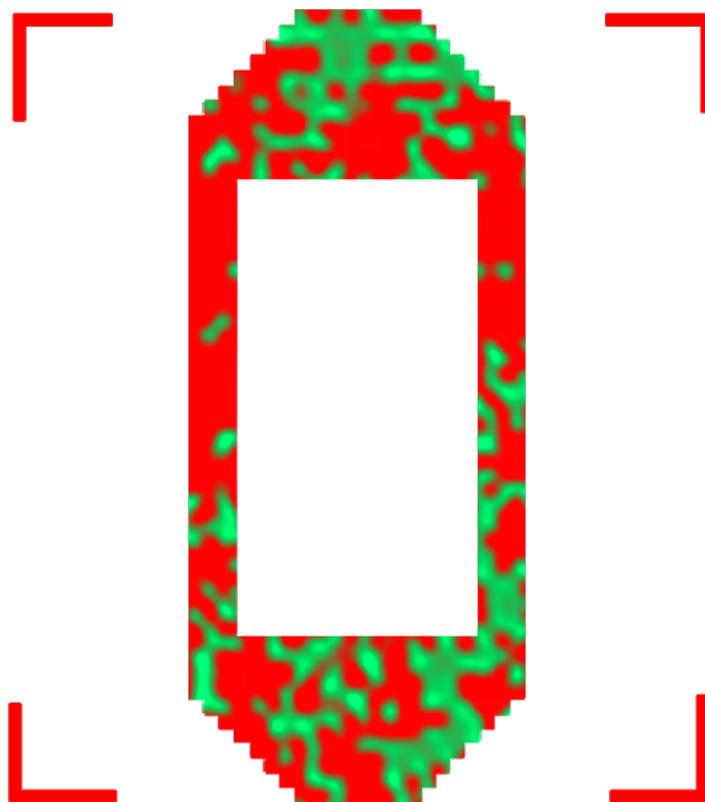
Stanislav Seleznev, avocat d'Agora, un groupe de défense des droits de l'homme qui représente des milliers de personnes sous le contrôle du Kremlin

depuis 2005, affirme qu'il n'a "absolument aucun doute" que le Kremlin exploite l'API de Telegram à grande échelle. La Russie a dépensé sans compter pour suivre ses citoyens sur Telegram et d'autres plateformes. En septembre 2021, Reuters a rapporté que le Kremlin devait dépenser 425 millions de dollars en outils pour renforcer son infrastructure Internet, y compris ceux qui recherchent automatiquement du contenu illégal sur les plateformes de médias sociaux. Seleznev dit que le Kremlin travaille également avec des entreprises technologiques russes comme SeusLab, qui traite un milliard de pages de réseaux sociaux et de chats de messagerie instantanée par jour, pour produire des profils détaillés d'utilisateurs en fonction de leur "activité politique". Evgeny Rabchevsky, directeur du SeusLaba déclaré à Reuters que "les autorités utilisent le produit pour évaluer les tensions sociales, identifier les problèmes d'intérêt [et] ajuster leurs activités".

Une communauté de renseignement open source pro-guerre en plein essor a également construit une armée de bots sur Telegram pour rechercher des utilisateurs via un nom d'utilisateur et voir dans quels groupes publics ils se trouvent et quels canaux ils suivent, ce qui les rend plus faciles à identifier. Selon Ksenia Ermoshina, chercheuse au Citizen Lab et au Center for Internet and Society, les personnes qui savent comment naviguer dans le système peuvent obtenir un portrait assez détaillé des activités publiques d'un utilisateur simplement en saisissant son identifiant Telegram, « ce qui est assez effrayant. »

Selon un rapport de Reuters, l'un des membres de cette communauté de renseignements open source est une ONG pro-Poutine appelée le Centre d'étude et de surveillance du réseau de l'environnement des jeunes, qui a développé un outil d'IA pour analyser les médias sociaux à la recherche de ce qu'il décrit comme contenu socialement dangereux. Le système, a déclaré le fondateur Denis Zavarzin, "surveille en permanence" environ 1,5 million de comptes.

Mais ces outils, aussi puissants soient-ils, ne peuvent scruter que les chats et les canaux publics de Telegram. Pour accéder à des discussions privées comme l'échange de Marina Matsapulina avec ses amis le jour où l'équipe SWAT a frappé à sa porte, sans parler des « discussions secrètes » cryptées de bout en bout, l'API de Telegram ne suffit pas. Pour accéder à ces conversations, le Kremlin semble avoir trouvé d'autres méthodes et, peut-être, d'autres complices.



LE 4 MARS, En 2022, la veille de l'arrestation de Matsapulina par la police pour "terrorisme", Vladimir Poutine a promulgué un projet de loi qui introduisait des peines de prison et des amendes prodigieuses pour quiconque publiait "sciemment de fausses informations" sur l'armée russe. En effet, toute personne critiquant la guerre en Ukraine sur les réseaux sociaux pourrait encourir jusqu'à 15 ans de prison. La loi est rapidement devenue la base d'une série croissante d'arrestations et de poursuites. Lorsque Telegram est devenu l'une des dernières oasis d'information et de discussion pour les Russes, il est également devenu une sorte d'entonnoir pour les agents du Kremlin. Seleznev d'Agora pense que l'API de Telegram permet aux enquêteurs de surveiller des groupes publics à grande échelle, puis de se

concentrer sur des suspects potentiels, qui peuvent ensuite être poursuivis dans des canaux privés par des agents d'infiltration – ou peut-être via une ordonnance du tribunal à Telegram.

La militante de l'opposition Ania Kurbatova s'est rendu compte que ses messages réguliers et ses conversations secrètes s'affichaient comme « lus » alors qu'elle savait que le destinataire ne les avait pas lus. Cela aurait dû être impossible.

Début avril, un producteur de musique et chauffeur de bus en Russie nommé Richard Rose a publié une vidéo sur Instagram accusant les troupes russes d'avoir assassiné des centaines de civils ukrainiens à Bucha, un événement qui a été internationalement condamné comme un massacre. Selon le média russe indépendant Meduza, la vidéo a rapidement attiré l'attention d'un officier du FSB dans la ville natale de Rose, Kirov. Dans les jours qui ont suivi, Rose a également envoyé des messages sur Telegram demandant des moyens d'aider les soldats ukrainiens. Rose soupçonne qu'il communiquait parfois avec des agents du FSB. Dans un message écrit à WIRED par l'intermédiaire de son avocat, Rose dit que ses soupçons se sont intensifiés lorsque ces interlocuteurs ont commencé à le persuader de prendre certaines mesures. « J'ai considéré cela comme une incitation à commettre un acte terroriste », dit Rose.

Agora pense que l'infiltration policière de Telegram est généralisée. En Biélorussie voisine, les services de sécurité travaillent à partir d'un manuel qui décrit « des outils et des méthodes » pour « désanonymiser » les utilisateurs de Telegram, y compris des conseils pour infiltrer des groupes. Ermoshina soupçonne que la même chose se produit en Russie, à en juger par la hausse des affaires pénales qui citent l'activité Telegram d'un suspect – un développement qu'elle attribue en partie à la plate-forme. "Telegram aurait pu devenir un endroit où les autorités russes ne sont pas les bienvenues", dit-elle. Un porte-parole de Telegram écrit : « Comme les utilisateurs ordinaires,

les représentants des organisations policières du monde entier sont susceptibles d'utiliser tous les services Internet disponibles pour communiquer. Telegram n'a connaissance d'aucun cas où nous aurions pu influencer leurs choix.

Le 13 avril, le FSB a obtenu une ordonnance du tribunal pour surveiller les appels téléphoniques de Rose et lire ses messages. On ne sait pas si Telegram s'est conformé à cet ordre. Le lendemain, Rose et sa femme, qui avaient également publié la vidéo sur Bucha, ont été arrêtés pour avoir diffusé « sciemment de fausses informations », les enquêteurs citant des messages Telegram que Rose avait envoyés à une personne inconnue avec un numéro de téléphone letton dans lequel il interrogé sur l'évacuation de sa famille de Russie. Pendant sa détention provisoire, Rose a appris que les autorités russes l'avaient qualifié d'« extrémiste ».

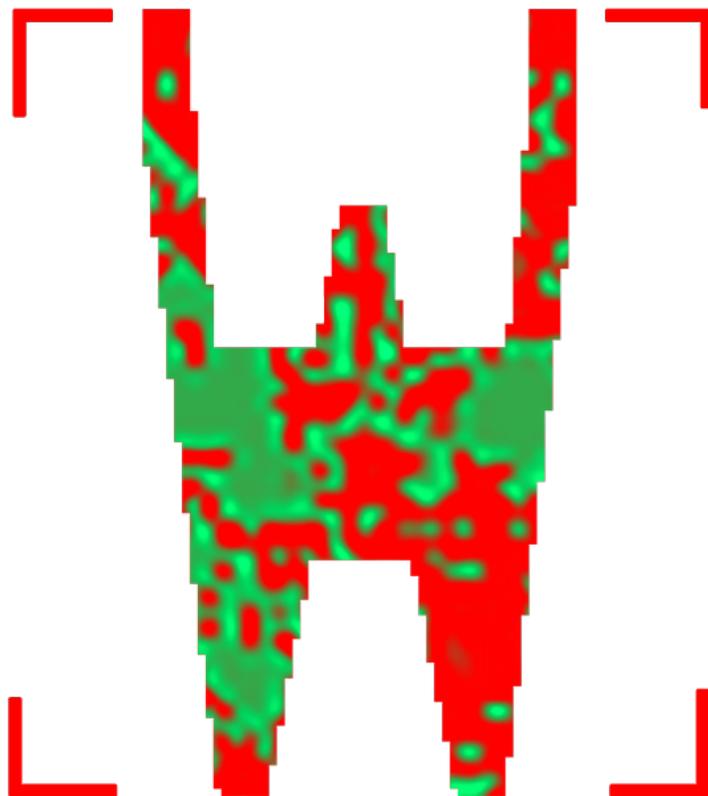
Comme Meduza l'a rapporté, il n'est pas clair si les enquêteurs ont accédé aux messages de Rose avant ou après l'avoir arrêté. Un porte-parole de Telegram a déclaré à WIRED que la société n'avait jamais partagé d'informations ou de messages d'utilisateurs avec le FSB ou le Kremlin. Il est possible que l'interlocuteur letton de Rose ait été un agent d'infiltration ou que les enquêteurs aient physiquement accédé aux messages de Rose lorsqu'il a été contraint de donner son téléphone pendant l'interrogatoire. (Selon un rapport récent du journal israélien *Haaretz*, les autorités russes possèdent un logiciel qui leur permet de contourner les codes d'accès sur les téléphones verrouillés.)

Encore plus de mystère entoure certaines activités fantomatiques que les dissidents ont rencontrées dans les paramètres les plus sécurisés de Telegram. La plate-forme affirme que sa fonctionnalité de « discussions secrètes » cryptées de bout en bout (à partir de laquelle les messages ne peuvent pas être transférés) est « sûre tant que votre appareil est en sécurité dans votre poche ». Mais début mai, la militante de l'opposition Ania Kurbatova s'est rendu compte que ses messages réguliers et ses conversations secrètes

s'affichaient comme « lus » alors qu'elle savait que le destinataire ne les avait pas lus. Elle a également remarqué parfois que lorsqu'elle se déconnectait d'un chat secret, la session était toujours marquée "ouverte" et les messages pouvaient toujours être lus. Cela aurait dû être impossible : chaque chat reçoit une clé de cryptage unique qui disparaît une fois la session terminée. Pour continuer la conversation, les utilisateurs doivent démarrer un nouveau chat et recevoir une nouvelle clé de cryptage. Les conversations privées, Kurbatova dit, en a inclus un avec "un journaliste ukrainien qui cherchait des informations sur les personnes qui ont été emmenées en Russie depuis les camps de filtration de la région de Donetsk et Louhansk". Il y a également eu « une conversation importante » avec le partenaire de Kurbatova, Ivan Astashin, un militant qui en 2009 a été condamné à 10 ans de prison pour avoir lancé un cocktail Molotov sur un bureau du FSB. Kurbatova dit qu'Astashin a remarqué les mêmes bizarreries dans ses propres conversations secrètes.

Kurbatova et Astashin ont demandé l'aide d'Ermoshina, qui leur a demandé de vérifier la fonction "sessions actives" de l'application, qui montre les autres appareils sur lesquels l'application est ouverte. Rien ne s'est produit. Ensuite, elle leur a demandé de réinstaller l'application. Même après ces précautions, les discussions secrètes continuaient d'apparaître comme lues et les anciennes sessions pouvaient toujours être rouvertes. Ermoshina était à court d'explications techniques, mais a noté qu'en tant que couple d'activistes bien connu, Kurbatova et Astachin sont une cible précieuse pour le Kremlin. Et leur cas n'est pas isolé. En août, Yana Teplitskaya, une militante des droits humains qui a enquêté sur les allégations de torture de prisonniers russes, a remarqué que nombre de ses conversations secrètes étaient marquées à tort comme lues.

Bien qu'il soit possible qu'un logiciel espion soit impliqué, de tels cas ont tourné les soupçons des dissidents vers Telegram lui-même. Pour de nombreux militants, cela représente une perte de confiance précipitée.



QU'EST-IL ARRIVÉ À Marina Matsapulina dans son appartement reflète étrangement quelque chose qui est arrivé une fois à Pavel Durov – un événement qui sert de mythe fondateur de Telegram. En décembre 2011, à la suite d'élections parlementaires très controversées, Durov, alors PDG de VKontakte, alors âgé de 27 ans, a reçu une demande du FSB de supprimer les pages des groupes d'opposition. Durov a refusé, puis s'est moqué théâtralement du gouvernement sur Twitter. Comme il l'a dit plus tard au

New York Times , une équipe du SWAT est rapidement arrivée à son appartement. Alors qu'ils frappaient à sa porte, Durov a appelé son frère aîné mais s'est vite rendu compte qu'il n'avait aucun moyen de communication sécurisé. À ce moment-là, a affirmé Durov, il a vu le besoin d'une plate-forme qui pourrait contourner la surveillance autoritaire. "C'est comme ça que Telegram a commencé."

Pendant plus d'une décennie, le "Mark Zuckerberg russe" s'est efforcé de maintenir une personnalité plus grande que nature en tant que croisé impétueux, vêtu de noir et libertaire contre la surveillance autoritaire, dont le principal repoussoir a été l'État russe. Mais comme Matsapulina l'a suggéré dans son fil Twitter en avril dernier, la relation de Telegram avec l'État russe semble avoir considérablement changé au cours des dernières années.

Qui a vraiment cligné des yeux ? Sur quelles conditions Telegram et Roskomnadzor s'étaient-ils mis d'accord ? Les deux parties ont fourni des explications clairessemées.

Comme elle l'a rappelé à ses abonnés, les relations entre la plateforme et les autorités étaient au plus bas en 2018. En avril, Durov a refusé un ordre du FSB de remettre les clés de chiffrement des utilisateurs russes. En réponse, le Kremlin a interdit Telegram de Russie et le régulateur des télécommunications Roskomnadzor s'est mis à bloquer l'accès à Telegram depuis l'Internet russe.

Des milliers de personnes ont protesté contre la décision à Saint-Pétersbourg, certaines brandissant des affiches représentant Durov comme une icône religieuse rayonnante portant le logo de l'avion en papier de Telegram. Ajoutant au récit du héros provocateur, le personnel de Durov a caché Telegram derrière les services d'hébergement de Google et d'Amazon pour déguiser et changer constamment ses adresses Web. Lors d'un bref dommage collatéral, Roskomnadzor a accidentellement bloqué quelque 16 millions

d'adresses IP en Russie, dont une grande partie de Twitter et Facebook. Telegram, pour la plupart des utilisateurs, a continué à fonctionner.

Mais en juin 2020, la Russie et Telegram ont soudainement conclu un accord pour débloquent l'application, dont les conditions exactes restent inconnues malgré les demandes de transparence des chercheurs en cybersécurité, des journalistes et des groupes de défense des droits de l'homme. La plupart des Russes, a noté Matsapulina dans son fil, ont ri de la possibilité que Telegram ait fait des concessions au Kremlin. Mais lorsque les autorités russes ont annoncé l'accord, a-t-elle écrit, elles ont "littéralement déclaré" que les deux parties l'avaient conclu "dans le contexte du terrorisme", le contexte même invoqué dans l'arrestation de Matsapulina et d'autres. En fait, l'histoire plus complète entourant l'interdiction et la réintégration de Telegram soulève la question de savoir si Moscou a acquis une certaine influence sur Durov.

En 2018, alors qu'il jouait au chat et à la souris avec Roskomnadzor, Telegram travaillait également à développer quelque chose qui lui avait toujours manqué : un moyen de gagner de l'argent. Comme la plate-forme n'avait jamais hébergé de publicités ni proposé d'abonnements, la société a entrepris de construire une économie entière au-dessus de Telegram, en créant le Telegram Open Network, ou TON, une plate-forme blockchain avec sa propre crypto-monnaie, appelée grammes, qui serait intégrée dans l'application principale. Comme de nombreuses startups blockchain, il collecterait des fonds grâce à une offre initiale de pièces, permettant aux investisseurs d'acheter des grammes. Les ambitions étaient élevées : deux semaines avant que Roskomnadzor ne bloque l'application, Telegram a annoncé que l'ICO avait levé 1,7 milliard de dollars, le plus important de l'histoire à l'époque. (Une grande partie de l'investissement, comme l'ont rapporté les médias russes indépendants, provenait d'oligarques,

Mais en 2019, la catastrophe a frappé. Juste au moment où TON devait être lancé, la Securities and Exchange Commission des États-Unis a accusé Telegram d'avoir omis illégalement d'enregistrer la crypto-monnaie et a

affirmé que la société s'était approprié des fonds destinés à TON pour payer ses factures. Durov a combattu l'action d'urgence de la SEC pendant un an mais a amèrement annoncé la fin de TON en mai 2020.

Creusez plus profondément avec notre newsletter Longreads

Inscrivez-vous pour recevoir nos meilleures fonctionnalités longues, enquêtes et essais stimulants dans votre boîte de réception tous les dimanches.

Votre e-mail

Entrer votre Email

En vous inscrivant, vous acceptez notre [accord d'utilisation](#) (y compris la [renonciation aux recours collectifs et les dispositions d'arbitrage](#)), notre [politique de confidentialité](#) et notre [déclaration sur les cookies](#) et de recevoir des e-mails marketing et liés au compte de WIRED. Vous pouvez vous désabonner à tout moment.

Forcé de rembourser les investisseurs et aux prises avec la flambée des coûts de serveur de Telegram, Durov avait besoin d'un afflux massif d'argent. À ce moment-là, les relations de Telegram avec la Russie ont commencé à se dégeler. Quelques semaines après la fin du projet TON, deux députés du parti pro-Kremlin au parlement russe ont proposé la levée de l'interdiction de Telegram, arguant qu'il pourrait être un outil de communication important pour le gouvernement en temps de crise. Durov a affiché son soutien à leur proposition sur Telegram, affirmant que la présence de l'entreprise en Russie pourrait aider à renforcer l'innovation technologique et la «sécurité nationale» du pays. Il a également affirmé que depuis 2018, son équipe avait amélioré "les méthodes de détection et de suppression de la propagande extrémiste", ainsi que "les mécanismes permettant de prévenir les attaques terroristes dans le monde" tout en protégeant la vie privée des utilisateurs.

Le 18 juin, Roskomnadzor a levé l'interdiction. Pour les utilisateurs et les médias occidentaux de l'époque, la détente semblait montrer que la ruse antiautoritaire de Durov avait prévalu. Telegram, a déclaré un expert au *Washington Post*, "semble avoir remporté un concours de regards avec Poutine et l'État de sécurité".

Mais qui a réellement cligné des yeux ? Sur quelles conditions Telegram et

Roskomnadzor s'étaient-ils mis d'accord ? Les deux parties ont fourni des explications clairessemées.

Dans un communiqué, le régulateur a salué la nouvelle attitude utile de Durov : "Nous saluons la volonté exprimée par le fondateur de Telegram de lutter contre le terrorisme et l'extrémisme". Des sources gouvernementales anonymes ont déclaré à l'agence de presse russe Interfax que Telegram avait accepté de coopérer avec les services de sécurité dans des cas spécifiques. Ces sources ont également noté que les développements technologiques avaient rendu le besoin de clés de chiffrement "non pertinent", mais n'ont pas expliqué davantage. Dans un article de Telegram après la décision, Durov a assuré aux utilisateurs russes qu'il n'y aurait "aucun changement en termes de sécurité des données personnelles". Poutine lui-même a célébré l'annonce à la télévision en direct un an plus tard lors de ses questions-réponses annuelles sur la ligne directe. "Nous avons conclu un accord avec Telegram", a-t-il déclaré. "Vous pouvez voir que tout fonctionne bien."

Selon une source gouvernementale proche du dossier, la banque publique russe VTB, qui entretient des liens étroits avec le Kremlin, a également été impliquée dans les négociations. En janvier 2021, des informations ont révélé que Telegram avait engagé VTB pour estimer la valeur de l'entreprise : jusqu'à 124 milliards de dollars d'ici 2022. Telegram a également déclaré qu'il commencerait à vendre des obligations à cinq ans. VTB aiderait à les vendre aux investisseurs. En mars 2021, Telegram avait levé plus d'un milliard de dollars auprès de ces bailleurs de fonds. Bien que l'on sache peu de choses sur leur identité - Durov a écrit sur sa chaîne Telegram seulement qu'ils étaient "certains des investisseurs les plus importants et les plus compétents du monde" - *The Moscow Times* a rapporté que les investissements comprenaient 75 millions de dollars provenant d'un partenariat conjoint entre un fonds d'État d'Abu Dhabi et un fonds souverain du Kremlin. Lorsque WIRED a posé des questions sur les termes de l'accord, un porte-parole de Telegram a écrit: "Nous n'avons jamais discuté de quoi que ce soit lié à l'annulation de Telegram avec quiconque travaillant chez VTB." Il a ajouté:

"Nous pouvons confirmer qu'aucun accord n'a été conclu pour inspirer le déblocage de Telegram. Cette décision a été prise uniquement par les autorités russes. (VTB n'a pas répondu aux demandes de commentaires.)

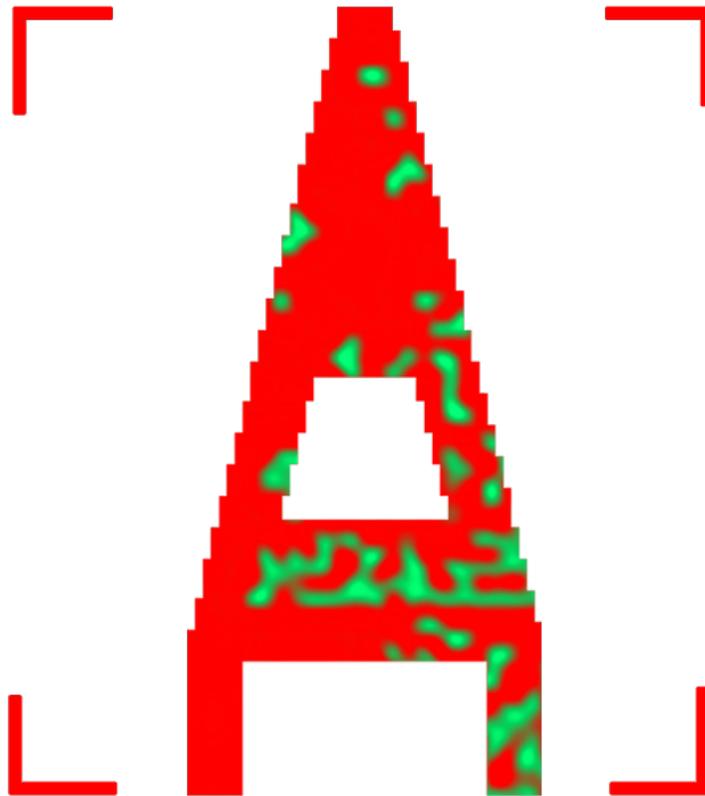
Trois semaines après l'accord de déblocage de Telegram, le vice-président de la société, Ilya Perekopsky, a participé à une conférence à l'extérieur de Kazan pour parler de la croissance de l'industrie informatique russe et a rejoint le Premier ministre Mikhail Mishustin dans un engagement à lutter contre la domination de la technologie américaine. Présentant un discours de Perekopsky dans lequel il a souligné les «racines russes» de Telegram, le vice-Premier ministre Dmitry Chernyshenko a également déclaré que c'était une «bonne nouvelle» que Telegram opère à nouveau en Russie. Les groupes de défense des droits de l'homme, les militants de l'opposition et les médias russes indépendants ont trouvé cette harmonie soudaine entre des ennemis autrefois acharnés aussi fascinante que préoccupante. Plusieurs ont noté le moment fortuit.

Depuis l'invasion de l'Ukraine par la Russie, Telegram et le Kremlin sont apparus encore plus synchronisés. Autorisé à rester debout dans un secteur Internet décimé, Telegram est devenu utile non seulement aux services de sécurité mais aussi à la machine de propagande de l'État. La censure générale des médias russes a fait de Telegram une source d'informations vitale pour les Russes, Meduza et d'autres médias partageant des rapports via des canaux publics sur la plate-forme. Mais la désinformation pro-Kremlin dépasse de loin le journalisme. "Le télégramme est désormais l'épine dorsale de la machinerie de désinformation russe", déclare Jānis Sārts, directeur du Centre d'excellence des communications stratégiques de l'OTAN. "C'est aussi la façon dont ils surmontent tous les barrages routiers construits par les plateformes occidentales." Deux semaines avant l'interdiction de Facebook, un message sur la chaîne Telegram du gouvernement russe résumait une réunion entre le vice-Premier ministre Dmitry Chernyshenko et des dirigeants de l'industrie informatique au cours de laquelle Chernyshenko a déclaré qu'«il est recommandé aux agences gouvernementales de créer des comptes sur Telegram et VKontakte». Telegram est désormais la plateforme de choix des

responsables du Kremlin.

La relation entre Telegram et VTB s'est également développée : quelques mois après le début de l'invasion et le retrait par Apple et Google de l'application VTB de leurs magasins, la société a annoncé qu'elle lançait une banque numérique sur Telegram "pour surmonter la restriction des sanctions pour les clients".

En plus du bureau de presse de Roskomnadzor, WIRED a contacté trois employés actuels et anciens du régulateur au sujet de l'accord, ainsi qu'un actuel et un ancien ministre du gouvernement censés être au courant. Aucun n'a accepté de parler. WIRED a envoyé un message, via Telegram, au chef adjoint de Roskomnadzor, Vadim Subbotin, au sujet de l'accord de 2020 ; il a dit de poser des questions au bureau de presse du régulateur, puis a supprimé l'historique du chat. Vadim Ampelonsky, un ancien porte-parole du régulateur, a répondu : « Je suis un *vatnik* », littéralement une veste matelassée, argot désignant un fervent adepte de la propagande gouvernementale. Il a ajouté que "dans la situation actuelle, participer à la recherche d'une publication américaine est *zapadlo*» – argot vulgaire qui signifie au-dessous de sa dignité. Il a signé : "Prenez soin de vous !"



À LA FIN du fil Twitter d'avril 2022 de Matsapulina, elle a déclaré qu'elle et ses collègues étaient passés de Telegram à Signal. "Je ne veux pas semer la panique, je ne veux pas prétendre que je suis une sorte d'expert sur cette question, mais je veux exhorter tout le monde à faire attention à ce qu'ils disent sur Telegram. Il est possible que ce ne soit plus l'espace sûr que tout le monde pensait que c'était.

Selon Ksenia Ermoshina, une grande partie du mouvement d'opposition russe a également abandonné Telegram. À la consternation générale, dit-elle, les chaînes pro-guerre ont commencé à publier des informations personnelles sur les militants en toute impunité – « en compilant des bases de données de militants anti-guerre russes avec leurs visages et des liens vers leurs [réseaux sociaux], et parfois même des adresses personnelles et d'autres données personnelles ». Lorsque les utilisateurs ont signalé ces incidents, dit-elle, la réponse de Telegram a été lente ou inexistante.

De nombreux chats et groupes où les utilisateurs organisaient des mouvements d'opposition ont été fermés. "Personne n'a organisé quoi que ce soit sur Telegram depuis février", déclare Ermoshina, décrivant une

"migration numérique" du mouvement d'opposition russe depuis Telegram. "Les gens ont quitté la Russie en exil", dit-elle, "et ils ont quitté Telegram en exil!"

Natalia Krapiva, avocate du groupe de défense des droits numériques Access Now, note que Telegram n'a jamais répondu aux demandes de clarté, y compris une lettre ouverte envoyée par son organisation et une coalition de groupes demandant un dialogue sur les "problèmes de sécurité qui affligent" l'application. . En ce qui concerne les inquiétudes selon lesquelles la plate-forme facilite la surveillance de l'État, dit-elle, "Telegram n'a pas fait grand-chose pour démontrer qu'en fait, ils ne coopèrent pas" avec les autorités.

Pendant ce temps, des cas de Telegram coopérant avec des gouvernements en dehors de la Russie sont apparus. En janvier 2022, après que Telegram ait ignoré les multiples demandes des autorités allemandes d'endiguer une vague de violentes manifestations contre le verrouillage de Covid qui avaient été coordonnées sur la plate-forme, le gouvernement allemand a débattu de son interdiction. En juin, a rapporté *Der Spiegel* , Telegram avait fourni à la police fédérale allemande des données personnelles d'utilisateurs soupçonnés de terrorisme et de maltraitance d'enfants. Et en Inde, où il y a plus de 100 millions d'utilisateurs de Telegram, la société a fourni en novembre à la Haute Cour de Delhi les noms, numéros de téléphone et adresses IP des utilisateurs

accusés de partager illégalement sur la plate-forme des supports de cours protégés par des droits d'auteur.

Pavel Durov n'a pas accordé d'interview aux médias occidentaux depuis 2017. Il a refusé de parler officiellement de cette histoire. Mais lors d'un appel vidéo l'automne dernier, l'un des associés de Durov a donné un aperçu de l'état d'esprit du fondateur de Telegram. Georgy Lobushkin était le responsable des relations publiques de VK et reste en contact avec son ancien patron, ayant assisté au 38e anniversaire de Durov à Dubaï en octobre. Il publie souvent des informations non officielles sur les activités de l'entreprise sur sa chaîne Telegram : "Parfois, en Russie, les gens m'appellent le cardinal gris de Telegram parce que je dis des choses au nom de Telegram, mais je ne fais pas officiellement partie de l'équipe. "

"Le marché russe est très important pour Durov", a déclaré Lobushkin, notant qu'il représente environ 7% des 700 millions d'utilisateurs de Telegram, sans parler de son importance symbolique. Bien sûr, Durov a déclaré qu'il ne coopérerait jamais avec les autorités russes et qu'il quitterait le marché en cas de coup dur, dit Lobushkin, mais cela pourrait être "un bluff" puisque la Russie détient un pourcentage si important des utilisateurs de la plate-forme.

Lobushkin dit qu'il n'a aucune information particulière sur les raisons pour lesquelles Telegram a été débloqué en 2020. Mais il pense que le Kremlin a vu le potentiel de la plate-forme. "La machine de propagande russe a appris à utiliser Telegram de manière efficace et efficiente", déclare Lobushkin.

Pavel Cherkashin, un capital-risqueur d'origine russe basé à San Francisco qui a investi dans le projet TON avant son effondrement, affirme que Durov est à l'aise d'opérer dans une zone grise - prêt à fermer les yeux sur le Kremlin parce que la relation est bonne pour la croissance . "Poutine devient un grand allié pour développer son entreprise, et il accepte cela comme un heureux hasard", déclare Cherkashin. Il ajoute que parce que Poutine contrôle quelles plates-formes peuvent opérer en Russie, "il force toutes les affaires - tout cela

est maintenant sur Telegram".

Il est vrai qu'un grand nombre de Russes continuent de dépendre de Telegram, et sa croissance dans le pays et dans le monde a été stimulée par la guerre en Ukraine plutôt que découragée - même *le New York Times* a ouvert une chaîne Telegram pour diffuser des informations sur la guerre. "Les gens font toujours confiance à Telegram pour une raison quelconque", déclare Andrei Soldatov, un journaliste indépendant qui a enquêté sur les services de sécurité russes pendant plus de 20 ans. "Mais je ne sais pas pourquoi."

Fin avril 2022, trois jours après avoir publié son fil, Matsapulina a reçu un message anonyme via le compte d'assistance officiel de Telegram. Elle s'est ensuite rendue sur Twitter pour raconter l'échange. "Nous avons lu votre histoire sur Twitter", a-t-il commencé. "Nous aimerions exprimer notre sympathie pour votre cas et partager les résultats d'une enquête menée par notre équipe." Le message indiquait que seuls deux appareils authentifiés avaient accès à ses messages Telegram : son téléphone et son ordinateur. Il a également noté une tentative de connexion infructueuse "après votre détention". Quelqu'un, que Matsapulina présumait être un policier, avait correctement saisi un code de vérification par SMS mais avait incorrectement saisi son mot de passe. "Du côté de Telegram, l'accès à vos messages privés n'a pas été accordé." Le message concluait que, très probablement,

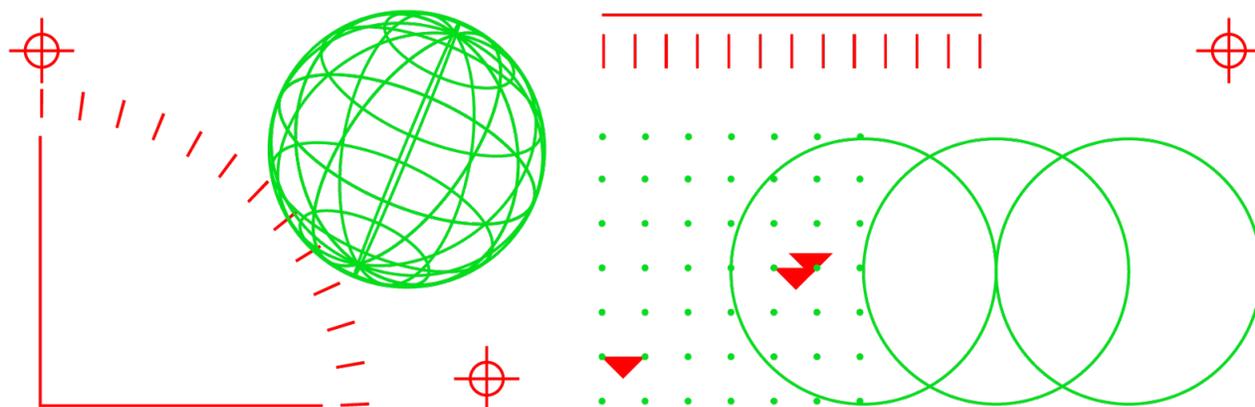
Matsapulina et ses amis ont ensuite demandé à Telegram de vérifier leurs journaux. Elle dit que la société a signalé qu'elle n'avait pas non plus été compromise. Cela a laissé Matsapulina là où elle avait commencé : comment les officiers ont-ils lu ses messages ?

Après avoir discuté de son cas avec des experts, Matsapulina pense maintenant que ses messages Telegram ont peut-être été compromis par une forme de logiciel espion. Lorsqu'on lui a dit qu'un dispositif de piratage informatique devrait être physiquement à proximité pour infiltrer son téléphone, un souvenir a refait surface : à certains moments avant son

arrestation, elle avait remarqué un camion banalisé avec un dôme sur le toit garé devant son immeuble. Elle l'avait même mentionné en plaisantant à des amis sur Telegram. Maintenant, se souvient-elle, alors que la police frappait à sa porte ce matin-là, elle avait repéré le même véhicule mystérieux garé à l'extérieur. Au moment où la police a pris d'assaut sa maison, le véhicule avait disparu.

Matsapulina a depuis recommencé à utiliser Telegram. D'une part, dit-elle, même si les services de sécurité russes suivaient son compte, elle a déjà quitté le pays. C'est aussi son seul moyen d'atteindre ses amis et sa famille : pour Matsapulina et pour des millions de Russes, le chiffrement d'une plateforme reste indispensable.

Reportage supplémentaire de Vadim Smyslov .



Faites-nous savoir ce que vous pensez de cet article. Envoyez une lettre à l'éditeur à mail@wired.com .

Plus de grandes histoires WIRED

-  Les dernières nouvelles sur la technologie, la science et plus encore : recevez nos newsletters !
- La vie de camionneur du 21e siècle
- L' enshittification de TikTok
- Big Tech est vraiment mauvais pour licencier les gens
- Internet engendre des hordes de fans adultes de Bluey
- ChatGPT arrive pour les salles de classe. Ne pas paniquer
-  Explorez l'IA comme jamais auparavant avec notre nouvelle base de données
-  Optimisez votre vie à la maison avec les meilleurs choix de notre équipe Gear, des aspirateurs robots aux matelas abordables en passant par les haut-parleurs intelligents