BC Society of Transition Houses

Préservation des preuves numériques:

Considérations pour les intervenantes antiviolence qui soutiennent les femmes

Les intervenantes antiviolence sont une source précieuse de soutien pour les femmes[1] qui subissent des violences facilitées par la technologie. Elles écoutent les femmes et créent avec elles des plans de sécurité technologique, explorant notamment la manière de collecter en toute sécurité des preuves numériques, dans le cadre du processus de planification de sécurité.

Le personnel antiviolence met l'accent sur les particularités des expériences des femmes, parce qu'elles connaissent leur situation mieux que quiconque et sont souvent les plus aptes à créer un plan de sécurité qui tienne compte de leurs besoins.

La violence facilitée par la technologie étant un phénomène relativement nouveau, les intervenantes antiviolence ne sont peut-être pas familières avec tous les moyens de préserver les preuves numériques ou ne pas connaître tous les rouages du système judiciaire. Cette méconnaissance peut avoir des conséquences négatives sur la préservation adéquate de preuves numériques, et sur les recours juridiques appropriés.

Voici les étapes de l'élaboration d'un plan de sécurité technologique pour une femme réagissant à la violence facilitée par la technologie.

Étape 1: Travailler avec les femmes pour identifier toutes les technologies utilisées à mauvais escient

Lors d'une rencontre avec une victime de violence, il est important d'aborder:

- le rôle de la technologie dans la violence, y compris l'ensemble des méthodes, appareils et programmes de communication utilisés au quotidien, et en particulier ceux utilisés pour communiquer avec l'auteur de la violence
- si et comment les auteurs ont accès aux dispositifs technologiques ou aux comptes (accès physique ou numérique)
- s'il y avait de la violence liée à la technologie dans leur relation et quel était le comportement violent (menaces, harcèlement, surveillance, publication de commentaires négatifs)

[1] Dans cette boîte à outils, nous utiliserons le terme «femme», «violence faite aux femmes» et les pronoms féminins par souci de simplicité et pour reconnaître l'impact significatif sur les femmes et les filles de la violence facilitée par la technologie. Les femmes et les filles sont confrontées à des taux plus élevés de la plupart des formes de violence facilitées par la technologie. Elles subissent également certaines des conséquences les plus graves de cette violence. La violence facilitée par la technologie a également un impact sur les personnes transgenres, non binaires, masculines et féminines.

- si elle soupçonne l'auteur d'accéder à ses appareils, ses comptes numériques ou sa localisation secrètement ou sans son consentement
- s'il existe des informations numériques ou électroniques auxquelles l'auteur de violence a accès et qui peuvent présenter un risque pour la sécurité ou la communication
- si des preuves risquent d'être perdues ou effacées
- toutes les possibilités de trouver des preuves numériques de la violence facilitée par la technologie.

Pour plus d'informations, voir la fiche d'information du BCSTH intitulée «Assessing for Technology—Facilitated Violence and Privacy Concerns for Anti-Violence Workers».

Étape 2: Protéger les données

Une fois les dispositifs technologiques et les comptes ayant été utilisés à mauvais escient identifiés, la recherche des preuves numériques peut commencer. C'est un bon moment pour dresser une liste des preuves à collecter et de celles que l'on a déjà en main.

Il faut ensuite déterminer le lieu de stockage de la preuve numérique (message texte sur son téléphone, courriel sur son compte de messagerie personnel, page Web de médias sociaux, compte iCloud, etc.) et explorer comment protéger ou geler les données avant de les préserver définitivement. Cela peut inclure le blocage de l'accès aux comptes de l'auteur de violence. Il faut savoir que le blocage d'un compte peut entrainer la suppression automatique des preuves numériques ou en entraver l'accès. Pour empêcher toute intrusion indésirable, il est recommandé de changer les mots de passe de toutes les plateformes et de tous les appareils concernés.

Il faut procéder à une évaluation de la sécurité avant de modifier les paramètres de confidentialité, le mot de passe, la liste de followers/amis, ou les données enregistrées d'un compte. De tels changements peuvent alerter l'agresseur au fait que la femme recueille des preuves ou reçoit du soutien. Cela peut entrainer une escalade de la violence ou l'effacement des preuves par l'auteur de l'infraction. Avant d'agir, il importe d'élaborer un plan de sécurité et de préservation des preuves en prévision de toute action en justice que la femme pourrait décider d'entreprendre.

Il est particulièrement important de modifier les mots de passe et les accès aux comptes cloud, comme iCloud ou Google Drive. Ces comptes sont généralement connectés à de nombreux appareils (téléphones fonctionnant sur le même système, tablettes, ordinateurs portables, ordinateurs de bureau, accessoires de fitness, etc.) et synchroniseront automatiquement les informations et sauvegarderont les données sur plusieurs appareils. Les auteurs de violence peuvent entrer dans des comptes cloud avec le mot de passe, ou encore, en accédant à un appareil configuré en fonction du compte cloud de sorte qu'un mot de passe n'est pas nécessaire. Les femmes doivent identifier les comptes cloud liés à leurs appareils et, si possible, les comptes auxquels les agresseurs ont accès. Il peut s'agir d'appareils auxquels

on ne pense pas, comme la smartwatch, l'enceinte Bluetooth ou la voiture intelligente du délinquant. L'accès à distance aux comptes cloud permet aux auteurs d'infractions de voir quelles preuves sont préservées par l'entremise des textes, courriels, vidéos et photos. L'accès à distance permet également aux délinquants de détruire les preuves qui y sont stockées.

Le stalkerware est un logiciel malveillant qui sert à surveiller l'activité d'un téléphone et suivre sa localisation. Si l'on craint que des appareils soient infectés par un stalkerware, il faut planifier la façon de changer les mots de passe sans alerter l'agresseur qui pourrait avoir accès à l'appareil. Par exemple, ne pas créer un nouveau mot de passe sur l'appareil surveillé. Une fois ce plan créé, les femmes et les intervenantes antiviolence peuvent générer des mots de passe forts qui ont peu de chances d'être découverts.

Le fonctionnement normal des appareils et des comptes peut également entrainer la perte de preuves numériques. Dans le but d'accroître la vitesse et la convivialité, de nombreuses entreprises configurent les appareils et les comptes de manière à supprimer automatiquement certaines informations. Il importe de savoir si les appareils ou les comptes sont configurés pour supprimer automatiquement les messages après un certain temps. Si oui, les paramètres du compte peuvent être modifiés pour mettre un terme à la suppression automatique et conserver toute preuve numérique.

Une sauvegarde secondaire des preuves numériques pouvant être compromises si un appareil est perdu, volé ou brisé peut faire toute la différence. Une sauvegarde secondaire peut se trouver sur un autre appareil ou compte, en version imprimée, ou les deux. Pour tenir compte de la possibilité d'accidents, prévoyez d'emblée comment sauvegarder les preuves efficacement.

Étape 3: Expliquer les limites de l'implication du personnel antiviolence dans la préservation des preuves

On demande souvent au personnel antiviolence de prendre des photos et de faire des enregistrements de la violence facilitée par la technologie afin de préserver les preuves. Il leur est également demandé de stocker des copies de preuves numériques pour les mettre à l'abri. Les organisations ont des politiques de gestion des documents qui peuvent aborder ce type de questions. En participant personnellement à la préservation des preuves numériques, vous courez le risque que votre dossier ou celui de votre cliente soit cité à comparaître au tribunal. Dans certaines circonstances, cela peut être approprié ou même nécessaire, mais il est préférable d'encourager les femmes à collecter ces preuves elles-mêmes ou à demander à un membre de leur famille ou à un proche de le faire, dans la mesure du possible.

Lorsque les preuves numériques sont préservées par une intervenante, l'organisation peut être tenue de présenter au tribunal les techniques utilisées pour préserver les preuves de la cliente, ainsi que les notes de cas dans son dossier. Si les preuves photographiques et numériques sont très importantes pour une

affaire judiciaire, leur authenticité sera évaluée en fonction des mesures prises par la personne qui les a préservées et stockées. Si une intervenante recueille des preuves numériques, elle peut être assignée à comparaître pour expliquer comment et pourquoi elle a recueilli ces preuves. Par exemple, elle peut être citée à comparaître pour témoigner qu'elle est bien celle qui a documenté ou stocké les preuves. Cela pourrait l'amener à être interrogée par la partie adverse ou le ministère public au sujet de son travail avec la femme et sa famille.

En outre, si les preuves photographiques ou numériques sont classées avec d'autres documents, tels que les notes des réunions avec des intervenantes, l'ensemble du dossier d'une femme peut devenir accessible au tribunal. Dans ce cas, les agresseurs, la partie adverse ou le procureur peuvent assigner les dossiers de l'organisation pour avoir accès aux copies des preuves. Si l'intervenante recueille des preuves, elle doit aborder ce risque d'assignation avec la cliente avant de le faire.

Pour ces motifs, il faut expliquer aux femmes que la conservation et le stockage de leurs preuves numériques par l'organisation risquent d'entrainer des conséquences inattendues qui pourraient leur être préjudiciables à long terme. De nombreux programmes antiviolence ont une politique de gestion des dossiers qui consiste à n'enregistrer que le minimum d'informations pour fournir les services requis. Vérifiez les politiques de l'organisation, et s'il n'en existe aucune, envisagez d'en élaborer une.

Les intervenantes peuvent discuter avec les femmes des conséquences possibles de la conservation des preuves par une tierce partie (comme leur organisation). Une partie intégrante de la planification de la sécurité technologique consiste à identifier les méthodes de préservation des preuves numériques qui sont dans l'intérêt de la femme à long terme.

Étape 4: Discuter de la manière de documenter les preuves

Il est courant que les femmes recueillent et préservent elles-mêmes les preuves en sauvegardant les courriels, en enregistrant les messages, en faisant des captures d'écran ou en les imprimant. Dans le cadre de la planification de la sécurité technologique, les intervenantes peuvent fournir des ressources expliquant quelles sont les informations à conserver, comment documenter la violence facilitée par la technologie aussi efficacement que possible, et quelles sont les étapes nécessaires pour préserver les preuves dans un format qui sera considéré comme authentique et complet.

Il est également suggéré d'encourager les femmes à stocker leurs preuves en plusieurs endroits, pour autant que cela puisse être fait en toute sécurité.

Il est préférable de documenter les preuves numériques par ordre chronologique. Fournissez aux femmes le Technology-Facilitated Violence Log de la BCSTH pour les aider à tenir un registre de leurs expériences de violence facilitée par la technologie.

La technologie est en constante évolution et il peut être difficile pour les intervenantes antiviolence de se tenir à jour. Vous ne connaissez peut-être pas toutes les technologies existantes, la manière dont elles peuvent être utilisées pour perpétuer la violence et les outils pour recueillir des preuves numériques. Il est utile de lire les documents de notre boîte à outils concernant les preuves numériques afin de se familiariser avec certaines des solutions.

Pour plus d'informations sur la manière de préserver et d'authentifier les preuves, consultez les ressources de cette boîte à outils.

Étape 5: Orientation vers des services juridiques

Les femmes peuvent avoir besoin d'informations ou de conseils juridiques sur les moyens de préserver les preuves numériques et sur les recours disponibles. Pour trouver des organisations en C.-B. qui fournissent des informations ou une aide juridique, voir:

- Rise Women's Legal Centre
- Legal Services Society
- PovNet

Étape 6: Fournir des ressources complémentaires en matière de sécurité technologique

Le projet de sécurité technologique de la BCSTH dispose de ressources en matière de sécurité technologique pour vous aider à soutenir les femmes victimes de violence facilitée par la technologie. La page Technology Safety Project Resource de la BCSTH contient des fiches d'information sur la technologie, les recours juridiques et la planification de sécurité.

Projet de sécurité technologique

Ce document fait partie d'une série qui explique comment préserver les preuves liées à l'utilisation abusive de la technologie dans les cas de violence familiale, d'agression sexuelle et de harcèlement. Cette série fait partie de la Boîte à outils pour la préservation des preuves numériques de la violence facilitée par la technologie. Ce document, ou toute partie de celui-ci, peut être reproduit ou utilisé de quelque manière que ce soit, à condition d'y citer la BC Society of Transition Houses.

Ce document a été publié en mars 2021.

BC Society of Transition Houses

Government of Canada Gouvernement du Canada