

## Sommaire :

[Documenter un Sujet pendant une Coupure Internet : Introduction](#)

[Configurer un Téléphone pour se Documenter Hors-ligne](#)

[Devrais-je Utiliser cette Appli de Documentation ?](#)

[Maintenir la Fiabilité des Informations pendant une Coupure Internet](#)

[Sauvegarder ses Données sans Internet ni Ordinateur](#)

[Partager des Fichiers et Communiquer lors d'une Coupure Internet](#)

## Documenter un Sujet pendant une Coupure Internet : Introduction

*En juin 2019, alors que les violations des droits de l'Homme et la crise humanitaire se poursuivaient au Myanmar, le ministère des Transports et des Communications du pays [a ordonné aux entreprises de télécommunications](#) de fermer leur service Internet mobile dans certaines parties de l'État de Rakhine et de l'État Chin voisin. Dénonçant des «troubles de la paix» et des «activités illégales», le gouvernement du Myanmar affirme avoir décrété la fermeture «[dans l'intérêt du peuple](#)». En réalité, la panne a privé [plus d'un million de personnes](#) d'un accès essentiel à l'information et à la communication et a perturbé les efforts humanitaires. Comme [l'a déclaré](#) Matthew Smith de [Fortify Rights](#), "Cette fermeture se produit dans un contexte de génocide en cours contre les Rohingyas et de crimes de guerre contre l'ethnie Rakhine, et même si elle visait à cibler des militants, elle est extrêmement disproportionnée".*

*La fermeture a été [partiellement levée sur cinq des cantons](#) en septembre 2019, mais se poursuit. Le même mois, au Bangladesh voisin où de nombreux Rohingyas ont fui, les autorités ont ordonné aux opérateurs de téléphonie mobile de [bloquer les services 3G et 4G](#) dans les camps de réfugiés Rohingyas et de cesser de vendre des cartes SIM aux Rohingyas. En ce début d'année 2020, [quatre cantons de Rakhine](#) sont toujours coupés du monde et le Bangladesh [continue de limiter les services mobiles](#) dans les camps de réfugiés.*

## Documenter un Sujet pendant une Coupure Internet

À l'échelle mondiale, les coupures d'Internet sont de plus en plus répandues. Selon la [campagne #KeepItOn](#) d'AccessNow, il y a eu 128 coupures intentionnelles entre janvier et juillet 2019, contre 196 dans toute l'année 2018, en forte augmentation par rapport aux chiffres de 106 en 2017 et 75 en 2016. De plus en plus, et partout dans le monde, des gouvernements, avec la coopération des entreprises de télécommunication, recourent aux coupures Internet comme stratégie pour réprimer des communautés, empêcher la mobilisation et éviter que les violations des droits humains commises soient documentées et diffusées.

## Les coupures internet vont de pair avec les violations des droits de l'Homme.

Berhan Taye, AccessNow

Il existe plusieurs stratégies de coupure, parmi lesquelles des [blocages spécifiques qui ciblent des applications et des sites populaires](#), [des arrêts de données mobiles](#), [une limitation de la bande passante](#) ou des [coupures totales d'Internet](#). Tous ces types de coupures sont destinés à perturber la capacité à diffuser des informations et à exposer les violations de droits en temps réel. Ils se produisent en général en période de manifestations, d'élections et d'instabilité politique en général, et s'accompagnent souvent d'une répression étatique accrue, d'offensives militaires et de violence. Bien que les gouvernements justifient ces coupures [au nom de la « sécurité publique » ou autres](#), celles-ci prennent clairement effet lorsque des États répressifs craignent de perdre le contrôle ténu qu'ils exercent sur leur population, l'information et le discours politique émanant du pays. Les coupures constituent des violations aux droits de l'Homme, perturbent gravement [la vie et les moyens de subsistance des populations](#), et ont également un [impact économique mondial](#).

**Documenter les violations des droits de l'Homme lors d'une coupure d'Internet est primordial.** Bien que l'information ne puisse être partagée sur le moment, sa documentation est un moyen d'archiver les voix que les autorités tentent de faire taire et de sauvegarder des preuves d'abus de droits qui pourront être utilisées pour demander justice ultérieurement. Bien sûr, le contexte répressif et les obstacles technologiques engendrés par une coupure Internet rendent la documentation des violations - et la conservation de ces documents en toute sécurité - beaucoup plus difficile et risquée. **Comment les militants peuvent-ils enregistrer et archiver leurs vidéos pendant une coupure, voire les partager hors ligne, de manière la plus sûre possible ?**

### Dans cette Série

Grâce à notre travail avec des militants qui ont connu des coupures d'Internet, nous avons compilé quelques conseils et approches utiles pour **capturer et sauvegarder des documents vidéo pendant une coupure Internet**, que nous déclinons dans cette série. Nous les avons rapportés pour les appareils opérés par Android, mais les conseils peuvent également être appliqués aux iPhones. Certaines de ces stratégies requièrent une planification préalable (et souvent un accès Internet), il est donc conseillé d'en prendre connaissance afin de mettre en œuvre toutes les étapes à exécuter avant de vous retrouver dans une situation où vous devrez documenter un sujet sans accès Internet. Enregistrez une copie des tutoriels pertinents afin de pouvoir vous y référer ou les partager pendant une coupure. Et enfin, commencez à vous entraîner au quotidien sur les techniques et les méthodes décrites afin qu'elles soient devenues une seconde nature lorsque vous vous trouverez en situation de crise.

- Préparer
  - [Configurer un téléphone pour se documenter hors-ligne](#)
- Capturer

- [Devrais-je utiliser cette appli de documentation ?](#)
- Sauvegarder
  - [Maintenir la Fiabilité des Informations pendant une Coupure Internet](#)
  - [Sauvegarder ses Données sans Internet et sans Ordinateur](#)
- Partager et Diffuser
  - [Partager des Fichiers et Communiquer lors d'une Coupure Internet](#)

Une dernière remarque : bien que ces conseils puissent vous aider à documenter de l'information lors d'une coupure, nous tenons à souligner que la solution ultime reste le rétablissement de l'accès à Internet et la défense [du droit des personnes à enregistrer](#), s'informer et se regrouper ainsi que la défense de la liberté d'expression. Heureusement, un mouvement mondial dirigé par des organisations telles que [NetBlocks](#), [AccessNow](#) et bien d'autres exerce une veille et communique activement des informations sur les coupures. Les défenseurs des droits humains à l'échelle globale engagent [des procès stratégiques contre les coupures Internet](#). Nous sommes solidaires de leur travail de défense des droits de l'Homme.

\*\*\*\*\*

## Configurer un Téléphone pour se Documenter Hors-ligne

*Cet article est extrait d'une série intitulée [Se Documenter lors d'une Coupure Internet](#)*

Dernière révision : 31 Janvier 2020

Malgré une coupure Internet, il existe toujours des possibilités de capturer des preuves vidéo importantes qui pourront être partagées hors ligne ou diffusées une fois la connexion rétablie.

Voici quelques conseils que nous avons collectés auprès d'activistes et autres militants pour configurer un téléphone afin de se documenter hors ligne. Notez que certaines étapes **nécessitent un accès à Internet**, elles doivent donc être effectuées avant qu'une coupure ne se produise ou pendant les périodes de restauration du réseau. De plus, n'attendez pas d'être dans une situation d'adversité pour mettre en œuvre ces étapes ; exécutez-les dès maintenant et prenez le temps de **vous entraîner à utiliser le téléphone** avant de devoir l'utiliser dans un contexte de crise.

Les coupures s'accompagnent souvent d'un contrôle accru de l'information et des restrictions à la liberté d'expression et d'association. Si vous êtes reporté, prenez des précautions supplémentaires pour vous protéger et protéger vos informations pendant ces périodes. S'il existe un risque que les autorités confisquent votre téléphone ou vous obligent à le déverrouiller et à en révéler le contenu (lors d'une coupure ou en dehors), envisagez d'utiliser un téléphone distinct de votre appareil personnel. Cela peut aider à minimiser le volume d'informations que vous transportez sur vous et qui peuvent être compromises (par exemple, vos contacts, identifiants, messages, etc...). Si vous n'avez pas accès à un autre appareil, vous pouvez suivre ce guide pour réduire la quantité de données sensibles et améliorer la sécurité sur votre téléphone principal.

## Si vous utilisez un ancien téléphone, reformatez-le d'abord

Pour reformater votre téléphone, exécutez une réinitialisation d'usine.

Remarque : [Des études](#) ont démontré que l'exécution d'une réinitialisation d'usine sur votre téléphone n'efface pas nécessairement toutes les données. En fait, le seul moyen sûr à 100% d'effacer l'intégralité des données est de détruire l'appareil, mais cette méthode n'est pas une option si vous souhaitez réutiliser le téléphone ! Dans [l'article suivant](#), un ingénieur Android suggère de s'assurer que le contenu de votre appareil est crypté avant la réinitialisation d'usine. Le cryptage est paramétré par défaut sur la plupart des téléphones actuels, mais dans le cas contraire, allez à Paramètres > Sécurité > Chiffrer/Crypter le téléphone avant de le réinitialiser. De cette façon, suite à la réinitialisation d'usine, la clé de cryptage est perdue et toutes les données éventuellement non effacées seront protégées.

## Adoptez les pratiques de sécurité de base

Il existe des pratiques générales de sécurité téléphonique pertinentes dans toute situation, que vous documentiez un sujet pendant une coupure d'Internet ou non. [Voici quelques contenus utiles provenant d'autres organisations collègues](#). Bien que rien ne garantisse une sécurité à 100 %, voici quelques conseils clés :

- Assurez-vous que votre téléphone soit crypté. Les téléphones les plus récents sont chiffrés par défaut. Si vous n'êtes pas certain pour le vôtre, vérifiez les paramètres de sécurité de votre téléphone.
- Exécutez régulièrement les mises à jour du système d'exploitation (OS), car elles corrigent souvent les failles de sécurité.
- Mettez à jour vos applications importantes (comme les messageries) régulièrement.
- Choisissez un mot de passe fort qui comporte au moins 6 chiffres et qui ne repose pas sur l'empreinte digitale ou l'identification faciale.
- Configurez un verrouillage automatique de l'écran avec un minuteur.
- Désactivez les services de localisation chaque fois que vous n'en avez pas l'utilité (y compris le service de localisation d'urgence, la précision de la localisation, l'historique des positions et les fonctionnalités de partage de position, ainsi que les options de recherche de connexion Wi-Fi et Bluetooth). Vérifiez également les autorisations de localisation en vigueur sur chaque application.
- Désactivez Bluetooth et Wi-Fi lorsque vous n'en avez pas besoin, afin d'éviter que le téléphone puisse être pisté.
- Éteignez le téléphone lorsque vous ne l'utilisez pas.

## Installez des applications de documentation utiles

Pour les captures photo ou vidéo, vous pouvez utiliser l'application de caméra intégrée à votre téléphone, mais également des applications de documentation plus spécialisées, comme [ProofMode](#) ou d'autres, qui proposent une capture et une exportation de métadonnées plus robustes, une identification et une authentification, un cryptage, des transferts sécurisés et d'autres fonctionnalités encore.

Une application utile pour documenter la coupure en elle-même est [OONI Probe](#), une application open source qui effectue des tests depuis votre téléphone pour vérifier si des sites ou des plates-formes sont bloqués. Il peut vous montrer comment, quand, où et par qui les sites sont bloqués. Assurez-vous prendre connaissance les [risques potentiels](#) avant d'utiliser cette application.

Vous ne savez pas quelle(s) application(s) de documentation utiliser ? Nous proposons quelques conseils et questions à se poser dans notre tutoriel « [Devrais-je utiliser cette appli de documentation ?](#) ».

## Installez des applications de la vie quotidienne

N'avoir que très peu de données et seulement quelques applications spécialisées sur votre téléphone peut éveiller les soupçons. Pour déguiser l'appareil comme s'il s'agissait d'un téléphone personnel utilisé au quotidien, installez des applications de la vie quotidienne qui sont courantes dans la zone dans laquelle vous documentez vos sujets (mais qui sont téléchargées à partir de sources fiables) et prenez des photos anodines pour votre galerie.

Pour les applications de réseaux sociaux, il pourrait vous être utile de créer et vous connecter à des comptes alternatifs, mais rappelons que les faux comptes enfreignent les conditions d'utilisation de la plupart de ces plateformes et que les exigences de vérification d'identité de certaines plateformes peuvent rendre difficile la création de ces faux comptes. De plus, vous devrez passer un peu de temps à créer un profil avec du contenu et des amis associés, ce qui peut être laborieux.

## Installer des applications lorsqu'il n'y a pas d'accès à Internet

Télécharger et installer des applications sans accès à Internet constitue un défi. Vous devez télécharger les applis à l'avance si vous anticipez une panne d'Internet.

Une stratégie qui pourra vous être utile, à vous et à d'autres le moment venu, consiste à télécharger et à enregistrer le fichier Android Package (.apk) de l'application (téléchargé à partir d'une source fiable, par exemple directement auprès du développeur) sur la mémoire de votre téléphone ou sur un disque dur. Avoir ces APK hors ligne vous permet, à vous ou à d'autres, de partager des applications lorsqu'il n'y a pas d'Internet.

Bien que nous n'ayons pas eu l'occasion d'essayer cela, l'appli [F-Droid](#) fournit une interface pour échanger ces APK hors ligne. Voici leur [tutoriel](#).

## Sauvegardez vos informations personnelles, privées ou sensibles hors de l'appareil

Dans la mesure du possible, réservez l'appareil pour documenter vos sujets. Ne l'utilisez pas pour échanger des e-mails, des appels téléphoniques ou des messages avec des contacts

personnels ou militants qui pourraient être mis en danger, et ne connectez pas cet appareil à l'un de vos vrais comptes.

## Utiliser des fonctionnalités pour masquer le contenu

Dans le cas où votre téléphone serait fouillé, il peut être utile de dissimuler vos intentions et votre contenu. Dans les cas où votre téléphone ne serait examiné que *superficiellement et rapidement*, vous pouvez employer des tactiques simples telles que :

- Changer les noms et les icônes des raccourcis à vos applis à l'aide d'une application Launcher (par exemple, [Nova Launcher](#), mais il y en existe d'autres) afin que les applications sensibles ne soient pas immédiatement repérables.
- Utiliser une fonction de confidentialité intégrée telle que le [mode privé](#) (Samsung) ou le [verrouillage du contenu](#) (LG), si votre téléphone est capable de l'exécuter.
- Placer un fichier vide nommé ".nomedia" dans n'importe quel dossier pour empêcher les médias d'un dossier d'apparaître dans votre galerie. Remarque : Si le média apparaît toujours, vous devrez peut-être effacer le cache de votre galerie. Il est possible que cela ne fonctionne pas sur certains appareils.
- Créer des dossiers cachés (dossiers commençant par un ".") à l'aide d'une appli de gestion de fichiers. Vous pouvez soit déplacer manuellement les fichiers vers le dossier caché, soit spécifier le dossier où les médias que vous enregistrez sont stockés dans le cas où vous utilisez une application de capture photo comme [Open Camera](#). Assurez-vous de désactiver l'option "Afficher les fichiers cachés" dans vos paramètres afin que les fichiers cachés restent invisibles.
- Certaines applications de documentation spécialisées, telles que [Tella](#) ou [Eyewitness to Atrocities](#), stockent les fichiers dans des galeries cryptées distinctes dont le contenu n'est accessible que via l'appli, ce qui peut éviter leur découverte en cas de fouille de votre téléphone. L'accès à la documentation stockée dans ces galeries sécurisées requière un mot de passe distinct, de sorte qu'elle reste inaccessible même lorsque votre téléphone est déverrouillé.

## Remarque importante concernant la dissimulation de vos contenus

Il est important de noter que les techniques ci-dessus peuvent être suffisantes pour duper quelqu'un qui ne fait que parcourir rapidement votre téléphone, mais **ne permettra pas de cacher efficacement votre contenu à quelqu'un qui cherche vraiment.**

Gardez également à l'esprit que certains pays peuvent avoir des lois qui restreignent ou interdisent l'utilisation d'applications de sécurité qui cryptent ou effacent vos données. Les utiliser pour empêcher les autorités d'accéder à vos données peut être considéré comme de la destruction de preuves ou l'obstruction d'une enquête, et peut être passible de poursuites judiciaires. Cette [carte](#) (complète, mais datant de 2017) constitue un bon point de départ si vous avez des interrogations concernant les lois applicables dans votre pays.

## Configurer le partage hors ligne

Dans une situation où vous n'avez pas accès à Internet après avoir capturé du contenu, vous pourriez avoir besoin d'effacer ce contenu de votre téléphone pour des raisons de sécurité, pour libérer de l'espace ou pour le partager avec d'autres. Il est souhaitable de supprimer régulièrement le contenu de votre appareil afin de minimiser la quantité d'informations compromises si votre téléphone devait être confisqué et déverrouillé.

Même dans l'incapacité de vous connecter à Internet, vous pourrez certainement vous connecter localement à des appareils compatibles via Wi-Fi ou Bluetooth, tels qu'un autre téléphone ou une clé USB Wi-Fi. Les téléphones sont généralement dotés d'une application ou interface pour vous connecter et transférer des fichiers. Si votre téléphone le permet, vous pouvez également connecter un disque dur ou une clé USB On-The-Go (OTG) pour décharger les fichiers sur le lecteur OTG ou un autre appareil.

Ces méthodes sont abordées plus en détail dans notre tutoriel [Partager des fichiers et communiquer lors d'une coupure Internet](#) et dans notre fiche de conseils [Preuve en vidéo : outils technologiques - transferts de fichiers](#).

## Entraînez-vous avant d'être en situation de crise

Configurez le téléphone maintenant si et pendant que vous avez accès à Internet. Commencez à vous entraîner à utiliser les applications dans des situations quotidiennes (qui ne posent pas de problèmes de sécurité) afin de vous familiariser avec leur utilisation. Appliquez par défaut les bonnes pratiques de sécurité téléphonique de base. Ces méthodes deviendront ainsi une seconde nature lorsque vous serez dans une situation de crise avec d'autres sujets de préoccupation.

\*\*\*\*\*

## Devrais-je Utiliser cette Appli de Documentation ?

Dernière révision : 31 Janvier 2020

Il existe de nombreuses applications qui permettent de capturer des vidéos, allant de [l'application appareil photo](#) par défaut de votre téléphone à des applis plus spécialisées telles que [ProofMode](#), [Tella](#) ou [Eyewitness to Atrocities](#). Certaines fonctionnalités de ces applis requièrent un accès à Internet, gardez donc à l'esprit que ces fonctionnalités peuvent ne pas être disponibles en cas de coupure.

Nous ne pouvons pas indiquer quelle application spécifique est la plus appropriée à votre cas, car cela dépend de votre situation, de vos besoins et des risques encourus (consultez



ce blog pour en savoir plus sur [la façon d'évaluer les risques et menaces vous concernant](#)). Avec votre évaluation des risques en main, les questions ci-dessous peuvent vous guider dans le choix de l'application de capture vidéo la mieux appropriée.

## Qui a créé l'application et puis-je leur faire confiance ?

Il est fortement conseillé de chercher à identifier les créateurs de toute appli que vous téléchargez et installez sur votre appareil, et d'évaluer si vous pouvez leur faire confiance pour ne pas vous mettre en danger, que ce soit de manière intentionnelle ou non.

Certains points de vigilance sont :

- Le développeur de l'application est-il digne de confiance ? Qu'en disent les membres de votre communauté ou de vos réseaux plus étendus à leur sujet et à propos des outils qu'il a développés ?
- Le développeur de l'application est-il vulnérable ? Tenez compte de son contexte géopolitique et de la probabilité qu'il se trouve contraint à transmettre vos données ou à en autoriser l'accès par le pouvoir en place (ou s'il l'a effectivement fait par le passé). Dans quel pays les données sont-elles stockées et quelles sont les lois en vigueur dans sa juridiction ?
- Le développeur de l'application assure-t-il encore la maintenance de l'application ? Les applis non mises à jour sont sensibles aux piratages qui en exploitent les vulnérabilités connues. Consultez le site du développeur ou la page Google Play de l'application pour connaître sa date de « dernière mise à jour ».
- Dans quelle mesure le développeur de l'application est-il établi et semble-t-il en capacité d'assurer la pérennité de ces maintenances ?
- L'application est-elle open source ? Les applications soumises à l'examen public sont plus susceptibles de voir leurs problèmes de sécurité résolus ou a minima identifiés. Le développeur est-il transparent sur l'efficacité et la sécurité de l'application ?
- Quelles motivations ou influences entraînent le travail du développeur, et qu'est-ce que cela implique concernant sa fiabilité ? Par exemple, est-il ouvertement motivé par la mission identifiée ? À but lucratif ? Parrainé par un bailleur de fonds ou mécène en particulier ?
- Bien qu'il ne s'agisse pas d'un indicateur direct de fiabilité, le coût de l'application peut être une considération importante. Certaines appliquent des frais d'abonnement mensuels élevés ou des tarifs par vidéo.

Pour en savoir plus, consultez le guide [EFF](#) d'autodéfense contre la surveillance sur [quelle appli choisir?](#)

## De quelle provenance l'application est-elle téléchargeable ?



Vous devez uniquement télécharger et installer des applications provenant de plateformes « d'app stores » ou de sites Web réputés. Même si vous avez effectué des recherches approfondies pour déterminer la fiabilité d'une application, des vendeurs d'applis peu recommandables déguisent parfois leurs produits afin de vous amener à télécharger un « logiciel imposteur » créé à des fins néfastes. Par exemple, l'année dernière, l'organisation de défense des droits numériques [SMEX](#) a émis [un avertissement](#) concernant divers sites Web commercialisant une application intitulée "WhatsApp Plus" (pour être clair, ceci n'était pas un produit WhatsApp!), qui pouvait potentiellement enregistrer et vendre les données de ses utilisateurs, et rendait les téléphones sur lesquels elle était installée vulnérables au piratage.

Certains développeurs soucieux de la cybersécurité fournissent même des clés de cryptage qui vous permettent de vérifier leur authenticité. Elles incluent souvent un mode d'emploi pour vérifier ces signatures.

## Où les données seront-elles stockées ?

Certaines applis de documentation ne stockent vos données et vos fichiers que localement sur votre appareil, tandis que d'autres envoient et stockent vos données ailleurs. Dans de nombreux cas, cela est inhérent à la conception de l'appli par rapport à l'objectif annoncé, comme par exemple l'appli Eyewitness to Atrocities, qui envoie une copie non altérée de vos fichiers dans une infrastructure de stockage Lexis Nexis afin qu'Eyewitness puisse se porter garant de la chaîne de responsabilité et de l'intégrité du contenu. Vous ne pouvez exporter vos médias hors de la galerie cryptée dans l'application Eyewitness qu'une fois leur envoi pour sauvegarde effectué.

C'est à vous de déterminer s'il est nécessaire que vos fichiers soient uniquement sauvegardés sur votre appareil, si vous avez besoin qu'ils soient transférés et stockés dans un emplacement à distance que vous contrôlez (c'est une option avec [Tella](#)), ou si vous devez l'envoyer à un organisme externe auquel vous donnez l'autorisation d'accès et d'utilisation de vos données. Gardez à l'esprit que lors d'une coupure Internet, vous ne pourrez pas transmettre vos fichiers immédiatement, vous aurez donc besoin d'une application qui vous permet au moins temporairement de stocker (et idéalement de sauvegarder) votre documentation localement (Consultez la rubrique [Sauvegarder ses données sans Internet ni ordinateur](#)).

Si vos fichiers sont destinés à être envoyés dans un emplacement à distance, soyez attentifs aux pays dans lesquels les données résideront même temporairement. Dans quelle mesure les données sont-elles susceptibles d'être saisies et exposées dans ces pays, que ce soit par ordonnance judiciaire ou par d'autres moyens ? Quels risques courez-vous en y envoyant vos données ?

## L'application chiffre-t-elle mes fichiers multimédias ?

Certaines applis, telles que Tella et Eyewitness to Atrocities, fournissent un service de cryptage de fichiers et/ou un stockage crypté pour votre documentation, distincts de la galerie principale et du cryptage inhérent à votre téléphone, de sorte que vos médias et vos métadonnées ne soient jamais consultables et non cryptés sur votre appareil, sauf si vous y accédez via l'appli avec un mot de passe. Cela signifie que même si votre téléphone est déverrouillé, vos fichiers restent cryptés, et fournit un niveau de protection supplémentaire pour votre documentation.

Si l'application envoie et stocke vos médias dans un emplacement à distance une fois votre connexion Internet rétablie, déterminez également si vous avez besoin que vos médias soient cryptés pendant leur transit et la durée de leur stockage à distance, comme le propose l'application EyeWitness, par exemple.

Gardez à l'esprit que bien que le cryptage soit légal dans la plupart des pays, certains pays peuvent avoir des lois qui restreignent ou criminalisent son utilisation. Cette [carte](#) (complète, mais datant de 2017) constitue un bon point de départ si vous avez des interrogations concernant les lois applicables dans votre pays.

## L'application capture-t-elle les métadonnées importantes (hors connexion) ?

[Les métadonnées](#) sont des données qui décrivent votre vidéo ou photo, comme la date et l'heure ou le lieu d'enregistrement. Ces informations sont précieuses afin d'identifier, de comprendre, d'authentifier et de vérifier votre vidéo ou photo en tant que témoignage d'un événement spécifique. Dans le cadre d'une coupure d'Internet, la capacité d'une application à collecter automatiquement certaines métadonnées et/ou à vous permettre de saisir facilement des informations descriptives sur place est un élément clé, car il peut s'écouler un long moment avant que vous ne puissiez partager la documentation avec qui que ce soit (durée pendant laquelle des détails peuvent être oubliés, les circonstances peuvent changer, etc...).

La plupart des applis de documentation spécialisées telles que ProofMode ont des fonctionnalités améliorées et collectent plus de métadonnées que la plupart des applications de caméra intégrées. Les métadonnées améliorées peuvent inclure des informations diverses comme les données récoltées par des capteurs, des signaux Wi-Fi ou Bluetooth à proximité, des données propres au périphérique, à l'algorithme de chiffrement ou même fournies par l'utilisateur, toutes choses améliorant les possibilités d'authentification et de vérification des fichiers multimédias ultérieurement.

Gardez à l'esprit que lors d'une coupure d'Internet, vous aurez besoin d'une application qui ne nécessite pas la transmission de données pour générer ou enregistrer des métadonnées. Certaines applications collectent certaines métadonnées via Internet plutôt que via les capteurs matériels intégrés à l'appareil. Par exemple, si les données de localisation sont capturées à partir des recherches effectuées sur le téléphone, les métadonnées enregistrées correspondront au dernier emplacement où les données mobiles étaient activées plutôt qu'à la localisation réelle de l'appareil. L'application devrait idéalement également vous permettre de stocker les métadonnées localement même hors ligne, y compris l'enregistrement de tous

formulaire que vous seriez amené à remplir (comme dans le cas du "mode hors ligne" de Tella).

## Puis-je exporter des données de l'application ?

En fonction de la destination de la documentation collectée, il peut être indispensable de pouvoir exporter la vidéo et ses métadonnées depuis l'application, dans un format qui n'est pas propre à cette appli de manière à pouvoir ouvrir, afficher et utiliser les médias et les métadonnées sur un support autre que l'application. La possibilité d'exporter permet de ne pas dépendre d'une seule application ou d'un seul fournisseur de services pour accéder à vos documents, et vous donne plus de latitude pour utiliser ce contenu à l'avenir. Gardez à l'esprit que certaines métadonnées peuvent ne pas être consultables si vous n'avez pas accès aux bases de données ou à certains tableaux de conversion adéquats pour interpréter les chiffres (par exemple, les identifiants des tours relais ou des réseaux Wi-Fi).

Notez que certaines applications peuvent entretenir une chaîne de responsabilité délibérément fermée et ne pas autoriser les utilisateurs à exporter des données, tandis que d'autres n'ont peut-être pas été conçues pour l'exportation. Sachez également que certaines applications, comme Eyewitness to Atrocities, ne vous permettent pas d'exporter tant que vous n'avez pas transféré le média sur un serveur à distance (ce pour quoi un accès Internet sera nécessaire), et d'autres applis vous permettront d'exporter le média seulement, mais pas les métadonnées (autres que celles qui sont inhérentes au fichier lui-même).

Si le transfert de données vous est indispensable, il vous faut idéalement une application qui vous permette d'exporter une copie du média sans aucune modification ni altération, ainsi qu'une copie des métadonnées dans un format texte lisible standardisé. Les métadonnées Tella, par exemple, sont stockées cryptées dans la galerie Tella, mais peuvent être exportées au format CSV. De plus, lors d'une coupure Internet, il est nécessaire de disposer d'options d'exportation vers des applications hors ligne ou des services non dépendants d'Internet. La plupart des applications qui vous permettent d'exporter présentent l'équivalent d'un bouton "Partager" qui déclenche un menu de partage, qu'Android remplit avec une liste d'applis installées sur votre téléphone et capables de gérer ce type de contenu. Malheureusement, les développeurs d'applications personnalisent leurs menus de partage et il n'y a pas de standardisation d'une appli à l'autre.

Pour gérer une plus grande quantité de documents, il peut être plus efficace d'accéder aux données stockées via une application gestionnaire de fichiers et de copier les fichiers à partir de là, bien que cette méthode puisse ne pas vous permettre d'accéder aux métadonnées stockées dans la base de données d'une application. Cette option n'est pas non plus disponible pour les applis qui fournissent leurs propres galeries sécurisées, car les fichiers seront cryptés avant leur stockage. Pour ces applications, il est nécessaire de disposer d'une fonction de partage au sein de l'application.

\*\*\*\*\*

# Maintenir la Fiabilité des Informations pendant une Coupure Internet

Cet article est extrait d'une série intitulée [Se Documenter lors d'une Coupure Internet](#)

Dernière révision : 31 Janvier 2020

[Les défenseurs des droits humains](#), [les enquêteurs](#), [les chercheurs](#) et [les journalistes](#) s'appuient souvent sur des documents de première main filmés par des témoins pour surveiller, signaler et traiter les violations des droits de l'Homme. Afin d'assurer la fiabilité des informations diffusées, ces utilisateurs prennent des mesures pour authentifier et vérifier la documentation qu'ils reçoivent, processus qui peut être long et fastidieux.

En tant que reporter, vous pouvez prendre des mesures simples pour permettre aux autres de vérifier et corroborer plus facilement vos documents, afin qu'ils soient utilisés de manière opportune et efficace. Ces quelques étapes supplémentaires sont encore plus précieuses lors d'une coupure Internet, étant donné que :

- Si vous n'avez pas la possibilité de mettre immédiatement le contenu en ligne, la date de publication et la localisation générées par les réseaux sociaux seront inutiles pour prouver que votre vidéo a bien été filmée antérieurement à une certaine date ou bien dans un certain lieu.
- Si à proximité il est également impossible pour d'autres de mettre du contenu en ligne, il risque d'y avoir trop peu de documentation disponible sur l'ensemble du sujet qui puisse être utilisée pour corroborer votre vidéo.
- Si votre vidéo doit passer entre plusieurs mains hors ligne pour arriver à bonne destination, il peut être plus difficile pour ses destinataires de retrouver la source de la vidéo.
- Si vous devez supprimer la vidéo d'origine de votre téléphone en raison d'une surveillance accrue ou d'une capacité de stockage limitée sans possibilité de sauvegarde dans le cloud, ou bien si vous devez vous débarrasser du téléphone, il peut être plus difficile de confirmer l'authenticité de la vidéo.
- Si vous oubliez les détails particuliers à une vidéo et que l'application que vous utilisez ne capture ou n'enregistre pas les métadonnées hors ligne, d'autres personnes risquent de ne pas pouvoir l'identifier plus tard.

Les conseils suivants peuvent vous aider à maintenir votre vidéo pendant une coupure Internet afin de maximiser sa vérifiabilité et sa facilité d'utilisation en tant que témoignage ultérieurement.

## Filmer ou fournir des détails d'identification dans la vidéo

Essayez d'inclure dans votre vidéo des détails qui permettent à un enquêteur ou à un journaliste d'identifier plus facilement l'heure et le lieu de la prise de vue, comme des points de repère spécifiques au lieu, la ligne d'horizon, les panneaux de signalisation, les devantures de magasins, les plaques d'immatriculation, les drapeaux, les horloges, les premières pages des journaux, etc... Vous pouvez également donner oralement des

informations de base telles que votre nom et vos coordonnées (si cela ne compromet pas votre sécurité), l'heure, la date et les coordonnées GPS (ou inscrire ces informations sur un morceau de papier et filmer le papier). Plus vous incluez de détails, plus il sera facile pour un tiers d'authentifier la vidéo plus tard, même s'il ne sait pas qui vous êtes et d'où provient la vidéo. Pour en savoir plus, consultez nos conseils sur les [Pratiques de base pour la capture, le stockage et le partage](#).

## Ajouter une description ou des métadonnées

Profitez de l'une des nombreuses applications de documentation spécialisées qui extraient de votre téléphone des métadonnées améliorées ou des informations techniques, et vous permettent de saisir manuellement des informations descriptives supplémentaires. Rappelez-vous que, lors d'une coupure, vous avez besoin d'une application qui ne nécessite pas d'accès à Internet pour enregistrer ou stocker ces métadonnées. Consultez « [Devrais-je utiliser cette appli de documentation ?](#) » pour en savoir plus sur la façon de choisir une application appropriée.

Même si vous n'utilisez pas une application spécialisée, vous pouvez toujours avoir recours à des notes, des cartes ou des photos enregistrées sur votre téléphone afin de générer des informations supplémentaires. Vous pouvez monter votre vidéo avec ces informations supplémentaires à l'aide de votre application favorite gestionnaire de fichiers. Les informations clés à inclure sont l'heure, la date, le lieu de l'incident enregistré, ainsi que la source de l'enregistrement (c'est-à-dire votre nom et vos coordonnées) si toutefois elles peuvent l'être sans compromettre votre sécurité. Exportez les métadonnées et incluez-les avec la vidéo (vous pouvez tout mettre dans un dossier et le compresser) lorsque vous la partagez.

## Faites une sauvegarde

Sauvegardez régulièrement les médias de votre téléphone, idéalement sur 2 périphériques de stockage distincts. Vous pouvez, par exemple, connecter des clés USB On-the-Go (OTG) ou sans fil à votre téléphone, même sans ordinateur. Consultez nos conseils de la rubrique "Sauvegarder ses données sans Internet ni ordinateur" pour plus de détails. La sauvegarde vous permettra de conserver une copie de votre vidéo en cas de perte ou de casse de votre téléphone, ou si vous vous trouviez contraint à supprimer ces vidéos de votre appareil. Le fait de disposer d'une copie sécurisée de votre vidéo originale permettra également à un enquêteur ou à un journaliste qui voit votre vidéo via d'autres moyens de récupérer la vidéo directement auprès de vous plus tard (à condition qu'il soit en mesure de remonter jusqu'à vous), engendrant ainsi une chaîne de responsabilité plus courte et plus facilement valable juridiquement.

\*\*\*\*\*

# Sauvegarder ses Données sans Internet ni Ordinateur

Cet article est extrait d'une série intitulée [Se Documenter lors d'une Coupure Internet](#)

Dernière révision : 31 Janvier 2020

[La sauvegarde](#) est essentielle pour garantir que vos données et votre documentation ne soient pas accidentellement supprimées, corrompues ou perdues si votre appareil est confisqué. Lors d'une coupure ou d'un ralentissement d'Internet, il ne vous sera peut-être pas possible de procéder à votre sauvegarde sur cloud régulière ou de transférer votre documentation dans un emplacement à distance sûr. Le déchargement sur un ordinateur de bureau ou portable est un moyen de sauvegarde, mais il arrive de n'avoir aucun accès à un ordinateur, voici quelques options à explorer et conseils pour sauvegarder vos médias à partir de votre téléphone pendant une coupure Internet et sans ordinateur.

## Utilisez un lecteur OTG ou sans fil

Les clés OTG, de l'anglais On-The-Go, sont un type de clé USB compatible avec la plupart des OS Android (mais pas tous). Vous pouvez brancher une clé USB OTG directement sur votre téléphone ou utiliser un adaptateur OTG vers USB pour connecter votre téléphone à un disque dur USB ordinaire. Avec OTG, votre téléphone fournit l'alimentation nécessaire au fonctionnement du lecteur.

Parmi les marques populaires de lecteurs OTG on retrouve SanDisk, Kingston et Samsung, bien qu'il en existe de nombreuses autres. Ils coûtent généralement entre 8 et 25 USD selon leur capacité de stockage.

Les clés USB ou disques durs sans fil sont similaires aux disques durs ordinaires, sauf qu'ils ne requièrent aucun câble. Cela vous permet de connecter des appareils qui d'ordinaire ne se connectent pas aux disques durs, tels que votre téléphone. L'un des avantages que présente un lecteur sans fil par rapport à un lecteur OTG est la possibilité de connecter plusieurs utilisateurs au même lecteur sans fil à la fois. Cela peut être utile, par exemple, dans une situation de manifestation lorsque vous filmez en équipe - les images de chacun peuvent être toutes sauvegardées sur un disque dur transporté par un autre membre de l'équipe. Notez que ces lecteurs n'étant pas alimentés électriquement par un téléphone, les disques sans fil dépendent de leur batterie et doivent être rechargés.

SanDisk est probablement la marque la plus populaire de clés USB sans fil, bien qu'il en existe d'autres. Les clés USB sans fil sont généralement plus chères que les clés OTG leur prix variant entre 25 et 100 USD environ, selon la capacité de stockage. Les premiers prix des disques durs externes sans fil plus grands sont à environ 150 USD et varient également selon la capacité de stockage.

## Alternative : utiliser un ancien téléphone inutilisé

Si vous n'avez pas de lecteur OTG ou sans fil, mais que vous disposez d'un ancien téléphone toujours fonctionnel que vous n'utilisez plus, vous pouvez également le reconvertir pour la sauvegarde de vos données. Tant que les deux téléphones se trouvent à portée physique l'un de l'autre, vous pouvez vous connecter et copier des médias de l'un à l'autre en utilisant le Bluetooth, la Wi-Fi ou la fonction Near Field Communication (NFC) / Android Beam. Le Bluetooth et Wi-Fi Direct sont deux technologies sans fil qui peuvent "jumeler" deux appareils sans aucun routeur ou point d'accès intermédiaire entre les deux. Wi-Fi Direct offre une portée plus large et un transfert de données plus rapide que Bluetooth, mais consomme beaucoup plus d'énergie. La technologie NFC a une portée beaucoup plus courte (~ 4 cm) et des vitesses de transfert beaucoup plus lentes que les précédentes, mais se connecte plus rapidement et utilise moins d'énergie, ce qui peut être utile pour faire des petits transferts rapides lorsque vous avez les deux appareils à portée de main.

Votre téléphone dispose probablement d'applications ou fonctionnalités Bluetooth, Wi-Fi Direct ou NFC intégrées qui vous permettent de choisir des appareils à proximité avec lesquels partager des données. Si « Files By Google » est installée sur les deux téléphones, vous pouvez également partager des fichiers hors ligne à l'aide de ces technologies au sein de l'application.

Important : le revers de la médaille de la facilité de connexion offerte par ces services est qu'ils ne sont pas sécurisés. Les balises/scanners Bluetooth et Wi-Fi peuvent être utilisés pour traquer votre position ou sonder votre appareil afin d'en obtenir des informations. Les infiltrés peuvent essayer de s'associer à votre appareil, vous envoyer des fichiers indésirables ou même prendre le contrôle de votre appareil s'il est vulnérable. **Pour plus de sécurité, désactivez ces services lorsque vous ne les utilisez pas et ne les activez que lorsque vous vous trouvez en lieu sûr, limitez les autorisations accordées aux applications au strict nécessaire et appliquez les bonnes pratiques de sécurité téléphonique, comme par exemple exécuter des mises à jour régulières et avoir un mot de passe renforcé.**

## Inclure toutes les descriptions et métadonnées non incluses dans le fichier

Lors de la copie d'un fichier sur un lecteur OTG, un lecteur sans fil ou un ancien téléphone, il est utile d'inclure toute information descriptive ou métadonnée indépendante du fichier. De nombreuses [applis de documentation](#), par exemple, génèrent des documents texte aux formats CSV ou JSON qui incluent des métadonnées extraites de l'appareil (géolocalisation, heure, date, etc...) et toute description saisie manuellement par l'utilisateur. Assurez-vous également d'extraire et d'inclure ces documents de métadonnées dans vos sauvegardes.

## Protéger le lecteur avec un mot de passe



De nombreux lecteurs sans fil peuvent être protégés par mot de passe via une application mobile fournie avec le disque. Notez que la protection par mot de passe n'est pas la même chose que le cryptage (voir ci-dessous). La plupart des lecteurs sans fil ou OTG ne permettent pas le chiffrement intégral du disque à l'aide d'un téléphone mobile, bien qu'ils puissent être chiffrés intégralement à l'aide d'un ordinateur.

## Envisagez de crypter les fichiers

Si vous avez besoin de stocker vos fichiers de manière plus sécurisée, vous pouvez envisager de crypter vos sauvegardes. Bien que le chiffrement de la plupart des lecteurs sans fil ou OTG soit impossible avec un téléphone mobile seulement, vous pouvez crypter les fichiers eux-mêmes avant de les déplacer sur le lecteur. Parmi les applications capables de crypter des fichiers sur Android on trouve ZArchiver et RAR. Sachez que vous devez retenir vos mots de passe de cryptage. Il n'y a aucun moyen de récupérer des fichiers cryptés si vous perdez le mot de passe.

Gardez à l'esprit que certains pays peuvent avoir des lois qui restreignent ou criminalisent l'utilisation du cryptage de données. Y avoir recours pour empêcher les autorités d'accéder à vos données peut être considéré comme la destruction de preuves ou l'obstruction d'une enquête, et peut être punissable par la loi. Cette [carte de 2017](#) est peut-être obsolète, mais constitue un bon point de départ si vous avez des interrogations sur les lois en vigueur dans votre pays.

## Faire 2 sauvegardes dans des emplacements distincts

Avoir une seule sauvegarde n'est pas toujours suffisamment fiable. Par exemple, le périphérique de sauvegarde peut être perdu, endommagé ou subir une panne aléatoire. Les experts en informatique conseillent généralement aux utilisateurs d'avoir 2 sauvegardes (c'est-à-dire 3 copies au total), sur des appareils distincts conservés dans des emplacements distincts. Cela permet de mitiger les risques sur une copie spécifique.

\*\*\*\*\*

## Partager des Fichiers et Communiquer lors d'une Coupure Internet

Cet article est extrait d'une série intitulée [Se Documenter lors d'une Coupure Internet](#)

Dernière révision : 31 Janvier 2020

*La répression et la coupure d'Internet – la plus longue coupure jamais imposée dans une démocratie – en cours au Cachemire, ont eu un [impact catastrophique](#) sur la vie des habitants de la région. Au comble de l'insulte, en décembre 2019, [les comptes WhatsApp des Cachemiris ont commencé à être révoqués](#) suite à 120 jours d'inactivité de leurs utilisateurs, conformément aux conditions de WhatsApp.*

*Au moment d'écrire ces lignes en janvier 2020, la Cour Suprême indienne a statué sur l'illégalité de la coupure Internet d'une durée indéterminée subie au Cachemire, précisant qu'elle constituait un abus de pouvoir. Une connexion limitée à l'Internet haut débit et aux réseaux mobiles a été rétablie dans certaines régions, mais uniquement pour certains sites Web «sur liste blanche».*

Les coupures Internet sont conçues pour empêcher les gens de partager des informations et de communiquer (et également pour pousser les gens vers des formes de communication moins sécurisées telles que le téléphone portable et les SMS, qui sont plus faciles à intercepter et à surveiller par les autorités). Il n'y a pas toujours de bonnes solutions de contournement lors d'arrêts complets. Pendant les périodes les plus strictes de la coupure au Cachemire, par exemple, les gens [ont eu recours à des notes manuscrites et à des courriers](#) pour envoyer des messages à leurs proches.

Nous n'avons pas de solutions infaillibles pour contourner tous les blocages, mais grâce à nos conversations avec des militants et des pairs, nous avons acquis certaines méthodes et approches pour communiquer et partager des données hors ligne qui peuvent fonctionner pour vous, selon les circonstances. Notez que certaines de ces options nécessitent une connexion Internet pour leur mise en place initiale (par exemple, pour télécharger des applications, etc...).

## Partagez des fichiers directement via Bluetooth, Wi-Fi Direct ou NFC

Vous n'avez pas besoin d'une connexion Internet pour connecter votre téléphone à un autre appareil à proximité via Bluetooth, Wi-Fi Direct ou la fonction Near Field Communication (NFC) (parfois nommée Android Beam sur des appareils plus anciens). Le Bluetooth et Wi-Fi Direct sont deux technologies sans fil qui peuvent "jumeler" deux appareils sans aucun routeur ou point d'accès intermédiaire entre les deux. Wi-Fi Direct offre une portée plus large et un transfert de données plus rapide que Bluetooth, mais consomme beaucoup plus d'énergie. La technologie NFC a une portée beaucoup plus courte (~ 4 cm) et des vitesses de transfert beaucoup plus lentes que les précédentes, mais se connecte plus rapidement et utilise moins d'énergie, ce qui peut être utile pour faire des petits transferts rapides lorsque vous avez les deux appareils à portée de main.

Votre téléphone dispose probablement d'applications ou fonctionnalités Bluetooth, Wi-Fi Direct ou NFC intégrées qui apparaissent automatiquement dans vos options de partage. Si « Files By Google » est installée sur les deux téléphones, vous pouvez également partager des fichiers hors ligne à l'aide de ces technologies au sein de l'application.

Important : le revers de la médaille de la facilité de connexion offerte par ces services est qu'ils ne sont pas sécurisés. Les balises/scanners Bluetooth et Wi-Fi peuvent être utilisés pour traquer votre position ou sonder votre appareil afin d'en obtenir des informations. Les infiltrés peuvent essayer de s'associer à votre appareil, vous envoyer des fichiers indésirables ou même prendre le contrôle de votre appareil s'il est vulnérable. **Pour plus de**

sécurité, désactivez ces services lorsque vous ne les utilisez pas et ne les activez que lorsque vous vous trouvez en lieu sûr, limitez les autorisations accordées aux applications au strict nécessaire et appliquez les bonnes pratiques de sécurité téléphonique, comme par exemple exécuter des mises à jour régulières et avoir un mot de passe renforcé.

## Partagez des fichiers avec un lecteur sans fil ou via un réseau local sans fil (WLAN : Wireless Local Area Network)

Un disque dur ou une clé USB sans fil peuvent être utilisés pour partager des fichiers au sein d'une équipe ou de plusieurs personnes à la fois. Le lecteur Wi-Fi est généralement accompagné d'instructions et/ou d'une application vous permettant de connecter votre téléphone au lecteur, et est relativement facile à utiliser. N'oubliez pas de verrouiller le lecteur avec un mot de passe pour des raisons de sécurité.

Si vous n'avez pas de lecteur sans fil, vous pouvez également partager des fichiers sur un lecteur USB ordinaire en le branchant sur un routeur sans fil. Les routeurs de voyage équipés d'un port USB, par exemple, sont économiques et très peu encombrants. Les utilisateurs peuvent se connecter à la clé USB via un réseau local (pas de connexion Internet requise). Pour accéder aux fichiers sur le lecteur USB connecté à votre téléphone, vous devrez utiliser une application gestionnaire de fichiers qui peut se connecter au stockage en réseau, comme [Solid Explorer](#). L'adresse IP de votre routeur se trouve généralement dans les paramètres Wi-Fi avancés de votre téléphone.

Il existe une autre option qui est [PirateBox](#), un projet « fait maison » qui fournit des logiciels sous licence gratuite. Les utilisateurs peuvent partager des fichiers de la même manière que ci-dessus, mais Piratebox leur permet de le faire de manière anonyme et inclut également des fonctionnalités de chat et de messagerie. La configuration de Piratebox nécessite le téléchargement, l'installation et la configuration de quelques logiciels. [Les instructions](#) se trouvent sur le site Web de Piratebox.

*Mise à jour : le projet Pirate Box [ferme lentement](#). Le site Web et le dépôt github sont toujours en ligne, mais le principal développeur du projet n'en assure plus activement la maintenance.*

## Communiquer via un chat peer-to-peer

[Briar](#) et [Bridgefy](#) sont deux relativement nouvelles applications de messagerie peer-to-peer dont nous avons pris connaissance via des réseaux activistes. Nous ne les avons pas encore essayés nous-même, mais nous connaissons des tiers qui les testent.

[Briar](#) est une application de messagerie cryptée de bout en bout open source qui ne repose pas sur un serveur central, mais synchronise les messages entre les appareils des utilisateurs (ainsi, le contenu est sauvegardé sur l'appareil de chaque utilisateur). Il peut se synchroniser même sans connexion Internet, via Bluetooth ou Wi-Fi (lorsqu'il y a Internet,

l'application synchronise les appareils via le réseau [Tor](#)). Briar propose également des groupes privés, des forums publics et des blogs. Lors d'une utilisation hors ligne, votre portée est limitée par votre portée Bluetooth ou Wi-Fi (maximum ~ 100 mètres).

[Bridgefy](#) est une application de messagerie cryptée de bout en bout (sauf lors de l'utilisation de la fonction "diffusion") qui utilise le Bluetooth pour envoyer des messages. Contrairement à Briar, les messages peuvent parcourir de plus longues distances en parcourant un réseau maillé d'autres utilisateurs de Bridgefy (seul le destinataire prévu peut lire le message). Bridgefy n'a pas les fonctionnalités de groupes privés, forums et blogs de Briar, mais il dispose d'un mode de diffusion par lequel vous pouvez envoyer un message simultanément jusqu'à 7 utilisateurs de Bridgefy à portée, même s'ils ne figurent pas dans vos contacts (les messages de diffusion ne sont pas nécessairement cryptés).

## Communiquer par SMS crypté

Les messages texte SMS sont transmis via les réseaux mobiles et ne dépendent pas d'Internet, ils peuvent donc toujours fonctionner pendant les coupures Internet. En revanche, les SMS sont considérés comme très peu sûrs. Contrairement aux applications dépendantes d'Internet comme WhatsApp ou Signal, les SMS ne sont pas cryptés de bout en bout. Cela signifie que les messages texte (et leurs métadonnées) peuvent être lus par les gouvernements et les opérateurs de téléphonie mobile, ou interceptés par des hackers. Les SMS peuvent également être «usurpés», ce qui signifie qu'un expéditeur peut manipuler ses coordonnées pour se faire passer pour un autre utilisateur.

Si vous avez besoin d'utiliser des SMS, [Silence](#) est une application qui crypte les messages SMS de bout en bout. C'est une appli open-source qui utilise le protocole de chiffrement Signal. Bien que nous ne l'ayons pas essayée nous-mêmes, nous avons entendu dire que d'autres l'avaient utilisée. Il est nécessaire pour qu'elle fonctionne que l'expéditeur et le destinataire l'aient installée et échangé des clés de chiffrement entre eux. Étant donné que les messages SMS passent nécessairement par les serveurs des opérateurs de téléphonie mobile, même via Silence, le fait que vous ayez envoyé un message crypté et les métadonnées de votre message seront accessibles à la société de télécommunication.

## Arrêts partiels : contourner les sites bloqués

Le terme « coupure Internet » ne désigne souvent pas une panne totale d'Internet, mais plutôt un blocage de l'accès à des sites Web ou à des plateformes de réseaux sociaux spécifiques. Les gouvernements, via les fournisseurs d'accès Internet (FAI), peuvent bloquer les sites en fonction de l'adresse IP, du contenu ou via des recherches DNS. Vous ne savez pas si un site est bloqué ? Des organisations comme l'[Open Observatory of Network Interference](#) et [Netblocks](#) surveillent et mesurent les perturbations et la censure d'Internet dans le monde entier.

Heureusement, tant que vous avez accès à Internet, il existe des moyens d'essayer de contourner les blocages. Comme dans le cas du cryptage de données, gardez à l'esprit que le contournement des sites bloqués peut être répréhensible dans votre pays.

## **VPN**

Une façon de contourner les blocages basés sur les adresses IP ou les contenus consiste à utiliser un réseau privé virtuel ou un VPN (Virtual Private Network), tel que [ProtonVPN](#) ou [TunnelBear](#). Lorsque vous vous connectez via un VPN, votre trafic Internet est crypté et acheminé via un serveur VPN situé à un autre endroit, un autre pays, masquant ainsi la véritable destination et le contenu de votre trafic à votre FAI.

Gardez à l'esprit que certains gouvernements interdisent l'utilisation du VPN ou peuvent essayer de détecter et de bloquer les connexions VPN. Il est également important d'utiliser un fournisseur de VPN digne de confiance, et de préférence un fournisseur qui ne stocke ni données ni registres d'activité, car votre activité sur Internet lui sera accessible. Renseignez-vous sur le pays d'accueil du fournisseur du VPN et sur les procédures juridiques auxquelles il peut être soumis selon sa juridiction. Considérez également que les VPN approuvés par le pouvoir en place peuvent en fait permettre la surveillance et l'inspection de vos données.

## **Serveurs DNS**

Les serveurs DNS ("domain name system") fonctionnent en traduisant les noms de domaine ou les URL qu'un utilisateur saisit dans un navigateur en adresses IP numériques qu'Internet utilise pour identifier les pages Web. Un FAI peut modifier les serveurs DNS qu'il contrôle pour bloquer certaines requêtes, ou renvoyer un message d'erreur indiquant que le site n'existe pas. En 2014, le Premier ministre turc Recep Tayyip Erdoğan [a tenté de bloquer Twitter](#) lors des élections turques en utilisant cette technique. L'interdiction a été [rapidement contrecarrée](#) par des militants qui ont partagé des tutoriels étape par étape sur la façon d'utiliser les VPN et de changer de serveurs DNS.

Vous pouvez modifier le serveur DNS par défaut dans les paramètres réseau ou Wi-Fi de votre téléphone. Au lieu du serveur DNS par défaut, vous pouvez utiliser des alternatives telles que [Google Public DNS](#).

Voici deux manières de contourner les techniques de blocage les plus courantes. Consultez les très utiles guides de [Internet Society](#), [Access Now](#), [Security-in-a-Box](#) ou encore [EFF](#) pour obtenir des informations plus détaillées.

\*\*\*\*\*