



# Outils de planification de la sécurité technologique en matière de VFGFT

## Une note sur la langue

Dans cette trousse, nous utiliserons parfois le mot femme et les pronoms féminins par souci de simplicité et pour reconnaître l'impact significatif de la violence facilitée par la technologie sur les femmes et les filles. Nous reconnaissons que la VFGFT a également un impact sur les personnes trans, non binaires et bispirituelles. Nous espérons que toutes les personnes touchées par la VFGFT trouveront ces documents utiles.

## Documenter la violence technologique

La façon dont la technologie est utilisée à des fins de harcèlement et de contrôle peut vous sembler invraisemblable. Cependant, il est important de faire confiance à votre instinct. Si vous pensez être surveillée ou harcelée par le biais de la technologie, c'est peut-être le cas. Le fait de préciser ce qui arrive, y compris les tactiques et les technologies utilisées, peut aider à déterminer s'il s'agit de violence fondée sur le genre facilitée par la technologie (VFGFT) et, le cas échéant, comment y remédier.

Voici quelques bonnes raisons de documenter tout ce qui vous arrive:

- Vous aurez une vue d'ensemble de la situation, ce qui peut s'avérer utile si vous souhaitez engager une action en justice.
- Vous serez alertée de toute escalade dans la surveillance et le contrôle, ce qui peut signaler que le danger augmente.
- Cela vous aidera à repérer les schémas de VFGFT et à déterminer comment l'auteur de violence utilise une technologie ou une autre.

## Conseils pour la documentation

- **Tenez un journal de tous les incidents**, même si vous n'êtes pas certaine de vouloir faire appel à la police. Parmi les informations que vous pouvez inclure, citons la date, l'heure, le lieu, les coordonnées de l'agent·e de police (si l'incident a été signalé), les témoins (s'il y en a), la technologie présumée utilisée (téléphone, courriel, etc.), et enfin, une brève description des faits.
- **Prenez-en note tout ce qui concerne l'événement ou l'incident.** Si vous recevez un message menaçant par courriel, SMS ou messagerie vocale, assurez-vous de le sauvegarder. Prenez une photo ou une capture d'écran. Même s'il peut être tentant de les supprimer, sauvegarder les messages pourrait révéler des tendances utiles pour établir des stratégies de sécurité et fournir les preuves nécessaires.
- **Réfléchissez à la technologie que l'auteur pourrait utiliser.** Dans certains cas, les femmes ont de forts soupçons quant à la technologie utilisée par l'auteur de violence en fonction du type d'abus, des tactiques de l'auteur et de ce qu'elles savent de lui.
- **Pensez d'abord à votre sécurité.** Dans certains cas, lorsqu'un auteur apprend qu'une femme documente les abus, la surveillance, le contrôle et la violence physique peuvent s'intensifier. Vous êtes la mieux placée pour évaluer la situation et les différents scénarios possibles. Faites confiance à votre instinct et veillez au mieux à votre sécurité.
- **Ne documentez que les informations pertinentes.** Gardez à l'esprit que ces informations pourraient éventuellement servir de preuves ou être partagées par inadvertance avec l'auteur des faits. Par exemple, vous ne souhaitez peut-être pas documenter des photos personnelles qui ne sont pas utilisées dans le cadre de la violence numérique.

## Ce qu'il faut documenter

### Courriels

- Les courriels contiennent des adresses IP qui pourraient révéler l'adresse IP d'origine et, par conséquent, l'identité de la personne qui a envoyé le message. Pour cette raison, il importe de ne pas supprimer le courriel et de ne pas le transférer.
- Si vous sauvegardez le contenu d'un courriel en l'imprimant ou en faisant des captures d'écran, veillez à sauvegarder également l'en-tête (souvent caché et pouvant être trouvé dans les paramètres). C'est là que sont stockées les informations IP. L'accès à l'en-tête peut varier en fonction de la messagerie que vous utilisez (Gmail, Outlook, Yahoo! Mail, etc.).
- Si vous craignez que l'auteur puisse accéder au compte et supprimer des courriels, il est suggéré d'imprimer ou de faire des captures d'écran du contenu, y compris des en-têtes. Les courriels transférés perdront les informations d'identification nécessaires à l'établissement de preuves.

### Messages texte

- Les messages texte (SMS) qui sont simplement stockés sur un téléphone peuvent être supprimés par inadvertance ou être automatiquement supprimés si vous manquez d'espace. Faites une capture d'écran ou une photo des SMS pour conserver les preuves.
- Faites également une capture d'écran de la page de contact pour montrer que les messages de harcèlement de l'auteur sont associés à son numéro de téléphone.
- Le contenu des SMS n'est conservé par le fournisseur de téléphonie mobile que pendant une durée limitée. Si vous travaillez avec les forces de l'ordre, demandez-leur d'envoyer une lettre au fournisseur de téléphonie dès que possible, pour l'aviser de ne pas détruire les données.

## Harcèlement dans les médias sociaux et sur Internet

- Pour conserver des preuves de harcèlement sur les médias sociaux, faites une capture d'écran du harcèlement ou de l'abus sur votre ordinateur ou appareil mobile.
- Certains sites proposent d'autres moyens de documenter l'activité sur le site ou sur votre page. Par exemple, en utilisant la fonction «Télécharger vos informations» (DYI) de Facebook, vous pouvez capturer tout le contenu et l'enregistrer pour plus tard.
- En cas de collaboration avec les forces de l'ordre, une lettre peut être envoyée à l'entreprise de médias sociaux ou au site Web pour leur demander de conserver les informations du compte, ou contactez l'équipe du [Service d'entraide internationale du ministère de la Justice](#).
- Vous pouvez envisager de signaler le harcèlement à l'entreprise de médias sociaux ou au site web. N'oubliez pas de documenter d'abord si vous voulez avoir des preuves car, si cela enfreint les conditions d'utilisation du site ou les directives relatives au contenu, l'entreprise peut supprimer le contenu.

## Harcèlement téléphonique

- Vous pouvez envisager d'enregistrer vos conversations téléphoniques pour conserver des preuves de harcèlement ou de menaces, car le Canada autorise l'enregistrement avec le consentement d'une seule partie.

## Usurpation de numéro de téléphone ou d'identité

- Documentez vos journaux d'appels en prenant une photo de l'identifiant de l'appelant. N'oubliez pas d'indiquer la date et l'heure des appels.
- Conservez vos registres téléphoniques pour indiquer le numéro de l'appel d'origine, la date et l'heure.

Notre modèle de journal de la violence facilitée par la technologie peut vous aider à documenter ce qui vous arrive. Pour plus d'informations sur la manière de stocker vos preuves numériques, consultez notre fiche d'information «Comment sauvegarder et stocker les preuves de violence facilitée par la technologie».

*La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Vous pouvez consulter [hebergementfemmes.ca](http://hebergementfemmes.ca) pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de créer un [plan de sécurité](#). Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.*

Adapté pour le Canada avec la permission du Safety Net Project de NNEDV, selon leur ressource [Documenting Abuse](#).

# Journal du harcèlement et des abus facilités par la technologie

## Qu'est-ce qu'un journal sur le harcèlement et les abus facilités par la technologie?

On parle de harcèlement et de violence fondée sur le genre facilitée par la technologie (TFGBV) lorsqu'un auteur de violence utilise la technologie comme outil pour surveiller une personne et lui causer du tort. Il peut s'agir de repérer l'endroit où vous vous trouvez, d'envoyer des SMS de harcèlement et de menacer de partager des images sans votre consentement. Parmi les technologies utilisées à mauvais escient figurent les appareils et les comptes.

Ce document comporte un modèle de journal permettant de documenter la violence en détail. Deux journaux sont fournis, sous forme longue et brève; choisissez celui qui convient le mieux à votre situation.

## Je tiens un journal sur le harcèlement et les abus facilités par la technologie pour:

- Documenter les preuves au moment où les abus se produisent, ce qui les rend plus fiables devant un tribunal
- Étayer les preuves recueillies
- Percevoir les schémas et les escalades en vue de planifier ma sécurité
- Fournir des preuves à la police et au personnel antiviolence un aperçu des risques auxquels je suis confrontée afin de recevoir un soutien adapté à mes besoins
- Reprendre le contrôle de ma vie et être proactive
- Valider mon expérience. Cela peut être utile si l'auteur de violence minimise ou nie ses actions, ou *gaslight* la personne. Le *gaslighting* est une forme d'abus psychologique où l'auteur prétend que l'abus n'a pas eu lieu et accuse la victime de «devenir folle».
- Ne pas oublier le comportement d'un auteur de violence. Les souvenirs peuvent s'estomper avec le temps. Un journal peut renforcer une plaidoirie devant un tribunal ou aider une survivante à décider ce qu'elle doit faire si un partenaire violent tente de rétablir le contact.

## Demeurez en sécurité pendant la collecte des preuves

**Pensez à l'endroit où vous pouvez entreposer vos journaux en toute sécurité. Il peut s'agir d'un bureau fermé à clé au travail, de l'intervenante qui vous soutient ou d'un-e ami-e proche. Faites-vous confiance. C'est vous qui connaissez le mieux votre situation.**

Si vous décidez de fournir vos journaux à la police ou à d'autres services, on vous demandera peut-être des détails supplémentaires sur l'auteur de violence. Ces éléments peuvent inclure des informations sur la technologie utilisée, notamment:

- Informations sur le fournisseur Internet ou téléphonique, et sur le compte;
- Appareils, tels que téléphones, ordinateurs, tablettes, appareils photo, drones, disques durs externes, USB, appareils pour enfants, etc.;
- Comptes ou applis qui ont été utilisés dans le cadre de l'abus, tels les médias sociaux ou les comptes bancaires;
- Adresses courriel, numéros de téléphone, comptes infonuagiques, noms d'utilisateur, avatars, pseudonymes, identifiants en ligne, etc.
- Toute autre information relative aux technologies utilisées: mots de passe, associés en ligne, appareils de surveillance, adresses de fournisseurs Internet, vol d'identité ou fraude, etc.

**Note: Bien qu'il puisse être utile de recueillir les informations ci-dessus si vous pouvez le faire en toute sécurité, ces détails ne sont pas inclus dans le journal de harcèlement car ils ne s'appliquent pas forcément à toutes les situations, ni ne sont toujours susceptibles d'affecter la sécurité. Réfléchissez à une manière créative de documenter les événements, tout en tenant compte de votre sécurité.**

**[Télécharger un journal sur le harcèlement et les abus facilités par la technologie](#)**

La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Vous pouvez consulter [hebergementfemmes.ca](http://hebergementfemmes.ca) pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de créer un plan de sécurité. Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.

Adapté pour le Canada avec la permission du Tech Safety Project de WESNET, d'après leur ressource: [Stalking and Tech-Facilitated Abuse Log](#).

---

Ce document fait partie du projet Sécurité technologique Canada d'Hébergement femmes Canada. Nous vous encourageons à visiter le site [www.securitetechnologie.ca](http://www.securitetechnologie.ca) pour trouver des informations et des ressources supplémentaires sur la violence facilitée par la technologie, la planification de la sécurité technologique et la préservation des preuves numériques. Ce document, ou toute partie de celui-ci peut être reproduit ou utilisé à condition de citer la source. Si vous souhaitez adapter le contenu, veuillez contacter Hébergement femmes Canada à l'adresse [info@endvaw.ca](mailto:info@endvaw.ca).

---

© copyright 2023 Hébergement femmes Canada | Tous droits réservés

Ce projet est rendu possible grâce au financement du ministère Femmes et Égalité des genres Canada (FEGC).



Femmes et Égalité  
des genres Canada

Women and Gender  
Equality Canada

Canada