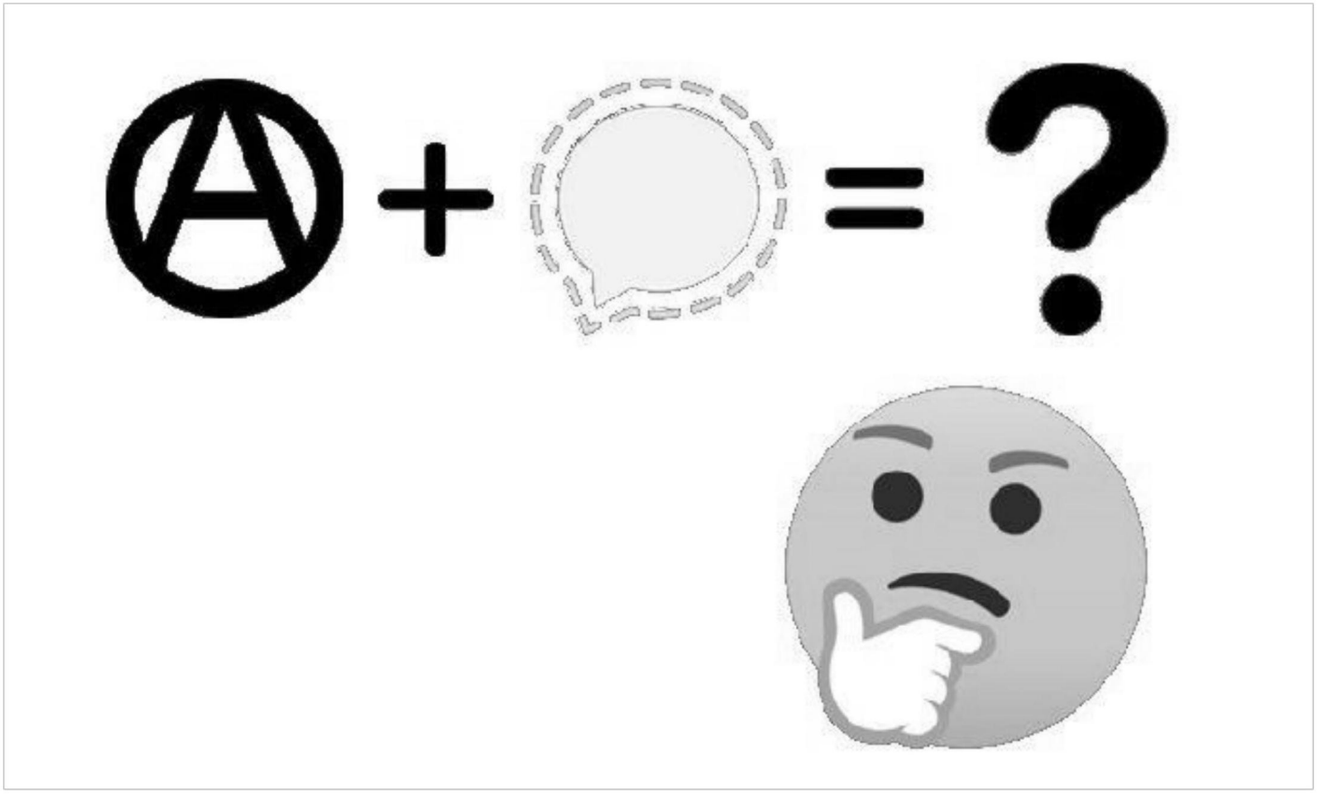


Signal *fails*

A propos de cette brochure et de sa traduction

La brochure qui suit a été initialement publiée en anglais, vous trouverez le lien vers l'original en dernière page. Je suis tombé dessus par hasard en me promenant sur les internets. Assez vite j'ai été frappé de voir à quel point l'auteur·e pointait du doigt les mêmes problèmes auxquels j'ai pu être confronté avec Signal – pour celleux qui l'ignorent encore Signal est une messagerie chiffrée utilisable depuis un smartphone ou un ordinateur, la première partie de la brochure revient plus longuement sur son origine et son usage. Ces derniers mois, la majorité de mon entourage s'est mis à utiliser Signal. L'existence de cette application m'a pas mal convaincu de posséder un smartphone, et je ne crois pas être le seul.

Visiblement en Amérique du Nord le phénomène s'est déjà produit il y a quelques années, entraînant un certain bouleversement des pratiques et des relations sociales dans les milieux autonomes. La même chose commence à arriver ici, en France, et comme l'explique l'auteur·e, il n'y a pas que du bon là-dedans. Si j'évoque l'injonction à être joignable en permanence, la surévaluation de la protection amenée par Signal, l'exclusion sociale des personnes non pourvu·e·s de Signal, les groupes où se répandent des vents de panique, etc, je suis sûr que ça parlera à beaucoup de monde. Tout ceci, et beaucoup d'autres choses sont discutées dans cette brochure, plus quelques conseils pour éviter les erreurs les plus grossières, et à minima inciter chacun·e à questionner et discuter son usage de Signal.

N'étant pas vraiment bilingue, quelques erreurs de traductions se sont sûrement glissées à quelques endroits, notamment lorsqu'il s'agissait de retranscrire de l'argot. Le texte original ayant été écrit depuis le Canada anglophone les références ne collent pas toujours avec la France, surtout lorsque sont évoqués des textes de lois. J'ai fait le choix modifier le texte à la marge, en ajoutant parfois des notes propres au contexte français. ■

Signal est une messagerie chiffrée existant sous différentes formes depuis environ 10 ans. Depuis, j'ai pu être témoin de son adoption dans les milieux anarchistes du Canada et des USA. De plus en plus, pour le meilleur et le pire, nos conversations personnelles ou de groupes ont lieu sur Signal, à tel au point que c'est devenu le moyen de communication privilégié des anarchistes sur ce continent, avec très peu de discussions publiques sur ce que ça implique.

Signal n'est qu'une application smartphone. On est aujourd'hui face à un changement de paradigme, on tend vers une vie où les écrans de smartphones et les réseaux sociaux deviennent des intermédiaires de plus en plus présents. Il n'a fallu que quelques années pour que les smartphones deviennent nécessaires à quiconque veut des amis ou cherche un travail, à quelques exceptions près. Jusqu'à peu, la sous-culture anarchiste était l'une de ces exceptions, où l'on pouvait refuser de posséder un smartphone et avoir une existence sociale. Maintenant j'en suis moins sûr, et c'est bien déprimant. Alors avec ce texte je vais répéter obstinément qu'il n'y a pas de substituts à des relations en face à face dans le monde réel, avec toute la richesse et la complexité du langage corporel, des émotions, du contexte physique, et que cela reste le moyen le plus sûr d'avoir une discussion privée. Alors s'il vous plait, laissons nos téléphones chez nous, retrouvons-nous dans la rue ou dans des forêts, conspirons ensemble, jouons de la musique, construisons des choses, détruisons-en d'autres et entretenons une vie hors-ligne. Je crois que c'est bien plus important que d'utiliser Signal correctement.

L'idée de ce texte m'est venu il y a environ un an, chez des amis d'une autre ville, alors que je blaguais sur les conversations Signal qui tournent au naufrage. Ça leur a tout de suite fait écho, et j'ai commencé à réaliser qu'il se passait la

même chose un peu partout. Quand j'en parlais autour de moi, tout le monde avait son avis et ses reproches, mais peu de pratiques collectives avaient été imaginées. Alors j'ai conçu une liste de questions que j'ai fait circuler. J'ai été agréablement surpris de recevoir une grosse douzaine de réponses détaillées, qui complétées par des discussions informelles, ont permis de constituer ce texte[1].

Je ne suis pas une experte – je n'ai pas étudié la cryptographie et je ne sais pas coder. Je suis un anarchiste qui s'intéresse à la sécurité globale mais qui est sceptique envers les technologies. Mon objectif avec ce texte est de montrer comment Signal est devenu central dans les modes de communication des anarchistes, d'évaluer les conséquences sur la sécurité collective et l'organisation sociale, et d'avancer quelques propositions pour développer des pratiques communes.

1. Merci à tou·te·s les participant·e·s ! Je vous ai volé beaucoup d'idées

Un bref historique de Signal

Il y a 25 ans, les plus techno-optimises parmi nous voyaient dans les prémices d'internet le potentiel d'un formidable outil émancipateur. Vous vous souvenez de ce vieux reportage sur CBC qui faisait l'éloge « d'un réseau d'ordinateurs appelé Internet » comme une « anarchie modulée » ? Bien qu'il y ait toujours des façons de communiquer de manière sécurisée, de se coordonner et de diffuser des idées en ligne, il est évident que l'État et les entreprises ont graduellement conquis de plus en plus d'espace en ligne pour nous soumettre à la surveillance et à un contrôle social de plus en plus poussé[2].

Internet a toujours été une course à l'armement. En 1991, un civil, Phil Zimmerman[3], cryptographe, libertaire et militant pacifiste, crée PGP, un logiciel open source qui permet de chiffrer ses fichiers et ses mails de bout en bout (*end to end*). J'éviterai les détails techniques, mais l'importance du procédé de chiffrement de bout en bout est de pouvoir communiquer directement et de manière sécurisée avec une autre personne, sans que votre service mail (que ce soit Google ou Riseup) puisse lire le message. Jusqu'à présent, autant que l'on en sache, le chiffrement PGP n'a jamais été brisé[4].

Pendant des années, bidouilleuses et bidouilleurs, geeks de certains milieux – anarchistes, journalistes, criminel·le·s, etc. –

2. Les modes de gouvernances à l'ère d'internet varient selon les endroits – les États autoritaires choisissent le filtrage et la censure, quand les démocraties créent ne sorte de « citoyenneté digitale » – mais la surveillance de masse et la cyber guerre deviennent la norme.

3. Ironiquement, le gouvernement des USA essaya plus tard d'inculper Zimmerman pour avoir librement publié le code source de PGP, en disant qu'il « exportait une arme ». Il a alors publié le code source dans un livre papier, et l'a posté aux quatre coins du monde, l'exportation des livres étant protégée par la Constitution américaine.

4. Le procès contre les Nouvelles Brigades Rouges en Italie (2003) et des pédopornographes aux USA (2006) ont démontré que les polices n'arrivent pas à briser PGP.

ont essayé de diffuser PGP dans leurs réseaux, en le présentant comme un mode de communication sécurisé, et y sont parvenu·e·s avec un certain succès. Mais tout a ses limites. Ce qui me chiffonne le plus avec PGP[5] est le manque de confidentialité persistante (*forward secrecy*) : cela signifie que si une clef de chiffrement est compromise, tous les mails envoyés avec cette clef jusqu'à ce jour peuvent être déchiffrés. C'est un vrai soucis, étant donné que la NSA a sûrement stocké quelque part chacun de vos mails chiffrés, et un jour un ordinateur quantique brisera PGP. Ne me demandez pas comment marche un ordinateur quantique – autant que j'en sache, c'est de la magie.

Le gros problème social avec PGP, qui a beaucoup influencé le projet Signal, c'est que son usage est resté marginal. Dans mon cas, il était même compliqué d'amener des anarchistes à utiliser PGP et à s'en servir proprement. Pendant les ateliers, beaucoup s'équipaient, mais dès qu'un ordinateur plante ou qu'un mot de passe est perdu, c'était retour à la case départ. Ça ne marchait tout simplement pas.

Vers 2010, les smartphones se sont répandus et tout a changé. L'ubiquité des médias sociaux, le textotage constant et la possibilité pour les compagnies téléphoniques (et donc les gouvernements) de pister les usagers et usagères[6] avait complètement changé la menace. Tous les efforts mis à améliorer la sécurité des ordinateurs étaient caduques : les smartphones ont une architecture différente des PC, amenant bien moins de contrôle, et l'arrivée des applications aux autorisations imposées rend risible l'idée d'avoir un smartphone sécurisé.

5. Jusqu'à récemment, PGP ne chiffrait pas les métadonnées (qui écrit à qui, sur quel serveur, quand, etc), ce qui était un gros problème. Un avocat de la NSA déclarait un jour « Si vous avez assez de métadonnées, vous n'avez pas vraiment besoin du contenu ».

6. Vous voulez lire un truc effrayant ? Renseignez-vous sur Google Sensorvault

C'est dans ce contexte que Signal est apparu. Le « cypherpunk » anarchiste Moxie Marlinspike commença à créer un logiciel pour amener le chiffrement de bout en bout sur smartphone, avec la confidentialité persistante, partant du principe que la surveillance de masse devait être contrée par le chiffrement de masse. Signal a été conçu pour être pratique, joli et sécurisé. Moxie accepta de travailler avec des géants de l'informatique comme WhatsApp, Facebook, Google et Skype pour aussi intégrer le protocole de chiffrage de Signal sur leurs plateformes.

« Notre grande victoire est que des millions de personnes utilisent WhatsApp et ilselles ne savent même pas que c'est chiffré » Moxie Marlinspike

Comprenons-nous, les anarchistes sont plus encleints·e·s à faire confiance à Signal – une fondation non lucrative dirigée par un anarchiste – qu'ilselles ont à faire faire confiance aux grosses entreprises technologiques, dont le principal business est de récolter et vendre les données des utilisateurs et utilisatrices. Signal a des avantages par rapport à ces plate-formes : open-source (et donc sujet à être revue par des paires), chiffre la plupart des métadonnées, stocke le moins de données possible, et offre des options très pratiques comme les messages éphémères et les numéros de sécurité pour se prémunir des interceptions.

Signal a été presque universellement salué par les expert·e·s en sécurité informatique, y compris par le lanceur d'alerte de la NSA Edward Snowden et a reçu la meilleure note de la respectée Electronic Frontier Fondation. En 2014, une fuite de document de la NSA décrivait Signal comme « une menace majeure » à sa mission (savoir tout sur tout le monde).

Personnellement, j'ai confiance en son chiffrement.

Mais Signal ne protège réellement qu'une chose, votre communication lorsqu'elle passe de votre appareil à un autre. C'est bien, mais ce n'est qu'une partie d'une stratégie de confidentialité. C'est pourquoi, lorsqu'on parle de sécurité, il est important de partir d'un Modèle de Menace. Les premières questions pour n'importe quelle stratégie de confidentialité sont : qui est l'adversaire, que veut-il connaître, et comment va-t-il tenter de le savoir ? L'idée de base c'est que les choses et les pratiques ne sont sécurisées ou non sécurisées que selon le type d'attaque dont on imagine devoir se défendre. Par exemple, il est inutile que vos données soient chiffrées avec très une bonne clef et le meilleur mot de passe si votre adversaire est prêt à vous torturer jusqu'à ce que vous craquiez.

Ici, je proposerai un Modèle de Menace fonctionnant face à deux types d'adversaires. Le premier est une agence de renseignement globale ou de puissants hackers faisant de la surveillance de masse et interceptant des communications. Le deuxième est un service de police, qui opère sur un territoire contrôlé par le Canada ou les USA, surveillant des anarchistes. Pour les flics, les bases de l'investigation incluent la surveillance de liste mails et des réseaux sociaux, l'envoie de flics en civils à des événements, et le recrutement d'indics. Lorsqu'ils ont plus de moyens, ou que notre réseau devient une priorité, ils passent aux moyens d'interceptions, aux perquisitions, aux saisies d'appareils pour analyses.

Notons que beaucoup de législations européennes contiennent une obligation pour les individus de livrer leurs clefs de chiffrement sous peine de prisons[7]. Peut-être que ce

7. C'est le cas en France avec l'article 434-15-2 du code pénal. Mais c'est circonscrit à certaines conditions, et à la décision d'un juge. Le déni plausible (https://en.wikipedia.org/wiki/Plausible_deniability#Use_in_cryptography), la confidentialité persistante, et la destruction des données chiffrées sont intégrés à certains outils de sécurité informatique, pour contrer ou du moins minimiser cette menace.

n'est qu'une question de temps, mais pour l'instant au Canada comme aux USA, nous ne sommes pas légalement contraint·e·s de dévoiler nos mots de passes aux autorités, sauf si l'on franchit une frontière[8].

Si vos appareils sont compromis par un keylogger, ou un autre logiciel malveillant, peu importe à quel point vos communications sont sécurisées. Si vous parlez avec une poucav ou un flic en civil, peu importe que vous soyez dans un parc avec la batterie de votre téléphone préalablement retirée. Ce texte ne traite pas des outils de sécurité informatique et de culture de la sécurité, mais ces concepts sont à prendre en compte pour se prémunir de ces deux menaces bien réelles. J'ai inclus quelques suggestions dans la section Pour aller plus loin.

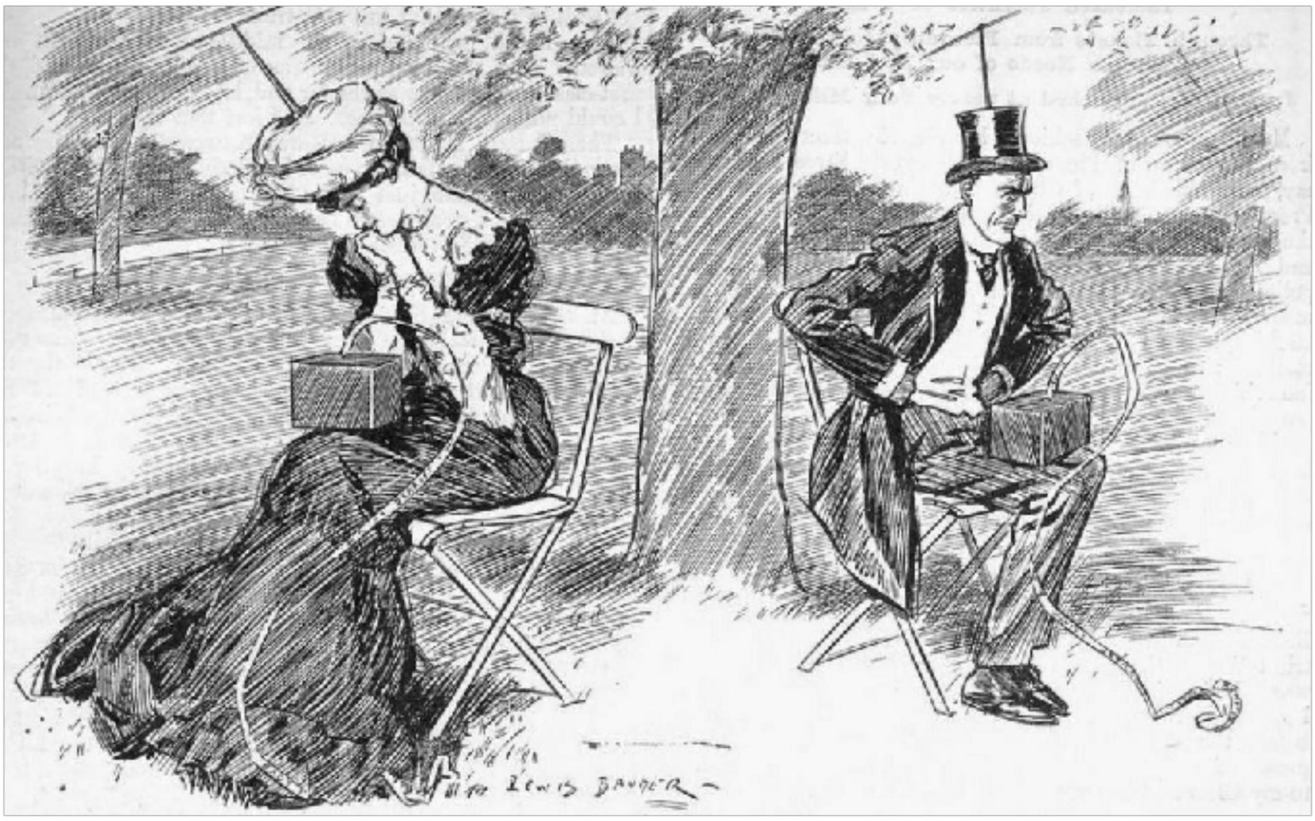
Il faut aussi mentionner que Signal n'est pas conçu pour l'anonymat. Votre compte Signal est enregistré avec un numéro de téléphone, à moins que vous ayez enregistré un portable à usage unique ou un numéro jetable en ligne vous n'êtes pas anonyme. Si vous perdez le contrôle de votre numéro de téléphone utilisé pour enregistrer votre compte, quelqu'un·e d'autre pourrait voler votre compte. C'est pourquoi il est hyper important, si vous utilisez un numéro anonyme pour un compte, d'activer l'option « blocage de l'inscription ».

Avant tout pour des raisons de sécurité, Signal est devenu le médium de communication standard parmi les anarchistes ces quatre dernières années, éclipsant tout le reste. Mais de la même manière que « le médium est le message », Signal a d'importants effets sur la façon dont les anarchistes s'organisent, des effets souvent négligés.

8. Dans beaucoup d'États, les empreintes digitales (et autres données biométriques) ne sont pas considérés comme des mots de passe, les verrouillages par empreinte digitale ne bénéficie pas des mêmes protections légales

La sociabilité Signal

« Signal est utile lorsqu'il remplace des formes de communications électroniques moins sécurisées, mais il devient mauvais…lorsqu'il remplace la discussion face à face » Un·e contributeur·trice



La plupart des conséquences de Signal ne sont pas spécifiques à l'application. Ce sont les conséquences du déplacement croissant de nos communications, expressions personnelles, efforts d'organisations, et tout le reste, vers des plateformes virtuelles médiatisées par des écrans. Mais ce que j'ai compris en lisant les réponses à mes questionnaires c'est qu'avant Signal, je connaissais plusieurs réfractaires aux smartphones que ce soit pour des raisons de sécurités ou de sociabilité. Quand Signal arriva avec une réponse aux principaux problèmes de sécurité, la position réfractaire a été significativement affaiblie. Aujourd'hui, la plupart des personnes qui refusaient les smartphones en ont un, soit parce qu'ilselles ont été convaincu d'utiliser Signal, soit parce que Signal est devenu obligatoire si l'on souhaite être inclus·e.

Signal a été un porte d'entrée vers les smartphones pour certain·e·s anarchistes. D'un autre côté, Signal réduit les risques pour celleux qui avaient déjà adopté les smartphones, et c'est une bonne chose. Je suis heureuse que des personnes qui sociabilisaient et s'organisaient sur des réseaux non chiffrées comme Facebook soient passé·e·s sur Signal. Dans mon quotidien, la conversation de groupe a remplacé la « petite liste mail », c'est pratique pour s'organiser avec ses amis ou partager des liens. Dans les réponses que j'ai collectées, le groupe Signal considéré comme le plus utile, ou le moins chiant, était ceux qui restaient restreints, spécifiques et pragmatiques. Signal est aussi un puissant et sûr moyen de diffuser une information urgente nécessitant une réponse rapide. Si l'organisation via Facebook a convaincu trop d'anarchistes que s'organiser en pouvant surprendre était impossible, Signal a en partie sauvé cette idée, et c'est bien.

Les échecs de Signal

J'avais imaginé ce projet comme une courte série de BD intitulées *« Les échecs de Signal »*, une pâle copie du livre *« Come Hell or High Water : A handbook on Collective Process Gone Awry »*. Il se trouve que c'est difficile de représenter Signal avec des images intéressantes, et que je suis nul en dessin. Désolé si j'avais promis ça, peut être pour une seconde édition…Bref, je vais partager quelques *« Échecs de Signal »* comme un moyen de se moquer de nous (moi y compris !) et peut être pour gentiment inciter tout le monde à être moins chiant.

Bond, James Bond : Avoir Signal ne vous rend pas invincible. Donne un peu de chiffrement à des personnes, et ilselles vont immédiatement imposer les trucs les plus tricards à tous leurs contacts. Votre téléphone est toujours un outil de flicage, et

la confiance est toujours quelque chose à construire. Parlez entre vous de ce que vous voulez bien dire au téléphone, et ce de que vous ne voulez pas dire.

Le silence n'est pas du consentement : déjà été à une réunion, planifié des choses, créé un groupe Signal pour la logistique, et ensuite avoir une ou deux personnes qui rapidement change le plan collectivement établi par une suite de messages auxquels personne n'a le temps de répondre ? Pas sympa.

L'enfer est une réunion éternelle : Un groupe Signal n'est pas une réunion. Je suis déjà trop souvent scotchée à mon téléphone, donc je n'aime pas être inondée par les messages de deux personnes discutant frénétiquement d'un sujet, ni par les états d'âme hors sujets d'une personne. J'apprécie les conversations qui ont un début et une fin.

Le flux : Je déteste particulièrement celui-là. Probablement à cause des réseaux sociaux, certain·e·s sont habitué·e·s à avoir une information déjà traitée et organisée pour nous par une plateforme. Mais, heureusement, Signal n'est pas un réseau social. Alors faites gaffe, lorsqu'un gros groupe Signal devient Le Flux, vous êtes mal. Si vous n'en faites pas parti·e·s ou que vous n'êtes pas attenti·f·ve·s, vous allez rater un tas d'informations importantes : prochains événements, personnes changeant de pronoms, ou joutes verbales menant à des conflits. Les gens vont oublier que vous existez et, éventuellement, vous disparaîtrez. TUEZ LE FLUX.

Feu dans un théâtre bondé : alias le problème du bouton panique. Vous être sur un gros groupe Signal avec tous vos potes chelou·e·s et leurs vrais numéros de téléphones, quand quelqu'un·e est arrêté·e pour un vol ou autre, et *surprise* son téléphone n'est pas chiffré ! C'est la panique à bord, tout le monde quitte le navire , mais c'est un peu trop tard, parce que si les flics sont en trains de regarder le téléphone en ce

moment même, ils peuvent voir toute personne quittant la conversation, et la carte sociale est faite. Tou doum tchi !

À la dérive : Un groupe est créé pour coordonner un événement spécifique et limité dans le temps. C'est fini, mais personne ne quitte le groupe. Désormais, cet outil spécifique et temporaire est l'ORGANISATION PERMANENTE décidant ce tout à propos de tout – indéfiniment.

Vers des pratiques communes

Si vous pensiez que ceci était un guide des bonnes pratiques sur Signal, ou des bonnes manières de discuter, désolé vous êtes arrivé·e·s jusque-là sans réaliser que ce n'était pas le cas. C'était plus une manière de dire « il faut que l'on parle de Signal ». Je crois au développement de pratique partagées spécifiques à des contextes particuliers, et je

conseille d'initier ce débat dans nos réseaux. Dans ce but, j'ai quelques propositions.

Il y a des obstacles aux pratiques communes. Des personnes n'ont pas Signal. Si c'est parce qu'ilselles construisent des relations sans smartphones, je n'ai que du respect pour ça. Si c'est parce qu'ilselles passent leurs journées sur Facebook mais que Signal « c'est trop compliqué », je ne cautionne pas. En dehors de ça, Signal est facile à installer et à utiliser pour n'importe qui avec un smartphone et une connexion internet

Je suis aussi en désaccord avec la vision orwellienne et fataliste imaginant le chiffrement inutile : « les condés savent déjà tout ! ». C'est très paralysant de voir l'État de cette façon, et heureusement ce n'est pas vrai – la lutte n'est pas encore inutile. La NSA et la DGSI ont des capacités, connues ou non, effrayantes. Mais il est largement prouvé que le chiffrement freine les investigations policières, ce pourquoi les gouvernements passent des lois contrecarrant ces outils. Peut-être le plus gros obstacle aux pratiques partagés est le manque général de « nous » – à quel point somme-nous redevables des autres, et si nous le sommes, de qui ? Comment s'y prendre pour construire éthiquement des normes sociales communes ? La plupart des anarchistes pensent qu'il ne faut pas parler aux flics, par exemple, mais comment en sommes-nous arrivé·e·s là ? Je pense qu'une sorte d'individualisme libéral est en train d'influencer l'anarchisme faisant de l'importante question des « objectifs » un quasi tabou. Mais c'est un autre sujet.

Quelques propositions de bonnes pratiques

1. *N'oublie pas l'IRL* – Comme l'a dit un·e contributeur·trice, « la communication n'est pas qu'un partage d'information ». La communication face à face dans le monde réel construit des relations pleines, ce qui inclue la confiance, et reste le moyen le plus sûr de communiquer.

2. *Laisse ton téléphone chez toi* – Au moins de temps en temps ? Surtout lorsque vous traversez une frontière, car vous pouvez être forcé de déchiffrer vos données. Si vous avez besoin d'un téléphone pendant votre voyage, achetez avec vos amis un téléphone qui ne contient pas de données sensibles, cela inclue l'absence de liste de contacts.

3. *Sécurise ton appareil* – La plupart des téléphones (et des ordinateurs) ont une option permettant de chiffrer entièrement le disque dur. La qualité du chiffrement dépend de celle de votre mot de passe et protège vos données « au repos ». Quand votre appareil est éteint. Votre écran de verrouillage protège votre appareil lorsqu'il est allumé, mais peut être contourné par une attaque sophistiquée. Certains systèmes d'exploitations obligent à avoir le même mot de passe pour le chiffrement et l'écran de verrouillage, ce qui est malheureux, car ce n'est pas pratique de rentrer un long mot de passe 25 fois par jour (parfois entouré·e de regards indiscrets ou de caméras de surveillances).

4. *Éteins ton appareil* – si vous laissez votre appareil sans surveillance, ou que vous allez dormir, éteignez-le. Achète un réveil pas cher (voles en un cher). Si ton domicile est perquisitionné au petit matin, vous serez ravi·e·s d'avoir votre ordinateur éteint. Si votre appareil est chiffré avec un bon mot de passe et éteint, il est peu probable que les flics

réussissent à lire vos données. Si vous voulez faire un pas en plus, trouvez un coffre fort et enfermez votre appareil dedans lorsque vous n'en avez pas besoin. Cela réduit les risques qu'il soit physiquement trafiqué.

5. *Fixez des limites* – Nous avons des seuils différents de ce dont on veut et ne veut pas discuter au téléphone. Parlez-en et créez des limites collectivement. En cas de désaccord, respectez les limites des autres même si vous estimez qu'elles sont superflues.

6. *Mettez en place un système de cooptation* – Si vous participez à un groupe discutant de sujets sensibles, créez et explicitez collectivement la manière dont une nouvelle personne peut rejoindre le groupe. À une époque où être anarchiste expose à une instruction pour association de malfaiteurs, un manque de communications à ce sujet peut envoyer des personnes en taule.

7. *Demandez d'abord* – si vous allez ajouter une personne à une discussion, dévoilant ainsi son numéro de téléphone à tout le groupe, demandez avant le consentement de la nouvelle personne et de tout le groupe.

8. *Minimisez la prise de décision* – Toutes types de décisions demandant une autre réponse que oui/non doivent être réservés aux réunions dans le monde réel, si possible. De mon expérience, Signal appauvrie les processus de décision.

9. *Définissez un but* – Idéalement, un groupe Signal a un but spécifique. Chaque nouvelle personne intégrée doit avoir ces buts clairement expliqués. Si les buts sont atteints, quittez et supprimez le groupe.

10. *Message éphémère* – Très utile pour faire le ménage. Allant de 5 secondes à 1 semaine, les messages éphémères peuvent être configurés en allant sur les trois points en haut à droite d'une conversation. Beaucoup de monde utilise par

défaut la limite d'une semaine, que la conversation soit sensible ou non. Choisissez votre temps d'expiration selon votre modèle de menace. Cela vous protège aussi si la personne avec qui vous communiquez n'a pas des pratiques de sécurité optimales.

11. *Vérifiez le numéro de sécurité* – C'est la meilleure protection contre une attaque du type interception des messages (*man-in-the-middle*). C'est assez simple à faire et plus facile physiquement – ouvrez votre conversation avec la personne que vous voulez vérifier et allez dans Paramètres > Paramètres de la conversation > Confidentialité > Afficher le numéro de sécurité et scannez le QR code ou comparez les numéros. La plupart des personnes interrogées répondent « je devrais le faire, mais non » . Profitez des gros rassemblements pour vérifier vos contacts. Passer pour un geek n'est pas un souci !

12. *Activez le blocage de l'inscription* – Faites le dans les paramètres Confidentialités de l'application, ainsi si une personne pique votre numéro de téléphone pour enregistrer votre compte, il devra avoir votre PIN pour voler votre identité. C'est particulièrement important pour les comptes Signal anonymes enregistrés avec une carte Sim à usage unique, puisqu'il est presque certains que ce numéro de téléphone soit réutilisé.

13. *Désactivez la prévisualisation des messages* – Empêchez les messages d'apparaître sur l'écran de verrouillage. Dans mon cas, j'ai dû configurer ça dans les paramètres de l'appareil (pas de Signal).

14. *Supprimez les vieux messages* – Soit en activant une limite à la taille des conversations (Paramètres > Conversation et médias > Élagage des messages), soit en supprimant manuellement les conversations entièrement. Ne gardez pas des messages dont vous n'avez plus besoin.

Conclusion

J'ai commencé ce projet pour montrer et comprendre l'impact de Signal sur les réseaux anarchistes aux USA et au Canada, du point de vue de la sécurité et de l'organisation sociale. Ce faisant, je crois avoir rencontrée une frustration assez partagée, spécialement à propos des gros groupes Signal, et réunis quelques idées à faire circuler. J'insiste encore, parce que c'est important pour moi, les smartphones font plus de mal que de bien à nos vies et à nos luttes. Nous devons préserver et construire ensemble d'autres moyens d'organisations, surtout hors ligne, pour la qualité de nos vies et la sécurité du mouvement. Si nous gardons des smartphones, il est dangereux que nos communications soient centralisées. Si les serveurs de Signal, Riseup, ou Protonmail, s'arrêtaient, imaginez combien ce serait dévastateur pour nos réseaux. Si les anarchistes venaient à devenir une menace imminente à l'ordre établi, ils viendraient sans pitié pour nous et nos infrastructures, y compris en suspendant les « protections légales » dont nous pourrions dépendre.

Pour le meilleur et pour le pire, je crois à la possibilité de ce scénario, alors nous devons être résilient·e·s. Les geeks parmi nous devraient continuer à expérimenter d'autres protocoles, d'autres logiciels et systèmes d'exploitations[9], les partager et prouver leur utilité. Les réfractaires doivent tenir, et trouver des moyens de se développer hors ligne. Pour le reste d'entre nous, diminuons notre degré de dépendance aux smartphones. De même que nous devons développer notre

9. Sur mon téléphone, j'ai récemment remplacé Android par LineageOS, un système d'exploitation dé-googelisé conçu pour protéger la vie privée. C'est génial, mais conçu uniquement pour quelques modèles de téléphones, ça annule votre garantie, et il faut du temps pour apprendre à le configurer, le garder à jour et adopter les applications open-source.

capacité à lutter, nous devons mener des vies qui valent le coup, avec une qualité relationnelle que des amis et co-conspirateurs potentielles trouveront fascinantes. C'est là peut être notre seul espoir. ■

Pour aller plus loin

Signal est mis à jour régulièrement. Pour les dernières informations techniques, allez sur signal.org, community.signalusers.org, et /r/signal sur reddit.

En anglais

Your Phone is a Cop
https://itsgoingdown.org/phone-cop-opsecinfosec-primer-dystopian-present/

Choosing the Proper Tool for the Task
https://crimethinc.com/2017/03/21/choosing-the-proper-tool-for-the-task-assessing-your-encryption-options

Towards a Collective Security Culture
https://crimethinc.com/2009/06/25/towards-a-collective-security-culture

Toronto G20 Main Conspiracy Group: The Charges And How They Came To Be
https://north-shore.info/archive/

En français

Guide d'autodéfense numérique
https://guide.boum.org/

Guide de sécurité Riseup
https://riseup.net/fr/security

Guide de self-défense face à surveillance par la Fondation Frontières Électroniques
https://ssd.eff.org/fr/module-categories/guides-sur-les-outils

Ne jamais éteindre son téléphone : une nouvelle approche à la culture de la sécurité
https://iaata.info/Ne-jamais-eteindre-son-telephone-une-nouvelle-approche-a-la-culture-de-la-2943.html

Cette brochure a été initiallement publiée en anglais en mai 2019 sur North Shore Counter-Info [https://north-shore.info]. La version française est parue en juillet 2019.

Pour contacter l'auteur·e anglophone,
signalfails [at] riseup [point] net