

discours dissidents, de réduire leurs capacités d'assemblée et de participation au débat politique, d'empêcher toute mobilisation contestataire, voire, dans certains cas, de contrôler les élections. Ces coupures limitent également fortement la liberté de la presse et mettent en difficulté des secteurs essentiels, tels que les services de soins de santé, le commerce ou l'enseignement.

Mais ces blocages peuvent également avoir lieu pour d'autres raisons. Comme en Irak, où plusieurs coupures ont été décrétées à l'occasion des sessions d'exams nationaux dans les écoles du pays en mai, juin, juillet, août et septembre 2025.

Des méthodes multiples à effets variables

Au-delà d'une coupure générale provoquée par un mécanisme extérieur, un dommage physique sur l'infrastructure concernée ou par un ordre de suspension aux opérateurs de télécommunications, il existe différents moyens de restreindre l'accès à Internet. Il est, par exemple, possible de procéder à une manipulation du routage réseau. Cela permet de modifier la circulation des informations à certains endroits clés du système et de bloquer le trafic de données entre les différentes branches du réseau.

Ces types de coupures sont extrêmement difficiles à contourner pour les populations civiles, puisque cela nécessite des infrastructures de télécommunications alternatives, telles que des liaisons par satellite ou par radio numérique dans certains cas.

Une autre manière de bloquer cet accès consiste à réduire fortement le flux de données sur un réseau, qui devient alors inutilisable. Cette technique n'est possible que si l'infrastructure technologique du pays le permet et si les fournisseurs de services internet se soumettent aux réglementations des autorités gouvernementales. Pour un réseau fixe (câbles ou fibre, *NdlR*), il est facile de localiser les échanges de données et de les bloquer, explique Olivier Bonaventure, professeur à l'École polytechnique de l'UCLouvain et expert en cybersécurité. Lorsqu'il s'agit d'un réseau mobile, celui-ci est utilisable grâce à des entreprises spécifiques qui bénéficient d'autorisations pour exploiter ce réseau. Il faut alors lever ces autorisations pour restreindre l'accès à Internet.

Les responsables de ces coupures concentrent parfois leurs restrictions sur certains services, notamment grâce à la manipulation du système de noms de domaine (DNS). "Il y a un service sur Internet qui fait automatiquement la conversion entre ces

noms de domaine et des adresses correspondantes. Pour bloquer l'accès à certains sites, on peut bloquer ce système pour que les données ne correspondent plus à leur adresse", détaille Olivier Bonaventure. Une autre restriction réside dans le blocage de certaines plateformes de communication, telles que WhatsApp, Facebook ou encore X, grâce notamment à des systèmes de filtrage.

Mais ces deux méthodes peuvent être facilement contournées en utilisant un VPN (Virtual Private Network). Cet outil crée une connexion internet sécurisée et privée, même sur un réseau public. Il "chiffre toutes les données émises et les envoie vers un serveur qui se trouve à l'étranger", précise Olivier Bonaventure. Les citoyens peuvent aussi utiliser un serveur DNS indépendant du réseau bloqué, pour peu que celui-ci ne soit pas également suspendu.

Mais les instigateurs de ces limitations peuvent également recourir au "Deep Packet Inspection" (DPI), qui consiste à analyser en profondeur les informations circulant sur un réseau informatique et regroupées en "paquets", non seulement par rapport à leurs métadonnées (*telles que les adresses correspondantes, NdlR*), mais également par rapport à leur contenu. Il permet donc aux acteurs gouvernementaux de contrôler la nature des informations échangées, notamment grâce à l'identification de certains mots-clés dits "sensibles". Tout ce qui est considéré comme "malveillant" par les autorités sera alors bloqué. Il est plus difficile d'éviter ces restrictions à l'aide d'un VPN, car le DPI est capable de le détecter et de couper la connexion.

Les acteurs étatiques ont en outre la possibilité de saturer le serveur d'un site afin de le ralentir fortement voire de le rendre indisponible ou encore d'utiliser un brouilleur de fréquences radio. Cette dernière option est peut-être la plus efficace puisqu'il est presque impossible de limiter ce type de brouillage.

Pékin à la pointe de la censure

Loin de pratiquer ces restrictions de manière temporaire, la Chine a pour sa part mis en place un véritable système de censure appelé le "Grand Firewall" ou "Bouclier doré", qui permet aux autorités de bloquer, filtrer et surveiller l'ensemble du trafic web. Pour ce faire, elle limite fortement le cryptage des données et utilise le filtrage DNS et le Deep Packet Inspection, limitant ainsi l'accès à plusieurs plateformes, comme Google, et inspectant les contenus échangés par les utilisateurs.

EN BREF

Proche-Orient

Quatre dépouilles supplémentaires d'otages remises à la Croix-Rouge

Le Hamas a remis mardi à la Croix-Rouge les dépouilles de quatre otages supplémentaires, ce qui signifie que 20 autres corps sont toujours à Gaza. Le groupe islamiste affirme avoir besoin de temps pour les localiser. Israël garde le passage frontalier de Rafah, entre la bande de Gaza et l'Egypte, fermé aux civils, rapportaient des médias israéliens mardi. L'accès des camions transportant l'aide humanitaire est aussi limité. Israël souhaiterait maintenir cette situation jusqu'à ce que tous les corps des otages décédés aient été rendus. (AFP)

États-Unis

La Cour suprême américaine rejette un appel du complotiste Alex Jones

La Cour suprême américaine a refusé mardi d'examiner l'appel du complotiste d'extrême droite Alex Jones. Celui-ci avait saisi la plus haute juridiction du pays parce qu'il a été condamné à verser 1,2 milliard d'euros aux proches des victimes de la fusillade de l'école primaire Sandy Hook pour avoir qualifié à plusieurs reprises la fusillade, qui a coûté la vie à vingt enfants et six adultes, de "canular". (AFP)

Union européenne

Terres rares : l'UE va discuter avec le G7 d'une "réponse coordonnée" à la Chine

L'Union européenne va discuter avec ses partenaires du G7 d'une "réponse coordonnée" aux restrictions annoncées la semaine dernière par la Chine sur les exportations de technologies liées aux terres rares, a-t-elle annoncé mardi. Ces contrôles "ont déjà contraint certaines entreprises européennes à suspendre leur production, provoquant des dégâts économiques réels", a déclaré le Commissaire européen au Commerce, Maros Sefcovic, soulignant que les mesures chinoises "ciblent directement des industries civiles". "Nous ne pouvons pas le tolérer, parce que cela affecte la bonne marche des entreprises dans toute l'UE", a-t-il ajouté. (AFP)

Mexique

Au moins 64 morts et 65 disparus après une semaine de pluies torrentielles

Les pluies torrentielles qui s'abattent depuis une semaine sur plusieurs États du centre et de l'est du Mexique ont dévasté plusieurs régions en faisant au moins 64 morts et 65 disparus, selon le dernier bilan disponible. Le nombre de décès et les dégâts les plus importants se concentrent principalement dans les États de Veracruz (est), Hidalgo et Puebla (centre), a indiqué la responsable nationale de la protection civile, Laura Velazquez. (AFP)

Épinglé

Un risque en Belgique ?

Dans notre pays, de tels blocages sont prohibés par le respect de la liberté d'expression et du droit à l'information, prévus par les articles 19 et 23 de la Constitution belge ainsi que par l'article 10 de la Convention européenne des droits de l'Homme.

Toutefois, quelques exceptions subsistent dans des cas spécifiques.

Le gouvernement belge pourrait donc suspendre ou restreindre temporairement l'accès au réseau internet en cas de menace grave contre la sécurité nationale, de troubles graves à l'ordre public ou dans le cadre d'une décision de justice.

C'est notamment le cas, lorsque des sites web sont déclarés illégaux, note Olivier Bonaventure, professeur à l'UCLouvain et expert en cybersécurité. Les autorités recourent alors à la manipulation du système de noms de domaine (DNS) à l'encontre du site concerné. C.T.

