CENSURE ET SURVEILLANCE DES JOURNALISTES : UN BUSINESS SANS SCRUPULES

REPORTERS SANS FRONTIERES
POUR LA LIBERTE DE L'INFORMATION

ENQUÊTE DE REPORTERS SANS FRONTIÈRES
REZA MOINI / BENJAMIN ISMAIL / ELODIE VIALLE

SOMMAIRE

INTRODUCTION

I. CENSURE : LES GÉANTS DU NET ENTRE SOUMISSION ET COLLABORATION ACTIVE 5

II. LE COMMERCE DOUTEUX MAIS LUCRATIF DE LA SURVEILLANCE 8

III. DES RÉGULATIONS INTERNATIONALES EN PANNE OU BLOQUÉES PAR LES LOBBIES 12

IV. LES RECOMMANDATIONS DE RSF FACE À LA CYBERCENSURE 16

V. JOURNALISTES, PROTÉGEZ VOS DONNÉES ET VOS COMMUNICATIONS 18

Couverture : FRED TANNEAU / AFP

INTRODUCTION

À l'occasion de la journée mondiale contre la cybercensure, Reporters sans frontières (RSF) déplore la soumission des géants du web qui n'hésitent pas à répondre favorablement aux injonctions de régimes autoritaires en matière de censure.

Par ailleurs, l'absence de mécanismes internationaux de régulation des technologies de surveillance permet à des entreprises de vendre des outils de surveillance en ligne à des régimes autoritaires. Quitte à mettre de côté les droits de l'Homme pour quelques parts de marché.

1 CENSURE : LES GÉANTS DU NET ENTRE SOUMISSION ET COLLABORATION ACTIVE

En novembre 2016, le New York Times révélait le développement par Facebook, en toute confidentialité et avec l'appui de son fondateur Mark Zuckerberg, d'un logiciel permettant de censurer des messages du fil d'information des utilisateurs, en fonction de leur localisation géographique. Selon les témoignages d'employés de la compagnie américaine, Facebook souhaite pouvoir répondre aux exigences du régime chinois en matière de censure. Avec cet outil, la compagnie viserait son retour sur le marché chinois dont elle avait été expulsée sept ans plus tôt, durant les révoltes de la minorité ouïghoure au Xinjiang, qui utilisait Facebook pour diffuser des informations sur la répression des émeutes.

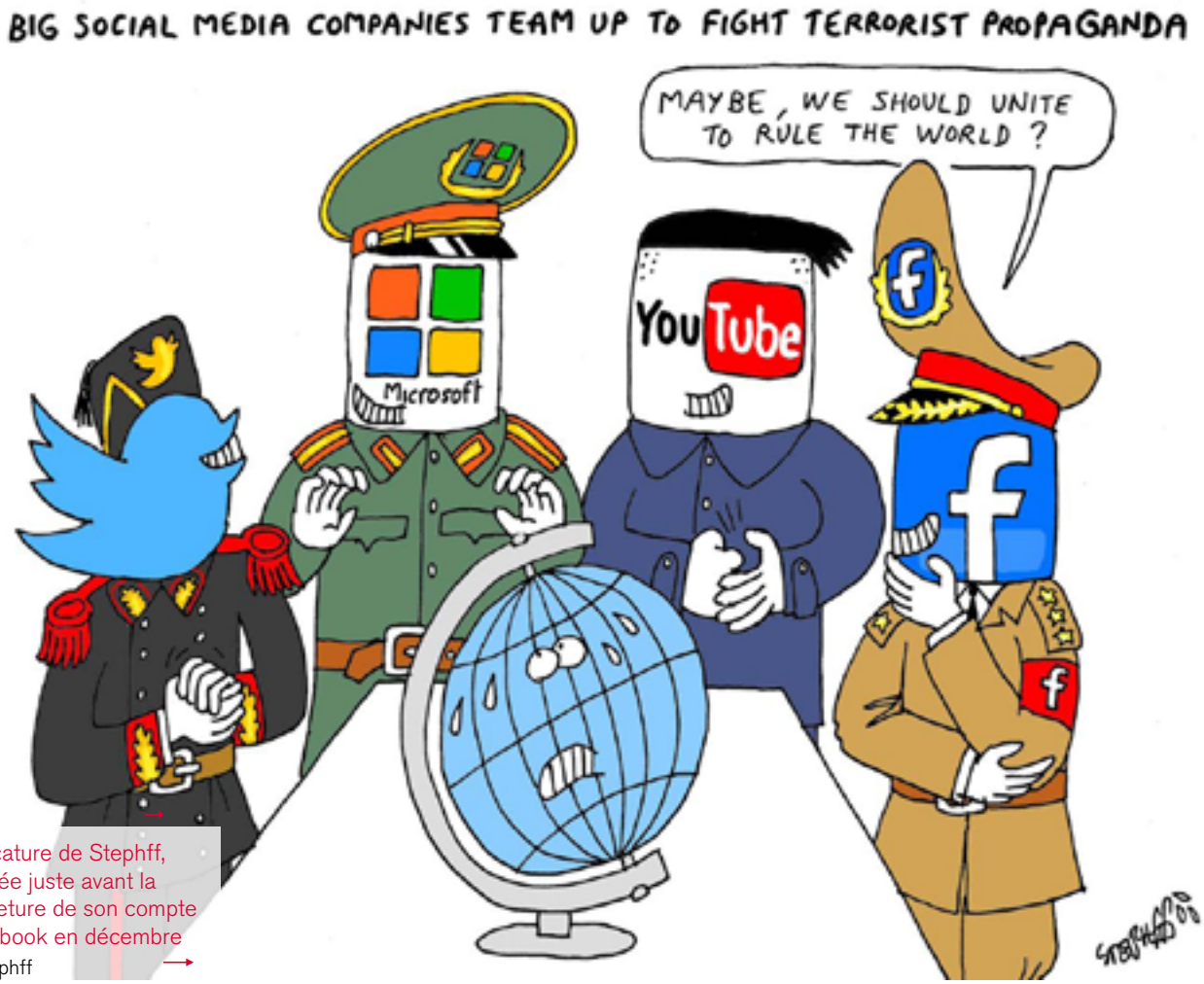
La firme californienne suscite des inquiétudes à cause de sa collaboration active avec certains États, de la suppression de contenus journalistiques et pour sa politique opaque de « modération » des contenus. À titre d'exemple, la fan page du site d'informations ARA News a été bloquée en décembre dernier par Facebook, et ce pendant plusieurs jours et sans aucune explication. Ce média publie généralement des informations sur la Syrie, l'Irak, la Turquie et le Moyen-Orient et dit attirer des milliers de visiteurs par jour sur sa page Facebook.

En Thaïlande, le caricaturiste Stephff, réputé pour ses dessins incisifs, a constaté la suppression de son compte juste après y avoir publié une caricature des réseaux sociaux, dont Facebook. En juin de la même année, le compte de David Thomson, journaliste de RFI spécialiste du djihadisme, a connu le même sort, pour une photo laissant entrevoir le drapeau du groupe État islamique. Le journaliste Kevin Sessums et la photo de la petite fille vietnamienne blessée par le napalm figurent parmi les nombreux cas de censure arbitraire soldés à chaque fois par le rétablissement du contenu ou du compte, la levée de l'interdiction de publier et le même message d'excuses : « *Nous sommes désolés de cette erreur. Le message a été enlevé par erreur et restauré dès que nous avons pu enquêter. Notre équipe traite des millions de rapports chaque semaine, et parfois nous commettons des erreurs* ».

> “ PARFOIS, NOUS COMMETTONS DES ERREURS ”
> FACEBOOK

La photo de la petite fille vietnamienne blessée par le napalm figure parmi les cas de censure arbitraire par Facebook

©www.presse-citron.



Caricature de Stephff, publiée juste avant la fermeture de son compte Facebook en décembre
©Stephff

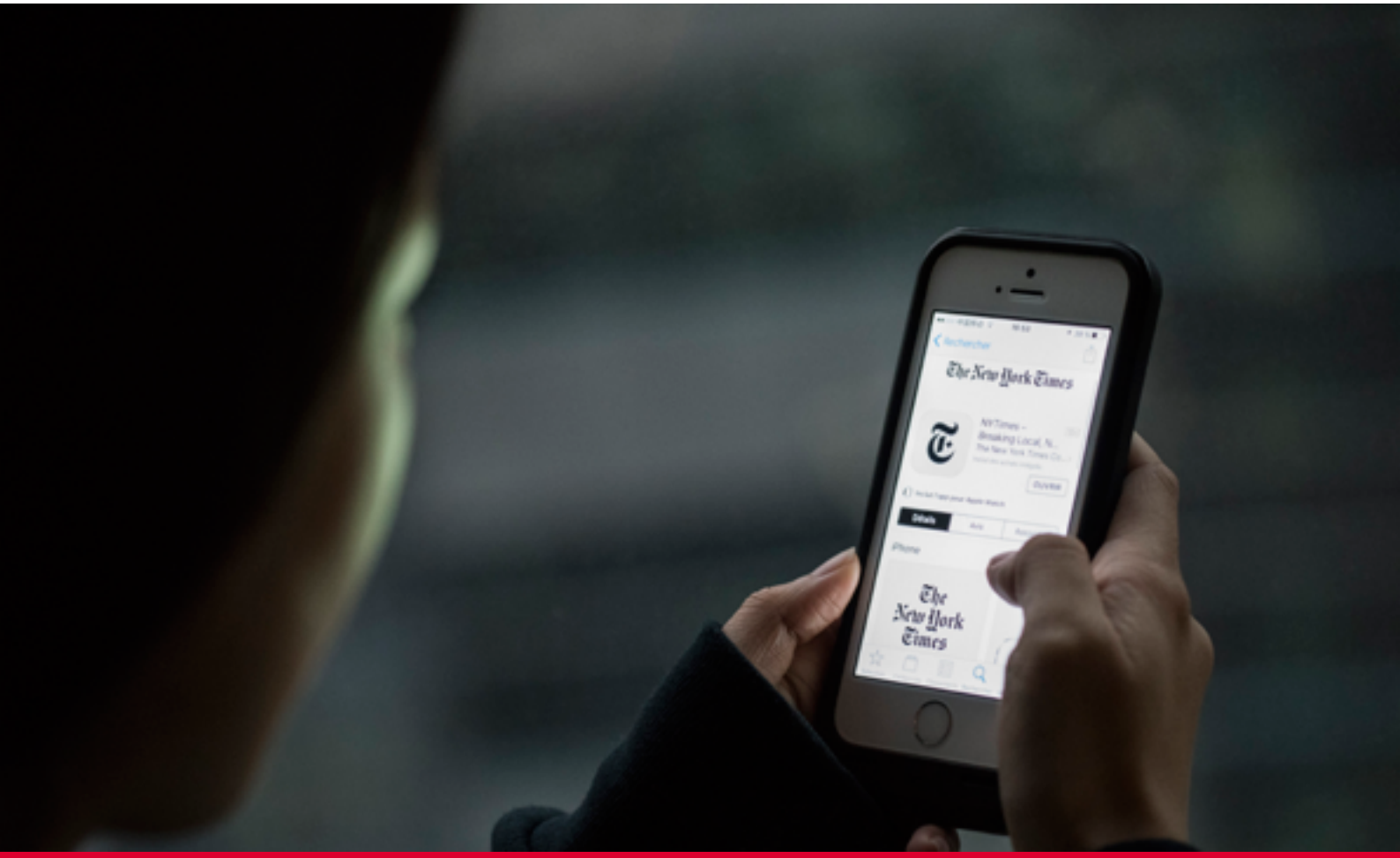
Les autres géants du Net ne sont pas en reste. Twitter a été accusé de censure de journalistes à plusieurs reprises en 2016. C'est aussi en Turquie que Twitter a décidé d'utiliser pour la première fois, en 2014, son outil de gestion locale des contenus interdisant l'accès à un compte ou à un tweet depuis une connexion turque. En Turquie, le réseau social, qui affirme sur son site ne prendre en compte que les requêtes « valides et correctement définies » a tôt fait d'appliquer des ordonnances rendues quelques jours seulement après la tentative de coup d'État du 15 juillet dernier, en censurant pas moins d'une vingtaine de comptes de journalistes et de médias. La majorité des comptes censurés sont ceux des anciens reporters et éditeurs du quotidien Zaman Amerika. La liste comprend également un journaliste kurde, @AmedDicleT, suivi par 186 000 followers, le quotidien kurde Özgür Gündem (@ozgurgundemweb1), et même le compte officiel de l'agence de presse kurde DIHA (@DicleHaberAjans).

Plus récemment, en janvier 2017, la firme Apple a elle aussi fait l'objet d'une controverse quand le New York Times a annoncé que les versions anglaise et chinoise de son application avaient été retirées de l'iTunes store à la demande de l'Administration du cyberespace en Chine (CAC), l'organe officiel de contrôle de l'Internet du Parti communiste chinois. L'autocensure de l'iTunes store avait déjà été constatée peu de temps après l'implantation de sa première boutique en Chine en 2008. Depuis, de nombreuses applications comme celles sur le Dalaï Lama et les sujets tabous dans le pays ont été bloqués par Apple. Fin 2015, un entrepreneur américain a, lui, constaté le blocage de l'application « News » alors qu'il se rendait en Chine continentale depuis Hong Kong.

La politique d'Apple ne concerne pas exclusivement la Chine.
En septembre 2015, la firme a bloqué l'application de Josh Begley, journaliste pour The Intercept, qui recensait toutes les attaques de drones lancées par les États-Unis, ainsi qu'une autre concernant la tuerie survenue à Ferguson, dans l'État du Missouri.

Apple avait retiré de l'iTunes store l'applicaiton du New York Times en Chine ↓

©FRED DUFOUR / AFP



2 LE COMMERCE DOUTEUX MAIS LUCRATIF DE LA SURVEILLANCE

La surveillance du Net et des télécommunications est avant tout l'apanage des « Ennemis d'Internet » - pays les plus répressifs au monde en matière de liberté de l'information sur le Web - au nom de soi-disant « intérêts vitaux de la Nation » . À la tête du peloton, des régimes autoritaires tels que la Chine, l'Iran, la Syrie ou l'Ouzbékistan ont acquis et continuent de se procurer des technologies leur permettant de traquer les moindres faits et gestes des journalistes, des blogueurs et des internautes critiques à leur encontre.

Dans les pays dits démocratiques tels que la France, le Royaume-uni, les États-unis, l'Australie ou encore le Mexique qui recourent à la surveillance au nom d'impératifs sécuritaires, la question de la protection des sources journalistiques est posée.

Une entrée éthique d'entreprises de télécommunications sur le marché iranien est-elle possible ?

L'Iran est l'un des meilleurs exemples de pays répressif en matière de contrôle des internautes. Une cyberpolice garde en permanence un œil sur les activités en ligne des Iraniens. Ces trois dernières années, plus d'une centaine d'internautes, dont de nombreux journalistes et journalistes-citoyens, ont été arbitrairement convoqués et arrêtés et certains d'entre eux lourdement condamnés dans différentes villes du pays.

La majorité de ces journalistes, professionnels ou non, sont victimes de surveillance et de traçage, effectués au moyen de technologies dites de « surveillance licite » (Lawful Interception Management System, LIMS). Même sous le régime des Gardiens de la révolution, les technologies couvertes par cet acronyme sont utilisées de manière illégale. Depuis l'accord historique sur le nucléaire en janvier 2015, un nombre croissant d'entreprises du secteur des télécommunications (Vodafone, Telecom Italia, AT&T et Nokia) envisagent d'investir dans le pays. La société française Orange est entrée en discussion pour se faire une place au capital de MCI, leader iranien de la téléphonie mobile aux mains des Gardiens de la révolution, en restant floue sur ses intentions : « *Comme d'autres opérateurs internationaux, le groupe étudie les opportunités qui se présentent sur le marché iranien* », répond la société. Selon Richard Marry, l'un des responsables de Vivaction, une autre société française aussi en « *phase de redécouverte du marché* », cela fait « *plus de douze mois que nous allons tous les mois à Téhéran afin de rencontrer l'écosystème des télécommunications* ».

« *Avec un taux moyen de pénétration des téléphones portables bien supérieur à 100 % et sachant que près d'un ménage sur deux dispose d'un abonnement à Internet fixe, il est non seulement légitime de s'enquérir de la façon dont les sociétés étrangères souhaitent s'implanter dans le pays, mais il est aussi fondamental que ces compagnies fassent preuve de transparence sur les accords qu'ils ont signés ou s'apprêtent à signer avec le régime,* déclare Reza Moïni, responsable du bureau Iran-Afghanistan de Reporters sans frontières. *Nous ne voulons surtout pas de nouvelles affaires Nokia-Siemens et Ericsson* ».

En effet, en septembre 2011, Reporters sans frontières avait dénoncé la coopération des entreprises occidentales avec le régime iranien et appelé à des sanctions internationales à leur encontre dès lors qu'il avait été avéré que les technologies ou les infrastructures qu'elles mettaient en place dans le pays permettaient au régime de surveiller et réprimer sa population.

HackingTeam et NSO : des entreprises dans l'ombre d'Ennemis d'Internet

En mars 2013, Reporters sans frontières publiait un rapport spécial sur la surveillance mettant pour la première fois en lumière une liste de cinq entreprises « mercenaires de l'ère digitale » - basées au Royaume-Uni, en Allemagne, en Italie, en France et aux États-Unis - dont les produits étaient utilisés par des pays répressifs pour commettre des violations des droits de l'Homme et de la liberté de l'information. Dans cette liste, la société milanaise Hacking Team avait été mise en cause pour la vente de technologies « offensives » de surveillance au Maroc et aux Émirats arabes unis, utilisées par ces régimes pour espionner des sites d'information et des militants des droits de l'Homme.

En juillet 2015, la société a de nouveau fait parler d'elle après le piratage de plusieurs centaines de giga de ses données, incluant notamment de nombreuses informations sur ses clients et les technologies vendues à ces derniers. Parmi eux, le Mexique serait le premier client d'Hacking Team, avec près de six millions d'euros d'achat par le pays. La liste des clients mexicains inclut le ministère de l'Intérieur, la police fédérale, l'armée, la marine, l'agence de renseignement intérieur, le bureau du procureur général, des gouvernements régionaux et même la compagnie pétrolière détenue par l'État, PEMEX.

Face à cette généralisation insidieuse de la surveillance en ligne par les autorités, en mars 2016, l'organisation de défense des droits numériques Red en Defensa de los Derechos Digitales (R3D) est montée au créneau, au nom d'un groupe de journalistes, d'activistes des droits de l'Homme et d'étudiants mexicains. Le 11 mai 2016, la 2e chambre de la Cour suprême du Mexique a refusé de remettre en cause la disposition de la loi fédérale sur les télécommunications (Federal Telecommunications Act), autorisant la rétention massive de données numériques (metadata), sans recours à un juge. Bien que la coalition R3D ait fait appel de cette décision auprès de la Cour interaméricaine des droits de l'Homme, journalistes, blogueurs et cyber-activistes demeurent aujourd'hui vulnérables aux abus du gouvernement, dont les relations commerciales avec Hacking Team illustrent clairement une volonté de surveillance massive d'Internet et des télécommunications.

« Comptez sur nous » : publicité de la société HackingTeam, mise en cause pour la vente de technologies « offensives » de surveillance

©Capture d'écran du site d'HackingTeam.

Interrogés à ce sujet, les intéressés se sont défendus en invoquant la nécessité de lutter contre le terrorisme, et en rappelant qu'ils répondent aux lois des pays dans lesquels ils sont implantés, à l'image d'Hacking Team en Italie. «Ce n'est pas suffisant dans la mesure où leurs technologies continuent d'être utilisés par des régimes autoritaires, ennemis d'internet pour surveiller et emprisonner des journalistes», réagit Christophe Deloire.

« En constatant les relations commerciales entre une multitude d'organismes gouvernementaux mexicains et l'un des principaux exportateurs de technologie de surveillance, on ne peut que s'interroger sur la capacité des journalistes à enquêter de manière indépendante et à protéger leurs sources, déclare Emmanuel Colombié, responsable du bureau Amérique latine de RSF. *L'opacité des autorités sur l'usage prévu de ces technologies acquises accroît cette inquiétude. Des garanties doivent être données pour en bannir l'usage systématique à l'encontre de tous les acteurs de l'information, professionnels des médias, blogueurs et défenseurs des droits. »*

LE MALWARE PEUT RÉCUPÉRER LES CONTACTS, DÉTAILS ET CONTENUS DES APPELS, DES SMS, DES MAILS, DES CONVERSATIONS WHATSAPP, SKYPE ET MÊME TELEGRAM, POURTANT RÉPUTÉE SÉCURISÉE.

Les récentes révélations impliquant la société israélienne NSO et le journaliste d'investigation mexicain Rafael Cabrera pourraient bien mettre en lumière un abus de surveillance par les autorités mexicaines. En août 2016, Citizen Lab et Lookout ont révélé l'existence d'un logiciel espion permettant de prendre le contrôle intégral des iPhones en exploitant plusieurs failles de sécurité (depuis corrigées). « Pegasus », qui serait le nom du malware, s'installerait sur le téléphone de la cible après que celle-ci a cliqué sur un lien hypertexte envoyé par sms. Le malware peut ainsi récupérer les contacts, détails et contenus des appels, des SMS, des mails, des conversations WhatsApp, Skype et même Telegram, pourtant réputée sécurisée. Ils peuvent également actionner à distance l'appareil photo de l'iPhone, son micro et savoir à tout moment où se trouve son utilisateur.

En réponse, NSO a déclaré : «*NSO contribue à rendre le monde plus sûr en fournissant aux organismes gouvernementaux autorisés des technologies qui les aident à combattre la terreur et la criminalité. Les clients peuvent utiliser nos produits exclusivement pour l'investigation et la prévention du crime et de la terreur. L'utilisation éthique et légale de ses produits par ses clients est d'une importance capitale pour l'entreprise. En cas de violation présumée du contrat, la société prendra les mesures appropriées avec le client en question*», des affirmations que RSF n'a pas été en mesure de vérifier.

Le journaliste **Rafael Cabrera**, qui travaille notamment pour le site d'information aristeguinoticias.com, a été la cible de « Pegasus » en août 2016 après avoir participé à l'enquête ayant mis à jour un scandale de corruption impliquant la famille du président mexicain Peña Nieto. D'après le New York Times, le gouvernement mexicain aurait payé 15 millions de dollars à NSO pour lancer trois projets indéfinis.

Le journaliste Rafael Cabrera et l'équipe de « Aristegui Noticias », cible du logiciel espion « Pegasus ». →

Le journaliste avait reçu plusieurs messages suspects l'invitant à se rendre dans les bureaux de la chaîne UNO TV, et « l'informant » que la présidence réfléchissait à porter plainte pour diffamation et à emprisonner les journalistes impliqués dans l'enquête sur la « Maison Blanche » mexicaine. NSO s'était défendu en affirmant que les logiciels que l'entreprise vendait étaient uniquement utilisés pour de la surveillance légale. Pourtant, au moment de ces révélations, Citizen Lab exposait une tentative de surveillance similaire sur le blogueur émirati, administrateur du forum de débat démocratique Al-Hewa, **Ahmed Mansoor**. Les 10 et 11 août 2016, le blogueur a reçu deux fois le même SMS sur son iPhone 6 l'incitant à cliquer sur un lien pour en apprendre plus sur les exactions du régime des Émirats. Analysé par le Citizen Lab, ce SMS a permis de remonter la trace de NSO et de son logiciel « Pegasus ».

3 DES RÉGULATIONS INTERNATIONALES EN PANNE OU BLOQUÉES PAR LES LOBBIES

La résolution sur « *la promotion, la protection et l'exercice des droits de l'Homme sur Internet* » adoptée par le Conseil des droits de l'Homme de l'ONU à l'occasion de sa 32e session, du 13 juin au 1er juillet 2016, affirme une nouvelle fois que « *les mêmes droits dont les personnes disposent hors ligne doivent être aussi protégés en ligne, en particulier la liberté d'expression, qui est applicable indépendamment des frontières et quel que soit le média que l'on choisisse, conformément aux articles 19 de la Déclaration universelle des droits de l'Homme et du Pacte international relatif aux droits civils et politiques* ». La résolution appelle « *tous les États à aborder les préoccupations de sécurité sur Internet conformément à leurs obligations internationales relatives aux droits de l'Homme afin de garantir la protection de la liberté d'expression, de la liberté d'association, du droit à la vie privée et d'autres droits de l'Homme en ligne, au moyen notamment d'institutions nationales démocratiques et transparentes, fondées sur les principes du droit, d'une manière qui garantisse la liberté et la sécurité sur Internet* ».

DES TEXTES NON CONTRAIGNANTS ET INEFFICACES LORSQU'IL S'AGIT D'EMPÊCHER LES ÉTATS LES PLUS RÉPRESSIFS EN MATIÈRE DE LIBERTÉS INDIVIDUELLES EN LIGNE.

Une autre résolution du Conseil, adoptée en septembre 2016, souligne « *qu'à l'ère numérique, les journalistes doivent pouvoir disposer d'outils de chiffrement et de protection de l'anonymat pour être à même de pratiquer librement leur profession et d'exercer leurs droits de l'Homme, en particulier leurs droits à la liberté d'expression et leur droit à la vie privée, notamment de sécuriser leurs communications et de protéger la confidentialité de leurs sources, et demande aux États de ne pas commettre d'ingérence dans l'utilisation de telles technologies en imposant des restrictions, et de s'acquitter ainsi de leurs obligations au regard du droit international des droits de l'Homme* ». Les résolutions du Conseil des droits de l'Homme n'en demeurent pas moins des textes non contraignants et inefficaces lorsqu'il s'agit d'empêcher les États les plus répressifs en matière de libertés individuelles en ligne.

Depuis les révélations d'Edward Snowden et la fin de l'hégémonie américaine dans la gouvernance d'Internet, les Ennemis d'Internet font pression afin d'obtenir un rôle croissant dans la régulation des réseaux, notamment via les agences onusiennes telles que l'Union internationale des Télécommunications (UIT), l'Unesco, et la Conférence des Nations unies sur le Commerce et Développement (CNUCED), qui ont toutes consacré plusieurs déclarations à la défense des libertés fondamentales en ligne et la gouvernance d'Internet. Après la Déclaration de principes résultant du sommet de Genève en 2003, le Sommet mondial sur la société de l'information (SMSI) constitue l'une des principales plateformes multilatérales de la gouvernance d'Internet, au sein de laquelle aucun texte contraignant ne voit le jour afin d'empêcher les régimes autoritaires de censurer et de surveiller massivement leurs populations.

« La lutte autour de la question stratégique de la gouvernance du Web menace de plus en plus d'aboutir à l'officialisation d'un Internet fragmenté et censuré, déclare Benjamin Ismaïl, responsable du bureau Asie de RSF. *Si chaque pays se met à réclamer sa souveraineté sur Internet, nous aurons alors affaire à un système dans lequel les régimes autoritaires auront toute légitimité pour restreindre la liberté d'expression et le droit d'informer en ligne. Pour éviter cela, il est vital que des mécanismes internationaux contraignants soient mis en place afin de garantir l'existence d'un Internet libre et mondial. Cette garantie passe aujourd'hui plus que jamais par un contrôle strict des entreprises du Net et des sociétés exportatrices de technologies de surveillance de masse ».*

Le lanceur d'alerte de la NSA, Edward Snowden
©FREDERICK FLORIN / AFP

Depuis 2014, RSF demande au Conseil des droits de l'Homme la création d'une convention internationale relative à la responsabilité des entreprises en matière de droits de l'Homme afin d'imposer aux États l'application d'un contrôle strict de l'exportation des technologies de surveillance et la mise en place de recours pour les individus victimes de surveillance et des conséquences qui peuvent en résulter (arrestations, emprisonnement, violences physiques, tortures).

Quelques mois plus tard, le 28 novembre 2014, RSF, Privacy International, Digitale Gesellshaft, la FIDH et Human Rights Watch, saluaient le « *premier pas de l'Europe en faveur d'un contrôle accru des technologies de surveillance* », par l'ajout de technologies de surveillance du Net à la liste des technologies à usage double (dual use technology) . Le 2 décembre 2014, les membres de la coalition Cause (Coalition Against Unlawful Surveillance Exports), RSF, Amnesty International, Digitale Gesellschaft, FIDH, Human Rights Watch, Open Technology Institute et Privacy International adressaient une lettre ouverte aux États participant à l'Assemblée plénière de l'Arrangement de Wassenaar sur la réglementation des exportations d'armes classiques et de biens et technologies à double usage - un traité regroupant 41 pays dont une majorité de l'Union européenne - pour leur demander de prendre des mesures contre la prolifération alarmante des technologies de surveillance accessibles aux pays répressifs connus pour perpétrer des violations systématiques des droits de l'Homme.

PRÈS DE TROIS ANS APRÈS CES APPELS EN FAVEUR D'UN CONTRÔLE EFFICACE DES ENTREPRISES PRIVÉES, L'UNION EUROPÉENNE SEMBLE AVOIR FAIT MACHINE ARRIÈRE.

Sous la pression du lobby de l'industrie des technologies numériques, la régulation des exportations des technologies de surveillance est aujourd'hui au point mort. Le lobby, notamment représenté par l'association DigitalEurope dont l'instance dirigeante inclut des cadres de sociétés telles que Nokia, Siemens, Ametic, IBM, Anitec, Cisco et Microsoft, avec l'appui d'un groupe de diplomates de neuf pays (l'Autriche, la Finlande, la France, l'Allemagne, la Pologne, la Slovénie, l'Espagne, la Suède et de Royaume-Uni) a obtenu que des modifications soient apportées à la proposition de « *régulation du Parlement européen et du Conseil* », afin d'amputer la liste initiale des technologies devant être placées sous contrôle, telles que certains matériels d'interception des télécommunications, les logiciels d'intrusion, les centres de surveillance et les systèmes de conservation des données.

Câbles attachés à un système de cybersécurité →
©PHILIPPE HUGUEN / AFP

La dernière proposition ne contient notamment plus les contrôles initialement prévus sur les équipements biométriques, les systèmes de géolocalisation ou les technologies dites de « deep packet inspection » (inspection des paquets en profondeur) permettant d'intercepter et d'inspecter les paquets de données transitant sur le réseau Internet. Dans un contexte de surveillance, l'utilisation du DPI peut permettre d'accéder au contenu d'emails, de conversations instantanées et d'échanges par VoIP et de découvrir si une communication est chiffrée ou non. La proposition ne mentionne pas d'obligation pour les États européens d'informer le public sur les entreprises qu'ils autorisent à exporter.

Au sein des Nations unies comme de l'Union européenne et dans la plupart des législations nationales, le cadre juridique relatif à la surveillance d'Internet, à la protection des données et à l'exportation de matériel de surveillance informatique reste à ce jour incomplet et insuffisant au regard des normes et standards internationaux de protection des droits de l'Homme. Dès lors, l'adoption d'un cadre juridique protecteur des libertés sur Internet reste primordiale, tant pour la question générale de la surveillance d'Internet que pour le problème particulier des entreprises exportatrices de matériel de surveillance.

4 LES RECOMMANDATIONS DE RSF POUR LUTTER CONTRE LA CYBERCENSURE

Pour lutter contre la cybercensure, Reporters sans frontières (RSF) demande :

Aux entreprises :

- De systématiser et d'améliorer les rapports de transparence et de publier les requêtes judiciaires des gouvernements qui demandent de retirer des contenus ou des comptes d'utilisateurs ;
- De respecter la Déclaration universelle des droits de l'Homme et les conventions des Nations unies relatives aux droits de l'Homme ;
- De respecter les Principes directeurs relatifs aux entreprises et aux droits de l'Homme des Nations unies et formuler des engagements précis quant à leur mise en œuvre ;
- D'adopter des chartes éthiques et des mécanismes efficaces de « traçabilité » des technologies qu'elles exportent ;
- De s'interdire l'export vers des pays non démocratiques et répressifs de technologies de surveillance, et d'exercer un devoir de vigilance de manière à identifier les risques et à prévenir les atteintes graves envers les droits humains, les libertés fondamentales, et la sécurité des personnes ;
- D'appliquer les principes de « contrats responsables » élaborés par le Représentant spécial du Secrétaire général chargé de la question des droits de l'Homme et des sociétés transnationales et autres entreprises John Ruggie, rendant ces dernières en partie responsables des violations des droits de l'Homme que pourraient entraîner leurs technologies.

Aux États :

- D'inclure l'accès libre à Internet et la garantie des libertés numériques dans les droits fondamentaux ;
- D'adopter des lois garantissant les libertés numériques, notamment la protection de la vie privée et des données personnelles face aux intrusions des forces de l'ordre ou des services de renseignement, et de mettre en place des mécanismes de recours appropriés ;
- De s'assurer que les mesures de surveillance des communications respectent strictement les principes de légalité, de nécessité et de proportionnalité conformément à l'article 19 du Pacte international relatifs aux droits civils et politiques ;
- De favoriser une plus grande transparence quant aux demandes de surveillance qu'ils adressent aux entreprises, leur nombre, leurs bases légales et leurs objectifs ;
- D'aligner leurs politiques sur celles des États contrôlant le mieux l'export de technologies et sanctionnant les entreprises ayant collaboré avec les régimes autoritaires.

À l'Union européenne :

- D'inclure l'accès libre à l'Internet de garantir les libertés numériques dans la Charte des droits fondamentaux de l'UE ;
- De considérer, dans les relations entre membres de l'UE et avec les États tiers ainsi que dans les instances internationales, notamment l'OMC, les mécanismes de surveillance d'Internet comme des mécanismes protectionnistes et des barrières aux échanges, et de les combattre comme tels ;
- D'assurer l'harmonisation et l'uniformisation des procédures et sanctions visant la surveillance et le contrôle des technologies de surveillance.

Aux Nations unies :

- De renforcer le mandat du groupe de travail des Nations unies « Droits de l'Homme et sociétés transnationales », notamment en l'habilitant à recevoir des plaintes individuelles et à enquêter sur des cas individuels de violations des droits de l'Homme liées aux entreprises ;
- De réfléchir à l'élaboration d'une convention internationale relative à l'exportation de technologies de surveillance d'Internet permettant notamment de contrôler et prohiber la fourniture de ces technologies dès lors qu'il existe un risque substantiel que ces matériels servent à commettre ou faciliter des violations des droits de l'Homme.

5 JOURNALISTES, PROTÉGEZ VOS DONNÉES ET VOS COMMUNICATIONS

Afin de lutter efficacement contre la surveillance et la censure, les journalistes, qu'ils soient professionnels ou non, peuvent recourir aux logiciels développés par des organisations de la société civile et mettre en œuvre des mesures concrètes grâce aux guides de cybersécurité disponibles en ligne. RSF a de son côté mis à jour en 2015 son Guide pratique de sécurité en y intégrant de nombreux conseils pratiques en matière de cybersécurité.

Les consignes résumées ci-dessous, valables tant pour votre ordinateur que pour votre smartphone, ne prétendent pas à l'exhaustivité. Reporters sans frontières organise régulièrement des sessions de formation à la cybersécurité et propose des tutoriels gratuits.

Attention : faites toujours des recherches sur les outils que vous vous apprêtez à utiliser et les techniques que vous allez mettre enœuvre. Les technologies évoluent rapidement et les conseils prodigués aujourd'hui sont susceptibles de ne plus l'être demain !

Des journalistes suivent le congrès national du parti communiste chinois.
©AFP PHOTO / Greg BAKER

Comportement général en ligne

Avant même de penser à sécuriser son ordinateur ou à installer des logiciels permettant de chiffrer ses communications ou ses données, il convient d'adopter une bonne hygiène numérique en respectant quelques conseils de bon sens qui vous éviteront de voir votre compte mail ou votre ordinateur piratés.

Évitez les regards indiscrets.

- Évitez de travailler dos à une fenêtre.
- En voyage, dans le train ou en avion, appliquez un filtre de confidentialité sur votre écran. Le filtre de confidentialité est une feuille transparente qui, une fois appliquée sur votre écran, restreint la vision latérale. Ainsi seule la personne située en face (vous) est capable de voir l'écran.
- Lors de vos déplacements, dans la mesure du possible, évitez de vous séparer de votre matériel. Cela permet d'éviter qu'un individu malveillant ne puisse récupérer des fichiers de votre ordinateur ou ne puisse y introduire un cheval de Troie.
- Tous les systèmes d'exploitation (Windows, MacOs et Linux) permettent de protéger votre session avec un mot de passe. Vous devez utiliser cette fonctionnalité.
- Ne téléchargez pas de fichiers ou ne cliquez pas sur des liens qui vous sont envoyés par des expéditeurs inconnus.
- Vérifiez soigneusement l'adresse mail ou le compte Twitter de ceux qui partagent un lien avec vous. En cas de doute, vérifiez l'identité de l'expéditeur auprès d'autres contacts ou par l'intermédiaire d'un moteur de recherche.
- Si un fichier et l'expéditeur vous semblent suspects, contactez des experts qui pourront vous aider. Citizen Lab est un organisme qui analyse les virus envoyés par des dissidents ou activistes et les aide à mieux se protéger.

Outre ces mesures, installez les logiciels suivants et activez les fonctions de protection intégrées à votre appareil :

- Utilisez un antivirus ET un anti-malware (tel que Malwarebytes)
- Activez votre firewall (pare-feu)
- Maintenez votre système d'exploitation (Windows, Mac OSX..etc) à jour

Traces numériques :

Si vous travaillez dans un cybercafé ou sur un ordinateur qui n'est pas le vôtre, veillez à ne pas laisser de traces une fois votre travail terminé :

- Si vous avez consulté votre boîte mail, votre compte Facebook ou votre compte Twitter, pensez à vous déconnecter.
- Effacez votre historique de navigation. Celui-ci comporte de nombreuses informations qui peuvent également permettre à un individu expert d'accéder à certains de vos comptes en ligne.
- Sur un ordinateur public, ne stockez jamais votre mot de passe dans le navigateur. Si par mégarde vous l'avez fait, pensez à les effacer de la mémoire du navigateur une fois votre travail terminé.
- Effacez les champs de formulaire.
- Supprimez les cookies.

Le nettoyage de ces données se fait différemment selon les navigateurs. Un bon moyen d'éviter les impairs est d'utiliser le mode « navigation privée » de Firefox ou de Chrome.

Messageries et accès aux services en ligne :

La plupart des services en ligne (Twitter, Facebook, WordPress, Tumblr, Skype etc.) permettent de récupérer un mot de passe perdu grâce à l'envoi d'un mot de passe dans votre boîte mail. Il est donc capital de protéger votre boîte mail le mieux possible. Si celle-ci est compromise, très souvent, c'est toute votre identité numérique qui le sera également.

Le service mail de Google, Gmail, permet de mettre en œuvre une sécurité supplémentaire : la « validation en deux étapes ». Ce service permet de protéger votre compte mail avec :

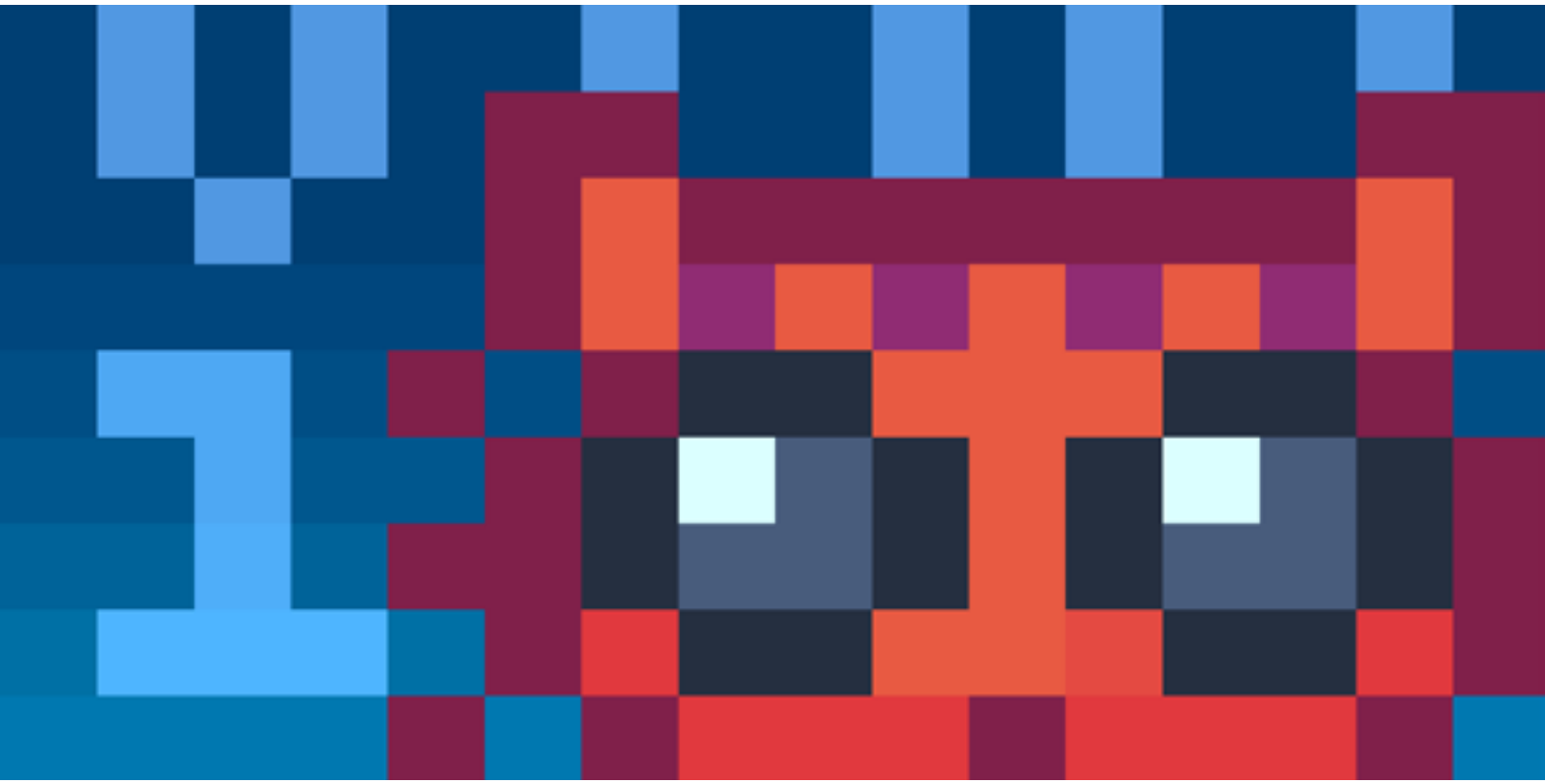
1. un nom d'utilisateur
2. un mot de passe
3. un code que vous recevrez sur votre téléphone portable chaque fois que vous vous connecterez sur votre boîte de réception.

Ainsi, sans votre téléphone portable, il est impossible d'accéder à vos mails.

Lorsque vous vous connectez sur votre boîte Gmail, pensez à cliquer sur le lien « détails », en bas de la page. Celui-ci ouvre une fenêtre affichant l'ensemble des connexions récentes à votre boîte. Vous serez ainsi à même de déceler une activité suspecte.

Vous devriez également chiffrer vos emails. Il existe aussi des outils de chiffrement très simples à utiliser, vous pouvez encourager vos sources à les utiliser pour converser avec elles de manière chiffrée :

- Cryptocat qui s'installe simplement sur un ordinateur, chiffre les conversations instantanées de bout en bout.
- Privnote et ZeroBin sont des sites permettant de créer des url vers des messages chiffrés pouvant s'autodétruire après lecture.
- Vous voulez pouvoir téléphoner, via Internet, à vos sources ? Pas de problème : mais utilisez Jitsi Meet, le «Skype du libre»



Logo de l'extension Cryptocat qui chiffre puis détruit les conversations instantanées sur ordinateur ↑
©Cryptocat

Phrases de passe :

La longueur d'un mot de passe est le facteur principal de sa solidité. D'où le fait qu'on ne parle plus de « mots de passe », qui sont à proscrire, mais de « phrases de passe », seule méthode capable de résister à une « attaque par force brute ». Chaque fois que vous créez une phrase de passe :

- Créez une phrase dans laquelle vous incluez des chiffres, des minuscules et des majuscules afin d'obtenir une chaîne de caractères relativement complexe mais en même temps plus facile à mémoriser qu'un mot de passe court mais abstrait (chiffres + caractères spéciaux).
- Utilisez une phrase de passe différente par service en ligne.
- Utilisez un gestionnaire de phrases de passe. Par exemple, LastPass est un gestionnaire de mots de passe disponible sous forme d'extension pour Firefox, Chrome et Safari. Il permet d'enregistrer l'ensemble de vos phrases de passe.

Empreinte sur les réseaux sociaux :

Facebook et Twitter sont des outils très efficaces pour communiquer. Toutefois, vous devez veiller à contrôler les informations que vous donnez à voir au public. Ces tutoriels et services en ligne vous aideront à mieux contrôler votre présence en ligne :

- Vérifiez votre présence sur Internet avec Namecheckr.
- Sécurisez votre compte Twitter.
- Gérez vos informations privées sur Facebook quand on partage un contenu.

Sécurisez votre navigation :

Ajoutez les fonctionnalités suivantes à Firefox et Chrome, via l'utilisation de plugins :

- https everywhere : afin de vérifier pour chaque site si une version https (chiffrée) existe, et d'éviter notamment certains hameçonnages.
- No script : afin de contrôler les scripts javascript lancés sur les sites web visités.
- Privacy Badger : pour bloquer les trackers utilisés par les sites.
- Certificate Patrol : pour vérifier les certificats présentés par les sites en « https ».
- Installez un VPN afin de chiffrer vos connexions sur Internet.
- Installez le navigateur Tor Browser qui permet de naviguer de manière anonyme.

Téléphonie mobile :

- **Créez et utilisez un système codé** pour communiquer avec vos sources et autres contacts. « Bippez » vos contacts pour communiquer (laissez sonner une fois ou deux le téléphone de votre correspondant et raccrochez aussitôt afin de lui indiquer que vous êtes bien arrivé à un endroit donné, ou que tout va bien par exemple).

- **N'utilisez pas les vrais noms de vos contacts** dans vos répertoires téléphoniques. Attribuez-leur des numéros ou des pseudonymes. De cette manière, si jamais les forces de sécurité saisissent votre téléphone ou votre carte SIM, elles ne disposeront pas de l'ensemble de votre réseau.

- **Amenez des cartes SIM de rechange** lors des manifestations si vous pensez qu'elles risquent d'être confisquées. Il est très important que vous ayez sur vous un téléphone portable qui fonctionne. Si jamais vous devez vous débarrasser de votre carte SIM, essayrez de la détruire physiquement.

- Si votre téléphone vous le permet, **verrouillez votre téléphone avec un mot de passe.** Toute carte SIM dispose d'un code PIN par défaut. Changez-le et verrouillez votre carte SIM avec ce code SIM. Un mot de passe (votre code PIN) vous sera demandé à chaque fois que vous utiliserez votre téléphone.

- Si vous pensez qu'une manifestation va se terminer par une forte répression des forces de sécurité, **activez le mode avion de votre téléphone.** Vous ne serez plus en mesure d'émettre ou de recevoir des appels mais vous pourrez toujours prendre des photos ou des vidéos et les uploader sur des sites internet plus tard. Cette tactique est également utile si vous pensez que les forces de sécurité vont cibler en priorité les personnes disposant d'un téléphone portable lors de la manifestation. Plus tard, le gouvernement pourra demander les enregistrements d'appels, de SMS ou de données téléphoniques de tout individu qui se trouvait à un endroit donné à un moment donné afin de procéder à des arrestations en masse.

- **Désactivez les fonctions de géolocalisation** de vos applications à moins que vous n'utilisiez cette fonction à des fins militantes en taggant certains médias lors d'un événement. Si vous utilisez votre téléphone portable pour diffuser de la vidéo en streaming live, désactivez les fonctions de GPS et de géolocalisation.

- Si votre téléphone fonctionne avec le système d'exploitation Android, vous pouvez utiliser de nombreux outils pour **chiffrer votre navigation internet, vos chats, SMS et messages vocaux** via les outils créés par le Guardian Project et WhisperSys. Lorsque vous utilisez votre portable pour accéder au Web, utilisez le https lorsque cela est possible.

Lutter contre la censure :

Certains outils présentés ci-dessus permettent de contourner la censure imposée par les autorités (anonymisation de la connexion, VPN, etc.). Pour aller plus loin :

- Consultez le site Collateral Freedom de Reporters sans frontières : pour contourner la censure technologique mise en place par des États irrespectueux des droits de l'Homme, RSF a utilisé un dispositif original fondé sur la technique du mirroring, consistant à dupliquer les sites censurés et à en héberger les copies sur des serveurs de géants du Web, tels Amazon, Microsoft ou Google.

- Visitez le site Circumvention Central, lancé par GreatFire (organisation à l'origine de l'initiative Collateral Freedom) pour en apprendre davantage sur les VPN.

- Consultez le site Security in-a-box de Tactical Tech et les articles d'Electronic Frontier Foundation pour mieux contourner la censure en ligne et rester anonyme.

Lancé en 2011, le site « Collateral Freedom » permet de rendre accessibles des sites ayant été censurés →

©RSF

REPORTERS SANS FRONTIÈRES assure la promotion et la défense de la liberté d'informer et d'être informé partout dans le monde. L'organisation, basée à Paris, compte dix bureaux à l'international (Berlin, Bruxelles, Genève, Madrid, New York, Stockholm, Tunis, Turin, Vienne, Washington DC, Rio) et plus de 150 correspondants répartis sur les cinq continents.

Secrétaire général : CHRISTOPHE DELOIRE
Rédactrice en chef : VIRGINIE DANGLES

Secrétariat international
CS 90247
75083 Paris Cedex 02
Tel. +33 1 44 83 84 84
Web : www.rsf.org

REPORTERS
SANS FRONTIERES
POUR LA LIBERTE DE L'INFORMATION